Algorithms for Testing Membership in Univariate Quadratic Modules over the Reals

Weifeng Shang
weifengshang@buaa.edu.cn
LMIB-School of Mathematical Sciences, Beihang University
Beijing, China

Chenqi Mou
chenqi.mou@buaa.edu.cn
LMIB-School of Mathematical Sciences, Beihang University
Beijing, China

Deepak Kapur
kapur@cs.unm.edu
Department of Computer Science, University of New Mexico
Albuquerque, New Mexico, USA

ABSTRACT

Quadratic modules in real algebraic geometry are akin to polynomial ideals in algebraic geometry, and have been found useful in the theory of Positivstellensatz to study Hilbert's 17th problem. Algorithms are presented in this paper for testing membership in univariate finitely generated quadratic modules over the reals and inclusion of two finitely generated quadratic modules. For a univariate unbounded quadratic module, an explicit upper bound on the degrees of sums of squares to construct any given polynomial is proved and then used to design an algorithm for testing membership in such a quadratic module. For a bounded quadratic module, a unique signature is associated with it based on the real values on which its finite basis is non-negative, and the signatures are used to furnish a criterion for inclusion of two finitely generated quadratic modules and a corresponding algorithm which solves the membership problem as a special case. It is also shown that a bounded quadratic module can be transformed to an equivalent one with two generators with an algorithm for performing this transformation. All the presented algorithms have been implemented.

CCS CONCEPTS

• **Computing methodologies** → **Algebraic algorithms**; • **Theory of computation** → *Design and analysis of algorithms.*

KEYWORDS

Quadratic module, membership test, sum of square, formal power series

ACM Reference Format:
Weifeng Shang, Chenqi Mou, and Deepak Kapur. 2022. Algorithms for Testing Membership in Univariate Quadratic Modules over the Reals. In *International Symposium on Symbolic and Algebraic Computation 2022, July 4–7, 2022, Lille, France.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Hilbert's 17th problem asks whether any non-negative polynomial f over $\mathbb{R}$, the field of real numbers, can be written in the form of a finite sum of squares of rational functions, i.e., $f = \sum q_i^2$ with $q_i \in \mathbb{R}(X)$ [13]? Artin gave an affirmative answer to this problem in 1927 [1]. However, computing a witness of f as a finite tuple of rational functions $q_1, \ldots, q_s$ remains elusive (see [10], however). Following a landmark result by Tarski-Seidenberg on the decidability of the theory of real closed fields [22, 24] leading to the Positivstellensatz discovered by Krivine and Stengle [8, 23], constructive methods for real algebraic geometry, paralleling methods for algebraic geometry, have been investigated since the 1960s [3]. Two exciting results in this direction are (i) by Schmüdgen [20] for a compact (bounded) semi-algebraic subset S of $\mathbb{R}^n$ defined by a finite set of non-negative polynomial inequalities $G = \{g_1, \cdots, g_s\}$ in $\mathbb{R}[X]$, characterizing every strictly positive polynomial f on S (a *preordering* generated by G) and its denominator-free representation as $f = \sum_{G' \subseteq G} \sigma_{G'} (\prod_{g \in G'} g)$ with $\sigma_{G'}$ being a sum of squares in $\mathbb{R}[X]$ and subsequently (ii) by Putinar [18], giving a simpler linear representation of a non-negative polynomial f on S (a *quadratic module* generated by G) of the form $f = \sigma_0 + \sum_{i=1}^{s} \sigma_i g_i$ with σ_i being a sum of squares in $\mathbb{R}[X]$. Various types of Positivstellensatz focusing on semi-algebraic sets, the associated algorithms and complexities are extensively studied [12, 13, 15, 21].

The membership problem for finitely generated quadratic modules is to decide whether a polynomial $f \in \mathbb{R}[X]$ is in the quadratic module generated by a finite set of polynomials $g_1, \ldots, g_s$, i.e., whether f can be expressed as $\sigma_0 + \sum_{i=1}^{s} \sigma_i g_i$ where σ_i's are sums of squares in $\mathbb{R}[X]$. Note that the membership problem for finitely generated preorderings can be solved naturally once the former membership test is feasible because such preorderings can be reformulated as finitely generated quadratic modules with the representations by Schmüdgen and Putinar above. Much like the importance of the ideal membership problem in algebraic geometry, the membership test for finitely generated quadratic modules is a fundamental problem of theoretical interest for Positivstellensatz.

Finding whether a polynomial f can be written as $f = \sigma_0 + \sum_{i=1}^{s} \sigma_i g_i$ with sums of squares $\sigma_0, \ldots, \sigma_s$ is closely related to finding the sum-of-squares decomposition of f [9, 11, 16, 17], but these two problems are different. If a quadratic module is generated by 1, the former problem degenerates to the latter, but in general, the case of a quadratic module with multiple generators other than 1 is different from the set of all sums of squares.

In Ph.D. theses by Augustin [2], Canto Cabral [4] and Wagner [26], decidability of the membership problem in finitely generated quadratic modules under certain conditions has been proved for, respectively, the univariate, bivariate, and multivariate cases. Augustin gave an algorithm for membership test for a bounded finitely generated quadratic module in $\mathbb{R}[x]$; for a stable quadratic module

ISSAC '22, July 4–7, 2022, Lille, France

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

where an upper bound on the degrees of the respective sums of squares is assumed to be given, she used the Gram matrix construction proposed by Powers and Wörmann [17] to decide membership. Canto Cabral gave an algorithmic procedure for the bivariate case for a finitely generated Archimedean quadratic module (in which there exists a natural number N such that $N - (x_1^2 + \cdots + x_n^2)$ is in the quadratic module); her approach does not generalize however to arbitrary number of variables. Wagner used a totally different approach based on Jacobi's representation theorem [6] and Jacobi and Prestel's characterization theorem [7] to give a decision procedure for the multivariate case using Abhyankar valuations.

The focus of this paper is on univariate finitely generated quadratic modules. We improve upon the results in [2] for both unbounded as well as bounded quadratic modules. For an unbounded quadratic module, we show that there is no need to specify a function bounding the degrees of its witnesses. For a bounded quadratic module, we show that any finite basis of a quadratic module can be reduced to a basis of two polynomials. Further, every such quadratic module has a unique signature based on its bounded semi-algebraic set represented as a finite union of intervals and isolated points in ascending order. This signature is used for checking whether a finitely generated quadratic module is a subset of another finitely generated quadratic module. Immediate corollaries of this result include the membership test for a polynomial to be in a finitely generated quadratic module as well as equivalence of two quadratic modules with two different bases. The paper presents algorithms for each of these subproblems, which have been implemented and tried on several examples.

2 PRELIMINARIES

2.1 Sum of squares

Consider the multivariate polynomial ring $\mathbb{R}[x_1, \ldots, x_n]$ with the indeterminates $x_1, \ldots, x_n$. We denote $X = (x_1, ..., x_n)$, and for any $\boldsymbol{a} = (a_1, ..., a_n) \in \mathbb{N}^n$, denote $X^{\boldsymbol{a}} = x_1^{a_1} \cdots x_n^{a_n}$.

A polynomial $f \in \mathbb{R}[X]$ is called a *sum of squares* in $\mathbb{R}[X]$ if it can be expressed as a sum of squares of polynomials in $\mathbb{R}[X]$. It is easy to show that any sum of squares $f \in \mathbb{R}[X]$ is of an even total degree and such that $f \geq 0$ over $\mathbb{R}$.

For an arbitrary non-negative integer m, denote $\Lambda_m = \{(\alpha_1, \ldots, \alpha_n) : \sum_{i=1}^n \alpha_i \leq m\}$. Then any polynomial $f \in \mathbb{R}[X]$ of total degree m can be written in the form $f = \sum_{\boldsymbol{\alpha} \in \Lambda_m} c_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}}$. In particular, let $k = |\Lambda_m| = \binom{m+n}{n}$ and order the elements of Λ_m as $(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_k)$ according to some order. Denote by $\bar{\boldsymbol{x}} = (X^{\boldsymbol{\beta}_1}, \ldots, X^{\boldsymbol{\beta}_k})$ the corresponding ordered set of terms of total degrees $\leq m$ in $\mathbb{R}[X]$. The following characterization of sums of squares in $\mathbb{R}[X]$ is well-known.

Theorem 1 ([17, Theorem 1]). *Let $f \in \mathbb{R}[X]$ be a polynomial of even total degree m and $\bar{\boldsymbol{x}} = (X^{\boldsymbol{\beta}_1}, \ldots, X^{\boldsymbol{\beta}_k})$ be as stated above. Then f is a sum of squares in $\mathbb{R}[X]$ if and only if there exists a real, symmetric, positive semi-definite matrix B of size $k \times k$ such that $f = \bar{\boldsymbol{x}} B \bar{\boldsymbol{x}}^t$, where $\bar{\boldsymbol{x}}^t$ is the transpose of $\bar{\boldsymbol{x}}$.*

This theorem allows one to test whether a polynomial is a sum of squares by applying semi-definite programming [25] or quantifier elimination [5], and the latter method is explained as follows. Consider a symmetric matrix B of size $k \times k$ with its entries as unknowns. Comparing the coefficients of both sides of $f = \bar{\boldsymbol{x}} B \bar{\boldsymbol{x}}^t$ furnishes constraints in the form of equations on the entries of B; positive semi-definiteness of B imposes constraints of inequalities on the entries. In this way, testing the existence of B in Theorem 1 is equivalent to determining whether the corresponding semi-algebraic set defined by the equations and inequations above is empty or not. An algorithm based on quantifier elimination can be used for this purpose, and there are also software tools available for performing this check.

2.2 Quadratic module in $\mathbb{R}[x]$

Definition 2. Let $G = \{g_1, ..., g_s\}$ be a set of polynomials in $\mathbb{R}[x]$. Then the *non-negative set* of G, denoted by $S(G)$, is defined to be $\{x \in \mathbb{R} \mid g_i(x) \geq 0, i = 1, \ldots, s\}$.

Definition 3. Let R be a commutative ring with unit 1. Then a subset $M \subseteq R$ is called a *quadratic module* in R if M is closed under addition, $1 \in M$, and for any $a \in R$ and $m \in M$, $a^2 m \in M$.

A quadratic module M in R is said to be *finitely generated* if there exists a finite set $G = \{g_1, ..., g_s\} \subseteq R$ such that $M = \{\sigma_0 + \sum_{i=1}^s \sigma_i g_i \mid \sigma_i$ is a sum of squares in $R, i = 0, \ldots, s\}$. In this case, we write $M = \mathrm{QM}(G)$. A finitely generated quadratic module $\mathrm{QM}(G)$ in $\mathbb{R}[x]$ is said to be *bounded* if the non-negative set $S(G)$ is a bounded set in $\mathbb{R}$ and *unbounded* otherwise.

Fix a polynomial set $G = \{g_1, ..., g_s\} \subset \mathbb{R}[x]$. For a polynomial $f \in \mathbb{R}[x]$, next we investigate the relationship between $f \in \mathrm{QM}(G)$ and $f|_{S(G)} \geq 0$. $f \in \mathrm{QM}(G)$ means that there exist sums of squares $\sigma_0, \sigma_1, \ldots, \sigma_s$ in $\mathbb{R}[x]$ such that $f = \sigma_0 + \sum_{i=1}^s \sigma_i g_i$, and clearly this implies $f|_{S(G)} \geq 0$; $f|_{S(G)} \geq 0$, however, does not necessarily imply $f \in \mathrm{QM}(G)$, as illustrated by the following example.

Example 4. Clearly $-x \geq 0$ on $S(-x^3)$ but $-x \notin \mathrm{QM}(-x^3)$. Suppose that $-x \in \mathrm{QM}(-x^3)$. Then $-x = s_0 - s_1 x^3$ for some non-zero sums of squares s_0 and s_1 in $\mathbb{R}[x]$. Since $\deg(s_0)$ and $\deg(s_1)$ are both even whereas $\deg(-s_1 x^3)$ is odd, there cannot be any cancellation of the leading terms of s_0 and $-s_1 x^3$, implying that $1 = \deg(-x) = \deg(s_0 - s_1 x^3) = \max\{\deg(s_0), \deg(-s_1 x^3)\} > 2$, which is a contradiction.

2.3 Formal power series

Augustin [2] related the membership problem of a bounded finitely generated quadratic module in $\mathbb{R}[x]$ to that in the ring of formal power series. In the following we follow the conventions in [2].

Let R be a commutative ring and x be a variable. Then the form $\sum_{i=0}^\infty r_i x^i$ with $r_i \in R$ is called a *formal power series* in x over R. The set of all formal power series in x over R forms a ring, and it is called the *ring of formal power series* in x over R and is denoted by $R[[x]]$.

For any $a \in \mathbb{R}$, instead of in $\mathbb{R}[[x]]$ we extensively work in $\mathbb{R}[[x-a]]$, in which all the elements are in the form of $\sum_{i=0}^\infty r_i (x-a)^i$. Let $\phi_a : \mathbb{R}[x] \to \mathbb{R}[[x-a]]$ be the natural embedding and denote by $\hat{f}_a := \phi_a(f)$ the image of a polynomial $f \in \mathbb{R}[x]$ in $\mathbb{R}[[x-a]]$. Supposing that $\deg(f) = n$, the Taylor expansion of f at a in $\mathbb{R}[x]$ is:

$$f = f(a) + f'(a)(x-a) + \frac{f^{(2)}(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

Then $\hat{f}_a = \sum_{i=0}^n c_i (x-a)^i$ in $\mathbb{R}[[x-a]]$ with $c_0 = f(a)$ and $c_i = \frac{f^{(i)}(a)}{i!}$ for $i = 1, \ldots, n$. With $\hat{f}_a$ in the form $\hat{f}_a = \sum_{i=0}^n c_i (x-a)^i$, we

define the *order* of f at a as $\mathrm{ord}_a(f) := \min\{i \mid c_i \neq 0\}$ and denote the sign of the first non-zero coefficient by $\epsilon_a(f) := \mathrm{sign}(c_{\mathrm{ord}_a(f)})$.

Let $d = \mathrm{ord}_a(f)$. Since $\mathbb{R}[[x-a]]$ is a local ring with the maximal ideal $\langle x-a\rangle$, we can write $\hat{f_a}$ uniquely as

$$\hat{f_a} = \epsilon_a(f)(x-a)^d|c_d|(1+q), \tag{1}$$

where q is some element in $\langle x-a\rangle \subseteq \mathbb{R}[[x-a]]$ and thus $|c_d|(1+q)$ is a unit in $\mathbb{R}[[x-a]]$. To differentiate the quadratic modules in $\mathbb{R}[[x-a]]$ from those in $\mathbb{R}[x]$, we use $\mathrm{QM}_a(G)$ to denote the quadratic module generated by a set G of formal power series in $\mathbb{R}[[x-a]]$. The following proposition characterizes the quadratic module generated by a single element in $\mathbb{R}[[x-a]]$.

Proposition 5 ([2, Page 32]). *Let f be a polynomial in $\mathbb{R}[x]$ with $\mathrm{ord}_a(f) = d$ and $\hat{f_a}$ be written as in (1) in $\mathbb{R}[[x-a]]$. Then $\mathrm{QM}_a(\hat{f_a}) = \mathrm{QM}_a(\epsilon_a(f)(x-a)^d)$ in $\mathbb{R}[[x-a]]$.*

For an arbitrary polynomial $f \in \mathbb{R}[x]$, denote by $Z(f)$ the set of its zeros in $\mathbb{R}$. Augustin used the following "local-global principle" for solving the membership problem.

Theorem 6 (Local-global principle [19, Corollary 3.17] [2, Theorem 2.9]). *Let f be a polynomial and $G = \{g_1, ..., g_s\}$ be a polynomial set in $\mathbb{R}[x]$ such that $S(G)$ is bounded. If $f|_{S(G)} \geq 0$ and $\hat{f_a} \in \mathrm{QM}_a(\hat{g_1}_a, \ldots, \hat{g_s}_a)$ for any $a \in Z(f) \cap S(G)$, then $f \in \mathrm{QM}(G)$.*

3 UNBOUNDED FINITELY GENERATED QUADRATIC MODULES

For a polynomial $f \in \mathbb{R}[x]$, denote its leading coefficient by $\mathrm{lc}(f)$. The following proposition characterizes unbounded non-negative sets of polynomial sets in $\mathbb{R}[x]$.

Proposition 7. *Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[x]$ be a polynomial set. Then $S(G)$ is unbounded if and only if the following two conditions hold simultaneously:* (1) *there is no polynomial in G of even degree with a negative leading coefficient;* (2) *either there is no polynomial in G of odd degree or the signs of leading coefficients of all such polynomials, if they exist, are the same.*

Proof. ($\Leftarrow$) Otherwise if $S(G)$ is bounded, then there exists an integer $M > 0$ such that when $x > M$, there exist two integers i and j such that $g_i(x) < 0$ and $g_j(-x) < 0$. If either $\deg(g_i)$ or $\deg(g_j)$ is even, then $\mathrm{lc}(g_i)$ or $\mathrm{lc}(g_j)$ is negative: this contradicts condition (1). Else if both the degrees of g_i and g_j are odd, then $\mathrm{lc}(g_i)$ is negative while $\mathrm{lc}(g_j)$ is positive: this contradicts condition (2).

($\Rightarrow$) Again we prove the contrapositive.

(1) If in G there exists a polynomial g_i of an even degree with $\mathrm{lc}(g_i) < 0$. Then there exists a positive number $M \in \mathbb{R}$ such that $g_i(x) < 0$ whenever $|x| > M$. In this case $S(G) \subseteq S(g_i) \subseteq [-M, M]$, and thus $S(G)$ is bounded: a contradiction.

(2) If in G there exist two polynomials g_i and g_j of odd degrees whose leading coefficients are of different signs, say $\mathrm{lc}(g_i) < 0$ and $\mathrm{lc}(g_j) > 0$ without loss of generality, then there exist two positive numbers $M_1, M_2 \in \mathbb{R}$ such that $g_i(x) < 0$ when $x > M_1$ and $g_j(x) < 0$ when $x < -M_2$. In this case $S(G) \subseteq S(g_i, g_j) \subseteq [-M_2, M_1]$, and thus $S(G)$ is bounded: a contradiction. □

Definition 8 ([14]). Let $G = \{g_1, \ldots, g_s\}$ be a polynomial set in $\mathbb{R}[x]$. The quadratic module $\mathrm{QM}(G)$ is said to be *stable* if there exists a function $N : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ such that for any $f \in \mathrm{QM}(G)$, there exist sums of squares $\sigma_0, \sigma_1, \ldots, \sigma_s$ such that $f = \sum_{i=0}^{s} \sigma_i g_i$ with $\deg(\sigma_i g_i) \leq N(\deg(f))$ for $i = 0, \ldots, s$, where $g_0 := 1$. In particular, if the function N is identity, $\mathrm{QM}(G)$ is said to be *totally stable*.

Theorem 9. *Any finitely generated quadratic module $\mathrm{QM}(G) \subseteq \mathbb{R}[x]$ with an unbounded $S(G)$ is totally stable.*

Proof. Let $G = \{g_1, \ldots, g_s\}$. For any $f \in \mathrm{QM}(G)$, write it in a uniform way as $f = \sum_{i=0}^{s} \sigma_i g_i$ with sums of squares $\sigma_0, \ldots, \sigma_s$ and $g_0 := 1$. From Theorem 7 we know that for any two distinct polynomials $g_i, g_j \in G$, if $\deg(g_i)$ and $\deg(g_j)$ are both odd or both even, then their leading terms do not cancel. Since σ_i and σ_j are both of even degrees, the leading terms of $\sigma_i g_i$ and $\sigma_j g_j$ do not cancel. Suppose that the leading terms of f and $\sigma_i g_i$ are the same for some integer i ($0 \leq i \leq s$). Then $\deg(f) = \deg(\sigma_i g_i) \geq \deg(\sigma_j g_j)$ for $j \neq i$, and the conclusions follow. In particular, the stability of $\mathrm{QM}(G)$ follows by setting N in Definition 8 as the identity function. □

The property that unbounded finitely generated univariate quadratic modules are stable easily follows from a more general result for multivariate quadratic modules (see, e.g., [13, Example 4.1.5]). Total stability of univariate unbounded quadratic modules proved above in Theorem 9 is likely to follow from general results about total stability of multivariate quadratic modules [14], but the conditions there for total stability are not easy to check. We believe that the above proof for the special case is much simpler than more general proofs.

Note that σ_i in the theorem is always of an even degree, we know that its degree is bounded by $2\lfloor \frac{\deg(f) - \deg(g_i)}{2} \rfloor$ more precisely. Based on these degree bounds, we have the following algorithm (Algorithm 1) to solve the membership problem of unbounded finitely generated quadratic modules in $\mathbb{R}[x]$ by using undetermined coefficients of these sums of squares and the existing algorithm for finding sums of squares. In Algorithm 1 below, $\mathsf{SOS2Semi}(\cdot)$ is a subroutine which takes a polynomial σ as input and outputs a semi-algebraic set Φ described by polynomial equations and inequations such that σ is a sum of squares if and only if $\Phi \neq \emptyset$. One can test whether a semi-algebraic set is empty or not by applying methods of quantifier elimination (in line 10). Note that a similar algorithm by constructing sums of squares via semi-definite programming is proposed in [2] assuming the bounding function on the degrees.

Example 10. Let $g_1 = x^2 - 1$, $g_2 = x + 1$, and $G = \{g_1, g_2\}$. Then one knows that $S(G) = \{-1\} \cup [1, \infty]$, and thus $\mathrm{QM}(G)$ is unbounded and totally stable by Theorem 9. Now we apply Algorithm 1 to test whether $f = 6x^3 + 15x^2 + x - 6$ is in $\mathrm{QM}(G)$. One first sees that $m = \min(\deg(g_1), \deg(g_2)) = 1 < 3 = \deg(f) = n$.

For $i = 1$: we know that the degree of σ_1 is bounded by $d_1 = 2\lfloor \frac{\deg(f) - \deg(g_1)}{2} \rfloor = 0$ and thus set $\sigma_1 = \lambda_{10}$ with $\lambda_{10} \in \mathbb{R}$ as an indeterminate. By applying Theorem 1, the subroutine $\mathsf{SOS2Semi}(\sigma_1)$ returns the semi-algebraic set $\{\lambda_{10} \geq 0\}$.

For $i = 2$: $d_2 = 2$ and thus we set $\sigma_2 = \lambda_{20} + \lambda_{21}x + \lambda_{22}x^2$ with $\lambda_{20}, \lambda_{21}$, and λ_{22} as indeterminates. This time the semi-algebraic set returned is $\mathsf{SOS2Semi}(\sigma_2) = \{-\lambda_{21}^2 + 4\lambda_{22}\lambda_{20} \geq 0, \lambda_{20} + \lambda_{22} \geq 0\}$.

Then for σ_0: we first compute $\sigma_0 = f - \sigma_1 g_1 - \sigma_2 g_2 = (-\lambda_{22} + 6)x^3 + (-\lambda_{10} - \lambda_{21} - \lambda_{22} + 15)x^2 + (-\lambda_{20} - \lambda_{21} + 1)x + (\lambda_{10} - \lambda_{20} - 6)$,

Algorithm 1: Algorithm for testing membership in unbounded quadratic modules $B := \mathsf{IsInUnbounded}(f, G)$

Input: A polynomial $f \in \mathbb{R}[x]$, a polynomial set $G = \{g_1, ..., g_s\} \subseteq \mathbb{R}[x]$ such that $S(G)$ is unbounded
Output: A boolean B such that B = true if $f \in \mathrm{QM}(G)$ and B = false otherwise

$\Phi := \emptyset$;
for $i = 1, \ldots, s$ **do**
  if $\deg(f) < \deg(g_i)$ **then** $\sigma_i := 0$;
  else
    $d_i := 2\lfloor \frac{\deg(f) - \deg(g_i)}{2} \rfloor$;
    Write $\sigma_i := \sum_{j=0}^{d_i} \lambda_{ij} x^j$;
    $\Phi := \Phi \cup \mathsf{SOS2Semi}(\sigma_i)$;
$\sigma_0 := f - \sum_{i=1}^{s} \sigma_i g_i$;
$\Phi := \Phi \cup \mathsf{SOS2Semi}(\sigma_0)$;
if $\Phi = \emptyset$ **then** $B :=$ false; **else** $B :=$ true;
return B;

and the corresponding semi-algebraic set is

$$\begin{aligned}\mathsf{SOS2Semi}(\sigma_0) = \{&-\frac{1}{4}\lambda_{20}^2 + \frac{1}{2}\lambda_{20}\lambda_{21} - \frac{1}{4}\lambda_{21}^2 - \frac{29}{2}\lambda_{20} + \frac{13}{2}\lambda_{21} \\ &- \frac{361}{4} - \lambda_{10}^2 + \lambda_{10}\lambda_{20} - \lambda_{21}\lambda_{10} - \lambda_{22}\lambda_{10} + \lambda_{22}\lambda_{20} + 21\lambda_{10} \\ &+ 6\lambda_{22} \geq 0, -\lambda_{21} - \lambda_{22} + 9 - \lambda_{20} \geq 0, -\lambda_{22} + 6 = 0\}.\end{aligned}$$

Taking the union of three semi-algebraic sets above, we have a semi-algebraic set Φ such that $f \in \mathrm{QM}(G)$ if and only if $\Phi \neq \emptyset$. Any algorithm for quantifier elimination (e.g., QEPCAD) can verify that $\Phi \neq \emptyset$ and thus $f \in \mathrm{QM}(G)$.

4 BOUNDED FINITELY GENERATED QUADRATIC MODULES

In [2], Augustin reduced the membership test in $\mathrm{QM}(G)$ for a finite polynomial set G in $\mathbb{R}[x]$ to that in $\mathrm{QM}_a(\hat{G}_a) \subseteq \mathbb{R}[[x-a]]$ for a being either a boundary or an isolated point of $S(G)$. The latter test is solved by studying the relationships of inclusion of quadratic modules in $\mathbb{R}[[x-a]]$. Next we recall this method.

Proposition 5 tells us that all the quadratic modules in $\mathbb{R}[[x-a]]$ generated by a single element are in the form $\mathrm{QM}_a(\pm(x-a)^d)$, and thus they can be categorized into four cases according to the sign and whether d is odd or even: $\mathrm{QM}_a(-(x-a)^{2k})$, $\mathrm{QM}_a((x-a)^{2k+1})$, $\mathrm{QM}_a(-(x-a)^{2k+1})$, and $\mathrm{QM}_a((x-a)^{2k})$. In particular, any element in $\mathrm{QM}_a((x-a)^{2k})$ is clearly a sum of squares in $\mathbb{R}[[x-a]]$, and we can safely ignore this case. The inclusive relationships between quadratic modules in the remaining three cases are illustrated in Figure 1 (see [2, Theorem 2.3]), where an arrow from a quadratic module Q_1 to another Q_2 indicates the proper inclusion $Q_1 \subsetneq Q_2$.

Now consider a polynomial set $G = \{g_1, ..., g_s\} \subset \mathbb{R}[x]$. For any $a \in \mathbb{R}$, the quadratic modules $\mathrm{QM}_a(\hat{g}_1), \ldots, \mathrm{QM}_a(\hat{g}_s)$ in $\mathbb{R}[[x-a]]$ belong to these three cases unless they are trivial ones. Because of the inclusive relationships of quadratic modules in this figure, for each case of quadratic modules we only need to pay attention to the one with the least exponent (or pictorially, the quadratic module at the top of each column in Figure 1). This observation justifies the following definition.

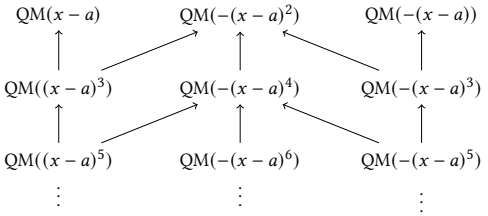

Figure 1: Inclusive relationships between quadratic modules of single generators in $\mathbb{R}[[x-a]]$

Definition 11 ([2, Page 43]). Let $G = \{g_1, ..., g_s\}$ be a polynomial set in $\mathbb{R}[x]$. For any $a \in \mathbb{R}$, define

$$\begin{aligned}k_a(G) &:= \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \text{ is even}, \epsilon_a(g_i) = -1\}, \\ k_a^+(G) &:= \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \text{ is odd}, \epsilon_a(g_i) = 1\}, \\ k_a^-(G) &:= \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \text{ is odd}, \epsilon_a(g_i) = -1\}.\end{aligned}$$

If the set to define $k_a(G)$, $k_a^+(G)$, or $k_a^-(G)$ is empty, the corresponding value is set to ∞.

Intuitively, $k_a(G)$ is the exponent of the top quadratic module in the middle column in Figure 1, while $k_a^+(G)$ and $k_a^-(G)$ are those for the left and right columns respectively. It is straightforward to see from Definition 11 that for any $a \in \mathbb{R}$, $k_a(G)$ is even and both $k_a^+(G)$ and $k_a^-(G)$ are odd when they are finite, and thus $k_a(G) \neq k_a^+(G)$ and $k_a(G) \neq k_a^-(G)$ unless they are ∞.

Example 12. Let $g_1 = (x+1)x^3(x-1)^6(x-2)^3$, $g_2 = x(x-1)$, $g_3 = -(x - \frac{1}{2})(x-1)^2(x-2)^4$, $g_4 = -(x+1)^3x^2(x-2)^3$, and $G = \{g_1, g_2, g_3, g_4\}$. Then one can compute $S(G) = [-1, 0] \cup \{1, 2\}$.

- For $a = -1$: $k_{-1}(G) = \infty$, $k_{-1}^+(G) = 1$, and $k_{-1}^-(G) = \infty$;
- For $a = 0$: $k_0(G) = \infty$, $k_0^+(G) = \infty$, and $k_0^-(G) = 1$;
- For $a = 1$: $k_1(G) = 2$, $k_1^+(G) = 1$, and $k_1^-(G) = \infty$;
- For $a = 2$: $k_2(G) = 4$, $k_2^+(G) = 3$, and $k_2^-(G) = 3$.

Consider a bounded non-negative set $S(G)$ for some polynomial set $G \subseteq \mathbb{R}[x]$. Then one knows that $S(G)$ is a collection of closed intervals and isolated points in $\mathbb{R}$.

Theorem 13 ([2, Theorem 2.18]). *Let $f \in \mathbb{R}[x]$ and $G = \{g_1, ..., g_s\} \subseteq \mathbb{R}[x]$ with $S := S(G)$ bounded. Then $f \in \mathrm{QM}(G)$ if and only if $f|_S \geq 0$ and the following statements hold.*

(1) *For every left boundary a of closed intervals of S, either* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - k_a^+(G) \in 2\mathbb{N}$.
(2) *For every right boundary b of closed intervals of S, either* $\mathrm{ord}_b(f)$ *is even or* $\mathrm{ord}_b(f) - k_b^-(G) \in 2\mathbb{N}$.
(3) *For every isolated point c of S, either* ($\mathrm{ord}_c(f)$ *is even and* $\epsilon_c(f) = 1$) *or one of the following cases happens.*

(Case 1) $\mathrm{ord}_c(f) \geq k_c(G)$, *if* $k_c(G) < k_c^+(G)$ *and* $k_c(G) < k_c^-(G)$;
(Case 2) ($\mathrm{ord}_c(f) - k_c^+(G) \in 2\mathbb{N}$ *and* $\epsilon_c(f) = 1$) *or* $\mathrm{ord}_c(f) \geq \min(k_c(G), k_c^-(G))$, *if* $k_c^+(G) \leq \min(k_c(G), k_c^-(G))$;
(Case 3) ($\mathrm{ord}_c(f) - k_c^-(G) \in 2\mathbb{N}$ *and* $\epsilon_c(f) = -1$) *or* $\mathrm{ord}_c(f) \geq \min(k_c(G), k_c^+(G))$, *if* $k_c^-(G) \leq \min(k_c(G), k_c^+(G))$.

Theorem 13 directly leads to an algorithm to test the membership in bounded finitely generated quadratic modules in $\mathbb{R}[x]$, while the following corollary, whose proof is straightforward, can be used to optimize the algorithm.

Corollary 14. *Let f, G, and S be as stated in Theorem 13.* (1) *If $f|_S > 0$, then $f \in \mathrm{QM}(G)$.* (2) *If $f|_S \geq 0$ and any of $Z(f)$ is neither a boundary nor an isolated point of S, then $f \in \mathrm{QM}(G)$.*

Instead of presenting the algorithm based on Theorem 13, we further make use of the fact that a quadratic module $\mathrm{QM}(G)$ is characterized by the values $(k_a(G), k_a^+(G), k_a^-(G))$ for any boundary or isolated point a of $S(G)$ to derive a simpler criterion based on which an algorithm will be presented.

Given a finite polynomial set $G \subseteq \mathbb{R}[x]$ with $S(G)$ bounded, let $S(G) = \bigcup_{i=1}^{n}[a_i, b_i]$ (note that $a_i = b_i$ is possible for an isolated point) such that any two distinct $[a_i, b_i]$ and $[a_j, b_j]$ do not intersect and $b_i < a_{i+1}$ for $i = 1, \ldots, n-1$. For any finite polynomial set $F \subseteq \mathbb{R}[x]$ such that $S(G) \subseteq S(F)$, we assign a tuple (k_i, k_i^+, k_i^-) to each interval $[a_i, b_i]$ for $i = 1, \ldots, n$ as follows.

(1) If $a_i \neq b_i$, set $k_i = \infty$, $k_i^+ = k_{a_i}^+(F)$, and $k_i^- = k_{b_i}^-(F)$.

(2) If $a_i = b_i = a$, set the values in the following five cases.

(Type A) If $k_a(F) < k_a^+(F)$ and $k_a(F) < k_a^-(F)$, set
$$k_i = k_a(F), \quad k_i^+ = k_a(F) + 1, \quad k_i^- = k_a(F) + 1.$$

(Type B) If $k_a(F) > k_a^+(F)$ and $k_a(F) > k_a^-(F)$, set
$$k_i = \max(k_a^+(F), k_a^-(F)) + 1, \quad k_i^+ = k_a^+(F), \quad k_i^- = k_a^-(F).$$

(Type C) If $k_a^+(F) < k_a(F) < k_a^-(F)$, set
$$k_i = k_a(F), \quad k_i^+ = k_a^+(F), \quad k_i^- = k_a(F) + 1.$$

(Type D) If $k_a^-(F) < k_a(F) < k_a^+(F)$, set
$$k_i = k_a(F), \quad k_i^+ = k_a(F) + 1, \quad k_i^- = k_a^-(F).$$

(Type E) If $k_a(F) = k_a^+(F) = \infty$, set $k_i = k_i^+ = \infty$ and $k_i^- = k_a^-(F)$, or if $k_a^-(F) = k_a(F) = \infty$, set $k_i = k_i^- = \infty$ and $k_i^+ = k_a^+(F)$.

Concatenating all the tuples together, we assign to F a signature $\omega_S(F) := (k_1, k_1^+, k_1^-, \ldots, k_n, k_n^+, k_n^-)$ with respect to S. When $S = S(F)$, the subscript S in $\omega_S(F)$ is omitted.

Note that all the three values $k_a(F)$, $k_a^+(F)$, and $k_a^-(F)$ can take infinity. When a strict inequality like $k_a(F) < k_a^+(F)$ occurs, it implies that the less value like $k_a(F)$ here is finite.

Example 15. Let us continue with Example 12. Writing isolated points also as intervals, $S(G) = [-1, 0] \cup [1, 1] \cup [2, 2]$, and in the following we compute the signature $\omega(G)$.

- For the proper closed interval $[-1, 0]$. With all the values computed in Example 12, one can easily see that $k_1 = \infty$, $k_1^+ = 1$, and $k_1^- = 1$;
- For the isolated point $[1, 1]$, since $k_1^+(G) < k_1(G) < k_1^-(G)$, one knows that it is of Type C in the definition, and thus one has $k_2 = 2$, $k_2^+ = 1$, and $k_2^- = 3$.
- For the isolated point $[2, 2]$, since $k_2(G) > k_2^+(G)$ and $k_2(G) > k_2^-(G)$, one knows that it is of Type B and $k_3 = 4$, $k_3^+ = 3$, and $k_3^- = 3$.

As a result, one has $\omega(G) = (\infty, 1, 1, 2, 1, 3, 4, 3, 3)$.

Our definition of the signature $\omega_S(F)$ here generalizes the similar notion $\omega^{\pm}(G)$ in [2] in the way that we allow to compute the signature of a polynomial set F with respect to the bounded non-negative set $S(G)$ of another polynomial set G as long as the condition $S(G) \subseteq S(F)$ is satisfied. This generalization results in a new type (Type E) for an isolated point a reflecting the case when $f(a) > 0$ for all $f \in F$ (which will not happen if one restricts himself to the signature $\omega(G)$ for only one polynomial set G). This generalization furnishes us the criterion (Theorem 19) below to test inclusion of finitely generated quadratic modules in $\mathbb{R}[x]$ by using their signatures, which naturally degenerates to a method to test membership in bounded quadratic modules. What is more interesting, this generalization which allows Type E naturally encodes Corollary 14, which can be considered as improvement of Theorem 13, in the criterion. In particular, the condition $S(G) \subseteq S(F)$ we impose on F means that the results we obtain below also apply to an unbounded quadratic module $\mathrm{QM}(F)$.

Fix a bounded non-negative set $S = S(G) = \bigcup_{i=1}^{n}[a_i, b_i]$. Then we can assign a partial order $\preceq$ to all the signatures with respect to S as follows: two signatures $\omega_S(F_1)$ and $\omega_S(F_2)$ are such that $\omega_S(F_1) \preceq \omega_S(F_2)$ if and only if $\omega_S(F_1)[i] \leq \omega_S(F_2)[i]$ for $i = 1, \ldots, 3n$, where $\omega_S(F_1)[i]$ denotes the i-th entry of the sequence $\omega_S(F_1)$. For any polynomial set $F \subseteq \mathbb{R}[x]$ and any $a \in \mathbb{R}$, denote the tuple $(k_a(F), k_a^+(F), k_a^-(F))$ by $L_a(F)$. Note that we can compare two tuples $L_a(F)$ and $L_a(G)$ with the same partial order $\preceq$.

In the following we first present three lemmas, the first of which is straightforward and we omit its proof.

Lemma 16. *Let f be a polynomial in $\mathbb{R}[x]$.* (1) *Among the three values of $L_a(f)$ there are at most one finite value.* (2) *If a polynomial set $F \subset \mathbb{R}[x]$ contains f, then $L_a(f) \succeq L_a(F)$.* (3) *If $f(a) > 0$, then $\hat{f}_a$ is a sum of squares in $\mathbb{R}[[x-a]]$ and $L_a(f) = (\infty, \infty, \infty)$.*

Lemma 17. *Let F be a finite polynomial set in $\mathbb{R}[x]$ with $S(F) = \bigcup_{i=1}^{n}[a_i, b_i]$ and $\omega(F) = [k_1, k_1^+, k_1^-, \ldots, k_n, k_n^+, k_n^-]$. Then for each $i = 1, \ldots, n$, if $a_i \neq b_i$, then $(x-a_i)^{k_i^+} \in \mathrm{QM}_{a_i}(F)$ and $-(x-b_i)^{k_i^-} \in \mathrm{QM}_{b_i}(F)$ in $\mathbb{R}[[x-a]]$; if $a_i = b_i = a$, then $-(x-a)^{k_i}$, $(x-a)^{k_i^+}$, and $-(x-a)^{k_i^-}$ are all in $\mathrm{QM}_a(F)$ in $\mathbb{R}[[x-a]]$.*

Proof. For each $i = 1, \ldots, n$, if $a_i \neq b_i$, then by the definition of $k_{a_i}^+(F)$ we know that there exists a polynomial $f \in F$ such that $\hat{f}_{a_i} = (x-a_i)^{k_i^+} \in \mathrm{QM}_{a_i}(F)$. Similarly, there exists another polynomial $g \in F$ such that $\hat{g}_{b_i} = -(x-b_i)^{k_i^-} \in \mathrm{QM}_{b_i}(F)$.

If $a_i = b_i = a$, then we discuss according to the type of (k_i, k_i^+, k_i^-). (Type A) In this case we know $k_i = k_a(F)$ is finite and by Definition 11 there exists a polynomial $f \in F$ such that $\mathrm{ord}_a(f) = k_i$ is even and $\epsilon_a(g_i) = -1$, which implies that $\hat{f}_a = -(x-a)^{k_i} \in \mathrm{QM}_a(F)$. Then by the inclusive relationship in Figure 1 we know that $-(x-a)^{k_i^-} = -(x-a)^{k_i+1}$ and $(x-a)^{k_i^+} = (x-a)^{k_i+1}$ are both in $\mathrm{QM}_a(F)$. (Type B) It suffices to prove $\mathrm{QM}_0(-x^{2n}) \subseteq \mathrm{QM}_0(x^{2n-1}, -x^{2n-1})$ for any positive integer n, and this inclusion can be shown with
$$-x^{2n} = x^{2n-1}(-x) = x^{2n-1}\left(\frac{-x+1}{2}\right)^2 + (-x^{2n-1})\left(\frac{-x-1}{2}\right)^2.$$
The proofs for Type C and Type D are similar to that of Type A. □

Lemma 18. *Let $f \in \mathbb{R}[x]$ be a polynomial whose factorization is $f = \prod_{i=1}^{m}(x-a_i)^{t_i} h(x)$, where $a_1, \ldots, a_m$ are pairwisely distinct and $h(x)$ is a product of quadratic irreducible polynomials. Then for each $i = 1, \ldots, m$, $\mathrm{ord}_{a_i}(f) = t_i$ and $\epsilon_{a_i}(f) = \mathrm{sign}(f(p_i))$, where p_i is any point to the right of a_i such that no root of f falls in $(a_i, p_i]$.*

Proof. For each $i = 1, \ldots, m$, from the factorization of f we know that a_i is a root of f of multiplicity t_i, and thus $f^{(j)}(a_i) = 0$

for $j = 0, \ldots, t_i - 1$ and $f^{(t_i)}(a_i) = (t_i!) \prod_{j=1, j\neq i}^{m} (a_i - a_j)^{t_j} h(a_i) \neq 0$. Then, $\mathrm{ord}_{a_i}(f) = t_i$.

Write f as $f = (x - a_i)^{t_i} \prod_{j=1, j\neq i}^{m} (x - a_j)^{t_j} h(x)$. Then $f(p_i) = (p_i - a_i)^{t_i} \prod_{j=1, j\neq i}^{m} (p_i - a_j)^{t_j} h(p_i)$. Comparing this expression with that of $f^{(t_i)}(a_i)$, we know that $f^{(t_i)}(a_i)$ and $f(p_i)$ share the same sign, for $p_i - a_i > 0$ and $(a_i, p_i]$ does not contain any root of f. □

Theorem 19. *Let $G = \{g_1, ..., g_s\}$ and $F = \{f_1, ..., f_t\}$ be two polynomial sets in $\mathbb{R}[x]$ such that $S(G)$ is bounded. Then $\mathrm{QM}(F) \subseteq \mathrm{QM}(G)$ if and only if $S(G) \subseteq S(F)$ and $\omega(G) \preceq \omega_{S(G)}(F)$.*

Proof. Without loss of generality, let $S(G) = \bigcup_{i=1}^{n} [a_i, b_i]$, $\omega(G) = (k_1, k_1^+, k_1^-, ..., k_n, k_n^+, k_n^-)$, and $\omega_{S(G)}(F) = (\tilde{k}_1, \tilde{k}_1^+, \tilde{k}_1^-, \ldots, \tilde{k}_n, \tilde{k}_n^+, \tilde{k}_n^-)$.

($\Rightarrow$) From the inclusion $\mathrm{QM}(F) \subseteq \mathrm{QM}(G)$ we know that for each $i = 1, \ldots, t$, f_i is in $\mathrm{QM}(G)$, and thus there exist sums of squares $\sigma_0, \sigma_1, \ldots, \sigma_s$ in $\mathbb{R}[x]$ such that $f_i = \sigma_0 + \sum_{j=1}^{s} \sigma_j g_j$. Then, $f_i|_{S(G)} \geq 0$ for $i = 1, \ldots, t$, and thus $S(G) \subseteq S(F)$. To prove $\omega(G) \preceq \omega_{S(G)}(F)$, it suffices to prove that for each $j = 1, \ldots, n$, $(k_j, k_j^+, k_j^-) \preceq (\tilde{k}_j, \tilde{k}_j^+, \tilde{k}_j^-)$.

(1) If $a_j \neq b_j$, then this is a closed interval and $\tilde{k}_j = k_j = \infty$. We first prove the inequality $k_j^+ \leq \tilde{k}_j^+$, which only involves the left boundary a_j. For each $f_i \in F$, we know that $f_i(a_j) \geq 0$. If $f_i(a_j) > 0$, then by Lemma 16(3) $k_{a_j}^+(f_i) = \infty$. Else if $f_i(a_j) = 0$, then by $f_i|_{[a_j, b_j]} \geq 0$ and Lemma 18, we know that $\epsilon_{a_j}(f_i) = 1$. When $\mathrm{ord}_{a_j}(f_i)$ is even, by Definition 11 $k_{a_j}^+(f_i) = \infty$; when $\mathrm{ord}_{a_j}(f_i)$ is odd, by Theorem 13(1) $k_{a_j}^+(f_i) = \mathrm{ord}_{a_j}(f_i) \geq k_{a_j}^+(G)$. Summarizing all the cases above, $\tilde{k}_j^+ = k_{a_j}^+(F) = \min_{1\leq i\leq t} k_{a_j}^+(f_i) \geq k_{a_j}^+(G) = k_j^+$.

Next we prove the remaining inequality $k_j^- \leq \tilde{k}_j^-$ which only involves b_j. As in the arguments above for a_j, we only need to consider the case when $f_i(b_j) = 0$ for each $f_i \in F$. When $\epsilon_{b_j}(f_i) = 1$, we know that $\mathrm{ord}_{b_j}(f_i)$ is even, for otherwise f_i will be negative at some point to the left of b_j, which contradicts the fact $f_i|_{[a_j, b_j]} \geq 0$. Now $k_{b_j}^-(f_i) = \infty$ by Definition 11. When $\epsilon_{b_j}(f_i) = -1$, we know that $\mathrm{ord}_{b_j}(f_i)$ is odd, for otherwise b_j would be an isolated point in $S(f_i)$. By Theorem 13(2) we know that $k_{b_j}^-(f_i) = \mathrm{ord}_{b_j}(f_i) \geq k_{b_j}^-(G)$. Summarizing all the cases above, $\tilde{k}_j^- = k_{b_j}^-(F) = \min_{1\leq i\leq t} k_{b_j}^-(f_i) \geq k_{b_j}^-(G) = k_j^-$.

(2) If $a_j = b_j = a$, then it is an isolated point: For any $f \in F$, if $\mathrm{ord}_a(f)$ is even and $\epsilon_a(f) = 1$, then as in the arguments above, we can show that $L_a(f) = (\infty, \infty, \infty)$. In this case such a polynomial f has no influence on our target comparison $(k_j, k_j^+, k_j^-) \preceq (\tilde{k}_j, \tilde{k}_j^+, \tilde{k}_j^-)$, and thus we can ignore this kind of polynomials in F. Next we consider the four types of (k_j, k_j^+, k_j^-).

Type A corresponds to Case 1 of Theorem 13(3), and thus for each $f_i \in F$, $f_i \in \mathrm{QM}(G)$ and therefore $\mathrm{ord}_a(f) \geq k_a(G) = k_i$, where k_i is a finite even number. When $\epsilon_a(f_i) = 1$ and $\mathrm{ord}_a(f_i)$ is odd, $k_a^+(f_i) = \mathrm{ord}_a(f_i) \geq k_j + 1 = k_j^+$; when $\epsilon_a(f_i) = -1$ and $\mathrm{ord}_a(f_i)$ is even, $k_a(f_i) = \mathrm{ord}_a(f_i) \geq k_i$; when $\epsilon_a(f_i) = -1$ and $\mathrm{ord}_a(f_i)$ is odd, $k_a^-(f_i) = \mathrm{ord}_a(f_i) \geq k_j + 1 = k_j^-$. In all the three cases above, we can draw the conclusion $L_a(f_i) \geq [k_j, k_j^+, k_j^-]$, for the remaining two values in $L_a(f_i)$ are both ∞ by Lemma 16(1). Then by the arbitrariness of f_i in F, $\tilde{k}_j = k_a(F) = \min_{1\leq i\leq t} k_a(f_i) \geq k_j$. Similarly the inequalities $\tilde{k}_j^+ \geq k_j^+$ and $\tilde{k}_j^- \geq k_j^-$ also hold, and thus, $(\tilde{k}_j, \tilde{k}_j^+, \tilde{k}_j^-) \geq (k_j, k_j^+, k_j^-)$.

In Type B, the case $k_j \geq k_j^+ \geq k_j^-$ corresponds to Case 3 of Theorem 13(3), while the remaining case $k_j \geq k_j^- \geq k_j^+$ to Case 2; Type C corresponds to Case 2; and Type D corresponds to Case 3. Performing similar analysis as done in Type A, we can draw the same conclusion $L_a(f_i) \geq (k_j, k_j^+, k_j^-)$ for each $f_i \in F$, and the inequality $(\tilde{k}_j, \tilde{k}_j^+, \tilde{k}_j^-) \geq (k_j, k_j^+, k_j^-)$ follows.

($\Leftarrow$) To prove the inclusion $\mathrm{QM}(F) \subseteq \mathrm{QM}(G)$, it suffices to prove $f_i \in \mathrm{QM}(G)$ for each $f_i \in F$. Since $S(G) \subseteq S(F) \subseteq S(f_i)$, $f_i|_{S(G)} \geq 0$, and thus by the local-global principle (Theorem 6), it suffices to show that $\hat{f}_{ia} \in \mathrm{QM}_a(G)$ for any $a \in S(G) \cap Z(f_i)$. Next we prove the inclusion for each interval $[a_j, b_j]$ of $S(G)$ for $j = 1, \ldots, n$.

(1) If $a_j \neq b_j$, then it is a closed interval. For any $a \in (a_j, b_j)$ such that $f_i(a) = 0$, we know that $\epsilon_a(f_i) = 1$ and $\mathrm{ord}_a(f_i)$ is even, and thus $\hat{f}_a$ is a sum of squares in $\mathbb{R}[[x - a]]$, implying $\hat{f}_a \in \mathrm{QM}_a(G)$ trivially. For the left boundary a_j, $\epsilon_{a_j}(f_i) = 1$. When $\mathrm{ord}_{a_j}(f_i)$ is even, we can show that $\hat{f}_{ia_j}$ is a sum of squares in $\mathbb{R}[[x - a_j]]$ and thus $\hat{f}_{ia_j} \in \mathrm{QM}_{a_j}(G)$ trivially. When $\mathrm{ord}_{a_j}(f_i)$ is odd, by Lemma 17 $(x - a_j)^{k_j^+} \in \mathrm{QM}_{a_j}(G)$, and thus from $\mathrm{ord}_{a_j}(f_i) = k_{a_j}^+(f_i) \geq \tilde{k}_j^+ \geq k_j^+$, we have $\hat{f}_{ia_j} = (x - a_j)^{\mathrm{ord}_{a_j}(f_i)} \in \mathrm{QM}_{a_j}(G)$. For the right boundary b_j, when $\epsilon_{b_j}(f_i) = 1$, $\mathrm{ord}_{b_j}(f_i)$ must be even, for otherwise f is negative at some point to the left of b_j, which contradicts the fact $f_i|_{[a_j, b_j]} \geq 0$. In this case $\hat{f}_{ib_j}$ is a sum of squares in $\mathbb{R}[[x - b_j]]$ and thus $\hat{f}_{ib_j} \in \mathrm{QM}_{b_j}(G)$ trivially. When $\epsilon_{b_j}(f_i) = -1$, $\mathrm{ord}_{b_j}(f_i)$ must be odd, for otherwise b_j is an isolated point of $S(f)$, another contradiction. By Lemma 17 we know that $-(x - b_j)^{k_j^-} \in \mathrm{QM}_{b_j}(G)$, and thus from $\mathrm{ord}_{b_j}(f_i) = k_{b_j}^-(f_i) \geq \tilde{k}_j^- \geq k_j^-$, $\hat{f}_{ib_j} = -(x - b_j)^{\mathrm{ord}_{b_j}(f_i)} \in \mathrm{QM}_{b_j}(G)$.

(2) If $a_j = b_j = a$, then it is an isolated point: by Lemma 16(2) we have that $L_a(f_i) \geq L_a(F) \geq (\tilde{k}_j, \tilde{k}_j^+, \tilde{k}_j^-) \geq (k_j, k_j^+, k_j^-)$, and thus $\hat{f}_{ia} = \epsilon_a(f_i)(x - a)^{\mathrm{ord}_a(f)}$ is in $\mathrm{QM}_a(\{-(x - a)^{k_j}, (x - a)^{k_j^+}, -(x - a)^{k_j^-}\})$ and thus in $\mathrm{QM}_a(G)$ by Lemma 17. □

Corollary 20. *Let $G \subseteq \mathbb{R}[x]$ be a polynomial set with bounded $S(G)$ and $f \in \mathbb{R}[x]$ be an polynomial. Then $f \in \mathrm{QM}(G)$ if and only if $f|_{S(G)} \geq 0$ and $\omega(G) \preceq \omega_{S(G)}(f)$.*

Based on Theorem 19, we directly derive an algorithm to test inclusion of finitely generated quadratic modules. This algorithm is summarized below as Algorithms 2, where Signature(F, S) is a subroutine to compute the signature of F with respect to a non-negative set S. Note that when the polynomial set F consists of a single polynomial f, Algorithm 2 indeed degenerates to an algorithm to test membership in bounded quadratic module $\mathrm{QM}(G)$.

From Theorem 19, the criterion for the equality of two quadratic modules, which is Corollary 2.27 in [2], is straightforward.

Corollary 21. *Let F and G be two polynomial sets in $\mathbb{R}[x]$ with bounded $S(F)$ and $S(G)$. Then $\mathrm{QM}(G) = \mathrm{QM}(F)$ if and only if $S(G) = S(F)$ and $\omega(G) = \omega(F)$.*

Algorithm 2: Algorithm for testing inclusion of finitely generated quadratic modules $B := \mathsf{IsIncluded}(F, G)$

Input: Two finite polynomial sets $F, G \subseteq \mathbb{R}[x]$ with bounded $S(G)$
Output: A boolean B such that B = true if $\mathrm{QM}(F) \subseteq \mathrm{QM}(G)$ and B = false otherwise

$S_F := S(F)$; $S_G := S(G)$;
if $S_G \subseteq S_F$ **then**
  $\omega_F := \mathsf{Signature}(F, S_F)$; $\omega_G := \mathsf{Signature}(G, S_G)$;
  if $\omega_G \preceq \omega_F$ **then** $B :=$ true; **else** $B :=$ false;
else $B :=$ false;
return B;

Example 22. (1) We first test whether the polynomial $f_1 = x^3(x-1)^3$ is in $\mathrm{QM}(G)$ with the polynomial set G in Example 12 by using Corollary 20. One can check that $S(f_1) = [-\infty, 0] \cup [1, \infty] \supseteq S(G)$ and $\omega_{S(G)}(f_1) = (\infty, \infty, 3, \infty, 3, \infty, \infty, \infty, \infty)$. Comparing $\omega_{S(G)}(f_1)$ with $\omega(G)$ computed in Example 15, one finds that $\omega(G) \preceq \omega_{S(G)}(f_1)$, and thus by Corollary 20 one has $f_1 \in \mathrm{QM}(G)$.

(2) Let $F = \{f_1, f_2, f_3\}$ with $f_2 = x^3(x-1)^6(x-2)$ and $f_3 = (x-1)^5(x-2)^4(x-2.5)$. Next we test whether the quadratic module $\mathrm{QM}(F)$ is included in $\mathrm{QM}(G)$. One can compute that $S(F) = [-\infty, 0] \cup [1, 1] \cup [2, 2] \cup [2.5, \infty] \supseteq S(G)$ and $\omega_{S(G)}(F) = (\infty, \infty, 3, 6, 3, 5, 4, 1, 5)$. The last tuples in $\omega_{S(G)}(F)$ and $\omega(G)$ are $(4, 1, 5)$ and $(4, 3, 4)$ respectively and $(4, 1, 5) \not\preceq (4, 3, 4)$. As a result, one knows that $\mathrm{QM}(F) \not\subseteq \mathrm{QM}(G)$ by Theorem 19.

(3) Let $H = \{(x+1)x(x-1)^2(x-2)^3, -(x-0.8)(x-1)(x-2)^3\}$. Then one can check that $S(H) = S(G)$ and $\omega(H) = \omega(G)$, and thus by Corollary 21 one knows $\mathrm{QM}(H) = \mathrm{QM}(G)$.

5 MINIMAL NUMBER OF GENERATORS OF BOUNDED QUADRATIC MODULES

A key result of this paper is to reduce the number of generators for any bounded finitely generated quadratic module $\mathrm{QM}(G)$ in $\mathbb{R}[x]$ to at most 2, the best possible in general, using Algorithm 3 below. This improves upon an algorithm in Augustin's thesis [2] to find a set of at most 3 generators by using the signature $\omega(G)$.

The key insight that led to the algorithm is that in the definition of (k_i, k_i^+, k_i^-) of a polynomial set F with respect to the i-th interval $[a_i, b_i]$ of $S(F)$, there are at least one redundant value in the above tuple. The redundant values are: (1) for a closed interval: k_i; (2) for an isolated point: k_i^+ and k_i^- for Type A, k_i for Type B, k_i^- for Type C, and k_i^+ for Type D.

Theorem 23. *Algorithm 3 generates a set of at most 2 generators for a given bounded finitely generated univariate quadratic module.*

Proof. Obviously Algorithm 3 outputs two polynomials f and g in finite steps, and it suffices to prove that the quadratic modules $\mathrm{QM}(f, g)$ is equal to $\mathrm{QM}(G)$. Then by Corollary 21, we only need to show the equality $S(f, g) = S(G)$ and $\omega(f, g) = \omega(G)$.

The algorithm handles $[a_1, b_1], \ldots, [a_n, b_n]$ in $S(G)$ one by one and updates f and g accordingly in each iteration. For each $i = 1, \ldots, n$, denote the updated f and g after the i-th iteration by f_i and g_i respectively, and let $S_i := \bigcup_{j=1}^{i} [a_j, b_j]$ and ω_i be the truncated sequence of $\omega(G)$ consisting of its first $3i$ elements. Next we prove by induction the equality $S(f_i, g_i) = S_i$ and $\omega(f_i, g_i) = \omega_i$ for all $i = 1, \ldots, n$, which completes the proof because clearly $S_n = S(G)$ and $\omega_n = \omega(G)$.

Algorithm 3: Algorithm for finding two generators of a bounded quadratic module $\{f, g\} := \mathsf{2Generators}(G)$

Input: A finite polynomial set $G \subseteq \mathbb{R}[x]$ with bounded $S(G)$
Output: Two polynomials f and g such that $\mathrm{QM}(G) = \mathrm{QM}(f, g)$

$f := -1$; $g := 1$;
$S := S(G)$ (assuming $= \bigcup_{i=1}^{n} [a_i, b_i]$);
$(k_1, k_1^+, k_1^-, \ldots, k_n, k_n^+, k_n^-) := \mathsf{Signature}(G, S)$;
for $i = 1, \ldots, n$ **do**
  if $a_i < b_i$ **then** $f := f(x - a_i)^{k_i^+}(x - b_i)^{k_i^-}$;
  else
    switch *Type of* (k_i, k_i^+, k_i^-) **do**
      case *Type A* **do** $f := f(x - a_i)^{k_i}$;
      case *Type B* **do**
        if $i = 1$ **then** $f := f(x - a_i)^{k_i^-}$; $g := g(x - a_i)^{k_i^+}$;
        else if $i = n$ **then**
          $f := f(-x + a_i)^{k_i^+}$; $g := g(-x + a_i)^{k_i^-}$;
        else
          $d := a_{i+1} - a_i$; $f := f(x - a_i)^{k_i^+}(x - (a_i + \frac{d}{5}))$;
          $g := g(x - a_i)^{k_i^-}(x - (a_i + \frac{2d}{5}))$;
      case *Type C* **do**
        $f := f(x - a_i)^{k_i}$;
        if $i = 1$ **then** $g := g(x - a_i)^{k_i^+}$;
        else $d := a_i - b_{i-1}$; $g := g(x - (a_i - \frac{d}{5}))(x - a_i)^{k_i^+}$;
      case *Type D* **do**
        $f := f(x - a_i)^{k_i}$;
        if $i = n$ **then** $g := g(-x + a_i)^{k_i^-}$;
        else $d := a_{i+1} - a_i$; $g := g(x - a_i)^{k_i^-}(x - (a_i + \frac{d}{5}))$;
return $\{f, g\}$;

(1) We start with $i = 1$. (a) If $a_1 < b_1$, then $[a_1, b_1]$ is a closed interval. By Algorithm 3, $f_1 = -(x - a_1)^{k_1^+}(x - b_1)^{k_1^-}$ and $g_1 = 1$. By the definitions of k_1^- and k_1^+, we know that both of them are odd, and thus $S(f_1) = [a_1, b_1]$. With $g_1 = 1$, clearly $S(f_1, g_1) = [a_1, b_1]$ and $f_1(x) < 0, g_1(x) > 0$ when $x > b_1$. From $\mathrm{ord}_{a_1}(f_1) = k_1^+$, $\epsilon_{a_1}(f_1) = 1$, $\mathrm{ord}_{b_1}(f_1) = k_1^-$, $\epsilon_{b_1}(f_1) = -1$, $\mathrm{ord}_{a_1}(g_1) = \mathrm{ord}_{b_1}(g_1) = 0$, and $\epsilon_{a_1}(g_1) = \epsilon_{b_1}(g_1) = 1$, we know that $k_{a_1}^+(f_1, g_1) = k_1^+$, $k_{b_1}^-(f_1, g_1) = k_1^-$, and $k_1(f_1, g_1) = k_1 = \infty$, which means $\omega(f_1, g_1) = \omega_1$.

(b) If $a_1 = b_1 = a$, then it is an isolated point. The discussions are divided into four cases according to the type of (k_1, k_1^+, k_1^-). We take Type A for example, where $f_1 = -(x - a)^{k_1}$ and $g_1 = 1$. Then, $k_a(f_1, g_1) = k_1$ and $k_a^+(f_1, g_1) = k_a^-(f_1, g_1) = \infty = k_1^+ = k_1^-$, which imply $\omega(f_1, g_1) = \omega_1$. The equality $S(f_1, g_1) = [a, a]$ is easy to verify. The proofs for the remaining three types are similar. Furthermore, f_1 and g_1 also satisfy the condition that $f(x) < 0$ and $g(x) > 0$ when $x > a + \frac{2d_1}{5}$ in all the four types, where $d_1 := a_2 - b_1$.

(2) Assume that for $i = 1, \ldots, m$, $S(f_i, g_i) = S_i$, $\omega(f_i, g_i) = \omega_i$, and $f_i(x) < 0, g_i(x) > 0$ when $x > b_i + \frac{2d_i}{5}$, where $d_i := a_{i+1} - b_i$. Next we prove the equality $S(f_i, g_i) = S_i$ and $\omega(f_i, g_i) = \omega_i$ and the inequality $f_i(x) < 0, g_i(x) > 0$ when $x > b_i + \frac{2d_i}{5}$ for $i = m + 1$.

(a) If $a_{m+1} < b_{m+1}$, then $f_{m+1} = f_m(x - a_{m+1})^{k_{m+1}^+}(x - b_{m+1})^{k_{m+1}^-}$ and $g_{m+1} = g_m$. (i) For any $x < a_{m+1}$, since both k_{m+1}^+ and k_{m+1}^- are odd, $(x - a_{m+1})^{k_{m+1}^+}(x - b_{m+1})^{k_{m+1}^-} > 0$. This means that when $x < a_{m+1}$, f_{m+1} and f_m share the same sign. In particular, one can

show that $S(f_{m+1}, g_{m+1}) \cap (-\infty, a_{m+1}) = S(f_m, g_m) \cap (-\infty, a_{m+1}) = S(f_m, g_m)$. (ii) For any $a_{m+1} \le x \le b_{m+1}$, $(x-a_{m+1})^{k^+_{m+1}}(x-b_{m+1})^{k^-_{m+1}} \le 0$. Since $f_m(x) < 0$ when $x > b_i + \frac{2d_i}{5}$ by the induction hypothesis, we know that $f_{m+1} \ge 0$ when $x \in [a_j, b_j]$. (iii) For any $x > b_{m+1}$, $(x-a_{m+1})^{k^+_{m+1}}(x-b_{m+1})^{k^-_{m+1}} > 0$ and $f_m(x) < 0$, and thus $f_{m+1}(x) < 0$.

Summarizing the arguments above, we know that $S(f_{m+1}, g_{m+1}) = S(f_m, g_m) \cup [a_{m+1}, b_{m+1}] = S_{m+1}$. Furthermore, by Lemma 18 we know that $\mathrm{ord}_{a_{m+1}}(f_{m+1}) = k^+_{m+1}$, $\mathrm{ord}_{b_{m+1}}(f_{m+1}) = k^-_{m+1}$, $\epsilon_{a_{m+1}}(f_{m+1}) = 1$, $\epsilon_{b_{m+1}}(f_{m+1}) = -1$, and thus $k_{m+1}(f_{m+1}, g_{m+1}) = \infty$, $k^+_{m+1}(f_{m+1}, g_{m+1}) = k^+_{m+1}$, and $k^-_{m+1}(f_{m+1}, g_{m+1}) = k^-_{m+1}$. Note that the first m elements in the signature $\omega(f_{m+1}, g_{m+1})$ are precisely $\omega(f_m, g_m)$, and thus $\omega(f_{m+1}, g_{m+1}) = \omega_{m+1}$. The conditions $f_{m+1}(x) < 0, g_{m+1}(x) > 0$ when $x > b_{m+1} + \frac{2d_{m+1}}{5}$ are easy to verify.

(b) If $a_{m+1} = b_{m+1}$, we study the four cases according to the type of $(k_{m+1}, k^+_{m+1}, k^-_{m+1})$. As can be found in Algorithm 3, we also need to distinguish whether $m + 1 = n$.

(b.1) When $m + 1 < n$. Note that for all the four types, both f_{m+1} and g_{m+1} are constructed from f_m and g_m by multiplying even numbers (counting multiplicities) of linear factors.

First we consider the signs of f_{m+1} and g_{m+1} for different intervals in the most complicated Type B. (i) When $x < a_{m+1}$, we know that both the multiplied factors $(x-a_{m+1})^{k^+_{m+1}}(x-(a_{m+1}+\frac{d}{5}))$ and $(x-a_{m+1})^{k^-_{m+1}}(x-(a_{m+1}+\frac{2d}{5}))$ are positive, and thus $S(f_{m+1}, g_{m+1}) \cap (-\infty, a_{m+1}) = S(f_m, g_m) \cap (-\infty, a_{m+1}) = S(f_m, g_m)$. (ii) When $x = a_{m+1}$, $f_{m+1}(a_{m+1}) = g_{m+1}(a_{m+1}) = 0$. (iii) When $a_{m+1} < x < a_{m+1} + \frac{2d_{m+1}}{5}$, $g_{m+1} < 0$. (iv) When $x \ge a_{m+1} + \frac{2d_{m+1}}{5}$, $f_{m+1} < 0$. With these four arguments, we know that $S(f_{m+1}, g_{m+1}) = S(f_m, g_m) \cup [a_{m+1}, a_{m+1}] = S_{m+1}$. In particular, $f_{m+1}(x) < 0$ and $g_{m+1}(x) > 0$ hold when $x > b_{m+1} + \frac{2d_{m+1}}{5}$, and it is easy to verify $\omega(f_{m+1}, g_{m+1}) = \omega_{m+1}$. The proofs for the remaining three types can be done with similar analysis as above.

(b.2) When $m+1 = n$, it suffices to study Types B and D. (i) For type B, $f_n = f_{n-1}(-x+a_n)^{k^+_n}$ and $g_n = g_{n-1}(-x+a_n)^{k^-_n}$, and thus $\mathrm{ord}_{a_n}(f) = k^+_n$, $\epsilon_{a_n}(f) = 1$, $\mathrm{ord}_{a_n}(g) = k^-_n$, and $\epsilon_{a_n}(g) = -1$. This implies that $k_n(f_n, g_n) = \infty$, $k^+_n(f_n, g_n) = k^+_n$, and $k^-_n(f_n, g_n) = k^-_n$, namely $\omega(f_n, g_n) = \omega_n$. For any $x > a_n$, $f_n > 0$ and $g_n < 0$, and thus $S(f_n, g_n) = S(f_{n-1}, g_{n-1}) \cup [a_n, a_n] = S_n$. (ii) For type D, $f_n = f_{n-1}(x-a_n)^{k_i}$ and $g_n(a_n) = 0$, and thus $S(f_n, g_n) = S(f_{n-1}, g_{n-1}) \cup [a_n, a_n] = S_n$. The equality $\omega(f_n, g_n) = \omega_n$ is easy to verify. □

The following pictures illustrate the changes we make to f_m and g_m at an isolated point a_{m+1} to construct f_{m+1} and g_{m+1}.

Example 24. Let us demonstrate Algorithm 3 with the polynomial set G as in Example 12. The two polynomials f and g are first initialized with -1 and 1 respectively. Then in lines 2 and 3 the algorithm computes $S(G) = \bigcup_{i=1}^{3}[a_i, b_i] = [-1, 0] \cup [1, 1] \cup [2, 2]$ and $\omega(G) = (\infty, 1, 1, 2, 1, 3, 4, 3, 3)$, as done in the previous examples. Next in the iteration for the 3 intervals:

For $i = 1$: since $-1 = a_1 \ne b_1 = 0$, in line 5 the algorithm updates $f = -1 \cdot (x-1)^1(x-0)^1 = -(x+1)x$ and g remains to be 1.

For $i = 2$: since $a_2 = b_2 = 1$ and $(k_2, k^+_2, k^-_2) = (2, 1, 3)$ is of Type C, the algorithm jumps to line 16 and updates $f = [-(x+1)x] \cdot [(x-1)^2] = -(x+1)x(x-1)^2$ and $g = 1 \cdot [x - (1 - \frac{1}{5})](x-1) = (x-0.8)(x-1)$ (for $d = 1-0 = 1$) respectively in lines 17 and 19.

For $i = 3$: since $a_3 = b_3 = 2$ and $(k_2, k^+_2, k^-_2) = (4, 3, 3)$ is of Type B, the algorithm jumps to line 9 and updates $f = [-(x+1)x(x-1)^2] \cdot (-x+2)^3 = (x+1)x(x-1)^2(x-2)^3$ and $g = [(x-0.8)(x-1)] \cdot (-x+2)^3 = -(x-0.8)(x-1)(x-2)^3$ respectively in line 12.

At the end, Algorithm 3 outputs $f = (x+1)x(x-1)^2(x-2)^3$ and $g = -(x-0.8)(x-1)(x-2)^3$. In Example 22(3) the equality $\mathrm{QM}(f, g) = \mathrm{QM}(G)$ is already proved.

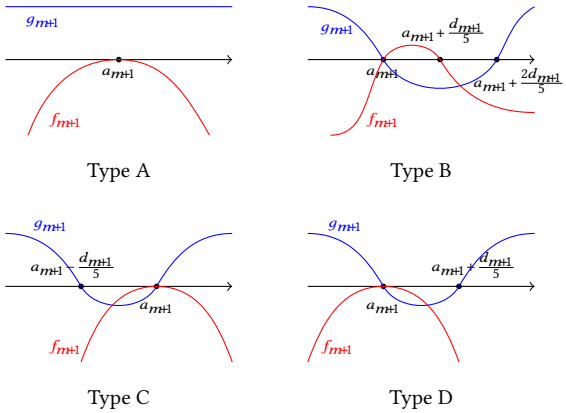

Figure 2: Illustrations of updates at a new isolated point

Example 25. In [2, Example 2.31] Augustin gave an example of a finitely generated bounded quadratic module for which her algorithm outputs three generators $f_1 := -x^4(x-1)^6$, $f_2 := x^3(x-1)^7$, and $f_3 := -(x-1)^5$. The proposed algorithm instead outputs two generators f_1 and $g := -x^3(x-0.2)(x-1)^5$ for the same quadratic module. It can be easily checked that $\mathrm{QM}(f_1, f_2, f_3)$ and $\mathrm{QM}(f_1, g)$ have the same non-negative set and signature, implying $\mathrm{QM}(f_1, f_2, f_3) = \mathrm{QM}(f_1, g)$. Certificates for $f_2, f_3 \in \mathrm{QM}(f_1, g)$ are: $f_2 = s_{2,0} + s_{2,1}f_1 + s_{2,2}g$ and $f_3 = s_{3,0} + s_{3,1}f_1 + s_{3,2}g$, where $s_{2,1} = 5(x-2)^2$, $s_{2,2} = 5(x-1)^2$, $s_{3,1} = 1$, $s_{3,2} = 1.25$, and

$$s_{2,0} = 5x^4(x-1)^6[(x-\frac{3}{2})^2 + \frac{3}{4}],$$
$$s_{3,0} = \frac{1}{2}(x-1)^6[\frac{7}{16}x^4 + x^2(\frac{5}{4}x+1)^2 + (x+1)^2 + 1].$$

6 CONCLUDING REMARKS AND ACKNOWLEDGEMENTS

Precise implementable algorithms for membership test for univariate finitely generated quadratic modules are presented. The algorithms discussed in the paper have been implemented and experimented with many examples. The paper thus improves upon results in [2].

An exhaustive enumerative algorithm can be given for generating a witness in the bounded case by incrementally constructing sums of squares $\sigma_0, \ldots, \sigma_s$ with undetermined coefficients degree by degree in the representation $\sigma_0 + \sum_{i=1}^{s} \sigma_i g_i$; however, it is unclear to us how a witness can be computed efficiently. Whether the concepts and techniques discussed in the paper can be generalized to the bivariate case is also an open problem. The complexity analysis of the proposed algorithms and a detailed comparisons with other existing algorithms are planned.

The second and third author would like to acknowledge respectively National Natural Science Foundation of China (NSFC 11971050) and National Science Foundation of the United States (CCF 1908804) for supporting this research.

REFERENCES

[1] Emil Artin. 1927. Über die Zerlegung definiter Funktionen in Quadrate. *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg* 5, 1 (1927), 100–115.

[2] Doris Augustin. 2008. *The Membership Problem for Quadratic Modules with Focus on the One Dimensional Case.* Ph.D. Dissertation. University of Regensburg.

[3] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. 2013. *Real Algebraic Geometry.* Springer Science & Business Media.

[4] Maria Eugenia Canto Cabral. 2005. *Archimedean Quadratic Modules: A Decision Problem in Dimension Two.* Ph.D. Dissertation. University of Konstanz.

[5] George Collins and Hoon Hong. 1991. Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation* 12, 3 (1991), 299–328.

[6] Thomas Jacobi. 1999. *Uber die Darstellung strikt positiver Polynome auf semialgebraischen Kompakta.* Ph.D. Dissertation. University of Konstanz.

[7] Thomas Jacobi and Alexander Prestel. 2001. Distinguished representations of strictly positive polynomials. *Journal für die reine und angewandte Mathematik* 532 (2001), 223–235.

[8] Jean-Louis Krivine. 1964. Anneaux préordonnés. *Journal d'Analyse Mathématique* 12, 1 (1964), 307–326.

[9] Jean-Bernard Lasserre. 2001. Global optimization with polynomials and the problem of moments. *SIAM Journal on optimization* 11, 3 (2001), 796–817.

[10] Henri Lombardi, Daniel Perrucci, and Marie-Françoise Roy. 2020. *An Elementary Recursive Bound for Effective Positivstellensatz and Hilbert's 17th Problem.* Memoirs of the American Mathematical Society, Vol. 263. American Mathematical Society.

[11] Victor Magron, Mohab Safey El Din, and Markus Schweighofer. 2019. Algorithms for weighted sum of squares decomposition of non-negative univariate polynomials. *Journal of Symbolic Computation* 93 (2019), 200–220.

[12] Ngoc Hoang Anh Mai and Victor Magron. 2022. On the complexity of Putinar–Vasilescu's Positivstellensatz. *Journal of Complexity* (2022), in press.

[13] Murray Marshall. 2008. *Positive Polynomials and Sums of Squares.* Mathematical Surveys and Monographs, Vol. 146. American Mathematical Society.

[14] Tim Netzer. 2009. Stability of quadratic modules. *Manuscripta Mathematica* 129, 2 (2009), 251–271.

[15] Jiawang Nie and Markus Schweighofer. 2005. On the complexity of Putinar's Positivstellensatz. *Journal of Complexity* 23, 1 (2005), 135–150.

[16] Pablo Parrilo. 2000. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization.* Ph.D. Dissertation. California Institute of Technology.

[17] Victoria Powers and Thorsten Wörmann. 1998. An algorithm for sums of squares of real polynomials. *Journal of Pure and Applied Algebra* 127, 1 (1998), 99–104.

[18] Mihai Putinar. 1993. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal* 42, 3 (1993), 969–984.

[19] Claus Scheiderer. 2003. Sums of squares on real algebraic curves. *Mathematische Zeitschrift* 245, 4 (2003), 725–760.

[20] Konrad Schmüdgen. 1991. The K-moment problem for compact semi-algebraic sets. *Mathematische Annalen* 289, 1 (1991), 203–206.

[21] Markus Schweighofer. 2004. On the complexity of Schmüdgen's Positivstellensatz. *Journal of Complexity* 20, 4 (2004), 529–543.

[22] Abraham Seidenberg. 1954. A new decision method for elementary algebra. *Annals of Mathematics* 60, 2 (1954), 365–374.

[23] Gilbert Stengle. 1974. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Mathematische Annalen* 207, 2 (1974), 87–97.

[24] Alfred Tarski. 1998. A decision method for elementary algebra and geometry. In *Quantifier elimination and cylindrical algebraic decomposition.* Springer, 24–84.

[25] Lieven Vandenberghe and Stephen Boyd. 1996. Semidefinite programming. *SIAM Review* 38, 1 (1996), 49–95.

[26] Sven Wagner. 2009. *Archimedean Quadratic Modules: A Decision Problem for Real Multivariate Polynomials.* Ph.D. Dissertation. University of Konstanz.