Computing Certificates of Members in Archimedean Quadratic Modules in $\mathbb{A}[X]$ and Certifying the Emptiness in Inconsistent Monogenic Archimedean Quadratic Modules in $\mathbb{A}[\overline{X}]$

Thesis Defense

Advisor: Prof. Deepak Kapur

Jose Abel Castellanos Joo

March 25, 2026

University of New Mexico

Agenda

Motivation & Problem

Algebraic reasoning with inequalities

Let $f = 1 - X^2$ and $g_1 = 2 - X - X^2, g_2 = 2 + X - X^2$

Algebraic reasoning with inequalities

Let $f = 1 - X^2$ and $g_1 = 2 - X - X^2, g_2 = 2 + X - X^2$
How can we certify that f is nonnegative where both g_1 and g_2 are nonnegative as well?

Algebraic reasoning with inequalities

Let $f = 1 - X^2$ and $g_1 = 2 - X - X^2, g_2 = 2 + X - X^2$
How can we certify that f is nonnegative where both g_1 and g_2 are nonnegative as well?
Notice that

Algebraic reasoning with inequalities

Let $f = 1 - X^2$ and $g_1 = 2 - X - X^2, g_2 = 2 + X - X^2$
How can we certify that f is nonnegative where both g_1 and g_2 are nonnegative as well?
Notice that

- If f_1 and f_2 are nonnegative over some set S, their sum $f_1 + f_2$ and product $f_1 f_2$ are also nonnegative in S

Algebraic reasoning with inequalities

Let $f = 1 - X^2$ and $g_1 = 2 - X - X^2, g_2 = 2 + X - X^2$
How can we certify that f is nonnegative where both g_1 and g_2 are nonnegative as well?
Notice that

- If f_1 and f_2 are nonnegative over some set S, their sum $f_1 + f_2$ and product $f_1 f_2$ are also nonnegative in S
- Sums of squares are nonnegative over $\mathbb{R}$

Algebraic reasoning with inequalities

- With the above, is clear that $\frac{1}{3}(X^2-1)^2+\frac{1}{6}(X+1)^2\cdot g_1+\frac{1}{6}(X-1)^2\cdot g_2$ is nonnegative over the intervals where both g_1, g_2 are nonnegative.

Algebraic reasoning with inequalities

- With the above, is clear that $\frac{1}{3}(X^2-1)^2+\frac{1}{6}(X+1)^2\cdot g_1+\frac{1}{6}(X-1)^2\cdot g_2$ is nonnegative over the intervals where both g_1, g_2 are nonnegative.
- Furthermore, $f=\frac{1}{3}(X^2-1)^2+\frac{1}{6}(X+1)^2\cdot g_1+\frac{1}{6}(X-1)^2\cdot g_2$, so f holds the desired property.

Algebraic reasoning with inequalities

- With the above, is clear that $\frac{1}{3}(X^2-1)^2+\frac{1}{6}(X+1)^2\cdot g_1+\frac{1}{6}(X-1)^2\cdot g_2$ is nonnegative over the intervals where both g_1, g_2 are nonnegative.
- Furthermore, $f=\frac{1}{3}(X^2-1)^2+\frac{1}{6}(X+1)^2\cdot g_1+\frac{1}{6}(X-1)^2\cdot g_2$, so f holds the desired property.
- This particular representation of f allows us to quickly check the nonnegativity over a solution set.

Algebraic reasoning with inequalities

- With the above, is clear that $\frac{1}{3}(X^2-1)^2+\frac{1}{6}(X+1)^2\cdot g_1+\frac{1}{6}(X-1)^2\cdot g_2$ is nonnegative over the intervals where both g_1, g_2 are nonnegative.
- Furthermore, $f=\frac{1}{3}(X^2-1)^2+\frac{1}{6}(X+1)^2\cdot g_1+\frac{1}{6}(X-1)^2\cdot g_2$, so f holds the desired property.
- This particular representation of f allows us to quickly check the nonnegativity over a solution set. How can we find such representations for any nonnegative polynomial over an arbitrary set of polynomials?

Naive approach

Iteratively "find" real coefficients for m summands of degree d

Naive approach

Iteratively "find" real coefficients for m summands of degree d

$$
\begin{aligned}
f = &\sum_{i=1}^{m} (a_{0,i,0} + a_{0,i,1}X + \cdots + a_{0,i,d}X^d)^2 \\
&+ \sum_{i=1}^{m} (a_{1,i,0} + a_{1,i,1}X + \cdots + a_{1,i,d}X^d)^2 \cdot g_1 \\
&+ \sum_{i=1}^{m} (a_{2,i,0} + a_{2,i,1}X + \cdots + a_{2,i,d}X^d)^2 \cdot g_2
\end{aligned}
$$

Naive approach

For $m = d = 1$, we have

$$\begin{aligned}
1 - a_{0,1,0}^2 - 2a_{1,1,0}^2 - 2a_{2,1,0}^2 &= 0 \\
-2a_{0,1,0}a_{0,1,1} + a_{1,1,0}^2 - 4a_{1,1,0}a_{1,1,1} - a_{2,1,0}^2 - 4a_{2,1,0}a_{2,1,1} &= 0 \\
-1 - a_{0,1,1}^2 + a_{1,1,0}^2 + 2a_{1,1,0}a_{1,1,1} - 2a_{1,1,1}^2 + a_{2,1,0}^2 - 2a_{2,1,0}a_{2,1,1} - 2a_{2,1,1}^2 &= 0 \\
2a_{1,1,0}a_{1,1,1} + a_{1,1,1}^2 + 2a_{2,1,0}a_{2,1,1} - a_{2,1,1}^2 &= 0 \\
a_{1,1,1}^2 + a_{2,1,1}^2 &= 0
\end{aligned}$$

Naive approach

For $m = d = 1$, we have

$$\begin{aligned}
1 - a_{0,1,0}^2 - 2a_{1,1,0}^2 - 2a_{2,1,0}^2 &= 0 \\
-2a_{0,1,0}a_{0,1,1} + a_{1,1,0}^2 - 4a_{1,1,0}a_{1,1,1} - a_{2,1,0}^2 - 4a_{2,1,0}a_{2,1,1} &= 0 \\
-1 - a_{0,1,1}^2 + a_{1,1,0}^2 + 2a_{1,1,0}a_{1,1,1} - 2a_{1,1,1}^2 + a_{2,1,0}^2 - 2a_{2,1,0}a_{2,1,1} - 2a_{2,1,1}^2 &= 0 \\
2a_{1,1,0}a_{1,1,1} + a_{1,1,1}^2 + 2a_{2,1,0}a_{2,1,1} - a_{2,1,1}^2 &= 0 \\
a_{1,1,1}^2 + a_{2,1,1}^2 &= 0
\end{aligned}$$

No solution exists for this system of equations

Naive approach

# of partial solutions	Minimum	Median	Average	Maximum	Successful runs
6	0.015574	0.0191525	0.0192074	0.02764	84/84
5	0.016363	0.0200115	0.0217022	0.060212	126/126
4	0.017195	0.0278745	0.0769109	2.53658	120/126
3	0.01968	0.07222	0.4273	7.32189	72/84
2	0.336124	0.951686	3.46394	12.4142	16/36
1	N/A	N/A	N/A	N/A	0/9

Table: Execution times of `FindInstance` with added partial solutions for the Naive approach search.

Extended Gram matrix approach

- A polynomial f is a sums of squares if and only if there exists a semidefinite positive matrix A such that $f = v^T A v$ for some vector of monomials v

Extended Gram matrix approach

- A polynomial f is a sums of squares if and only if there exists a semidefinite positive matrix A such that $f = v^T A v$ for some vector of monomials v
- Uses semidefinite programming (SDP) to find the sums of squares for the certificate

Extended Gram matrix approach

- A polynomial f is a sums of squares if and only if there exists a semidefinite positive matrix A such that $f = v^T A v$ for some vector of monomials v
- Uses semidefinite programming (SDP) to find the sums of squares for the certificate
- SDP solvers rely on interior points methods (numerical methods), so the answer is an approximation

Extended Gram matrix approach

Example

Consider $f = 1 - X + X^2 - X^3 + X^4$

Extended Gram matrix approach

Example

Consider $f = 1 - X + X^2 - X^3 + X^4$

Since

$$A = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix}^T \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix},$$

and

Extended Gram matrix approach

Example

Consider $f = 1 - X + X^2 - X^3 + X^4$

Since

$$A = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix}^T \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix},$$

and

$f = \begin{pmatrix} 1 & X & X^2 \end{pmatrix} A \begin{pmatrix} 1 \\ X \\ X^2 \end{pmatrix}$, then f is a sums of squares

Extended Gram matrix approach

Example

Consider $f = 1 - X + X^2 - X^3 + X^4$

Since

$$A = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix}^T \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix},$$

and

$f = \begin{pmatrix} 1 & X & X^2 \end{pmatrix} A \begin{pmatrix} 1 \\ X \\ X^2 \end{pmatrix}$, then f is a sums of squares

In fact, $f = \left(1 - \frac{1}{2}X\right)^2 + \left(\frac{\sqrt{3}}{2}X - \frac{1}{\sqrt{3}}X^2\right)^2 + \left(\sqrt{\frac{2}{3}}X^2\right)^2$

Extended Gram matrix method

$$A_0 = \begin{pmatrix} 0.333333 & 2.783040 \times 10^{-17} & -0.333333 \\ 2.783040 \times 10^{-17} & 3.871773 \times 10^{-8} & -2.073324 \times 10^{-17} \\ -0.333333 & -2.073324 \times 10^{-17} & 0.333334 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 0.166667 & 0.166667 & -1.197158 \times 10^{-14} \\ 0.166667 & 0.166667 & 2.533843 \times 10^{-8} \\ -1.197158 \times 10^{-14} & 2.533843 \times 10^{-8} & 2.533843 \times 10^{-8} \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 0.166667 & -0.166667 & -1.198342 \times 10^{-14} \\ -0.166667 & 0.166667 & -2.533843 \times 10^{-8} \\ -1.198342 \times 10^{-14} & -2.533843 \times 10^{-8} & 2.533844 \times 10^{-8} \end{pmatrix}$$

$$m^T = (1 \quad X \quad X^2)$$

Extended Gram matrix method

$$A_0 = \begin{pmatrix} 0.333333 & 2.783040 \times 10^{-17} & -0.333333 \\ 2.783040 \times 10^{-17} & 3.871773 \times 10^{-8} & -2.073324 \times 10^{-17} \\ -0.333333 & -2.073324 \times 10^{-17} & 0.333334 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 0.166667 & 0.166667 & -1.197158 \times 10^{-14} \\ 0.166667 & 0.166667 & 2.533843 \times 10^{-8} \\ -1.197158 \times 10^{-14} & 2.533843 \times 10^{-8} & 2.533843 \times 10^{-8} \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 0.166667 & -0.166667 & -1.198342 \times 10^{-14} \\ -0.166667 & 0.166667 & -2.533843 \times 10^{-8} \\ -1.198342 \times 10^{-14} & -2.533843 \times 10^{-8} & 2.533844 \times 10^{-8} \end{pmatrix}$$

$$m^T = (1 \quad X \quad X^2)$$

$$f = \sum_{i=0}^{2} (m^T A_i m) \cdot g_i$$

$$\approx (0.57735 + 4.82037 * 10^{-17} X - 0.57735 X^2)^2$$
$$+ (0.000196768 X + 3.60686 * 10^{-14} X^2)^2 + (0.000196768 X^2)^2$$
$$+ ((0.408248 + 0.408248 X - 2.93243 * 10^{-14} X^2)^2 + (0.000253093 X + 0.000100115 X^2)^2$$
$$+ (0.000123755 X^2)^2) \cdot g_1$$
$$+ ((0.000253093 X - 0.000100115 X^2)^2 + (0.408248 - 0.408248 X - 2.93533 * 10^{-14} X^2)^2$$
$$+ (0.000123755 X^2)^2) \cdot g_2$$
$$= 1 + 2.77705 * 10^{-16} X - X^2$$
$$-9.69776 * 10^{-17} X^3 + 6.85159 * 10^{-8} X^4 - 2.36719 * 10^{-17} X^5 - 5.06769 * 10^{-8} X^6$$

Literature about the problem

- Constructive real algebraic geometry [LPR14; Lom92]

Literature about the problem

- Constructive real algebraic geometry [LPR14; Lom92]
- Complexity degree bounds for effective Positivstellensatz [Sch02; PR01; NS07; Las01]

Literature about the problem

- Constructive real algebraic geometry [LPR14; Lom92]
- Complexity degree bounds for effective Positivstellensatz [Sch02; PR01; NS07; Las01]
- Membership checking using valuation theory [Jac99; JP01; CP08; Wag09]

Literature about the problem

- Constructive real algebraic geometry [LPR14; Lom92]
- Complexity degree bounds for effective Positivstellensatz [Sch02; PR01; NS07; Las01]
- Membership checking using valuation theory [Jac99; JP01; CP08; Wag09]
- Certificate computation using symbolic-numeric approaches [PP08; MS18; Kal+08]

Background

Preliminaries

Let $\mathbb{A} \subseteq \mathbb{R}$ be the set of real algebraic numbers, and $\mathbb{A}[\overline{X}] = \mathbb{A}[X_1, \ldots, X_n]$.

Preliminaries

Let $\mathbb{A} \subseteq \mathbb{R}$ be the set of real algebraic numbers, and $\mathbb{A}[\overline{X}] = \mathbb{A}[X_1, \ldots, X_n]$.

- Given a polynomial $f \in \mathbb{A}[\overline{X}]$, $\mathcal{Z}(f)$ denotes the real zeros of f

Preliminaries

Let $\mathbb{A} \subseteq \mathbb{R}$ be the set of real algebraic numbers, and $\mathbb{A}[\overline{X}] = \mathbb{A}[X_1, \ldots, X_n]$.

- Given a polynomial $f \in \mathbb{A}[\overline{X}]$, $\mathcal{Z}(f)$ denotes the real zeros of f
- $\sum \mathbb{A}[\overline{X}]^2$ denotes $\left\{\sum_{i=1}^{n} f_i^2 \mid f_i \in \mathbb{A}[\overline{X}]\right\}$

Preliminaries

Let $\mathbb{A} \subseteq \mathbb{R}$ be the set of real algebraic numbers, and $\mathbb{A}[\overline{X}] = \mathbb{A}[X_1, \ldots, X_n]$.

- Given a polynomial $f \in \mathbb{A}[\overline{X}]$, $\mathcal{Z}(f)$ denotes the real zeros of f
- $\sum \mathbb{A}[\overline{X}]^2$ denotes $\left\{\sum_{i=1}^{n} f_i^2 \mid f_i \in \mathbb{A}[\overline{X}]\right\}$
- The semialgebraic set of $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[\overline{X}]$, denoted by $\mathcal{S}(G)$, is defined by $\mathcal{S}(G) := \{\boldsymbol{x} \in \mathbb{R}^n \mid g_i(\boldsymbol{x}) \geq 0, 1 \leq i \leq s\}$.

Preliminaries

Let $\mathbb{A} \subseteq \mathbb{R}$ be the set of real algebraic numbers, and $\mathbb{A}[\overline{X}] = \mathbb{A}[X_1, \ldots, X_n]$.

- Given a polynomial $f \in \mathbb{A}[\overline{X}]$, $\mathcal{Z}(f)$ denotes the real zeros of f
- $\sum \mathbb{A}[\overline{X}]^2$ denotes $\left\{\sum_{i=1}^{n} f_i^2 \mid f_i \in \mathbb{A}[\overline{X}]\right\}$
- The semialgebraic set of $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[\overline{X}]$, denoted by $\mathcal{S}(G)$, is defined by $\mathcal{S}(G) := \{\boldsymbol{x} \in \mathbb{R}^n \mid g_i(\boldsymbol{x}) \geq 0, 1 \leq i \leq s\}$.
- Given $S \subseteq \mathbb{R}^n$, $\mathrm{Pos}(S) := \{f \in \mathbb{A}[\overline{X}] \mid f(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in S\}$.

Preliminaries

Definition

A **quadratic module** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication with squares in $\mathbb{A}[\overline{X}]$, and contains 1.

Preliminaries

Definition

A **quadratic module** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication with squares in $\mathbb{A}[\overline{X}]$, and contains 1.
Given a set of polynomials $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[\overline{X}]$, the quadratic module generated by G (abbreviated $\mathrm{QM}(G)$) is the set

$$\left\{ \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i \mid \sigma_i \in \sum \mathbb{A}[\overline{X}]^2, 0 \leq i \leq n \right\}$$

Preliminaries

Definition

A **quadratic module** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication with squares in $\mathbb{A}[\overline{X}]$, and contains 1.
Given a set of polynomials $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[\overline{X}]$, the quadratic module generated by G (abbreviated $\mathrm{QM}(G)$) is the set

$$\left\{ \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i \mid \sigma_i \in \sum \mathbb{A}[\overline{X}]^2, 0 \leq i \leq n \right\}$$

A **preordering** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication, and contains the sums of squares $\sum \mathbb{A}[\overline{X}]^2$ of $\mathbb{A}[\overline{X}]$.

Preliminaries

Definition

A **quadratic module** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication with squares in $\mathbb{A}[\overline{X}]$, and contains 1.
Given a set of polynomials $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[\overline{X}]$, the quadratic module generated by G (abbreviated $\mathrm{QM}(G)$) is the set

$$\left\{ \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i \mid \sigma_i \in \sum \mathbb{A}[\overline{X}]^2, 0 \leq i \leq n \right\}$$

A **preordering** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication, and contains the sums of squares $\sum \mathbb{A}[\overline{X}]^2$ of $\mathbb{A}[\overline{X}]$.
The preordering generated by a set of polynomials G (abbreviated $\mathrm{PO}(G)$) is the set

$$\left\{ \sum_{(e_1,\ldots,e_s)\subseteq\{0,1\}^s} \sigma_{(e_1,\ldots,e_s)} \cdot g_1^{e_1} \cdots g_s^{e_s} \mid \sigma_{(e_1,\ldots,e_s)} \in \sum \mathbb{A}[\overline{X}]^2 \right\}$$

Preliminaries

Definition

A **quadratic module** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication with squares in $\mathbb{A}[\overline{X}]$, and contains 1.
Given a set of polynomials $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[\overline{X}]$, the quadratic module generated by G (abbreviated $\mathrm{QM}(G)$) is the set

$$\left\{ \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i \mid \sigma_i \in \sum \mathbb{A}[\overline{X}]^2, 0 \leq i \leq n \right\}$$

A **preordering** in $\mathbb{A}[\overline{X}]$ is a subset that is closed under addition, closed under multiplication, and contains the sums of squares $\sum \mathbb{A}[\overline{X}]^2$ of $\mathbb{A}[\overline{X}]$.
The preordering generated by a set of polynomials G (abbreviated $\mathrm{PO}(G)$) is the set

$$\left\{ \sum_{(e_1,\ldots,e_s)\subseteq\{0,1\}^s} \sigma_{(e_1,\ldots,e_s)} \cdot g_1^{e_1} \cdots g_s^{e_s} \mid \sigma_{(e_1,\ldots,e_s)} \in \sum \mathbb{A}[\overline{X}]^2 \right\}$$

A quadratic module Q is called **Archimedean** if Q contains a polynomial of the form $N - \sum_{i=1}^{n} X_i^2$ where $N \in \mathbb{N}^+$.

Problem statement

- We refer to the sums of squares σ_i's in the above definition as the **certificates**.

Problem statement

- We refer to the sums of squares σ_i's in the above definition as the **certificates**.
- The **certificate problem for quadratic modules:** Given a set of generators G and a member $f \in \mathrm{QM}(G)$, to find the sums of squares multipliers $\sigma_0, \sigma_1, \ldots, \sigma_s$ such that $f = \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i$.

Problem statement

- We refer to the sums of squares σ_i's in the above definition as the **certificates**.
- The **certificate problem for quadratic modules:** Given a set of generators G and a member $f \in \mathrm{QM}(G)$, to find the sums of squares multipliers $\sigma_0, \sigma_1, \ldots, \sigma_s$ such that $f = \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i$.
- We refer to the polynomial f as the **input polynomial**.

Problem statement

- We refer to the sums of squares σ_i's in the above definition as the **certificates**.
- The **certificate problem for quadratic modules:** Given a set of generators G and a member $f \in \mathrm{QM}(G)$, to find the sums of squares multipliers $\sigma_0, \sigma_1, \ldots, \sigma_s$ such that $f = \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i$.
- We refer to the polynomial f as the **input polynomial**.
- This thesis is concerned with the computational aspects of finding certificates for members in Archimedean quadratic modules in $\mathbb{A}[X]$.

Core ideas and main ingredients

- The Membership Problem for quadratic modules with focus on the one dimensional case [Aug08; Aug12]
- Computing Certificates of Strictly Positive Polynomials in Archimedean Quadratic Modules [Sha+25]
- Positivity, sums of squares and the multi-dimensional moment problem [KM02]
- Positivity, sums of squares and the multi-dimensional moment problem II[KMS05]

Core ideas and main ingredients

- The Membership Problem for quadratic modules with focus on the one dimensional case [Aug08; Aug12]
  - Provides a decision algorithm to check membership in Archimedean quadratic modules in $\mathbb{R}[X]$
- Computing Certificates of Strictly Positive Polynomials in Archimedean Quadratic Modules [Sha+25]

- Positivity, sums of squares and the multi-dimensional moment problem [KM02]

- Positivity, sums of squares and the multi-dimensional moment problem II[KMS05]

Core ideas and main ingredients

- The Membership Problem for quadratic modules with focus on the one dimensional case [Aug08; Aug12]
  - Provides a decision algorithm to check membership in Archimedean quadratic modules in $\mathbb{R}[X]$
- Computing Certificates of Strictly Positive Polynomials in Archimedean Quadratic Modules [Sha+25]
  - Describes an algorithm to compute certificates of strictly positive polynomials
- Positivity, sums of squares and the multi-dimensional moment problem [KM02]

- Positivity, sums of squares and the multi-dimensional moment problem II[KMS05]

Core ideas and main ingredients

- The Membership Problem for quadratic modules with focus on the one dimensional case [Aug08; Aug12]
  - Provides a decision algorithm to check membership in Archimedean quadratic modules in $\mathbb{R}[X]$
- Computing Certificates of Strictly Positive Polynomials in Archimedean Quadratic Modules [Sha+25]
  - Describes an algorithm to compute certificates of strictly positive polynomials
- Positivity, sums of squares and the multi-dimensional moment problem [KM02]
  - Introduces natural generators
- Positivity, sums of squares and the multi-dimensional moment problem II[KMS05]

Core ideas and main ingredients

- The Membership Problem for quadratic modules with focus on the one dimensional case [Aug08; Aug12]
  - Provides a decision algorithm to check membership in Archimedean quadratic modules in $\mathbb{R}[X]$
- Computing Certificates of Strictly Positive Polynomials in Archimedean Quadratic Modules [Sha+25]
  - Describes an algorithm to compute certificates of strictly positive polynomials
- Positivity, sums of squares and the multi-dimensional moment problem [KM02]
  - Introduces natural generators
- Positivity, sums of squares and the multi-dimensional moment problem II[KMS05]
  - Introduces the Basic Lemma and a constructive proof of it

Membership check

Definition

Let f be a non-zero polynomial in $\mathbb{R}[X]$. Given a point $a \in \mathbb{R}$, the **order** of f at a, denoted $\mathrm{ord}_a(f)$, is the minimum natural number n such that $\frac{d^n f}{dX^n}(a) \neq 0$.

Membership check

Definition

Let f be a non-zero polynomial in $\mathbb{R}[X]$. Given a point $a \in \mathbb{R}$, the **order** of f at a, denoted $\mathrm{ord}_a(f)$, is the minimum natural number n such that $\frac{d^n f}{dX^n}(a) \neq 0$.
The **epsilon-sign** of f at a, denoted $\epsilon_a(f)$, is defined as 1 if $\frac{d^n f}{dX^n}(a) > 0$ where $n = \mathrm{ord}_a(f)$ and -1 otherwise.

Membership check

Definition

Let f be a non-zero polynomial in $\mathbb{R}[X]$. Given a point $a \in \mathbb{R}$, the **order** of f at a, denoted $\mathrm{ord}_a(f)$, is the minimum natural number n such that $\frac{d^n f}{dX^n}(a) \neq 0$.
The **epsilon-sign** of f at a, denoted $\epsilon_a(f)$, is defined as 1 if $\frac{d^n f}{dX^n}(a) > 0$ where $n = \mathrm{ord}_a(f)$ and -1 otherwise.

Definition

[[Aug08, p. 43]] Let $G := \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$.

Membership check

Definition

Let f be a non-zero polynomial in $\mathbb{R}[X]$. Given a point $a \in \mathbb{R}$, the **order** of f at a, denoted $\mathrm{ord}_a(f)$, is the minimum natural number n such that $\frac{d^n f}{dX^n}(a) \neq 0$.
The **epsilon-sign** of f at a, denoted $\epsilon_a(f)$, is defined as 1 if $\frac{d^n f}{dX^n}(a) > 0$ where $n = \mathrm{ord}_a(f)$ and -1 otherwise.

Definition

[[Aug08, p. 43]] Let $G := \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$.

$$\kappa_a(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}, \epsilon_a(g_i) = -1\}$$

Membership check

Definition

Let f be a non-zero polynomial in $\mathbb{R}[X]$. Given a point $a \in \mathbb{R}$, the **order** of f at a, denoted $\mathrm{ord}_a(f)$, is the minimum natural number n such that $\frac{d^n f}{dX^n}(a) \neq 0$.
The **epsilon-sign** of f at a, denoted $\epsilon_a(f)$, is defined as 1 if $\frac{d^n f}{dX^n}(a) > 0$ where $n = \mathrm{ord}_a(f)$ and -1 otherwise.

Definition

[[Aug08, p. 43]] Let $G := \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$.

$$\kappa_a(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}, \epsilon_a(g_i) = -1\}$$

$$\kappa_a^+(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}+1, \epsilon_a(g_i) = 1\}$$

Membership check

Definition

Let f be a non-zero polynomial in $\mathbb{R}[X]$. Given a point $a \in \mathbb{R}$, the **order** of f at a, denoted $\mathrm{ord}_a(f)$, is the minimum natural number n such that $\frac{d^n f}{dX^n}(a) \neq 0$.
The **epsilon-sign** of f at a, denoted $\epsilon_a(f)$, is defined as 1 if $\frac{d^n f}{dX^n}(a) > 0$ where $n = \mathrm{ord}_a(f)$ and -1 otherwise.

Definition

[[Aug08, p. 43]] Let $G := \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$.

$$\kappa_a(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}, \epsilon_a(g_i) = -1\}$$

$$\kappa_a^+(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}+1, \epsilon_a(g_i) = 1\}$$

$$\kappa_a^-(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}+1, \epsilon_a(g_i) = -1\}$$

Membership check

Definition

Let f be a non-zero polynomial in $\mathbb{R}[X]$. Given a point $a \in \mathbb{R}$, the **order** of f at a, denoted $\mathrm{ord}_a(f)$, is the minimum natural number n such that $\frac{d^n f}{dX^n}(a) \neq 0$.
The **epsilon-sign** of f at a, denoted $\epsilon_a(f)$, is defined as 1 if $\frac{d^n f}{dX^n}(a) > 0$ where $n = \mathrm{ord}_a(f)$ and -1 otherwise.

Definition

[[Aug08, p. 43]] Let $G := \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$.

$$\kappa_a(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}, \epsilon_a(g_i) = -1\}$$

$$\kappa_a^+(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}+1, \epsilon_a(g_i) = 1\}$$

$$\kappa_a^-(G) := \min_{1 \leq i \leq s} \{\mathrm{ord}_a(g_i) \mid \mathrm{ord}_a(g_i) \in 2\mathbb{N}+1, \epsilon_a(g_i) = -1\}$$

Each of these functions take the value ∞ if there is no polynomial g_i in G satisfying the conditions.

Membership check

Theorem ([Aug08, p. 47])

Let $f \in \mathbb{R}[X]$ *and* $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$ *with* $S = \mathcal{S}(G)$ *bounded. Then* $f \in \mathrm{QM}(G)$ *if and only if* $f|_S \geq 0$ *and*

Membership check

Theorem ([Aug08, p. 47])

Let $f \in \mathbb{R}[X]$ *and* $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$ *with* $S = \mathcal{S}(G)$ *bounded. Then* $f \in \mathrm{QM}(G)$ *if and only if* $f|_S \geq 0$ *and*

1. *for every left boundary point* a *of* $S \setminus S_{isol}$*, we have* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - \kappa_a^+(G) \in 2\mathbb{N}_0$

Membership check

Theorem ([Aug08, p. 47])

Let $f \in \mathbb{R}[X]$ *and* $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$ *with* $S = \mathcal{S}(G)$ *bounded. Then* $f \in \mathrm{QM}(G)$ *if and only if* $f|_S \geq 0$ *and*

1. *for every left boundary point* a *of* $S \setminus S_{isol}$*, we have* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - \kappa_a^+(G) \in 2\mathbb{N}_0$
2. *for every right boundary point* a *of* $S \setminus S_{isol}$*, we have* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - \kappa_a^-(G) \in 2\mathbb{N}_0$

Membership check

Theorem ([Aug08, p. 47])

Let $f \in \mathbb{R}[X]$ *and* $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$ *with* $S = \mathcal{S}(G)$ *bounded. Then* $f \in \mathrm{QM}(G)$ *if and only if* $f|_S \geq 0$ *and*

1. *for every left boundary point* a *of* $S \setminus S_{isol}$*, we have* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - \kappa_a^+(G) \in 2\mathbb{N}_0$
2. *for every right boundary point* a *of* $S \setminus S_{isol}$*, we have* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - \kappa_a^-(G) \in 2\mathbb{N}_0$
3. *for every isolated point* a *of* S*, we have* $\mathrm{ord}_a(f)$ *is even and* $\epsilon_a(f) = 1$ *or*

Membership check

Theorem ([Aug08, p. 47])

Let $f \in \mathbb{R}[X]$ *and* $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$ *with* $S = \mathcal{S}(G)$ *bounded. Then* $f \in \mathrm{QM}(G)$ *if and only if* $f|_S \geq 0$ *and*

1. *for every left boundary point* a *of* $S \setminus S_{isol}$*, we have* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - \kappa_a^+(G) \in 2\mathbb{N}_0$
2. *for every right boundary point* a *of* $S \setminus S_{isol}$*, we have* $\mathrm{ord}_a(f)$ *is even or* $\mathrm{ord}_a(f) - \kappa_a^-(G) \in 2\mathbb{N}_0$
3. *for every isolated point* a *of* S*, we have* $\mathrm{ord}_a(f)$ *is even and* $\epsilon_a(f) = 1$ *or*

   Case 1: $\mathrm{ord}_a(f) \geq \kappa_a(G)$ *if* $\kappa_a(G) < \kappa_a^+(G)$ *and* $\kappa_a(G) < \kappa_a^-(G)$
   Case 2: $(\mathrm{ord}_a(f) - \kappa_a^+(G) \in 2\mathbb{N}_0$ *and* $\epsilon_a(f) = 1)$ *or* $\mathrm{ord}_a(f) \geq \min\{\kappa_a(G), \kappa_a^-(G)\}$ *if* $\kappa_a^+(G) \leq \min\{\kappa_a(G), \kappa_a^-(G)\}$
   Case 3: $(\mathrm{ord}_a(f) - \kappa_a^-(G) \in 2\mathbb{N}_0$ *and* $\epsilon_a(f) = -1)$ *or* $\mathrm{ord}_a(f) \geq \min\{\kappa_a(G), \kappa_a^+(G)\}$ *if* $\kappa_a^-(G) \leq \min\{\kappa_a(G), \kappa_a^+(G)\}$

The Certificate algorithm

It computes certificates in $\mathbb{R}[\overline{X}]$. It extends a semi-constructive result in [Ave13].

The Certificate algorithm

It computes certificates in $\mathbb{R}[\overline{X}]$. It extends a semi-constructive result in [Ave13].

Lemma

[Ave13, Lemma 7 p. 4] Let $G = \{g_1, \ldots, g_s\}$, $S := \mathcal{S}(G)$, and let $f \in \mathbb{A}[X]$ be strictly positive on S. Let B be a compact subset of $\mathbb{R}^d$. Then there exists $g \in \mathrm{QM}(G)$ such that $f - g$ is strictly positive on B.

The Certificate algorithm

It computes certificates in $\mathbb{R}[\overline{X}]$. It extends a semi-constructive result in [Ave13].

Lemma

[Ave13, Lemma 7 p. 4] Let $G = \{g_1, \ldots, g_s\}$, $S := \mathcal{S}(G)$, and let $f \in \mathbb{A}[X]$ be strictly positive on S. Let B be a compact subset of $\mathbb{R}^d$. Then there exists $g \in \mathrm{QM}(G)$ such that $f - g$ is strictly positive on B.

The algorithm has a specialized version for the univariate case.

The Certificate algorithm

It computes certificates in $\mathbb{R}[\overline{X}]$. It extends a semi-constructive result in [Ave13].

Lemma

[Ave13, Lemma 7 p. 4] Let $G = \{g_1, \ldots, g_s\}$, $S := \mathcal{S}(G)$, and let $f \in \mathbb{A}[X]$ be strictly positive on S. Let B be a compact subset of $\mathbb{R}^d$. Then there exists $g \in \mathrm{QM}(G)$ such that $f - g$ is strictly positive on B.

The algorithm has a specialized version for the univariate case.

1. Computes a polynomial g in $\mathrm{QM}(G)$ with bounded semialgebraic set.

The Certificate algorithm

It computes certificates in $\mathbb{R}[\overline{X}]$. It extends a semi-constructive result in [Ave13].

Lemma

[Ave13, Lemma 7 p. 4] Let $G = \{g_1, \ldots, g_s\}$, $S := \mathcal{S}(G)$, and let $f \in \mathbb{A}[X]$ be strictly positive on S. Let B be a compact subset of $\mathbb{R}^d$. Then there exists $g \in \mathrm{QM}(G)$ such that $f - g$ is strictly positive on B.

The algorithm has a specialized version for the univariate case.

1. Computes a polynomial g in $\mathrm{QM}(G)$ with bounded semialgebraic set.
2. Uses a constructive result of Lemma 7 in [Ave13] and a generalization result of the latter which produces a polynomial of the form $f - \tilde{g}$ that is strictly positive over $\mathbb{R}$ where $\tilde{g} \in \mathrm{QM}(G)$. The latter is a sums of squares in the univariate case.

Natural generators

Definition

[KM02] For a given semialgebraic set $S \neq \emptyset$, the natural generators of S, denoted $\mathrm{Nat}(S)$, are the set of polynomials including:

(i) If $a \in S$ and $(-\infty, a) \cap S = \emptyset$, then $X - a \in \mathrm{Nat}(S)$. This is called the left natural generator or simply the **left generator** of $\mathrm{Nat}(S)$.

(ii) If $b, c \in S, b < c, (b, c) \cap S = \emptyset$, then $(X - b)(X - c) \in \mathrm{Nat}(S)$. This is called a **quadratic generator** of $\mathrm{Nat}(S)$.

(iii) If $d \in S$ and $(d, \infty) \cap S = \emptyset$, then $-(X - d) \in \mathrm{Nat}(S)$. This is called the right natural generator or simply the **right generator** of $\mathrm{Nat}(S)$.

(iv) $\mathrm{Nat}(S)$ has no other elements except these.

If $S = \emptyset$, then the set of natural generators is $\{-1\}$.

The Basic Lemma

Theorem

[KMS05, Basic Lemma (Lemma 2.1)] Suppose $f, g \in \mathrm{Pos}(\mathcal{S}(G))$ *are relatively prime. There exist strictly positive polynomials* σ, τ *over* $\mathcal{S}(G)$ *such that* $1 = \sigma f + \tau g$.

The Basic Lemma

Theorem

[KMS05, Basic Lemma (Lemma 2.1)] Suppose $f, g \in \mathrm{Pos}(\mathcal{S}(G))$ *are relatively prime. There exist strictly positive polynomials* σ, τ *over* $\mathcal{S}(G)$ *such that* $1 = \sigma f + \tau g$.

Theorem

[KMS05, Corollary 2.3 (i)] Given $f, g \in \mathrm{Pos}(\mathcal{S}(fg))$ *being relatively prime, where* $\mathcal{S}(fg)$ *is compact, there exists* $\sigma, \tau \in \sum \mathbb{R}[X]^2$ *such that* $1 = \sigma f + \tau g$.

The Basic Lemma

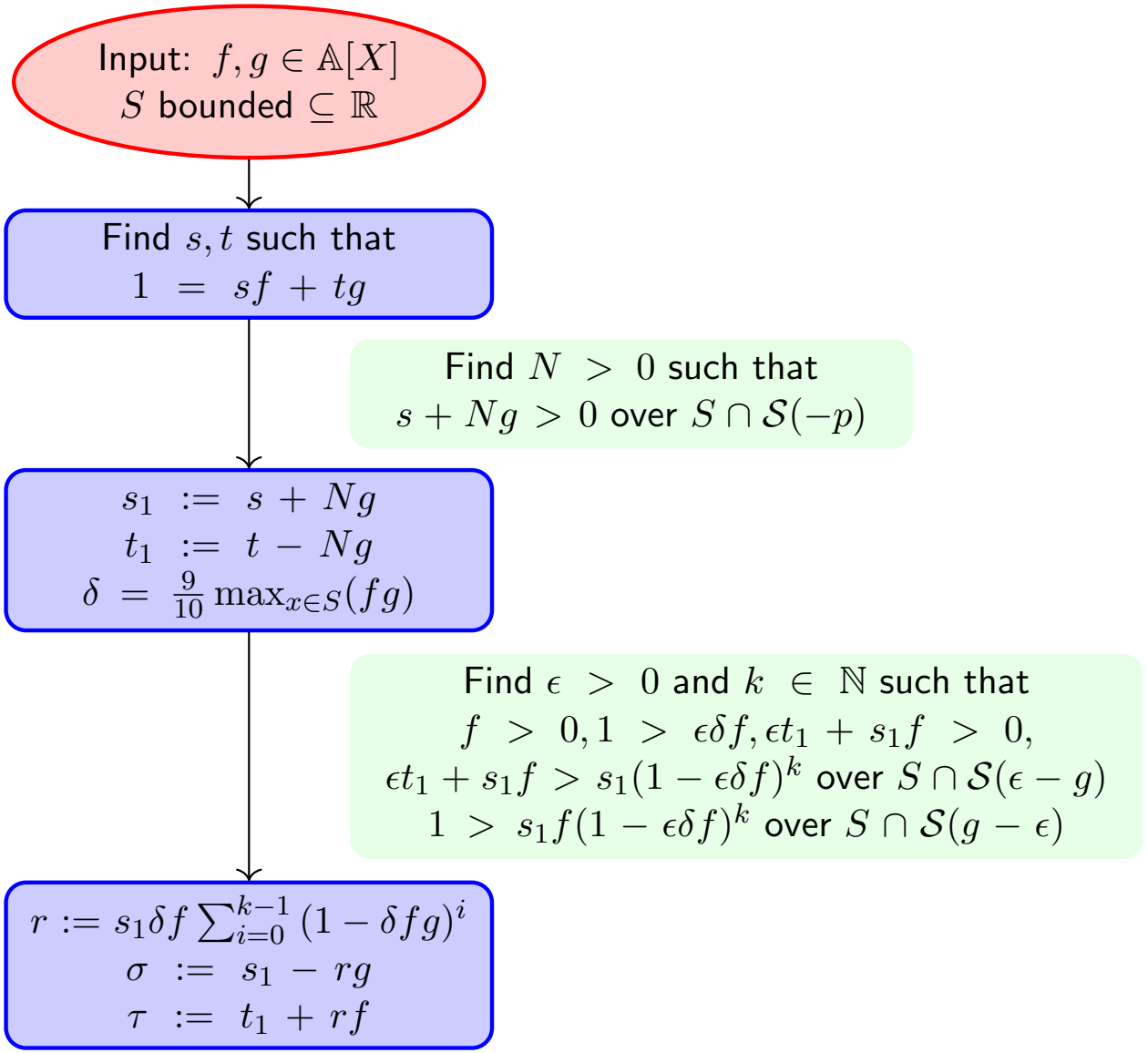

Figure: High-level description of the Basic Lemma construction

Assumptions

- For algorithmic results, we assume the polynomials considered have rational coefficients

Assumptions

- For algorithmic results, we assume the polynomials considered have rational coefficients
- The real roots of the polynomials are obtainable [BPR06]

Assumptions

- For algorithmic results, we assume the polynomials considered have rational coefficients
- The real roots of the polynomials are obtainable [BPR06]
- Sign conditions of the evaluation of a polynomials at algebraic points is computable [BPR06], i.e., given $f \in \mathbb{A}[X]$ and $a \in \mathbb{A}$, we can decide whether $f(a)$ is negative, zero, or positive

Notation

Definition

Let $G = \{g_1, \ldots, g_s\}$, $H = \{h_1, \ldots, h_t\}$ be such that $\mathrm{QM}(G) \subseteq \mathrm{QM}(H)$ and $f \in \mathrm{QM}(G)$.

Notation

Definition

Let $G = \{g_1, \ldots, g_s\}$, $H = \{h_1, \ldots, h_t\}$ be such that $\mathrm{QM}(G) \subseteq \mathrm{QM}(H)$ and $f \in \mathrm{QM}(G)$. Assume that we have a certificate of $f = \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i$ in $\mathrm{QM}(G)$ and certificates for each $g_i = \sigma_{0,i} + \sum_{j=1}^{t} \sigma_{j,i} \cdot h_j$ in $\mathrm{QM}(H)$.

Notation

Definition

Let $G = \{g_1, \ldots, g_s\}$, $H = \{h_1, \ldots, h_t\}$ be such that $\mathrm{QM}(G) \subseteq \mathrm{QM}(H)$ and $f \in \mathrm{QM}(G)$. Assume that we have a certificate of $f = \sigma_0 + \sum_{i=1}^{s} \sigma_i \cdot g_i$ in $\mathrm{QM}(G)$ and certificates for each $g_i = \sigma_{0,i} + \sum_{j=1}^{t} \sigma_{j,i} \cdot h_j$ in $\mathrm{QM}(H)$.
We refer to **lifting** f from $\mathrm{QM}(G)$ to $\mathrm{QM}(H)$ as the action of obtaining a certificate of f in $\mathrm{QM}(H)$ by replacing the certificates of each g_i in $\mathrm{QM}(H)$ with the certificate of f in $\mathrm{QM}(G)$, i.e., $f = (\sigma_0 + \sum_{i=1}^{s} \sigma_i \sigma_{0,i}) + \sum_{j=1}^{t} (\sum_{i=1}^{s} \sigma_i \sigma_{j,i}) \cdot h_j$.

Notation

Notice that if we consider certificates as vectors of dimension $1 \times n + 1$ where n is the number of generators, lifting can be formulated as a matrix multipliciation operation, i.e.,

$$\begin{pmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_s \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \sigma_{0,0} & \sigma_{1,1} & \cdots & \sigma_{t,1} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{0,s} & \sigma_{1,s} & \cdots & \sigma_{t,s} \end{pmatrix}$$
$$= \begin{pmatrix} \sigma_0 + \sum_{i=1}^{s} \sigma_i \sigma_{0,i} & \sum_{i=1}^{s} \sigma_i \sigma_{1,i} & \cdots & \sum_{i=1}^{s} \sigma_i \sigma_{t,i} \end{pmatrix}$$

Main Results

Contributions

1. Compactification algorithm: This algorithm allows us to take a polynomial f in $\mathrm{QM}(G)$ and compute another element h in $\mathrm{QM}(G)$ such that

Contributions

1. Compactification algorithm: This algorithm allows us to take a polynomial f in $\mathrm{QM}(G)$ and compute another element h in $\mathrm{QM}(G)$ such that
   - $\mathcal{S}(h)$ is bounded,

Contributions

1. Compactification algorithm: This algorithm allows us to take a polynomial f in $\mathrm{QM}(G)$ and compute another element h in $\mathrm{QM}(G)$ such that
   - $\mathcal{S}(h)$ is bounded,
   - h have the same zeros of f

Contributions

1. Compactification algorithm: This algorithm allows us to take a polynomial f in $\mathrm{QM}(G)$ and compute another element h in $\mathrm{QM}(G)$ such that
   - $\mathcal{S}(h)$ is bounded,
   - h have the same zeros of f
   - the order and ϵ sign conditions of f and h are the same

Contributions

1. Compactification algorithm: This algorithm allows us to take a polynomial f in $\mathrm{QM}(G)$ and compute another element h in $\mathrm{QM}(G)$ such that
   - $\mathcal{S}(h)$ is bounded,
   - h have the same zeros of f
   - the order and ϵ sign conditions of f and h are the same
2. Solve the certificate problem of saturated quadratic modules by lifting a certificate in the preordering structure using natural geneators

Contributions

1. Compactification algorithm: This algorithm allows us to take a polynomial f in $\mathrm{QM}(G)$ and compute another element h in $\mathrm{QM}(G)$ such that
   - $\mathcal{S}(h)$ is bounded,
   - h have the same zeros of f
   - the order and ϵ sign conditions of f and h are the same
2. Solve the certificate problem of saturated quadratic modules by lifting a certificate in the preordering structure using natural geneators
3. Identify redundancies in the generator and input polynomial in the monogenic case

Contributions

1. Compactification algorithm: This algorithm allows us to take a polynomial f in $\mathrm{QM}(G)$ and compute another element h in $\mathrm{QM}(G)$ such that
   - $\mathcal{S}(h)$ is bounded,
   - h have the same zeros of f
   - the order and ϵ sign conditions of f and h are the same
2. Solve the certificate problem of saturated quadratic modules by lifting a certificate in the preordering structure using natural geneators
3. Identify redundancies in the generator and input polynomial in the monogenic case
4. Solve the certificate problem of monogenic quadratic modules by combining the Basic Lemma and removing roots with even multiplicities

Contributions

5. We define the concept of **pure** and **mixed** polynomials with respect to a set of generators

Contributions

5. We define the concept of **pure** and **mixed** polynomials with respect to a set of generators
6. Introduce a set of intermediate generators $H_{f,G}$ with the property that certificates of products of its members are computable

Contributions

5. We define the concept of **pure** and **mixed** polynomials with respect to a set of generators
6. Introduce a set of intermediate generators $H_{f,G}$ with the property that certificates of products of its members are computable
7. Solve the general certificate problem of Archimedean quadratic modules in the univariate case with a symbolic and exact algorithm

Contributions

5. We define the concept of **pure** and **mixed** polynomials with respect to a set of generators
6. Introduce a set of intermediate generators $H_{f,G}$ with the property that certificates of products of its members are computable
7. Solve the general certificate problem of Archimedean quadratic modules in the univariate case with a symbolic and exact algorithm
8. Certify the emptiness of a quadratic modules in the multivariate case by computing a certificate of -1 for a single generator

Key Ideas, Constructions & Examples

Compactification

- A specialized version of the Basic Lemma (Theorem 9), further assumes that if $S = \mathcal{S}(fg)$ is bounded, then σ, τ can be chosen to be sums of squares

Compactification

- A specialized version of the Basic Lemma (Theorem 9), further assumes that if $S = \mathcal{S}(fg)$ is bounded, then σ, τ can be chosen to be sums of squares
- If $\mathcal{S}(fg)$ is **not bounded**, we cannot use the SOS variant of the Basic Lemma

Compactification

- A specialized version of the Basic Lemma (Theorem 9), further assumes that if $S = \mathcal{S}(fg)$ is bounded, then σ, τ can be chosen to be sums of squares
- If $\mathcal{S}(fg)$ is **not bounded**, we cannot use the SOS variant of the Basic Lemma
- Compactification aims to ensure we can use the SOS variant of the Basic Lemma even though $\mathcal{S}(fg)$ is not bounded.

Compactification

- A specialized version of the Basic Lemma (Theorem 9), further assumes that if $S = \mathcal{S}(fg)$ is bounded, then σ, τ can be chosen to be sums of squares
- If $\mathcal{S}(fg)$ is **not bounded**, we cannot use the SOS variant of the Basic Lemma
- Compactification aims to ensure we can use the SOS variant of the Basic Lemma even though $\mathcal{S}(fg)$ is not bounded.
- The method is a specialized and efficient version of the Basic Lemma applied to the inputs f, $\epsilon - f$ for some $\epsilon > 0$, and a set of generators G

Compactification

- Given a polynomial $f \in \mathrm{QM}(G)$, the compactified polynomial of f, denoted $\mathrm{compact}_G(f)$, is a polynomial such that $\mathcal{S}(\mathrm{compact}_G(f))$ is bounded and $\mathrm{compact}_G(f)$ satisfies the same order and sign conditions at the roots of f.

Compactification

- Given a polynomial $f \in \mathrm{QM}(G)$, the compactified polynomial of f, denoted $\mathrm{compact}_G(f)$, is a polynomial such that $\mathcal{S}(\mathrm{compact}_G(f))$ is bounded and $\mathrm{compact}_G(f)$ satisfies the same order and sign conditions at the roots of f.
- To accomplish the latter, we find an auxiliary strictly positive polynomial h such that fh satisfies the above properties of $\mathrm{compact}_G(f)$; therefore, we define $\mathrm{compact}_G(f) := fh$. Consequently, $\mathrm{compact}_G(f) \in \mathrm{QM}(G)$.

Compactification

- Given a polynomial $f \in \mathrm{QM}(G)$, the compactified polynomial of f, denoted $\mathrm{compact}_G(f)$, is a polynomial such that $\mathcal{S}(\mathrm{compact}_G(f))$ is bounded and $\mathrm{compact}_G(f)$ satisfies the same order and sign conditions at the roots of f.
- To accomplish the latter, we find an auxiliary strictly positive polynomial h such that fh satisfies the above properties of $\mathrm{compact}_G(f)$; therefore, we define $\mathrm{compact}_G(f) := fh$. Consequently, $\mathrm{compact}_G(f) \in \mathrm{QM}(G)$.
- We distinguished three cases:

Compactification

- Given a polynomial $f \in \mathrm{QM}(G)$, the compactified polynomial of f, denoted $\mathrm{compact}_G(f)$, is a polynomial such that $\mathcal{S}(\mathrm{compact}_G(f))$ is bounded and $\mathrm{compact}_G(f)$ satisfies the same order and sign conditions at the roots of f.
- To accomplish the latter, we find an auxiliary strictly positive polynomial h such that fh satisfies the above properties of $\mathrm{compact}_G(f)$; therefore, we define $\mathrm{compact}_G(f) := fh$. Consequently, $\mathrm{compact}_G(f) \in \mathrm{QM}(G)$.
- We distinguished three cases:
  - When $\mathcal{S}(f)$ is unbounded to the right

Compactification

- Given a polynomial $f \in \mathrm{QM}(G)$, the compactified polynomial of f, denoted $\mathrm{compact}_G(f)$, is a polynomial such that $\mathcal{S}(\mathrm{compact}_G(f))$ is bounded and $\mathrm{compact}_G(f)$ satisfies the same order and sign conditions at the roots of f.
- To accomplish the latter, we find an auxiliary strictly positive polynomial h such that fh satisfies the above properties of $\mathrm{compact}_G(f)$; therefore, we define $\mathrm{compact}_G(f) := fh$. Consequently, $\mathrm{compact}_G(f) \in \mathrm{QM}(G)$.
- We distinguished three cases:
  - When $\mathcal{S}(f)$ is unbounded to the right
  - When $\mathcal{S}(f)$ is unbounded to the left

Compactification

- Given a polynomial $f \in \mathrm{QM}(G)$, the compactified polynomial of f, denoted $\mathrm{compact}_G(f)$, is a polynomial such that $\mathcal{S}(\mathrm{compact}_G(f))$ is bounded and $\mathrm{compact}_G(f)$ satisfies the same order and sign conditions at the roots of f.
- To accomplish the latter, we find an auxiliary strictly positive polynomial h such that fh satisfies the above properties of $\mathrm{compact}_G(f)$; therefore, we define $\mathrm{compact}_G(f) := fh$. Consequently, $\mathrm{compact}_G(f) \in \mathrm{QM}(G)$.
- We distinguished three cases:
  - When $\mathcal{S}(f)$ is unbounded to the right
  - When $\mathcal{S}(f)$ is unbounded to the left
  - When $\mathcal{S}(f)$ is unbounded on both sides

Compactification with $\mathcal{S}(f)$ unbounded to the right

Algorithm 1: Computing auxiliary polynomial h when $\mathcal{S}(f)$ is unbounded to the right

Input: $f \in \mathbb{A}[X], bound \in \mathbb{A}$
Output: $\sigma \in \mathbb{A}^+$ and $\tau, h \in \mathbb{A}[X]$
Requires: $\deg(f) = n$ is odd and the leading coefficient of f is positive
Ensures: $1 = \sigma f + \tau h$, $\sigma, \tau \in \sum \mathbb{A}[X]^2$

1 **if** f *has* $r_1 < \cdots < r_n$ *as roots* **then**
2 Let C be the Cauchy bound of f;
3 **else**
4 Let C be the Cauchy bound of $\frac{d}{dX} f$;
5 $I := [-C, \max(bound, C)]$;
6 $\epsilon := \max_{x \in I}(f)$;
7 $\alpha :=$ real root of $\epsilon - f$ of odd degree;
8 $\sigma := \frac{1}{\epsilon}$;
9 $h := -(X - \alpha)$;
10 $\tau := \sigma \cdot quotient(\epsilon - f, h)$;
11 **return** σ, τ, h;

Compactification with $\mathcal{S}(f)$ unbounded to the right

Example

1. Let $G = \{-(X+1)(X-1)\}$ and $f = (X+2)(X-2)(X-3)$.

Compactification with $\mathcal{S}(f)$ unbounded to the right

Example

1. Let $G = \{-(X+1)(X-1)\}$ and $f = (X+2)(X-2)(X-3)$.
2. The semialgebraic set of G is $[-1,1]$ while $\mathcal{S}(f) = [-2,2] \cup [3,\infty)$.

Compactification with $\mathcal{S}(f)$ unbounded to the right

Example

1. Let $G = \{-(X+1)(X-1)\}$ and $f = (X+2)(X-2)(X-3)$.
2. The semialgebraic set of G is $[-1,1]$ while $\mathcal{S}(f) = [-2,2] \cup [3,\infty)$.
3. We calculate the Cauchy bound of f, which is 20. Then we compute the maximum value of f over I, which is 6732 at $x = 20$, that is, at the right end point of I.

Compactification with $\mathcal{S}(f)$ unbounded to the right

Example

1. Let $G = \{-(X+1)(X-1)\}$ and $f = (X+2)(X-2)(X-3)$.
2. The semialgebraic set of G is $[-1,1]$ while $\mathcal{S}(f) = [-2,2] \cup [3,\infty)$.
3. We calculate the Cauchy bound of f, which is 20. Then we compute the maximum value of f over I, which is 6732 at $x = 20$, that is, at the right end point of I.
4. We have $\epsilon - f = 6720 + 4X + 3X^2 - X^3 = (336(\frac{17}{672}X + 1)^2 + \frac{1055}{1344}X^2) \cdot (-(X-20))$. Hence, $h = -(X-20)$, which is strictly positive over $\mathcal{S}(G)$.

Certificate problem for saturated quadratic modules

- A saturated quadratic module contains all the nonnegative polynomials over the associated semialgebraic set $\mathcal{S}(G)$

Certificate problem for saturated quadratic modules

- A saturated quadratic module contains all the nonnegative polynomials over the associated semialgebraic set $\mathcal{S}(G)$
- Equivalently, the signature only admits single multiplicities at the end points [KMS05, Theorem 3.2]

Certificate problem for saturated quadratic modules

- A saturated quadratic module contains all the nonnegative polynomials over the associated semialgebraic set $\mathcal{S}(G)$
- Equivalently, the signature only admits single multiplicities at the end points [KMS05, Theorem 3.2]
- Our approach lifts a certificate in the preordering structure using natural generators by computing certificates of the products of the natural generators and obtaining certificates of the natural generators in terms of the original generators

Certificate problem for saturated quadratic modules

Example

The natural generators are $n_1 = X + 1$ and $n_2 = -(X - 1)$.

Certificate problem for saturated quadratic modules

Example

The natural generators are $n_1 = X + 1$ and $n_2 = -(X - 1)$. Then, we compute the certificate of f in terms of the preordering generated by the natural generators $\mathrm{PO}(n_1, n_2)$. In this case, we note that f is the product of n_1 and n_2.

Certificate problem for saturated quadratic modules

Example

The natural generators are $n_1 = X + 1$ and $n_2 = -(X - 1)$.
Then, we compute the certificate of f in terms of the preordering generated by the natural generators $\mathrm{PO}(n_1, n_2)$. In this case, we note that f is the product of n_1 and n_2.
To lift the certificate of f from $\mathrm{PO}(n_1, n_2)$ to $\mathrm{QM}(n_1, n_2)$, we compute the certificate of the product of n_1 and n_2 in $\mathrm{QM}(n_1, n_2)$. For the latter, we obtain
$n_1 n_2 = \frac{1}{2}(X - 1)^2 \cdot n_1 + \frac{1}{2}(X + 1)^2 \cdot n_2$.

Certificate problem for saturated quadratic modules

Example

To obtain a certificate of f in the quadratic modules generated by G, we obtain certificates of natural generators in terms of $\mathrm{QM}(G)$.

Certificate problem for saturated quadratic modules

Example

To obtain a certificate of f in the quadratic modules generated by G, we obtain certificates of natural generators in terms of $\mathrm{QM}(G)$. This step is done using the Basic Lemma construction as follows:

Certificate problem for saturated quadratic modules

Example

To obtain a certificate of f in the quadratic modules generated by G, we obtain certificates of natural generators in terms of $\mathrm{QM}(G)$. This step is done using the Basic Lemma construction as follows:

1. First, we obtain a certificate of n_1 using g_2 applying the Basic Lemma with n_1 and $\frac{g_2}{n_1} = -(X-2)$. We obtain $\frac{1}{3}n_1 + \frac{1}{3}\frac{g_2}{n_1} = 1$; therefore, multiplying n_1 by the previous equation we have $n_1 = \frac{1}{3}n_1^2 + \frac{1}{3}\cdot g_2$, which is a certificate of n_1 in $\mathrm{QM}(g_2)$.

Certificate problem for saturated quadratic modules

Example

To obtain a certificate of f in the quadratic modules generated by G, we obtain certificates of natural generators in terms of $\mathrm{QM}(G)$. This step is done using the Basic Lemma construction as follows:

1. First, we obtain a certificate of n_1 using g_2 applying the Basic Lemma with n_1 and $\frac{g_2}{n_1} = -(X-2)$. We obtain $\frac{1}{3}n_1 + \frac{1}{3}\frac{g_2}{n_1} = 1$; therefore, multiplying n_1 by the previous equation we have $n_1 = \frac{1}{3}n_1^2 + \frac{1}{3}\cdot g_2$, which is a certificate of n_1 in $\mathrm{QM}(g_2)$.
2. Now, we obtain a certificate of n_2 using g_1 applying the Basic Lemma with n_2 and $\frac{g_1}{n_2} = (X+2)$. We obtain $\frac{1}{3}n_2 + \frac{1}{3}\frac{g_1}{n_2} = 1$; therefore, multiplying n_2 by the previous equation we obtain $n_2 = \frac{1}{3}n_2^2 + \frac{1}{3}\cdot g_1$, which is a certificate of n_2 in $\mathrm{QM}(g_1)$.

Certificate problem for saturated quadratic modules

Example

Finally, we lift the certificate of f from $\mathrm{QM}(n_1, n_2)$ to $\mathrm{QM}(G)$ substituting the certificates of n_1 and n_2, respectively. We obtain

$$
\begin{aligned}
f &= \frac{1}{2}(X-1)^2 \cdot n_1 + \frac{1}{2}(X+1)^2 \cdot n_2 \\
&= \frac{1}{2}(X-1)^2(\frac{1}{3}n_1^2 + \frac{1}{3}\cdot g_2) + \frac{1}{2}(X+1)^2(\frac{1}{3}n_2^2 + \frac{1}{3}\cdot g_1) \\
&= (\frac{1}{6}((X-1)(X+1))^2 + \frac{1}{6}(X-1)^2 \cdot g_2) \\
&\quad + (\frac{1}{6}((X+1)(X-1))^2 + \frac{1}{6}(X+1)^2 \cdot g_1) \\
&= \frac{1}{3}((X-1)(X+1))^2 + \frac{1}{6}(X+1)^2 \cdot g_1 + \frac{1}{6}(X-1)^2 \cdot g_2
\end{aligned}
$$

Comparison with alternative approaches

Example

Consider $f = X + 2$ and $g_1 = -(X + 2)(X + 1)(X - 1)(X - 3)$

Comparison with alternative approaches

Example

Consider $f = X + 2$ and $g_1 = -(X+2)(X+1)(X-1)(X-3)$

- Our approach: $X + 2 = s_0 + \frac{1}{15} \cdot g_1$ where $s_0 = \frac{3}{5}((X+2)(-\frac{5}{18}X + 1))^2 + \frac{11}{540}((X+2)X)^2$. In expanded form, the degrees of the certificates are $\deg(s_0) = 4$ and $\deg(s_1) = 0$.

Comparison with alternative approaches

Example

- Shang's et al approach: We obtain the certificates $X + 2 = s_2 + s_3 \cdot g_1$ where

Comparison with alternative approaches

Example

- Shang's et al approach: We obtain the certificates $X + 2 = s_2 + s_3 \cdot g_1$ where
  - $s_2 = \frac{63}{125}((X+2)(\frac{521}{559872}X^4 + \frac{13513}{435456}X^3 - \frac{61819}{483840}X^2 - \frac{16}{63}X + 1))^2 + \frac{2153239}{10080000}((X+2)(\frac{39646495}{2092948308}X^4 - \frac{3092335}{38758302}X^3 - \frac{558449}{2153239}X^2 + X))^2 + \frac{21390631747541989}{4286358134784000000}((X+2)(\frac{2168515100327669 0}{577547057183633703}X^4 - \frac{25691071038847010}{64171895242625967}X^3 + X^2))^2 + \frac{2027475291423881129393 83}{898201183331987134905600 00}((X+2)(-\frac{92347100995522667731314 5}{36494555245629860329088 94}X^4 + X^3))^2 + \frac{59573723983908118887294869491}{13791788753274864784463186035584000}((X+2)(X^4))^2$

Comparison with alternative approaches

Example

- Shang's et al approach: We obtain the certificates $X+2 = s_2 + s_3 \cdot g_1$ where
  - $s_2 = \frac{63}{125}((X+2)(\frac{521}{559872}X^4 + \frac{13513}{435456}X^3 - \frac{61819}{483840}X^2 - \frac{16}{63}X + 1))^2 + \frac{2153239}{10080000}((X+2)(\frac{39646495}{2092948308}X^4 - \frac{3092335}{38758302}X^3 - \frac{558449}{2153239}X^2 + X))^2 + \frac{21390631747541989}{4286358134784000000}((X+2)(\frac{2168515100327669 0}{577547057183633703}X^4 - \frac{256910710388470 10}{641718952426259 67}X^3 + X^2))^2 + \frac{2027475291423881129393 83}{898201183331987134905600 00}((X+2)(-\frac{923471009955226677313145}{364945552456298603290889 4}X^4 + X^3))^2 + \frac{595737239839081188872948694 91}{137917887532748647844631860355840 00}((X+2)(X^4))^2$
  - $s_3 = \frac{1}{15}\frac{(X-(-1))^2}{(-2-(-1))^2}\frac{(X-1)^2}{(-2-1)^2}\frac{(X-3)^2}{(-2-3)^2}$

Comparison with alternative approaches

Example

- Shang's et al approach: We obtain the certificates $X+2 = s_2 + s_3 \cdot g_1$ where
  - $s_2 = \frac{63}{125}((X+2)(\frac{521}{559872}X^4 + \frac{13513}{435456}X^3 - \frac{61819}{483840}X^2 - \frac{16}{63}X + 1))^2 + \frac{2153239}{10080000}((X+2)(\frac{39646495}{2092948308}X^4 - \frac{3092335}{38758302}X^3 - \frac{558449}{2153239}X^2 + X))^2 + \frac{21390631747541989}{4286358134784000000}((X+2)(\frac{2168515100327669 0}{57754705718363370 3}X^4 - \frac{256910710388470 10}{641718952426259 67}X^3 + X^2))^2 + \frac{2027475291423881129393 83}{898201183331987134905600 00}((X+2)(-\frac{923471009955226677313145}{364945552456298603290889 4}X^4 + X^3))^2 + \frac{595737239839081188872948694 91}{137917887532748647844631860355840 00}((X+2)(X^4))^2$
  - $s_3 = \frac{1}{15}\frac{(X-(-1))^2}{(-2-(-1))^2}\frac{(X-1)^2}{(-2-1)^2}\frac{(X-3)^2}{(-2-3)^2}$

  In expanded form, the degrees of the certificates are $\deg(s_2) = 10$ and $\deg(s_3) = 6$.

Comparison with alternative approaches

Example

- Extended Gram matrix approach: We obtain the certificates

$$
\begin{aligned}
f &= ((m^3)^T A_0 m^3) + ((m^3)^T A_1 m^3) \cdot g_1 \\
&\approx (1.5492 + 0.344267X - 0.21517X^2)^2 + (0. + 0.000581784X^2)^2 \\
&\quad + (0. + 0.285441X + 0.14272X^2)^2 \\
&\quad + ((0.258205 + 1.75314 * 10^{-6}X - 0.0000967477X^2)^2 \\
&\quad + (0. + 0.00708567X + 6.68609 * 10^{-6}X^2)^2 \\
&\quad + (0. + 0.000136995X^2)^2) \cdot g_1
\end{aligned}
$$

In expanded form, the degrees of the certificates are $\deg((m^3)^T A_0 m^3) = 4$ and $\deg((m^3)^T A_1 m^3) = 4$.

Experimental comparison

The following benchmark compares `CertSatQM` with `RealCertify` and `MomentPolynomialOpt`.

[1] These are interval variables of the package

Experimental comparison

The following benchmark compares `CertSatQM` with `RealCertify` and `MomentPolynomialOpt`.
We use monogenic generator of the form $g = -\prod_{n=1}^{k}(X^2 - n^2)$ and strictly positive polynomials of the form $(X + k) + 1$ and $-(X - k) + 1$.

[1] These are interval variables of the package

Experimental comparison

The following benchmark compares `CertSatQM` with `RealCertify` and `MomentPolynomialOpt`.
We use monogenic generator of the form $g = -\prod_{n=1}^{k}(X^2 - n^2)$ and strictly positive polynomials of the form $(X + k) + 1$ and $-(X - k) + 1$.
We use the `multivsos` command from `RealCertify` with settings [1] $\texttt{algo} = 1, \texttt{gmp} = true$ allowing `RealCertify` to find exact certificates;

[1] These are interval variables of the package

Experimental comparison

The following benchmark compares `CertSatQM` with `RealCertify` and `MomentPolynomialOpt`.
We use monogenic generator of the form $g = -\prod_{n=1}^{k}(X^2 - n^2)$ and strictly positive polynomials of the form $(X + k) + 1$ and $-(X - k) + 1$.
We use the `multivsos` command from `RealCertify` with settings [1] $\texttt{algo} = 1, \texttt{gmp} = true$ allowing `RealCertify` to find exact certificates;
We use the `sos_decompose` command from `MomentPolynomialOpt` with settings $\texttt{exact} = true, \texttt{round} = 10000$ to obtain exact certificates and allow the software to handle high-precision terms.

[1] These are interval variables of the package

Experimental comparison

	`RealCertify`		`MomentPolynomialOpt`		`CertSatQM`	
k	Time	Degree	Time	Degree	Time	Degree
1	0.03	4	0.071	2	0.094	2
2	0.06	4	0.289	4	0.021	4
3	0.012	6	0.085	6	0.029	6
4	0.027	8	0.104	8	0.035	8
5	0.037	10	0.124	10	0.044	10
6	N/A	N/A	0.154	12	0.055	12
7	N/A	N/A	0.173	14	0.068	14
8	N/A	N/A	0.191	16	0.083	16
9	N/A	N/A	0.221	18	0.094	18
10	N/A	N/A	N/A	N/A	0.161	20

Table: Computing certificates of strictly positive polynomials of the form $(X + k) + 1$

Experimental comparison

	`RealCertify`		`MomentPolynomialOpt`		`CertSatQM`	
k	Time	Degree	Time	Degree	Time	Degree
1	0.03	4	0.115	2	0.093	2
2	0.005	4	0.261	4	0.019	4
3	0.012	6	0.086	6	0.027	6
4	0.027	8	0.102	8	0.04	8
5	0.036	10	0.122	10	0.046	10
6	N/A	N/A	0.146	12	0.056	12
7	N/A	N/A	0.176	14	0.067	14
8	N/A	N/A	0.2009	16	0.083	16
9	N/A	N/A	0.214	18	0.095	18
10	N/A	N/A	N/A	N/A	0.157	20

Table: Computing certificates of strictly positive polynomials of the form $-(X-k)+1$

Certificate problem for monogenic quadratic modules

- A monogenic quadratic module is generated by a single generator

Certificate problem for monogenic quadratic modules

- A monogenic quadratic module is generated by a single generator
- Our approach separates concerns by simplifying the input polynomial based on the signature structure and "factoring out" a strictly positive polynomial and "in-between" factors

Certificate problem for monogenic quadratic modules

- A monogenic quadratic module is generated by a single generator
- Our approach separates concerns by simplifying the input polynomial based on the signature structure and "factoring out" a strictly positive polynomial and "in-between" factors
- The remaining part of the input polynomial is processed using the SOS variant of the Basic Lemma in order to compute a certificate of such factor from the generator

Certificate problem for monogenic quadratic modules

- A monogenic quadratic module is generated by a single generator
- Our approach separates concerns by simplifying the input polynomial based on the signature structure and "factoring out" a strictly positive polynomial and "in-between" factors
- The remaining part of the input polynomial is processed using the SOS variant of the Basic Lemma in order to compute a certificate of such factor from the generator
- Finally, we combine the previous certificates for each factor mentioned to obtain a certificate of the input polynomial

Certificate problem for monogenic quadratic modules

Example

Let $G = g$ where $g = -(X+1)^2(X-1)^2$ and the input polynomial $f = (X+1)^3$.

Certificate problem for monogenic quadratic modules

Example

Let $G = g$ where $g = -(X+1)^2(X-1)^2$ and the input polynomial $f = (X+1)^3$.
The common isolated point of even multiplicity is -1. Hence, we work on the problem of finding a certificate of $f_1 := X + 1$ in $\mathrm{QM}(-(X-1)^2)$. Since f_1 is strictly positive over $\mathcal{S}(-(X-1)^2) = \{1\}$, we use Certificate to compute a certificate, we obtain $f_1 = s_0 + s_1 \cdot (-(X-1)^2)$ where

Certificate problem for monogenic quadratic modules

Example

Let $G = g$ where $g = -(X+1)^2(X-1)^2$ and the input polynomial $f = (X+1)^3$.
The common isolated point of even multiplicity is -1. Hence, we work on the problem of finding a certificate of $f_1 := X+1$ in $\mathrm{QM}(-(X-1)^2)$. Since f_1 is strictly positive over $\mathcal{S}(-(X-1)^2) = \{1\}$, we use Certificate to compute a certificate, we obtain $f_1 = s_0 + s_1 \cdot (-(X-1)^2)$ where

- $s_0 = \frac{19}{10}(-\frac{4}{19}X + 1)^2 + \frac{31}{38}(X)^2$
- $s_1 = \frac{9}{10}$

Certificate problem for monogenic quadratic modules

Example

Let $G = g$ where $g = -(X+1)^2(X-1)^2$ and the input polynomial $f = (X+1)^3$.
The common isolated point of even multiplicity is -1. Hence, we work on the problem of finding a certificate of $f_1 := X+1$ in $\mathrm{QM}(-(X-1)^2)$. Since f_1 is strictly positive over $\mathcal{S}(-(X-1)^2) = \{1\}$, we use Certificate to compute a certificate, we obtain $f_1 = s_0 + s_1 \cdot (-(X-1)^2)$ where

- $s_0 = \frac{19}{10}(-\frac{4}{19}X + 1)^2 + \frac{31}{38}(X)^2$
- $s_1 = \frac{9}{10}$

Multiplying $(X+1)^2$ by the certificate of f_1, we obtain $f = (X+1)^2 s_0 + \frac{9}{10}(X+1)^2 \cdot g$.

Experimental comparison

This benchmark uses a monogenic generator $g_n := -\prod_{m=1}^{n} (X^2 - m^2)^2$ whose semialgebraic set consists of only isolated points; the semialgebraic set of g_n is $\bigcup_{m=-n}^{n} \{m\}$.

Experimental comparison

This benchmark uses a monogenic generator $g_n := -\prod_{m=1}^{n} (X^2 - m^2)^2$ whose semialgebraic set consists of only isolated points; the semialgebraic set of g_n is $\bigcup_{m=-n}^{n} \{m\}$. We compute certificates for the left generalized natural generator $(X + n)^3$ and the intermediate generalized natural generator $(X + 1)^3(X - 1)^3$.

Experimental comparison

	Shang's general method		MonogenicCert	
n	Degree	Time (seconds)	Degree	Time (Seconds)
1	6	0.009	4	0.008
2	10	0.016	8	0.015
3	14	0.024	12	0.020
4	18	0.045	16	0.032
5	22	0.037	20	0.072
6	26	0.049	24	0.052
7	30	0.062	28	0.074
8	34	0.093	32	0.087
9	38	0.087	36	0.171

Table: Benchmark for left generalized natural generator $(X + n)^3$

Experimental comparison

	Shang's general method		MonogenicCert	
n	Degree	Time (seconds)	Degree	Time (Seconds)
1	8	0.014	8	0.003
2	12	0.020	8	0.090
3	16	0.027	12	0.102
4	20	0.036	16	0.234
5	24	0.055	20	0.369
6	28	0.057	24	1.549
7	32	0.078	28	0.950
8	36	0.107	32	1.524
9	40	0.106	36	2.328

Table: Benchmark for intermediate generalized natural generator $(X+1)^3(X-1)^3$

Certificate problem for general univariate quadratic modules

- We extend the simplification procedure introduced in the monogenic case to handle multiple polynomials

Certificate problem for general univariate quadratic modules

- We extend the simplification procedure introduced in the monogenic case to handle multiple polynomials
- Introduce the following concepts:

Certificate problem for general univariate quadratic modules

- We extend the simplification procedure introduced in the monogenic case to handle multiple polynomials
- Introduce the following concepts:
  - Matching, pseudo-matching, and pair-matching

Certificate problem for general univariate quadratic modules

- We extend the simplification procedure introduced in the monogenic case to handle multiple polynomials
- Introduce the following concepts:
  - Matching, pseudo-matching, and pair-matching
  - Pure and mixed polynomials using $\mathrm{LocalRelativeGens}$ and $\mathrm{RelativeGens}$

Certificate problem for general univariate quadratic modules

- We extend the simplification procedure introduced in the monogenic case to handle multiple polynomials
- Introduce the following concepts:
  - Matching, pseudo-matching, and pair-matching
  - Pure and mixed polynomials using $\mathrm{LocalRelativeGens}$ and $\mathrm{RelativeGens}$
- Introduce the intermediate set of generator $H_{f,G}$ to recover the input polynomial by making products of its members

Certificate problem for general univariate quadratic modules

Definition

Let $f, g, h \in \mathbb{A}[X]$, and $a \in \mathbb{A}$.

1. f **matches** g at a if
   - $\mathrm{ord}_a(f)$ is even and $\epsilon_a(f) = 1$, or
   - $0 \leq \mathrm{ord}_a(f) - \mathrm{ord}_a(g)$ is even and $\epsilon_a(f) = \epsilon_a(g)$

Certificate problem for general univariate quadratic modules

Definition

Let $f, g, h \in \mathbb{A}[X]$, and $a \in \mathbb{A}$.

1. f **matches** g at a if
   - $\mathrm{ord}_a(f)$ is even and $\epsilon_a(f) = 1$, or
   - $0 \leq \mathrm{ord}_a(f) - \mathrm{ord}_a(g)$ is even and $\epsilon_a(f) = \epsilon_a(g)$
2. f **pseudo-matches** g at a if
   - $f(a) > g(a)$, or
   - $\mathrm{ord}_a(g) + 1 \leq \mathrm{ord}_a(f)$ is odd, $\mathrm{ord}_a(g)$ is even, and $\epsilon_a(g) = -1$

Certificate problem for general univariate quadratic modules

Definition

Let $f, g, h \in \mathbb{A}[X]$, and $a \in \mathbb{A}$.

1. f **matches** g at a if
   - $\mathrm{ord}_a(f)$ is even and $\epsilon_a(f) = 1$, or
   - $0 \leq \mathrm{ord}_a(f) - \mathrm{ord}_a(g)$ is even and $\epsilon_a(f) = \epsilon_a(g)$
2. f **pseudo-matches** g at a if
   - $f(a) > g(a)$, or
   - $\mathrm{ord}_a(g) + 1 \leq \mathrm{ord}_a(f)$ is odd, $\mathrm{ord}_a(g)$ is even, and $\epsilon_a(g) = -1$
3. f **pair-matches** (g, h) at a if the following hold
   - $\max(\mathrm{ord}_a(g), \mathrm{ord}_a(h)) + 1 \leq \mathrm{ord}_a(f)$ is even,
   - $\mathrm{ord}_a(g), \mathrm{ord}_a(h)$ are odd, and
   - $\epsilon_a(gh) = \epsilon_a(f) = -1$

Certificate problem for general univariate quadratic modules

1. **matching**: this case detects when f is a local sums of squares at a, or identifies the generators with same order parity and signs with f at a.

Certificate problem for general univariate quadratic modules

1. **matching**: this case detects when f is a local sums of squares at a, or identifies the generators with same order parity and signs with f at a.
2. **pseudo-matching**: this case detects when f is a strictly positive polynomial over $\mathcal{S}(G)$, particularly at a, or identifies the generators with even order, $\mathrm{ord}_a(f)$ is odd and the sign of the associated generator g at a is negative.

Certificate problem for general univariate quadratic modules

1. **matching**: this case detects when f is a local sums of squares at a, or identifies the generators with same order parity and signs with f at a.
2. **pseudo-matching**: this case detects when f is a strictly positive polynomial over $\mathcal{S}(G)$, particularly at a, or identifies the generators with even order, $\mathrm{ord}_a(f)$ is odd and the sign of the associated generator g at a is negative.
3. **pair-matching**: this case identifies the pairs of generators with both odd orders and $\mathrm{ord}_a(f)$ is even, and the sign with f at a is negative.

Certificate problem for general univariate quadratic modules

Definition

Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[X]$ and $f \in \mathbb{A}[X]$. Let us define $\mathrm{LocalRelativeGens}(f, G, a)$ and $\mathrm{RelativeGens}(f, G)$ as subsets of G as

$$\mathrm{LocalRelativeGens}(f, G, a) := \{g \in G \mid f \text{ matches or pseudo-matches } g \text{ at } a\}$$

$$\mathrm{RelativeGens}(f, G) := \bigcap_{a \in \mathcal{Z}(f)} \mathrm{LocalRelativeGens}(f, G, a)$$

Certificate problem for general univariate quadratic modules

Definition

Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[X]$ and $f \in \mathbb{A}[X]$. Let us define $\mathrm{LocalRelativeGens}(f, G, a)$ and $\mathrm{RelativeGens}(f, G)$ as subsets of G as

$$\mathrm{LocalRelativeGens}(f, G, a) := \{g \in G \mid f \text{ matches or pseudo-matches } g \text{ at } a\}$$

$$\mathrm{RelativeGens}(f, G) := \bigcap_{a \in \mathcal{Z}(f)} \mathrm{LocalRelativeGens}(f, G, a)$$

We say that f is **pure** with respect to G if $\mathrm{RelativeGens}(f, G)$ is not empty. We say that f is **mixed** with respect to G if f is not pure with respect to G or there are $g_i, g_j \in G$ and a point $a \in \mathcal{Z}(f)$ such that f pair-matches (g_i, g_j) at a.

Certificate problem for general univariate quadratic modules

Definition

Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{A}[X]$ and $f \in \mathbb{A}[X]$. Let us define $\mathrm{LocalRelativeGens}(f, G, a)$ and $\mathrm{RelativeGens}(f, G)$ as subsets of G as

$$\mathrm{LocalRelativeGens}(f, G, a) := \{g \in G \mid f \text{ matches or pseudo-matches } g \text{ at } a\}$$

$$\mathrm{RelativeGens}(f, G) := \bigcap_{a \in \mathcal{Z}(f)} \mathrm{LocalRelativeGens}(f, G, a)$$

We say that f is **pure** with respect to G if $\mathrm{RelativeGens}(f, G)$ is not empty. We say that f is **mixed** with respect to G if f is not pure with respect to G or there are $g_i, g_j \in G$ and a point $a \in \mathcal{Z}(f)$ such that f pair-matches (g_i, g_j) at a.

The motivation for the above definitions allows us to distinguish two cases of members in a quadratic module. If $f \in \mathrm{QM}(G)$ is pure and $f \geq 0$ over $\mathcal{S}(\mathrm{compact}_G(g))$ for some $g \in \mathrm{RelativeGens}(f, G)$, then $f \in \mathrm{QM}(\mathrm{compact}_G(g))$.

Certificate problem for general univariate quadratic modules

The intermediate set of generators $H_{f,G}$ satisfies the following conditions:

Certificate problem for general univariate quadratic modules

The intermediate set of generators $H_{f,G}$ satisfies the following conditions:

1. The strictly positive factor f_{pos} of f is strictly positive over $\mathcal{S}(H_{f,G})$.

Certificate problem for general univariate quadratic modules

The intermediate set of generators $H_{f,G}$ satisfies the following conditions:

1. The strictly positive factor f_{pos} of f is strictly positive over $\mathcal{S}(H_{f,G})$.
2. Let $f_{non-neg} := \frac{f}{f_{pos}}$. $\mathcal{S}(H_{f,G}) \subseteq \mathcal{S}(f_{non-neg}) \cap [\alpha, \beta]$ for some $\alpha < \mathcal{S}(G) < \beta$.

Certificate problem for general univariate quadratic modules

The intermediate set of generators $H_{f,G}$ satisfies the following conditions:

1. The strictly positive factor f_{pos} of f is strictly positive over $\mathcal{S}(H_{f,G})$.
2. Let $f_{non-neg} := \frac{f}{f_{pos}}$. $\mathcal{S}(H_{f,G}) \subseteq \mathcal{S}(f_{non-neg}) \cap [\alpha, \beta]$ for some $\alpha < \mathcal{S}(G) < \beta$.

The first condition allows us to simplify the input polynomial, as the method processes the real roots of the input polynomial.

Certificate problem for general univariate quadratic modules

The intermediate set of generators $H_{f,G}$ satisfies the following conditions:

1. The strictly positive factor f_{pos} of f is strictly positive over $\mathcal{S}(H_{f,G})$.
2. Let $f_{non-neg} := \frac{f}{f_{pos}}$. $\mathcal{S}(H_{f,G}) \subseteq \mathcal{S}(f_{non-neg}) \cap [\alpha, \beta]$ for some $\alpha < \mathcal{S}(G) < \beta$.

The first condition allows us to simplify the input polynomial, as the method processes the real roots of the input polynomial.
The second condition ensures that the semialgebraic set of $H_{f,G}$ is bounded and $f_{non-neg}$ remains nonnegative over $\mathcal{S}(H_{f,G})$.
Additionally, we can use the Certificate algorithm to compute a certificate of f_{pos} in $\mathrm{QM}(H_{f,G})$.

Certificate problem for general univariate quadratic modules

Example

Let $f = (X+1)(X-1)$ with the set of generators $G = \{g_1, g_2\}$ where $g_1 = -(X+2)(X+1)^3(X-1)(X-2)$ and $g_2 = (X+1)(X-1)^3$.

Certificate problem for general univariate quadratic modules

Example

Let $f = (X+1)(X-1)$ with the set of generators $G = \{g_1, g_2\}$ where $g_1 = -(X+2)(X+1)^3(X-1)(X-2)$ and $g_2 = (X+1)(X-1)^3$.
We obtain
$H_{f,G} = \{X+3, (X+1)X, (X+\frac{1}{2})(X-\frac{1}{2}), X(X-1), -(X-3)\}$ and their certificates in $\mathrm{QM}(G)$.

Certificate problem for general univariate quadratic modules

Example

Let $f = (X+1)(X-1)$ with the set of generators $G = \{g_1, g_2\}$ where $g_1 = -(X+2)(X+1)^3(X-1)(X-2)$ and $g_2 = (X+1)(X-1)^3$.
We obtain
$H_{f,G} = \{X+3, (X+1)X, (X+\frac{1}{2})(X-\frac{1}{2}), X(X-1), -(X-3)\}$ and their certificates in $\mathrm{QM}(G)$.
The certificate of the product $(X+1)X, X(X-1)$ in $\mathrm{QM}(H_{f,G})$ is
$(X+1)X^2(X-1) = \frac{1}{2}(X-1)^2 \cdot (X+1)X + \frac{1}{2}(X+1)^2 \cdot X(X-1)$.
Now, we apply the BasicLemma algorithm with inputs f, X^2 and $H_{f,G}$ to obtain σ, τ strictly positive over $\mathcal{S}(H_{f,G})$ such that $1 = \sigma f + \tau X^2$. We obtain:

Certificate problem for general univariate quadratic modules

Example

- $\sigma = \frac{1}{360}(\frac{-1440-19X^2+19X^4}{1440})^{160}(-\frac{1}{4}+X^2)(-(-1440-19X^2+19X^4))$
- $\tau = 1-4(-1+X)(1+X)+\frac{19}{1440}(-1+4X^2)\sum_{i=0}^{160}(1-\frac{19(-1+X)X^2(1+X)}{1440})^i((X+1)(X-1))^2$

We check τ is a nonnegative polynomial over $\mathbb{R}$ so it can be decomposed into a sums of squares. On the other hand, σ is not nonnegative over $\mathbb{R}$ as $\mathcal{S}(\sigma) \approx [-3.03646, -\frac{1}{2}] \cup [\frac{1}{2}, 3.03646]$ but only strictly positive over $\mathcal{S}(H_{f,G})$; hence, we compute a certificate of σ in $\mathrm{QM}(H_{f,G})$ using the Certificate algorithm.

Certificate problem for general univariate quadratic modules

Example

We obtain
$\sigma = s_0 + s_1 \cdot (X+3) + s_2 \cdot (X+1)X + s_3 \cdot (X+\frac{1}{2})(X-\frac{1}{2}) + s_4 \cdot X(X-1) + s_5 \cdot (-(X-3))$
where

- $s_0 = \frac{4}{1440}(\frac{-1440-19X^2+19X^4}{1440})^{160}(\frac{130387}{8442}((-\frac{1}{2}-X)^2(\frac{1}{2}-X)^2(3-X)^2(-\frac{1279974}{2567725}-\frac{426658X}{2567725})^{140}) + \frac{130387}{8442}((-\frac{1279974}{2567725}+\frac{426658X}{2567725})^{140}(-\frac{1}{2}+X)^2(\frac{1}{2}+X)^2(3+X)^2))$
- $s_1 = \frac{4}{1440}(\frac{-1440-19X^2+19X^4}{1440})^{160}(\frac{130387}{8442}(-\frac{1}{2}-X)^2(\frac{1}{2}-X)^2(3-X)^2(-\frac{1279974}{2567725}-\frac{426658X}{2567725})^{140}(\frac{71(1-\frac{12X}{71})^2}{210}+\frac{2X^2}{213}) + \frac{130387}{8442}(-\frac{1279974}{2567725}+\frac{426658X}{2567725})^{140}(-3+X)^2(-\frac{1}{2}+X)^2(\frac{1}{2}+X)^2(\frac{71(1+\frac{12X}{71})^2}{210}+\frac{2X^2}{213}))$
- $s_2 = 0$
- $s_3 = \frac{4}{1440}(\frac{-1440-19X^2+19X^4}{1440})^{160}(1440 - (\frac{651935}{804}(3-X)(-\frac{1279974}{2567725}-\frac{426658X}{2567725})^{140}) + 19X^2 - 19X^4 - (\frac{651935}{804}(-\frac{1279974}{2567725}+\frac{426658X}{2567725})^{140}(3+X)) + (\frac{130387}{1407}(3-X)^2(-\frac{1279974}{2567725}-\frac{426658X}{2567725})^{140}(3+X)^2(\frac{71}{210}(1-\frac{12X}{71})^2+\frac{2X^2}{213})) + (\frac{130387}{1407}(3-X)^2(-\frac{1279974}{2567725}+\frac{426658X}{2567725})^{140}(3+X)^2(\frac{71}{210}(1+\frac{12X}{71})^2+\frac{2X^2}{213})))$
- $s_4 = 0$
- $s_5 = \frac{4}{1440}(\frac{-1440-19X^2+19X^4}{1440})^{160}((\frac{130387}{8442}(-3-X)^2(-\frac{1}{2}-X)^2(\frac{1}{2}-X)^2(-\frac{1279974}{2567725}-\frac{426658X}{2567725})^{140}((\frac{71}{210}(1-\frac{12X}{71})^2)+\frac{2X^2}{213})) + (\frac{130387}{8442}(-\frac{1279974}{2567725}+\frac{426658X}{2567725})^{140}(-\frac{1}{2}+X)^2(\frac{1}{2}+X)^2(3+X)^2((\frac{71}{210}(1+\frac{12X}{71})^2)+\frac{2X^2}{213})))$

Certificate problem for general univariate quadratic modules

Example

We obtain a certificate of $f \in \mathrm{QM}(H_{f,G})$ by multiplying f to the equation $1 = \sigma f + \tau X^2$. We obtain

$$\begin{aligned} f &= f^2\sigma + \tau X^2 f \\ &= f^2(s_0 + s_1 \cdot (X+3) + s_3 \cdot (X+\frac{1}{2})(X-\frac{1}{2}) + s_5 \cdot (-(X-3))) \\ &\quad + \tau(\frac{1}{2}(X-1)^2 \cdot (X+1)X + \frac{1}{2}(X+1)^2 \cdot X(X-1)) \\ &= f^2 s_0 + f^2 s_1 \cdot (X+3) + \frac{1}{2}\tau(X-1)^2 \cdot (X+1)X \\ &+ f^2 s_3 \cdot (X+\frac{1}{2})(X-\frac{1}{2}) + \frac{1}{2}\tau(X+1)^2 \cdot X(X-1) + f^2 s_5 \cdot (-(X-3)) \end{aligned}$$

Finally, we obtain a certificate of $f \in \mathrm{QM}(G)$ by lifting from $\mathrm{QM}(H_{f,G})$ to $\mathrm{QM}(G)$.

Conclusions & Future work

Conclusions

- This thesis develops a method for computing certificates of members in Archimedean univariate quadratic modules specified by a finite set of generators in the univariate case.

Conclusions

- This thesis develops a method for computing certificates of members in Archimedean univariate quadratic modules specified by a finite set of generators in the univariate case.
- We started our study with simpler cases, such as the saturated and monogenic case. These cases provided interesting insights to tackle the general problem; the methods developed in the saturated case allow us to compute certificates of products that were possible to generalize to multiplicities greater than 1, and the monogenic case, in combination with the compactification method, provides a framework for computing certificates of nonnegative factors.

Conclusions

- This thesis develops a method for computing certificates of members in Archimedean univariate quadratic modules specified by a finite set of generators in the univariate case.
- We started our study with simpler cases, such as the saturated and monogenic case. These cases provided interesting insights to tackle the general problem; the methods developed in the saturated case allow us to compute certificates of products that were possible to generalize to multiplicities greater than 1, and the monogenic case, in combination with the compactification method, provides a framework for computing certificates of nonnegative factors.
- The proposed methods are novel, symbolic, and obtain certificates in terms of the original generators.

Future work

- The Basic Lemma is a fundamental tool in the algorithms presented in this thesis, especially for the problems in the univariate case. However, the original result from Theorem 8 applies to the multivariate case. We believe that this result can be further optimized for the univariate case.

Future work

- The Basic Lemma is a fundamental tool in the algorithms presented in this thesis, especially for the problems in the univariate case. However, the original result from Theorem 8 applies to the multivariate case. We believe that this result can be further optimized for the univariate case.
- Similarly, the Certificate algorithm from [Sha+25] is widely used in the algorithms of this thesis. The fundamental constructive results of the Certificate algorithm are a Lemma by Averkov [Ave13] and a technique to approximate non-negative polynomials as sums of squares by Lasserre in [Las07]; both of these results hold for the multivariate case.

Future work

- The Basic Lemma is a fundamental tool in the algorithms presented in this thesis, especially for the problems in the univariate case. However, the original result from Theorem 8 applies to the multivariate case. We believe that this result can be further optimized for the univariate case.
- Similarly, the Certificate algorithm from [Sha+25] is widely used in the algorithms of this thesis. The fundamental constructive results of the Certificate algorithm are a Lemma by Averkov [Ave13] and a technique to approximate non-negative polynomials as sums of squares by Lasserre in [Las07]; both of these results hold for the multivariate case.
- Although the univariate case does not benefit from specializing Lasserre's approximation theorem, improving the construction of Averkov's lemma to the univariate case would optimize different aspects of certificate computation of strictly positive polynomials over compact semialgebraic sets in the univariate case.

Future work

- The Basic Lemma is a fundamental tool in the algorithms presented in this thesis, especially for the problems in the univariate case. However, the original result from Theorem 8 applies to the multivariate case. We believe that this result can be further optimized for the univariate case.
- Similarly, the Certificate algorithm from [Sha+25] is widely used in the algorithms of this thesis. The fundamental constructive results of the Certificate algorithm are a Lemma by Averkov [Ave13] and a technique to approximate non-negative polynomials as sums of squares by Lasserre in [Las07]; both of these results hold for the multivariate case.
- Although the univariate case does not benefit from specializing Lasserre's approximation theorem, improving the construction of Averkov's lemma to the univariate case would optimize different aspects of certificate computation of strictly positive polynomials over compact semialgebraic sets in the univariate case.
- Special algorithms of this kind would also make the complexity analysis of them more suitable.

Thank you for your attention!

References I


Augustin, Doris. "The Membership Problem for finitely generated quadratic modules in the univariate case". In: *Journal of Pure and Applied Algebra* 216.10 (2012), pp. 2204–2212. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2012.02.004. URL: http://www.sciencedirect.com/science/article/pii/S0022404912000436.


— . "The Membership Problem for quadratic modules with focus on the one dimensional case". Ph.D. thesis. PhD thesis. Universität Regensburg, 2008.


Averkov, Gennadiy. "Constructive Proofs of Some Positivstellensätze for Compact Semialgebraic Subsets of Źd". In: *J. Optim. Theory Appl.* 158.2 (Aug. 2013), pp. 410–418. ISSN: 0022-3239. DOI: 10.1007/s10957-012-0261-9. URL: https://doi.org/10.1007/s10957-012-0261-9.

References II

- Basu, Saugata, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Berlin, Heidelberg: Springer-Verlag, 2006. ISBN: 3540330984.
- Cabral, Maria Eugênia Canto and Alexander Prestel. "Quadratic modules of polynomials in two variables". In: *Advances in Geometry* 8.2 (2008), pp. 189–204. DOI: doi:10.1515/ADVGEOM.2008.014. URL: https://doi.org/10.1515/ADVGEOM.2008.014.
- Jacobi, Thomas. "Über die Darstellung positiver Polynome auf semi-algebraischen Kompakta". PhD thesis. Konstanz: Universität Konstanz, 1999.
- Jacobi, Thomas and Alexander Prestel. "Distinguished representations of strictly positive polynomials". In: *Crelle's Journal* 2001 (2001).

References III


Kaltofen, Erich et al. "Exact Certification of Global Optimality of Approximate Factorizations via Rationalizing Sums-of-Squares with Floating Point Scalars". In: *Proceedings of the Twenty-First International Symposium on Symbolic and Algebraic Computation*. ISSAC '08. Linz/Hagenberg, Austria: Association for Computing Machinery, 2008, pp. 155–164. ISBN: 9781595939043. DOI: 10.1145/1390768.1390792. URL: https://doi.org/10.1145/1390768.1390792.


Kuhlmann, S. and M. Marshall. "Positivity, sums of squares and the multi-dimensional moment problem". In: 354.11 (July 2002), pp. 4285–4301. DOI: 10.1090/s0002-9947-02-03075-1. URL: https://doi.org/10.1090/s0002-9947-02-03075-1.

References IV

- Kuhlmann, S., M. Marshall, and N. Schwartz. "Positivity, sums of squares and the multi-dimensional moment problem II". In: 5.4 (Sept. 2005), pp. 583–606. DOI: 10.1515/advg.2005.5.4.583. URL: https://doi.org/10.1515/advg.2005.5.4.583.
- Lasserre, Jean B. "A Sum of Squares Approximation of Nonnegative Polynomials". In: *SIAM Review* 49.4 (Jan. 2007), pp. 651–669. ISSN: 1095-7200. DOI: 10.1137/070693709. URL: http://dx.doi.org/10.1137/070693709.
- — . "Global Optimization with Polynomials and the Problem of Moments". In: *SIAM Journal on Optimization* 11.3 (Jan. 2001), pp. 796–817. ISSN: 1095-7189. DOI: 10.1137/s1052623400366802. URL: http://dx.doi.org/10.1137/S1052623400366802.
- Lombardi, Henri. "Une borne sur les degres pour le theoreme des zeros reel effectif". In: 1992.

References V


Lombardi, Henrri, Daniel Perrucci, and Marie-Françoise Roy. "An Elementary Recursive Bound for Effective Positivstellensatz and Hilbert's 17th problem". In: *Memoirs of the American Mathematical Society* 263 (Apr. 2014). DOI: 10.1090/memo/1277.


Magron, Victor and Mohab Safey El Din. "On Exact Polya and Putinar's Representations". In: *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation* (July 2018). DOI: 10.1145/3208976.3208986. URL: http://dx.doi.org/10.1145/3208976.3208986.


Nie, Jiawang and Markus Schweighofer. "On the Complexity of Putinar's Positivstellensatz". In: *J. Complex.* 23.1 (Feb. 2007), pp. 135–150. ISSN: 0885-064X. DOI: 10.1016/j.jco.2006.07.002. URL: https://doi.org/10.1016/j.jco.2006.07.002.

References VI


Peyrl, Helfried and Pablo A. Parrilo. "Computing sum of squares decompositions with rational coefficients". In: *Theoretical Computer Science* 409.2 (2008). Symbolic-Numerical Computations, pp. 269–281. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2008.09.025. URL: https://www.sciencedirect.com/science/article/pii/S0304397508006452.


Powers, Victoria and Bruce Reznick. "A new bound for Pólya's Theorem with applications to polynomials positive on polyhedra". In: *Journal of Pure and Applied Algebra* 164.1–2 (Oct. 2001), pp. 221–229. ISSN: 0022-4049. DOI: 10.1016/s0022-4049(00)00155-9. URL: http://dx.doi.org/10.1016/S0022-4049(00)00155-9.

References VII


Schweighofer, Markus. "An algorithmic approach to Schmüdgen's Positivstellensatz". In: *Journal of Pure and Applied Algebra* 166.3 (2002), pp. 307–319. ISSN: 0022-4049. DOI: https://doi.org/10.1016/S0022-4049(01)00041-X. URL: https://www.sciencedirect.com/science/article/pii/S002240490100041X.


Shang, Weifeng et al. *Computing Certificates of Strictly Positive Polynomials in Archimedean Quadratic Modules*. 2025. arXiv: 2503.11119 [math.AC]. URL: https://arxiv.org/abs/2503.11119.


Wagner, Sven. "Archimedean Quadratic Modules : A Decision Problem for Real Multivariate Polynomials". In: (Jan. 2009).