Computing certificates in compact quadratic modules in $\mathbb{R}[x]$ and Archimedean monogenic quadratic modules in $\mathbb{R}[x, y]$

Thesis Proposal Defense

Jose Abel Castellanos Joo

September 19, 2023

Motivation

Ideal in Polynomial Ring

Let $f = -x(x-1)^3$ and $B = \{-(x+1)(x-1), -(x-1)^2\}$

Ideal in Polynomial Ring

Let $f = -x(x-1)^3$ and $B = \{-(x+1)(x-1), -(x-1)^2\}$
How can we certify that $f \in \langle B \rangle$?

Ideal in Polynomial Ring

Let $f = -x(x-1)^3$ and $B = \{-(x+1)(x-1), -(x-1)^2\}$
How can we certify that $f \in \langle B \rangle$?
Notice that:

Ideal in Polynomial Ring

Let $f = -x(x-1)^3$ and $B = \{-(x+1)(x-1), -(x-1)^2\}$
How can we certify that $f \in \langle B \rangle$?
Notice that:

- $x - 1 = -\frac{1}{2}(-(x+1)(x-1)) + \frac{1}{2}(-(x-1)^2)$

Ideal in Polynomial Ring

Let $f = -x(x-1)^3$ and $B = \{-(x+1)(x-1), -(x-1)^2\}$
How can we certify that $f \in \langle B \rangle$?
Notice that:

- $x - 1 = -\frac{1}{2}(-(x+1)(x-1)) + \frac{1}{2}(-(x-1)^2)$
- $x - 1 | f$

Ideal in Polynomial Ring

Let $f = -x(x-1)^3$ and $B = \{-(x+1)(x-1), -(x-1)^2\}$
How can we certify that $f \in \langle B \rangle$?
Notice that:

- $x - 1 = -\frac{1}{2}(-(x+1)(x-1)) + \frac{1}{2}(-(x-1)^2)$
- $x - 1 | f$

$$f = -x(x-1)^2(x-1)$$
$$= \frac{1}{2}x(x-1)^2 \quad (-(x+1)(x-1)) \quad - \frac{1}{2}x(x-1)^2 \quad (-(x-1)^2)$$

Ideal in Polynomial Ring

Let $f = -x(x-1)^3$ and $B = \{-(x+1)(x-1), -(x-1)^2\}$
How can we certify that $f \in \langle B \rangle$?
Notice that:

- $x - 1 = -\frac{1}{2}(-(x+1)(x-1)) + \frac{1}{2}(-(x-1)^2)$
- $x - 1 | f$

$$f = -x(x-1)^2(x-1)$$
$$= \underbrace{\frac{1}{2}x(x-1)^2}_{\text{not a sum of squares}} (-(x+1)(x-1)) \underbrace{-\frac{1}{2}x(x-1)^2}_{\text{not a sums of squares}} (-(x-1)^2)$$

Reasoning over inequalities

If $f = s_0 + s_1(-(x+1)(x-1)) + s_2(-(x-1)^2)$ where each s_i is a sums squares then $f \geq 0$ over

$$\{x \in \mathbb{R} \mid -(x+1)(x-1) \geq 0, -(x-1)^2 \geq 0\}$$

Reasoning over Inequalities

In fact,

Reasoning over Inequalities

In fact,

$$x = \frac{1}{2}(x^2 + 1) + \frac{1}{2}(-(x-1)^2)$$

Reasoning over Inequalities

In fact,

$$x = \frac{1}{2}(x^2 + 1) + \frac{1}{2}(-(x-1)^2)$$

$$-(x-1)^3 = \frac{1}{2}((x-1)^4 + (x-1)^2) + \frac{1}{2}x^2(-(x-1)^2)$$

Reasoning over Inequalities

In fact,

$$x = \frac{1}{2}(x^2 + 1) + \frac{1}{2}(-(x-1)^2)$$

$$-(x-1)^3 = \frac{1}{2}((x-1)^4 + (x-1)^2) + \frac{1}{2}x^2(-(x-1)^2)$$

Thus,

Reasoning over Inequalities

In fact,

$$x = \frac{1}{2}(x^2 + 1) + \frac{1}{2}(-(x-1)^2)$$

$$-(x-1)^3 = \frac{1}{2}((x-1)^4 + (x-1)^2) + \frac{1}{2}x^2(-(x-1)^2)$$

Thus,

$$f = \underbrace{\frac{1}{4}\left((x^2+1)((x-1)^4 + (x-1)^2) + x^2(-(x-1)^2)^2\right)}_{\textit{a sums of squares}} + \underbrace{\frac{1}{4}\left(((x-1)^4 + (x-1)^2) + (x^2+1)x^2\right)}_{\textit{a sums of squares}}(-(x-1)^2)$$

Preliminaries

Quadratic modules

Definition

- A *quadratic module* in $\mathbb{R}[\overline{X}] := \mathbb{R}[X_1, \ldots, X_n]$ is a subset that is closed under addition and closed under multiplication with squares in $\mathbb{R}[\overline{X}]$.

Quadratic modules

Definition

- A *quadratic module* in $\mathbb{R}[\overline{X}] := \mathbb{R}[X_1, \ldots, X_n]$ is a subset that is closed under addition and closed under multiplication with squares in $\mathbb{R}[\overline{X}]$.
- Given a set of polynomials $G = \{g_1, \ldots, g_n\} \subseteq \mathbb{R}[\overline{X}]$,

Quadratic modules

Definition

- A *quadratic module* in $\mathbb{R}[\overline{X}] := \mathbb{R}[X_1, \ldots, X_n]$ is a subset that is closed under addition and closed under multiplication with squares in $\mathbb{R}[\overline{X}]$.
- Given a set of polynomials $G = \{g_1, \ldots, g_n\} \subseteq \mathbb{R}[\overline{X}]$,
  - the quadratic module generated by G is the set $\mathrm{QM}(G) := \left\{ s_0 + \sum_{i=1}^{n} s_i g_i \mid s_i \in \sum \mathbb{R}[\overline{X}]^2 \text{ for } 0 \leq i \leq n \right\}$.

Quadratic modules

Definition

- A *quadratic module* in $\mathbb{R}[\overline{X}] := \mathbb{R}[X_1, \ldots, X_n]$ is a subset that is closed under addition and closed under multiplication with squares in $\mathbb{R}[\overline{X}]$.
- Given a set of polynomials $G = \{g_1, \ldots, g_n\} \subseteq \mathbb{R}[\overline{X}]$,
  - the quadratic module generated by G is the set $\mathrm{QM}(G) := \left\{s_0 + \sum_{i=1}^{n} s_i g_i \mid s_i \in \sum \mathbb{R}[\overline{X}]^2 \text{ for } 0 \leq i \leq n\right\}$.
  - the semialgebraic set of G is the set $\mathcal{S}(G) := \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \text{ for } 1 \leq i \leq n\}$

Quadratic modules

Definition

- A *quadratic module* in $\mathbb{R}[\overline{X}] := \mathbb{R}[X_1, \ldots, X_n]$ is a subset that is closed under addition and closed under multiplication with squares in $\mathbb{R}[\overline{X}]$.
- Given a set of polynomials $G = \{g_1, \ldots, g_n\} \subseteq \mathbb{R}[\overline{X}]$,
  - the quadratic module generated by G is the set $\mathrm{QM}(G) := \left\{ s_0 + \sum_{i=1}^{n} s_i g_i \mid s_i \in \sum \mathbb{R}[\overline{X}]^2 \text{ for } 0 \leq i \leq n \right\}$.
  - the semialgebraic set of G is the set $\mathcal{S}(G) := \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \text{ for } 1 \leq i \leq n\}$
- A *compact quadratic module* is a quadratic module for which the semialgebraic set of its generators is compact.

Multiplicities matter

In [Ste96], the author noticed

Multiplicities matter

In [Ste96], the author noticed

$$1 - x^2 \notin \mathrm{QM}(\{(1 - x^2)^3\})$$

Multiplicities matter

In [Ste96], the author noticed

$$1 - x^2 \notin \mathrm{QM}(\{(1 - x^2)^3\})$$

- Otherwise, exists sums of squares s_0, s_1 such that $1 - x^2 = s_0 + s_1(1 - x^2)^3$.

Multiplicities matter

In [Ste96], the author noticed

$$1 - x^2 \notin \mathrm{QM}(\{(1 - x^2)^3\})$$

- Otherwise, exists sums of squares s_0, s_1 such that $1 - x^2 = s_0 + s_1(1 - x^2)^3$.
- The left hand side vanishes at $x = 1$. The multiplicity of $x - 1$ is one.

Multiplicities matter

In [Ste96], the author noticed

$$1 - x^2 \notin \mathrm{QM}(\{(1 - x^2)^3\})$$

- Otherwise, exists sums of squares s_0, s_1 such that $1 - x^2 = s_0 + s_1(1 - x^2)^3$.
- The left hand side vanishes at $x = 1$. The multiplicity of $x - 1$ is one.
- The right hand side must vanish at $x = 1$. The multiplicity of $x - 1$ in s_0 would be even, which contradicts the left hand side.

Deciding membership in Quadratic module when $n = 1$

In [Aug08, p. 47], the author provided an algorithm to test the membership of polynomials in compact univariate quadratic modules.

Deciding membership in Quadratic module when $n = 1$

In [Aug08, p. 47], the author provided an algorithm to test the membership of polynomials in compact univariate quadratic modules.

The algorithm relies on the orders and signs at the end points of the associated semialgebraic set of generators.

Deciding membership in Quadratic module when $n = 1$

In [Aug08, p. 47], the author provided an algorithm to test the membership of polynomials in compact univariate quadratic modules.
The algorithm relies on the orders and signs at the end points of the associated semialgebraic set of generators.

Definition

Let $f \in \mathbb{R}[x]$ with $\deg(f) = n$, the Taylor series of $f \in \mathbb{R}[x]$ centered at $a \in \mathbb{R}$ is

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

We define:

- $\mathrm{ord}_a(f)$ as the least integer i such that $\frac{f^{(i)}(a)}{i!}$ is not zero.
- $\epsilon_a(f)$ as 1 if $\frac{f^{(i)}(a)}{i!} > 0$ where $i = \mathrm{ord}_a(f)$ and -1 otherwise.

Deciding membership in Quadratic module when $n = 1$

Definition

Let $G := \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[x]$. We define:

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

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

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

In any of the three cases we define $k_a(G), k_a^+(G), k_a^-(G)$ to be ∞ if the corresponding set is empty.

Deciding membership in Quadratic module when $n = 1$

Theorem 2.18 in [Aug08, p. 47] provides a criterion to check membership in compact univariate quadratic modules.

Deciding membership in Quadratic module when $n = 1$

Theorem 2.18 in [Aug08, p. 47] provides a criterion to check membership in compact univariate quadratic modules.
A member must be non-negative over the associated semialgebraic set of the generators G and satisfy conditions involving the orders and signs at the endpoints of $\mathcal{S}(G)$ using k_a, k_a^+, k_a^-.

Deciding membership in Quadratic module when $n = 1$

Theorem 2.18 in [Aug08, p. 47] provides a criterion to check membership in compact univariate quadratic modules.
A member must be non-negative over the associated semialgebraic set of the generators G and satisfy conditions involving the orders and signs at the endpoints of $\mathcal{S}(G)$ using k_a, k_a^+, k_a^-.

$$x + 1 \notin \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$$

Deciding membership in Quadratic module when $n = 1$

Theorem 2.18 in [Aug08, p. 47] provides a criterion to check membership in compact univariate quadratic modules.
A member must be non-negative over the associated semialgebraic set of the generators G and satisfy conditions involving the orders and signs at the endpoints of $\mathcal{S}(G)$ using k_a, k_a^+, k_a^-.

$$x + 1 \notin \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$$

$$(x+1)^3 = \frac{1}{8}(x+1)^4((x-2)^2+3) + \frac{1}{8}(-(x+1)^3(x-1)^3)$$
$$\in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$$

Monogenic case

Observations

Let $G \subseteq \mathbb{R}[x]$. If $\mathcal{S}(G)$ is compact, then $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$

Observations

Let $G \subseteq \mathbb{R}[x]$. If $\mathcal{S}(G)$ is compact, then $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$

- We will assume $\mathcal{S}(G)$ is represented as ordered intervals.

Observations

Let $G \subseteq \mathbb{R}[x]$. If $\mathcal{S}(G)$ is compact, then $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$

- We will assume $\mathcal{S}(G)$ is represented as ordered intervals.
- We refer to the intervals $a_i = b_i$ as *isolated points*.

Observations

Let $G \subseteq \mathbb{R}[x]$. If $\mathcal{S}(G)$ is compact, then $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$

- We will assume $\mathcal{S}(G)$ is represented as ordered intervals.
- We refer to the intervals $a_i = b_i$ as *isolated points*.
- $\mathcal{S}(\{f\})$ is compact if and only if f has even degree and the leading coefficient of f is negative.

Observations

Let $G \subseteq \mathbb{R}[x]$. If $\mathcal{S}(G)$ is compact, then $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$

- We will assume $\mathcal{S}(G)$ is represented as ordered intervals.
- We refer to the intervals $a_i = b_i$ as *isolated points*.
- $\mathcal{S}(\{f\})$ is compact if and only if f has even degree and the leading coefficient of f is negative.

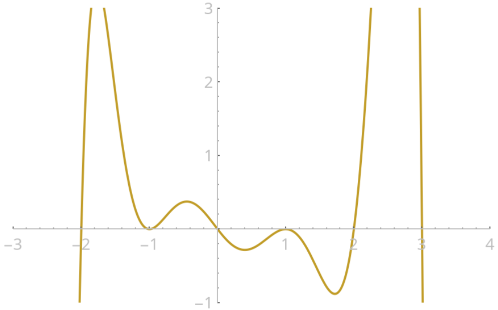

Figure: $\mathcal{S}(-\frac{1}{10}(x+2)(x+1)^2x(x-1)^2(x-2)(x-3))$ is compact

Removing quadratic irreducible factors don't change the problem

Theorem

Let $G \subseteq \mathbb{R}[x]$, $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$ *and* $f \in \mathbb{R}[x]$ *be a polynomial such that* $f = f_1 * ((x-b)^2 + c^2)$ *with* $b \in \mathbb{R}, c \in \mathbb{R} \setminus 0$. *If* $f \in \mathrm{QM}(G)$ *then* $f_1 \in \mathrm{QM}(G)$.

Removing quadratic irreducible factors don't change the problem

Theorem

Let $G \subseteq \mathbb{R}[x]$, $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$ *and* $f \in \mathbb{R}[x]$ *be a polynomial such that* $f = f_1 * ((x-b)^2 + c^2)$ *with* $b \in \mathbb{R}, c \in \mathbb{R} \setminus 0$. *If* $f \in \mathrm{QM}(G)$ *then* $f_1 \in \mathrm{QM}(G)$.

Intuitively, this is because a polynomial of the form $(x-b)^2 + c^2$ with $c \neq 0$ does not change the semialgebraic set nor the orders of any polynomial f.

Removing quadratic irreducible factors don't change the problem

Theorem

Let $G \subseteq \mathbb{R}[x]$, $\mathcal{S}(G) = \bigcup_{i=1}^{n} [a_i, b_i]$ *and* $f \in \mathbb{R}[x]$ *be a polynomial such that* $f = f_1 * ((x - b)^2 + c^2)$ *with* $b \in \mathbb{R}, c \in \mathbb{R} \setminus 0$. *If* $f \in \mathrm{QM}(G)$ *then* $f_1 \in \mathrm{QM}(G)$.

Intuitively, this is because a polynomial of the form $(x - b)^2 + c^2$ with $c \neq 0$ does not change the semialgebraic set nor the orders of any polynomial f.

Additionally, these are sums of squares already which can be absorbed by the sums of squares multipliers in the representation of the polynomial f_1 above.

Example

Consider $f = 2 + 4x + x^2 - x^3 + x^4 + x^5$.
We want to check $f \in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$

Example

Consider $f = 2 + 4x + x^2 - x^3 + x^4 + x^5$.
We want to check $f \in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$
Notice that

$$
\begin{aligned}
f &= ((x-1)^2+1)(x+1)^3 \\
&= ((x-1)^2+1)\left(\frac{1}{8}(x+1)^4((x-2)^2+3) + \frac{1}{8}(-(x+1)^3(x-1)^3)\right) \\
&= \underbrace{\frac{1}{8}(x+1)^4((x-1)^2+1)((x-2)^2+3)}_{\textit{a sums of squares}} \\
&\quad + \underbrace{\frac{1}{8}((x-1)^2+1)}_{\textit{a sums of squares}}(-(x+1)^3(x-1)^3) \\
&\in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})
\end{aligned}
$$

Example

Consider $f = 2 + 4x + x^2 - x^3 + x^4 + x^5$.
We want to check $f \in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$
Notice that

$$f = ((x-1)^2+1)(x+1)^3$$

$$= \underbrace{\frac{1}{8}(x+1)^4((x-1)^2+1)((x-2)^2+3)}_{\text{a sums of squares}}$$

$$+ \underbrace{\frac{1}{8}((x-1)^2+1)}_{\text{a sums of squares}}(-(x+1)^3(x-1)^3)$$

$$\in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$$

Example

Consider $f = 2 + 4x + x^2 - x^3 + x^4 + x^5$.
We want to check $f \in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$
Notice that

$$f = ((x-1)^2 + 1)(x+1)^3$$

$$\in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$$

Example

Consider $f = 2 + 4x + x^2 - x^3 + x^4 + x^5$.
We want to check $f \in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})$
Notice that

$$
\begin{aligned}
f &= ((x-1)^2+1)(x+1)^3 \\
&= ((x-1)^2+1)\left(\frac{1}{8}(x+1)^4((x-2)^2+3) + \frac{1}{8}(-(x+1)^3(x-1)^3)\right) \\
&= \underbrace{\frac{1}{8}(x+1)^4((x-1)^2+1)((x-2)^2+3)}_{\textit{a sums of squares}} \\
&\quad + \underbrace{\frac{1}{8}((x-1)^2+1)}_{\textit{a sums of squares}}(-(x+1)^3(x-1)^3) \\
&\in \mathrm{QM}(\{-(x+1)^3(x-1)^3\})
\end{aligned}
$$

Suitable components

Definition

Let $g \in \mathbb{R}[x]$ be a polynomial. We define *suitable components*, denoted as $\mathbb{R}_g$, as $\{x_i \in \mathbb{R} \mid g(x_i) > 0$ and $g^{'}(x_i) = 0\}$, i.e., an ordered set by positive integers of local maxima of g, for which g is positive.

Suitable components

Definition

Let $g \in \mathbb{R}[x]$ be a polynomial. We define *suitable components*, denoted as $\mathbb{R}_g$, as $\{x_i \in \mathbb{R} \mid g(x_i) > 0 \text{ and } g^{'}(x_i) = 0\}$, i.e., an ordered set by positive integers of local maxima of g, for which g is positive.

Observation: $g^{'}$ is a polynomial, then any $\mathbb{R}_g$ is a finite collection of points in $\mathbb{R}$.

Suitable factors

Definition

The *suitable factors* of f with respect to g is the set of polynomials $\{f_i \mid 0 \leq i \leq |\mathbb{R}_g|\}$ defined as:

$$f_i = c_i \prod_{\substack{r \in \mathcal{Z}(f) \\ x_i < r < x_{i+1} \\ (x_i, x_{i+1}) \in \mathbb{R}_g}} (x - r)^{\mathrm{ord}_r(f)} \tag{1}$$

where $x_0 := -\infty, x_{l+1} := \infty$, $c_i = 1$ if $0 \leq i < |\mathbb{R}_g|$, and $c_{|\mathbb{R}_g|} = -1$.

Example

Let us consider

- $g := -(x+2)^3(x+1)x^2(x-1)(x-2)^3$
- $f := -(x+2)^5(x+\frac{1}{2})x^2(x-\frac{1}{2})(x-3)$

Example

Let us consider

- $g := -(x+2)^3(x+1)x^2(x-1)(x-2)^3$
- $f := -(x+2)^5(x+\frac{1}{2})x^2(x-\frac{1}{2})(x-3)$

The components of $\mathbb{R}_g$ are $(-\infty, -\sqrt{2})$, $(-\sqrt{2}, \sqrt{2})$, and $(\sqrt{2}, \infty)$.

Example

Let us consider

- $g := -(x+2)^3(x+1)x^2(x-1)(x-2)^3$
- $f := -(x+2)^5(x+\frac{1}{2})x^2(x-\frac{1}{2})(x-3)$

The components of $\mathbb{R}_g$ are $(-\infty, -\sqrt{2})$, $(-\sqrt{2}, \sqrt{2})$, and $(\sqrt{2}, \infty)$.

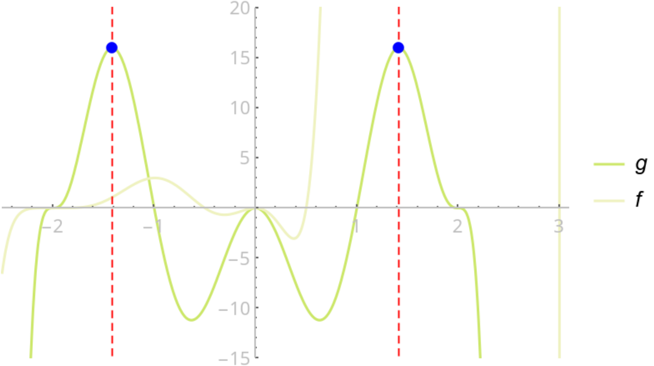

Figure: Suitable factors of f with respect to $\mathbb{R}_g$

Example (Cont'd)

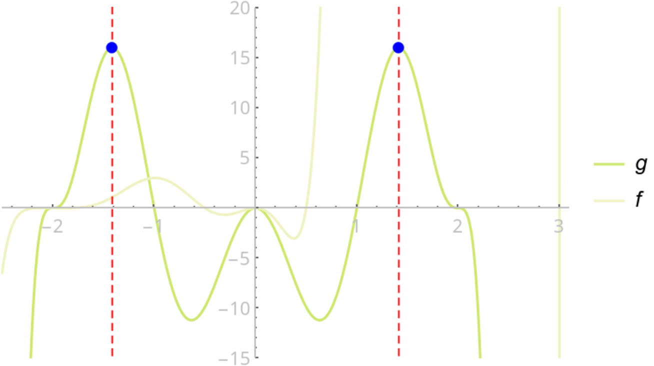

Figure: Suitable factors of f with respect to $\mathbb{R}_g$

Example (Cont'd)

The suitable factors of f with respect to $\mathbb{R}_g$ are:

- $(x+2)^5$
- $(x+\frac{1}{2})x^2(x-\frac{1}{2})$
- $-(x-3)$

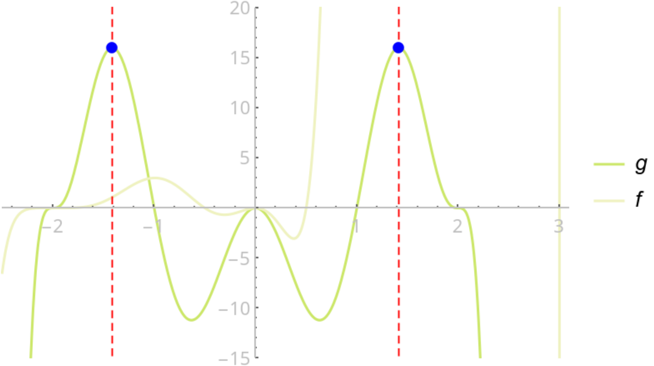

Figure: Suitable factors of f with respect to $\mathbb{R}_g$

Key idea about decomposition

Algorithm 1: Monogenic certificates

Input: $f, g \in \mathbb{R}[x]$
Output: $s_0, s_1 \in \sum \mathbb{R}[x]^2$
Requires: $\mathcal{S}(g) = \bigcup_{i=1}^{n} [a_i, b_i], f \in \mathrm{QM}(\{g\})$
Ensures: $f = s_0 + s_1 g$
`//` $\mathbb{R}_g$ `is of the form` $\{x_1, \ldots, x_m\}$ `with` $x_1 < x_2 < \cdots < x_m$

1 Let $\mathbb{R}_g$ be the suitable components of g
2 Let f_{Left} be the factors of f with roots r such that $r \leq x_1$
3 Let $f_{InBetween}$ be the factors of f with roots r such that $x_1 < r < x_m$
4 Let f_{Right} be the factors of f with roots r such that $x_m \leq r$

Key idea about decomposition

Compute certificates $s_{0,L}, s_{1,L}$ of left suitable factor of g
for r *is root in* f_{Left} **do**
    if r *is equal to* a_1 **then**
        Use $s_{0,L}, s_{1,L}$ to compute certificates of $(x - a_1)^{\mathrm{ord}_{a_1}(f)}$
    else
        Use $s_{0,L}, s_{1,L}$ to compute certificates of $(x - r)$
        Use certificates of $(x - r)$ to compute certificates of $(x - r)^{\mathrm{ord}_r(f)}$
    end if
end for

Key idea about decomposition

Compute certificates $s_{0,R}, s_{1,R}$ of right suitable factor of g
for r *is root in* f_{Right} **do**
    if r *is equal to* a_m **then**
        Use $s_{0,R}, s_{1,R}$ to compute certificates of $-(x-a_m)^{\mathrm{ord}_{a_m}(f)}$
    else
        Use $s_{0,R}, s_{1,R}$ to compute certificates of $-(x-r)$
        Use certificates of $-(x-r)$ to compute certificates of $-(x-r)^{\mathrm{ord}_r(f)}$
    end if
end for

Key idea about decomposition

for $x_i \in \mathbb{R}_g$ **do**

  Compute certificates $s_{0,i,B}, s_{1,i,B}$ of $\prod_{\substack{r \in \mathcal{Z}(f) \\ x_i < r < x_{i+1}}} (x - r)^{\mathrm{ord}_r(f)}$

end for

Collect and rearrange certificates obtained in previous steps by multipliying each expression.

Computing certificates for suitable factors

Left Suitable Factor

Monomials of the form

$$(x - a_1)^{k_{a_1}^{+}} \tag{2}$$

Left Suitable Factor

Monomials of the form

$$(x - a_1)^{k_{a_1}^{+}} \tag{2}$$

Two cases:

Left Suitable Factor

Monomials of the form

$$(x - a_1)^{k_{a_1}^+} \tag{2}$$

Two cases:

- Semialgebraic starts with interval

Left Suitable Factor

Monomials of the form

$$(x - a_1)^{k_{a_1}^+} \tag{2}$$

Two cases:

- Semialgebraic starts with interval
- Semialgebraic starts with isolated point

Semialgebraic starts with interval

Generator $g := (x - a_1)^{k_{a_1}^+} (x - b_1)^{k_{b_1}^-} g_2$ where

$g_2 = -\prod_{\substack{i=2 \\ a_i < b_i}}^{m} (x - a_i)^{k_{a_i}^+} (x - b_i)^{k_{b_i}^-} \prod_{\substack{i=2 \\ a_i = b_i}}^{m} (x - a_i)^{k_{a_i}}$.

Semialgebraic starts with interval

Generator $g := (x-a_1)^{k_{a_1}^+}(x-b_1)^{k_{b_1}^-} g_2$ where
$g_2 = -\prod_{\substack{i=2 \\ a_i<b_i}}^m (x-a_i)^{k_{a_i}^+}(x-b_i)^{k_{b_i}^-} \prod_{\substack{i=2 \\ a_i=b_i}}^m (x-a_i)^{k_{a_i}}$.

Problem: Find $s_0, s_1 \in \sum \mathbb{R}[x]^2$ such that $(x-a_1)^{k_{a_1}^+} = s_0 + s_1 g$.

Semialgebraic starts with interval

Generator $g := (x - a_1)^{k_{a_1}^+} (x - b_1)^{k_{b_1}^-} g_2$ where
$g_2 = -\prod_{\substack{i=2 \\ a_i < b_i}}^{m} (x - a_i)^{k_{a_i}^+} (x - b_i)^{k_{b_i}^-} \prod_{\substack{i=2 \\ a_i = b_i}}^{m} (x - a_i)^{k_{a_i}}$.

Problem: Find $s_0, s_1 \in \sum \mathbb{R}[x]^2$ such that $(x - a_1)^{k_{a_1}^+} = s_0 + s_1 g$.

Approach: Find $s_1 \in \sum \mathbb{R}[x]^2$ such that

$$(x - a_1)^{k_{a_1}^+} - s_1 g \in \sum \mathbb{R}[x]^2$$

Example

Consider $g = -(x+2)^3(x+1)x^2(x-1)(x-2)^3$ from previous example.

Example

Consider $g = -(x+2)^3(x+1)x^2(x-1)(x-2)^3$ from previous example.

The left-most generalized natural generator is $(x+2)^3$.

Example

Consider $g = -(x+2)^3(x+1)x^2(x-1)(x-2)^3$ from previous example.
The left-most generalized natural generator is $(x+2)^3$.
Notice that $(x+2)^3 = s_0 + s_1 g$. Hence,
$(x+2)^3 + s_1(x+2)^3(x+1)x^2(x-1)(x-2)^3$ is a sums of squares for some sums of squares s_1.

Example

Consider $g = -(x+2)^3(x+1)x^2(x-1)(x-2)^3$ from previous example.
The left-most generalized natural generator is $(x+2)^3$.
Notice that $(x+2)^3 = s_0 + s_1 g$. Hence,
$(x+2)^3 + s_1(x+2)^3(x+1)x^2(x-1)(x-2)^3$ is a sums of squares for some sums of squares s_1.

$$(x+2)^3(1 + s_1(x+1)x^2(x-1)(x-2)^3)$$

We need to "complete" the root $x = -2$. Notice that $(x+1)x^2(x-1)(x-2)^3|_{x \to -2} = -768$. Setting $s_1 = \frac{1}{768}$ forces a root at $x = -2$ in $1 + s_1(x+1)x^2(x-1)(x-2)^3$.

Example

In this case, the roots of $1 + s_1(x+1)x^2(x-1)(x-2)^3$ are a single real root at $x = -2$ and the rest are complex conjugates. We have completed the even root for $(x+2)^3$, thus $s_0 = (x+2)^3(1 + s_1(x+1)x^2(x-1)(x-2)^3)$ is a sums of squares.

Example

In this case, the roots of $1 + s_1(x+1)x^2(x-1)(x-2)^3$ are a single real root at $x = -2$ and the rest are complex conjugates.
We have completed the even root for $(x+2)^3$, thus $s_0 = (x+2)^3(1 + s_1(x+1)x^2(x-1)(x-2)^3)$ is a sums of squares.
Setting $s_1 = \frac{1}{768}$ we have

$$(x+2)^3 = s_0 + s_1 g$$

Example

In this case, the roots of $1 + s_1(x+1)x^2(x-1)(x-2)^3$ are a single real root at $x = -2$ and the rest are complex conjugates.
We have completed the even root for $(x+2)^3$, thus $s_0 = (x+2)^3(1 + s_1(x+1)x^2(x-1)(x-2)^3)$ is a sums of squares.
Setting $s_1 = \frac{1}{768}$ we have

$$(x+2)^3 = s_0 + s_1 g$$

In general, we would expected that the expression $1 - s_1 \frac{g}{(x-a_1)^{k^+_{a_1}}}$ to have negative intervals. Our algorithm fixes each negative interval by updating s_1 with square terms at the midpoints of these negative intervals.

Example

Consider

$$g = -x^3(x-1)^5(x-2)(x-3)(x-4)(x-7)$$
$$(x-8)(x-10)(x-14)(x-15)(x-16)^2(x-19)(x-20)$$

The left-most generalized natural generator is x^3.

Example

Consider

$$g = -x^3(x-1)^5(x-2)(x-3)(x-4)(x-7)$$
$$(x-8)(x-10)(x-14)(x-15)(x-16)^2(x-19)(x-20)$$

The left-most generalized natural generator is x^3.

We first set $s_1 = \frac{1}{274563072000}$ to complete the root.

Example

Consider

$$g = -x^3(x-1)^5(x-2)(x-3)(x-4)(x-7)$$
$$(x-8)(x-10)(x-14)(x-15)(x-16)^2(x-19)(x-20)$$

The left-most generalized natural generator is x^3.

We first set $s_1 = \frac{1}{274563072000}$ to complete the root.

We find that the negative intervals of $1 - \frac{1}{274563072000} g$ are contained in the intervals $(4,7) \cup (8,10) \cup (14,15) \cup (19,20)$.

Example

Consider

$$g = -x^3(x-1)^5(x-2)(x-3)(x-4)(x-7)$$
$$(x-8)(x-10)(x-14)(x-15)(x-16)^2(x-19)(x-20)$$

The left-most generalized natural generator is x^3.

We first set $s_1 = \frac{1}{274563072000}$ to complete the root.

We find that the negative intervals of $1 - \frac{1}{274563072000}g$ are contained in the intervals $(4,7) \cup (8,10) \cup (14,15) \cup (19,20)$.

The following plots illustrate the updates to s_1 and how the polynomial $1 - s_1 g$ becomes strictly positive to the right of $x = 0$.

Example (Cont'd)

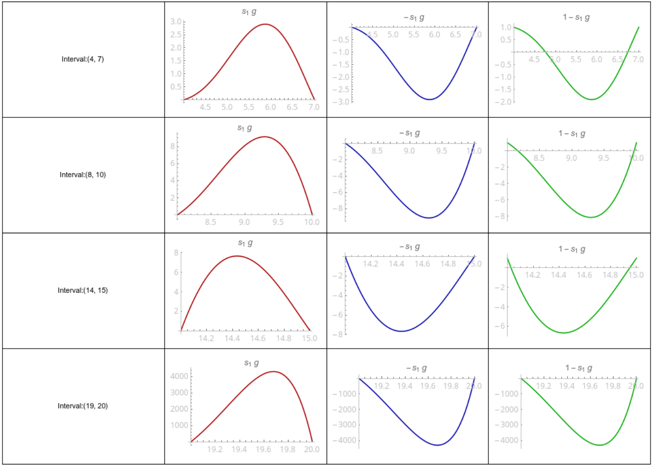

Figure: $s_1 = \frac{1}{274563072000}$

Example (Cont'd)

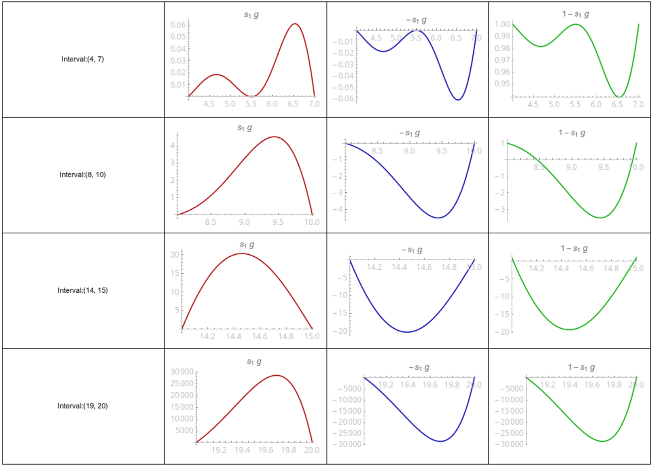

Figure: $s_1 = \frac{1}{8305532928000}(x - (4+7)/2)^2$

Example (Cont'd)

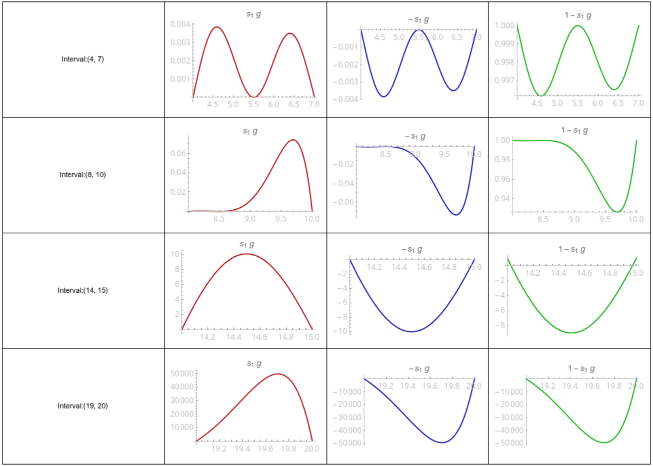

Figure: $s_1 = \frac{1}{600074754048000}(x-(4+7)/2)^2(x-(8+10)/2)^2$

Example (Cont'd)

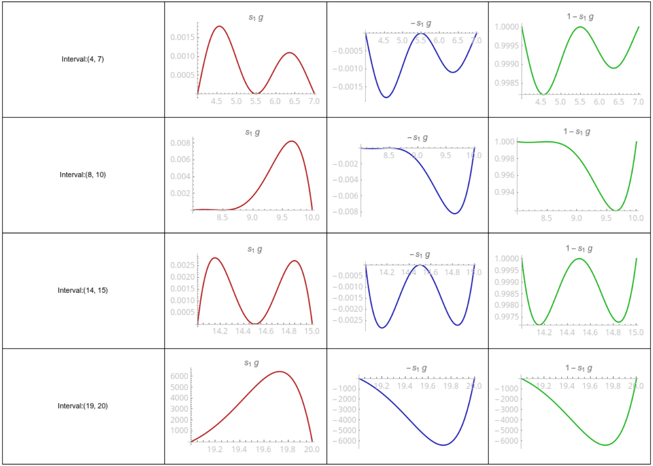

Figure:
$$s_1 = \frac{1}{1261657170385920000}(x-(4+7)/2)^2(x-(8+10)/2)^2(x-(14+15)/2)^2$$

Example (Cont'd)

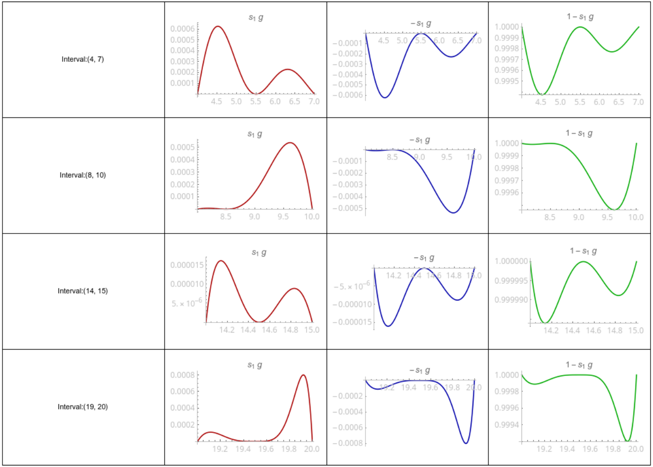

Figure: $s_1 = \frac{1}{182423089119673321920000}(x-(4+7)/2)^2(x-(8+10)/2)^2(x-(14+15)/2)^2(x-(19+20)/2)^4$

Right Suitable Factor

Key ideas:

Right Suitable Factor

Key ideas:

- Sum of squares are closed by involution maps: $x \mapsto -x$

Right Suitable Factor

Key ideas:

- Sum of squares are closed by involution maps: $x \mapsto -x$
- Applying a involution map, we reduce the problem to the Left Suitable Factor case.

Right Suitable Factor

Key ideas:

- Sum of squares are closed by involution maps: $x \mapsto -x$
- Applying a involution map, we reduce the problem to the Left Suitable Factor case.
- A second involution maps the reduced problem to the original one.

Properties

Proposition

If $s \in \sum \mathbb{R}[x]^2$ *then* $s^\diamond \in \sum \mathbb{R}[x]^2$

Properties

Proposition

If $s \in \sum \mathbb{R}[x]^2$ *then* $s^\diamond \in \sum \mathbb{R}[x]^2$

Proposition

If $f \in \mathbb{R}[x]$ *belongs to a compact quadratic module* $\mathrm{QM}(G)$ *for some* $G = \{g_i \mid 1 \leq i \leq m\}$ *then* $f^\diamond \in \mathrm{QM}(G^\diamond)$.

Properties

Proposition

If $s \in \sum \mathbb{R}[x]^2$ *then* $s^\diamond \in \sum \mathbb{R}[x]^2$

Proposition

If $f \in \mathbb{R}[x]$ *belongs to a compact quadratic module* $\mathrm{QM}(G)$ *for some* $G = \{g_i \mid 1 \leq i \leq m\}$ *then* $f^\diamond \in \mathrm{QM}(G^\diamond)$.

Theorem

The involution of the left (resp. right)-most generalized natural generator of a compact quadratic module $\mathrm{QM}(G)$ *for some* $G = \{g_i \mid 1 \leq i \leq m\}$ *is the right (resp. left) most generalized natural generator of* $\mathrm{QM}(G^\diamond)$.

Strictly Positive Left Suitable Factor

These are monomials of the form:

Strictly Positive Left Suitable Factor

These are monomials of the form:

- $x - c$ where $c < \mathcal{S}(G)$, (denoted as left strictly positive linear factor), or

Strictly Positive Left Suitable Factor

These are monomials of the form:

- $x - c$ where $c < \mathcal{S}(G)$, (denoted as left strictly positive linear factor), or
- $-(x - c)$ where $c > \mathcal{S}(G)$ (denoted as right strictly positive linear factor).

Strictly Positive Left Suitable Factor

These are monomials of the form:

- $x - c$ where $c < \mathcal{S}(G)$, (denoted as left strictly positive linear factor), or
- $-(x - c)$ where $c > \mathcal{S}(G)$ (denoted as right strictly positive linear factor).

It is enough to consider the left case as the right one can be solved using the involution technique.

Strictly Positive Left Suitable Factor

These are monomials of the form:

- $x - c$ where $c < \mathcal{S}(G)$, (denoted as left strictly positive linear factor), or
- $-(x - c)$ where $c > \mathcal{S}(G)$ (denoted as right strictly positive linear factor).

It is enough to consider the left case as the right one can be solved using the involution technique.

Theorem

$x - c \in \mathrm{QM}(g - g(c))$. *Furthermore, the sums of squares certificates of the latter are computable.*

Key ideas

Use a truncated Gaussian polynomial to fix the negative intervals of polynomials of the form:
$(x-a)^{2m_1+1}\prod_{i=1}^{l}(x-c_i)^{2n_i}(x-b)^{2m_2+1}$ where $m_1, m_2, n_i \in \mathbb{N}$, $a < c_1 < \cdots < c_l < b$ and $a, b \in \partial(\mathcal{S}(\{g\}))$.

Definition

We define $\mathrm{Trunc}_n(X)$ as the truncated Taylor series expansion of $e^{-X^2/2}$ where the highest exponent is even and its leading coefficient is positive, i.e. $\mathrm{Trunc}_n(X) := \sum_{k=0}^{2n} \frac{(-1)^k}{2^k k!} X^{2k}$

Example

Consider $g = -(x+2)^3(x+1)x^2(x-1)(x-2)^3$, we will find certificates for $(x+1)x^2(x-1)$.

Example

Consider $g = -(x+2)^3(x+1)x^2(x-1)(x-2)^3$, we will find certificates for $(x+1)x^2(x-1)$.
Since $(x+1)x^2(x-1) \in \mathrm{QM}(\{g\})$, then $(x+1)x^2(x-1) = s_0 + s_1 g$, thus it is enough to find s_1 such that

$$(x+1)x^2(x-1) + s_1(x+2)^3(x+1)x^2(x-1)(x-2)^3$$

Example

Consider $g = -(x+2)^3(x+1)x^2(x-1)(x-2)^3$, we will find certificates for $(x+1)x^2(x-1)$.
Since $(x+1)x^2(x-1) \in \mathrm{QM}(\{g\})$, then $(x+1)x^2(x-1) = s_0 + s_1 g$, thus it is enough to find s_1 such that

$$(x+1)x^2(x-1) + s_1(x+2)^3(x+1)x^2(x-1)(x-2)^3$$

We can factor out x^2 and include it back without changing the certificates problem for the original polynomial.

$$(x+1)(x-1)(1 + s_1(x+2)^3(x-2)^3)$$

Example

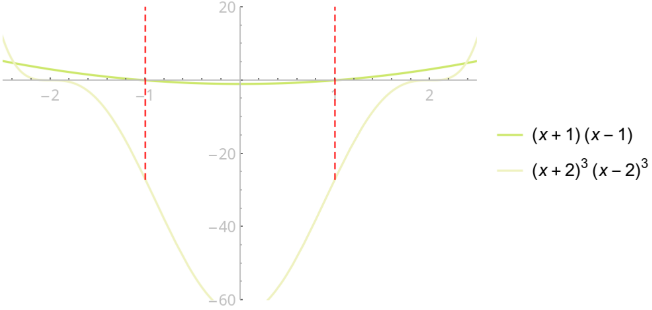

Figure: In-between case lifting step

Example

In this case, since $(x+2)^3(x-2)^3$ has $(-2,2)$ as negative interval, it is enough to "shrink" by a suitable constant such that $s_1(x+2)^3(x-2)^3$ completes the squares of $(x+1)(x-1)$.

Example

In this case, since $(x+2)^3(x-2)^3$ has $(-2,2)$ as negative interval, it is enough to "shrink" by a suitable constant such that $s_1(x+2)^3(x-2)^3$ completes the squares of $(x+1)(x-1)$. Setting $s_1 = 1/27$ we have that $1 + s_1(x+2)^3(x-2)^3$ has $x=-1$ and $x=1$ as real roots and the rest of its roots are complex conjugates. Thus, $(x+1)(x-1)(1+s_1(x+2)^3(x-2)^3)$ is a sums of squares.

Example

Setting $s_0 = (x+1)(x-1)(1 + s_1(x+2)^3(x-2)^3)$ we obtain

$$(x+1)(x-1) = s_0 - s_1(x+2)^3(x+1)(x-1)(x-2)^3$$

Example

Setting $s_0 = (x+1)(x-1)(1 + s_1(x+2)^3(x-2)^3)$ we obtain

$$(x+1)(x-1) = s_0 - s_1(x+2)^3(x+1)(x-1)(x-2)^3$$

Thus,

$$\begin{aligned}(x+1)x^2(x-1) &= x^2 s_0 - s_1(x+2)^3(x+1)x^2(x-1)(x-2)^3 \\ &= x^2 s_0 + s_1 g\end{aligned}$$

Example

In general, we would expect the term $\frac{g}{in-between-factor}$ to have more than one negative interval.

Example

In general, we would expect the term $\frac{g}{in-between-factor}$ to have more than one negative interval.

Using a truncated Gaussian the goal is to minimize the negative intervals outside the negative interval where the odd factors are located such a suitable constant can be obtained to complete these odd factors.

Proposed work

For the univariate case

- Preliminary work:

For the univariate case

- Preliminary work:
  - Reduction from a general 2-basis quadratic module [SMK22] to a monogenic problem.

For the univariate case

- Preliminary work:
  - Reduction from a general 2-basis quadratic module [SMK22] to a monogenic problem.
  - Identify certificates in the preorder representation.

For the univariate case

- Preliminary work:
  - Reduction from a general 2-basis quadratic module [SMK22] to a monogenic problem.
  - Identify certificates in the preorder representation.
- Work to be done:

For the univariate case

- Preliminary work:
  - Reduction from a general 2-basis quadratic module [SMK22] to a monogenic problem.
  - Identify certificates in the preorder representation.
- Work to be done:
  - Find certificates for the products in the preorder structure to have certificates in terms of the quadratic module structure.

For the bivariate subcase

- Preliminary work:
    - Procedure to compute certificates for a special kind of monogenic quadratic modules satisfying certain properties.

For the bivariate subcase

- Preliminary work:
  - Procedure to compute certificates for a special kind of monogenic quadratic modules satisfying certain properties.
- Work to be done:

For the bivariate subcase

- Preliminary work:
  - Procedure to compute certificates for a special kind of monogenic quadratic modules satisfying certain properties.
- Work to be done:
  - Investigate if the identified prerequisites are enough for the monogenic case or if the method can be generalized for missing cases in the monogenic case.

For the bivariate subcase

- Preliminary work:
  - Procedure to compute certificates for a special kind of monogenic quadratic modules satisfying certain properties.

- Work to be done:
  - Investigate if the identified prerequisites are enough for the monogenic case or if the method can be generalized for missing cases in the monogenic case.
  - Solve the certificates problem for a zero dimensional polynomial systems

Conclusions

Conclusions

1. We have presented a solution to computing certificates in the monogenic case problem.

Conclusions

1. We have presented a solution to computing certificates in the monogenic case problem.
2. The method is symbolic and produces exact certificates.

Conclusions

1. We have presented a solution to computing certificates in the monogenic case problem.
2. The method is symbolic and produces exact certificates.
3. We have compared a prototypical tool in `Mathematica` and `RealCertify` [MD18] identifying strictly positive polynomials which our approach can solve but `RealCertify` cannot.

Conclusions

1. We have presented a solution to computing certificates in the monogenic case problem.
2. The method is symbolic and produces exact certificates.
3. We have compared a prototypical tool in `Mathematica` and `RealCertify` [MD18] identifying strictly positive polynomials which our approach can solve but `RealCertify` cannot.
4. Our current progress in the remaining work shows the feasibility of the approach to be used for the general case.

Thank you for your attention!

References I

- Augustin, Doris. "The Membership Problem for quadratic modules with focus on the one dimensional case". In: *Ph.D. thesis*. Ph.D. thesis. 2008.
- Magron, Victor and Mohab Safey El Din. *RealCertify: a Maple package for certifying non-negativity*. 2018. DOI: 10.48550/ARXIV.1805.02201. URL: https://arxiv.org/abs/1805.02201.
- Shang, Weifeng, Chenqi Mou, and Deepak Kapur. "Algorithms for Testing Membership in Univariate Quadratic Modules over the Reals". In: *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*. ISSAC '22. Villeneuve-d'Ascq, France: Association for Computing Machinery, 2022, pp. 429–437. ISBN: 9781450386883. DOI: 10.1145/3476446.3536176. URL: https://doi.org/10.1145/3476446.3536176.

References II

Stengle, Gilbert. "Complexity Estimates for the Schmüdgen Positivstellensatz". In: *Journal of Complexity* 12.2 (June 1996), pp. 167–174. ISSN: 0885-064X. DOI: 10.1006/jcom.1996.0011. URL: http://dx.doi.org/10.1006/jcom.1996.0011.