

On Exact Reznick, Hilbert-Artin and Putinar's Representations

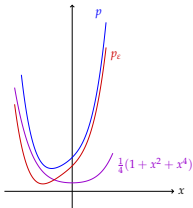
Victor Magron, LAAS CNRS

Joint work with

Mohab Safey El Din (Sorbonne Univ. -INRIA-LIP6 CNRS)

JNCF

04th February 2019



Deciding Non-negativity

$$X = (X_1, \dots, X_n)$$

$$f \in \mathbb{Q}[X]$$

co-NP hard problem: check $f \geq 0$ on \mathbb{K}

Deciding Non-negativity

$X = (X_1, \dots, X_n)$ **co-NP hard problem: check $f \geq 0$ on \mathbf{K}**
 $f \in \mathbb{Q}[X]$

1 Unconstrained $\rightsquigarrow \mathbf{K} = \mathbb{R}^n$

2 Constrained

$\rightsquigarrow \mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geq 0, \dots, g_m(\mathbf{x}) \geq 0\} \quad g_j \in \mathbb{Q}[X]$

$\deg f, \deg g_j \leq d$



[Collins 75] 💡 CAD **doubly exp. in n poly. in d**



[Grigoriev-Vorobjov 88, Basu-Pollack-Roy 98]



Critical points **singly exponential time** $(m + 1) \tau d^{O(n)}$

Deciding Non-negativity

💡 Sums of squares (SOS)

$$\sigma = h_1^2 + \dots + h_p^2$$

Deciding Non-negativity

💡 Sums of squares (SOS)

$$\sigma = h_1^2 + \dots + h_p^2$$

HILBERT 17TH PROBLEM: f SOS of rational functions?



[Artin 27] **YES!**

💡 [Lasserre/Parrilo 01] **Numerical** solvers compute σ

Semidefinite programming (SDP) \rightsquigarrow **approximate** certificates

$$\boxed{\approx \rightarrow =}$$

The Question of Exact Certification

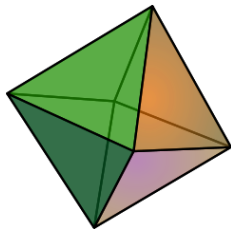
How to go from **approximate** to **exact** certification?

What is Semidefinite Programming?

- Linear Programming (LP):

$$\begin{array}{ll} \min_{\mathbf{z}} & \mathbf{c}^\top \mathbf{z} \\ \text{s.t.} & \mathbf{A} \mathbf{z} \geq \mathbf{d} . \end{array}$$

- Linear cost \mathbf{c}
- Linear inequalities “ $\sum_i A_{ij} z_j \geq d_i$ ”



Polyhedron

What is Semidefinite Programming?

- Semidefinite Programming (SDP):

$$\begin{aligned} \min_{\mathbf{z}} \quad & \mathbf{c}^\top \mathbf{z} \\ \text{s.t.} \quad & \sum_i \mathbf{F}_i z_i \succcurlyeq \mathbf{F}_0 . \end{aligned}$$

- Linear cost \mathbf{c}
- Symmetric matrices $\mathbf{F}_0, \mathbf{F}_i$
- Linear matrix inequalities “ $\mathbf{F} \succcurlyeq 0$ ”
(\mathbf{F} has nonnegative eigenvalues)



Spectrahedron

What is Semidefinite Programming?

- Semidefinite Programming (SDP):

$$\begin{aligned} \min_{\mathbf{z}} \quad & \mathbf{c}^\top \mathbf{z} \\ \text{s.t.} \quad & \sum_i \mathbf{F}_i z_i \succcurlyeq \mathbf{F}_0, \quad \mathbf{A} \mathbf{z} = \mathbf{d}. \end{aligned}$$

- Linear cost \mathbf{c}
- Symmetric matrices $\mathbf{F}_0, \mathbf{F}_i$
- Linear matrix inequalities “ $\mathbf{F} \succcurlyeq 0$ ”
(\mathbf{F} has nonnegative eigenvalues)



Spectrahedron

Lasserre's Hierarchy

- Prove **polynomial inequalities** with SDP:

$$f(a, b) := a^2 - 2ab + b^2 \geq 0 .$$

- Find \mathbf{z} s.t. $f(a, b) = \underbrace{\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}}_{\geq 0}$.

- Find \mathbf{z} s.t. $a^2 - 2ab + b^2 = z_1 a^2 + 2z_2 ab + z_3 b^2 \quad (\mathbf{A} \mathbf{z} = \mathbf{d})$

- $\begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{\mathbf{F}_1} z_1 + \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\mathbf{F}_2} z_2 + \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{\mathbf{F}_3} z_3 \succcurlyeq \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}}_{\mathbf{F}_0}$

Lasserre's Hierarchy

- Choose a cost \mathbf{c} e.g. $(1, 0, 1)$ and solve:

$$\begin{aligned} \min_{\mathbf{z}} \quad & \mathbf{c}^\top \mathbf{z} \\ \text{s.t.} \quad & \sum_i \mathbf{F}_i z_i \succcurlyeq \mathbf{F}_0, \quad \mathbf{A} \mathbf{z} = \mathbf{d}. \end{aligned}$$

- Solution $\begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \succcurlyeq 0$ (eigenvalues 0 and 2)

- $a^2 - 2ab + b^2 = (a \ b) \underbrace{\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}}_{\succcurlyeq 0} \begin{pmatrix} a \\ b \end{pmatrix} = (a - b)^2.$

- Solving **SDP** \implies Finding **SUMS OF SQUARES** certificates

Lasserre's Hierarchy

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set

$$\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geq 0, \dots, g_m(\mathbf{x}) \geq 0\}$$

Lasserre's Hierarchy

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set

$$\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geq 0, \dots, g_m(\mathbf{x}) \geq 0\}$$

- $:= [0, 1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geq 0, \quad x_2(1 - x_2) \geq 0\}$

Lasserre's Hierarchy

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set

$$\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geq 0, \dots, g_m(\mathbf{x}) \geq 0\}$$

- $:= [0, 1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geq 0, \quad x_2(1 - x_2) \geq 0\}$

$$\underbrace{f}_{x_1 x_2} = -\frac{1}{8} + \overbrace{\frac{1}{2} \left(x_1 + x_2 - \frac{1}{2} \right)^2}^{\sigma_0} + \overbrace{\frac{1}{2} x_1(1 - x_1)}^{\sigma_1} + \overbrace{\frac{1}{2} x_2(1 - x_2)}^{\sigma_2}$$

Lasserre's Hierarchy

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set

$$\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geq 0, \dots, g_m(\mathbf{x}) \geq 0\}$$

- $:= [0, 1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geq 0, \quad x_2(1 - x_2) \geq 0\}$

$$\underbrace{f}_{x_1 x_2} = -\frac{1}{8} + \frac{1}{2} \overbrace{\left(x_1 + x_2 - \frac{1}{2}\right)^2}^{\sigma_0} + \frac{1}{2} \overbrace{x_1(1 - x_1)}^{g_1} + \frac{1}{2} \overbrace{x_2(1 - x_2)}^{g_2}$$

- $\Sigma =$ Sums of squares (SOS) σ_i

Lasserre's Hierarchy

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set

$$\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geq 0, \dots, g_m(\mathbf{x}) \geq 0\}$$

- $:= [0, 1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geq 0, \quad x_2(1 - x_2) \geq 0\}$

$$\underbrace{f}_{x_1 x_2} = -\frac{1}{8} + \overbrace{\frac{1}{2} \left(x_1 + x_2 - \frac{1}{2} \right)^2}^{\sigma_0} + \overbrace{\frac{1}{2} x_1(1 - x_1)}^{\sigma_1} + \overbrace{\frac{1}{2} x_2(1 - x_2)}^{\sigma_2}$$

- Σ = Sums of squares (SOS) σ_i

- Bounded degree:

$$\mathcal{Q}_d(\mathbf{K}) := \left\{ \sigma_0 + \sum_{j=1}^m \sigma_j g_j, \text{ with } \deg \sigma_j g_j \leq 2d \right\}$$

Lasserre's Hierarchy

- **Hierarchy of SDP relaxations:**

$$\lambda_d := \sup \left\{ \lambda : f - \lambda \in \mathcal{Q}_d(\mathbf{K}) \right\}$$



- Convergence guarantees $\lambda_d \uparrow f^*$ [Lasserre 01]
- Can be computed with SDP solvers (CSDP, SDPA)
- **“No Free Lunch” Rule:** $\binom{n+2d}{n}$ SDP variables

Certifying Non-negativity

APPROXIMATE SOLUTIONS

sum of squares of $a^2 - 2ab + b^2$?



$(1.00001a - 0.99998b)^2!$



$$a^2 - 2ab + b^2 \simeq (1.00001a - 0.99998b)^2$$

$$a^2 - 2ab + b^2 \neq 1.0000200001a^2 - 1.9999799996ab + 0.9999600004b^2$$

$$\boxed{\simeq \rightarrow = ?}$$

Certifying Non-negativity

1 Reznick's representation

positive definite form f

[Reznick 95]

$$f = \frac{\sigma}{(X_1^2 + \dots + X_n^2)^D}$$

2 Hilbert-Artin's representation

$f \geq 0$

[Artin 27]

$$f = \frac{\sigma}{h^2}$$

3 Putinar's representation

$f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m$ $f > 0$ on compact K

$\deg \sigma_i \leq 2D$

[Putinar 93]

One Answer when $K = \mathbb{R}^n$

💡 Hybrid **SYMBOLIC/NUMERIC** methods



[Peyrl-Parrilo 08]

[Kaltofen-Yang-Zhi 08]

↔ can handle degenerate situations when $f \in \partial\Sigma$

$$f(X) \simeq \mathbf{v}_D^T(X) \tilde{\mathbf{Q}} \mathbf{v}_D(X) \quad \tilde{\mathbf{Q}} \succcurlyeq 0$$

$\mathbf{v}_D(X)$: vector of monomials of $\deg \leq D$

One Answer when $\mathbf{K} = \mathbb{R}^n$

💡 Hybrid **SYMBOLIC/NUMERIC** methods



[Peyrl-Parrilo 08]

[Kaltofen-Yang-Zhi 08]

↔ can handle degenerate situations when $f \in \partial\Sigma$

$$f(X) \simeq \mathbf{v}_D^T(X) \tilde{\mathbf{Q}} \mathbf{v}_D(X) \quad \tilde{\mathbf{Q}} \succcurlyeq 0$$

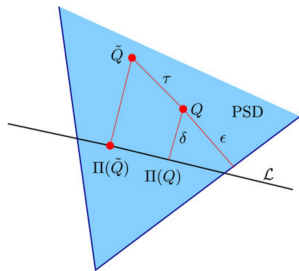
$\mathbf{v}_D(X)$: vector of monomials of $\deg \leq D$

$$\boxed{\simeq \rightarrow =}$$

💡 $\tilde{\mathbf{Q}}$ Rounding \mathbf{Q} Projection $\Pi(\mathbf{Q})$

$$f(X) = \mathbf{v}_D^T(X) \Pi(\mathbf{Q}) \mathbf{v}_D(X)$$

$\Pi(\mathbf{Q}) \succcurlyeq 0$ when $\varepsilon \rightarrow 0$



One Answer when $\mathbf{K} = \mathbb{R}^n$

💡 Hybrid **SYMBOLIC/NUMERIC** methods



[Peyrl-Parrilo 08]

[Kaltofen-Yang-Zhi 08]

↪ can handle degenerate situations when $f \in \partial\Sigma$

$$f(X) \simeq \mathbf{v}_D^T(X) \tilde{\mathbf{Q}} \mathbf{v}_D(X) \quad \tilde{\mathbf{Q}} \succcurlyeq 0$$

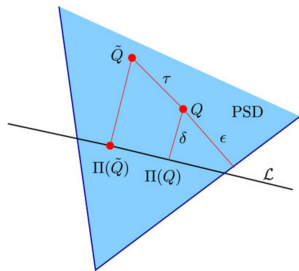
$\mathbf{v}_D(X)$: vector of monomials of $\deg \leq D$

$$\boxed{\simeq \rightarrow =}$$

💡 $\tilde{\mathbf{Q}}$ Rounding \mathbf{Q} Projection $\Pi(\mathbf{Q})$

$$f(X) = \mathbf{v}_D^T(X) \Pi(\mathbf{Q}) \mathbf{v}_D(X)$$

$\Pi(\mathbf{Q}) \succcurlyeq 0$ when $\varepsilon \rightarrow 0$



COMPLEXITY?

One Answer when $\mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geq 0\}$

💡 Hybrid **SYMBOLIC/NUMERIC** methods

📄 Magron-Allamigeon-Gaubert-Werner 14

$$f \simeq \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$$

$$u = f - \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$$

One Answer when $\mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geq 0\}$

💡 Hybrid **SYMBOLIC/NUMERIC** methods

📄 Magron-Allamigeon-Gaubert-Werner 14

$$f \simeq \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$$

Compact $\mathbf{K} \subseteq [0, 1]^n$

$$u = f - \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$$

$$\boxed{\simeq \rightarrow =}$$

💡 $\forall \mathbf{x} \in [0, 1]^n, u(\mathbf{x}) \leq -\varepsilon$

$$\min_{\mathbf{K}} f \geq \varepsilon \text{ when } \varepsilon \rightarrow 0$$

COMPLEXITY?



Related Work: Exact Methods

Existence Question


Does there exist $h_i \in \mathbb{Q}[X], c_i \in \mathbb{Q}^{>0}$ s.t. $f = \sum_i c_i h_i^2$?

Related Work: Exact Methods

Existence Question

Does there exist $h_i \in \mathbb{Q}[X], c_i \in \mathbb{Q}^{>0}$ s.t. $f = \sum_i c_i h_i^2$?

$$n = 1 \quad \deg f = d$$

 $f = c_1 h_1^2 + c_2 h_2^2 + c_3 h_3^2 + c_4 h_4^2 + c_5 h_5^2$ [Pourchet 72]

 $f = c_1 h_1^2 + \dots + c_d h_d^2$ [Schweighofer 99]


 $f = c_1 h_1^2 + \dots + c_{d+3} h_{d+3}^2$ [Chevillard et. al 11]

Related Work: Exact Methods


Existence Question

Does there exist $h_i \in \mathbb{Q}[X], c_i \in \mathbb{Q}^{>0}$ s.t. $f = \sum_i c_i h_i^2$?

$$n = 1 \quad \deg f = d$$

 $f = c_1 h_1^2 + c_2 h_2^2 + c_3 h_3^2 + c_4 h_4^2 + c_5 h_5^2$ [Pourchet 72]

 $f = c_1 h_1^2 + \dots + c_d h_d^2$ [Schweighofer 99]

 $f = c_1 h_1^2 + \dots + c_{d+3} h_{d+3}^2$ [Chevillard et. al 11]

$$n > 1 \quad \deg f = d$$

SOS with Exact LMIs $f = \mathbf{v}_d^T(X) \mathbf{G} \mathbf{v}_d^T(X)$ $\mathbf{G} \succcurlyeq 0$

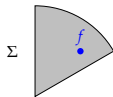
 Solving over the rationals [Guo-Safey El Din-Zhi 13]

 Solving over the reals [Henrion-Naldi-Safey El Din 16]

The Cost of Exact Polynomial Optimization

$f \in \mathbb{Q}[\mathbf{X}] \cap \mathring{\Sigma}[X]$ (interior of the SOS cone)

bit size τ $\deg f = d$



Complexity Question(s)

What is the output bit size of $\sum_i c_i h_i^2$?

1 **Reznick's** representation

positive definite form f

$$f = \frac{\sigma}{(X_1^2 + \dots + X_n^2)^D}$$

2 **Hilbert-Artin's** representation

$f \geq 0$ and $\sigma \in \mathring{\Sigma}[X]$

$$f = \frac{\sigma}{h^2}$$

3 **Putinar's** representation

$$f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m$$

$f > 0$ on compact \mathbf{K}

$$\deg \sigma_i \leq 2D$$

Exact algorithm? BOUNDS on D , $\tau(\sigma_i)$?

Contributions

Complexity cost of certifying non-negativity

💡 Algorithm intsos \rightsquigarrow **OUTPUT BIT SIZE** = $\tau d^{d^{\mathcal{O}(n)}}$

Complexity cost $d^{\mathcal{O}(n)}$ for **Deciding**

1 **Reznick's representation**

💡 Algorithm Polyasos

positive definite form f **OUTPUT BIT SIZE** = $2^{2^{\tau \mathcal{O}(1) \cdot (4d+6)^{\mathcal{O}(n)}}$

2 **Hilbert-Artin's representation**

💡 Algorithm Hilbertsos

$$f = \frac{\sigma}{h^2}$$

$$\deg h = D \quad \tau(h) = \tau_D$$

OUTPUT BIT SIZE = $\tau_D D^{D^{\mathcal{O}(n)}}$

3 **Putinar's representation**

💡 Algorithm Putinarsos

$f > 0$ on compact \mathbf{K}

OUTPUT BIT SIZE = $D^{D^{\mathcal{O}(n)}}$ with $\log D = \mathcal{O}(2^{\tau d^n c_K})$

Deciding Non-negativity

Exact SOS Representations

Exact Reznick's Representations

Exact Putinar's Representations

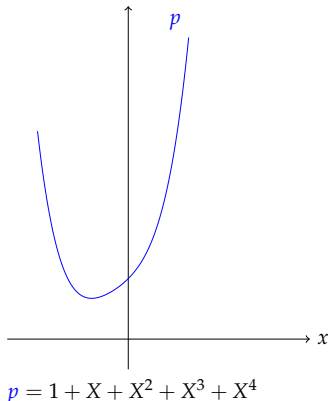
Benchmarks

Conclusion and Perspectives

intsos with $n = 1$ and SDP Approximation

Algorithm adapted from [Chevillard-Harrison-Joldes-Lauter 11]

$$p \in \mathbb{Z}[X], \deg p = d = 2k, p > 0$$



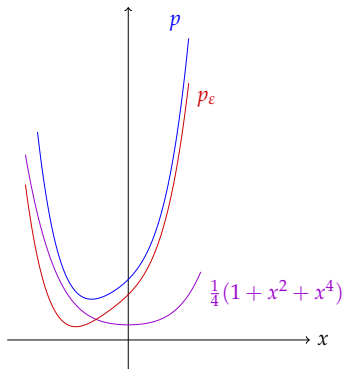
intsos with $n = 1$ and SDP Approximation

Algorithm adapted from [Chevallard-Harrison-Joldes-Lauter 11]

$$p \in \mathbb{Z}[X], \deg p = d = 2k, p > 0$$

💡 **PERTURB:** find $\varepsilon \in \mathbb{Q}$ s.t.

$$p_\varepsilon := p - \varepsilon \sum_{i=0}^k X^{2i} > 0$$



$$p = 1 + X + X^2 + X^3 + X^4$$

$$\varepsilon = \frac{1}{4}$$

$$p > \frac{1}{4}(1 + X^2 + X^4)$$

intsos with $n = 1$ and SDP Approximation

Algorithm adapted from [Chevallard-Harrison-Joldes-Lauter 11]

$p \in \mathbb{Z}[X]$, $\deg p = d = 2k$, $p > 0$

💡 **PERTURB**: find $\varepsilon \in \mathbb{Q}$ s.t.

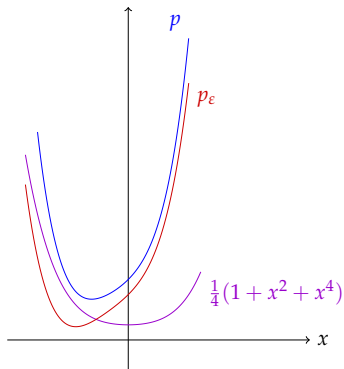
$$p_\varepsilon := p - \varepsilon \sum_{i=0}^k X^{2i} > 0$$

💡 **SDP approximation**:

$$p - \varepsilon \sum_{i=0}^k X^{2i} = s_1^2 + s_2^2 + u$$

💡 **ABSORB**: small enough u_i

$\implies \varepsilon \sum_{i=0}^k X^{2i} + u$ SOS



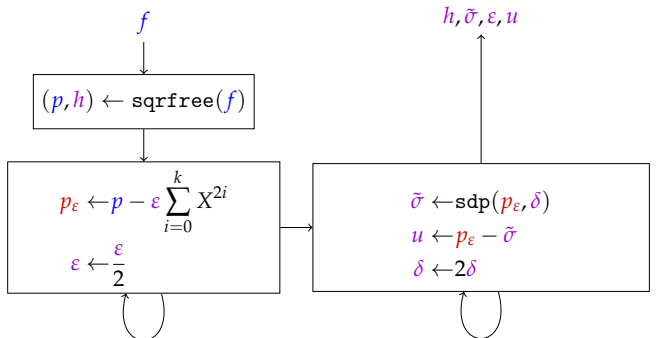
$$p = 1 + X + X^2 + X^3 + X^4$$

$$\varepsilon = \frac{1}{4}$$

$$p > \frac{1}{4}(1 + X^2 + X^4)$$

intsos with $n = 1$ and SDP Approximation

- **Input:** $f \geq 0 \in \mathbb{Q}[X]$ of degree $d \geq 2$, $\varepsilon \in \mathbb{Q}^{>0}$, $\delta \in \mathbb{N}^{>0}$
- **Output:** SOS decomposition with coefficients in \mathbb{Q}



while
 $p_\varepsilon \leq 0$

while
$$\varepsilon < \frac{|u_{2i+1}| + |u_{2i-1}|}{2} - u_{2i}$$

intsos with $n = 1$: Absorbion

$$\text{💡 } X = \frac{1}{2}[(X+1)^2 - 1 - X^2]$$

$$\text{💡 } -X = \frac{1}{2}[(X-1)^2 - 1 - X^2]$$

intsos with $n = 1$: Absorbion

$$\text{💡 } X = \frac{1}{2}[(X+1)^2 - 1 - X^2]$$

$$\text{💡 } -X = \frac{1}{2}[(X-1)^2 - 1 - X^2]$$

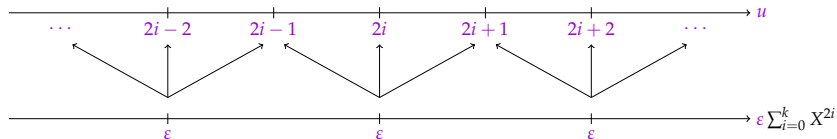
$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2} [(X^{i+1} + \text{sgn}(u_{2i+1})X^i)^2 - X^{2i} - X^{2i+2}]$$

intsos with $n = 1$: Absorbion

$$\text{💡 } X = \frac{1}{2}[(X+1)^2 - 1 - X^2]$$

$$\text{💡 } -X = \frac{1}{2}[(X-1)^2 - 1 - X^2]$$

$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2} [(X^{i+1} + \text{sgn}(u_{2i+1})X^i)^2 - X^{2i} - X^{2i+2}]$$

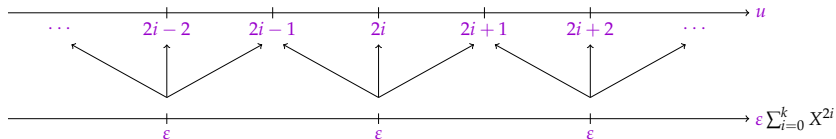


intsos with $n = 1$: Absorbion

$$\text{💡 } X = \frac{1}{2}[(X+1)^2 - 1 - X^2]$$

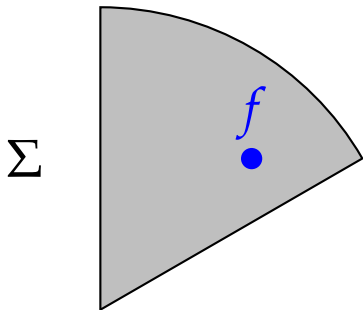
$$\text{💡 } -X = \frac{1}{2}[(X-1)^2 - 1 - X^2]$$

$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2} [(X^{i+1} + \text{sgn}(u_{2i+1})X^i)^2 - X^{2i} - X^{2i+2}]$$



$$\epsilon \geq \frac{|u_{2i+1}| + |u_{2i-1}|}{2} - u_{2i} \implies \epsilon \sum_{i=0}^k X^{2i} + u \quad \text{SOS}$$

intsos with $n \geq 1$: Perturbation



PERTURBATION idea

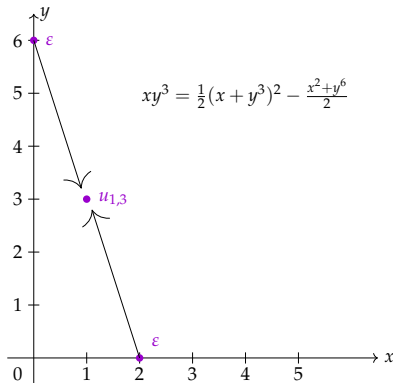
💡 Approximate SOS Decomposition

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

intsos with $n \geq 1$: Absorbion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

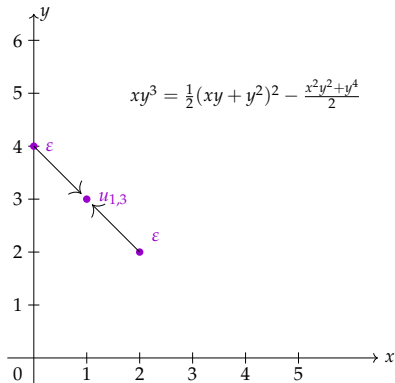
Choice of \mathcal{P} ?



intsos with $n \geq 1$: Absorbion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

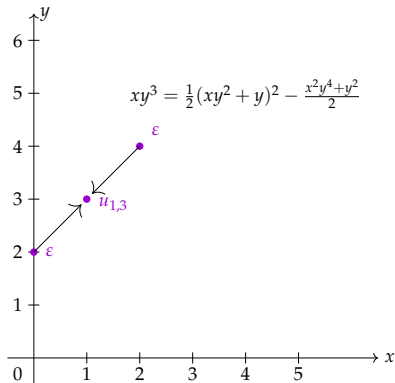
Choice of \mathcal{P} ?



intsos with $n \geq 1$: Absorbion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

Choice of \mathcal{P} ?



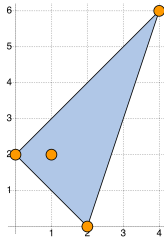
intsos with $n \geq 1$: Absorbion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

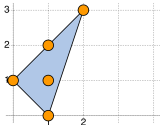
Choice of \mathcal{P} ?

$$f = 4x^4y^6 + x^2 - xy^2 + y^2$$
$$\text{spt}(f) = \{(4, 6), (2, 0), (1, 2), (0, 2)\}$$

Newton Polytope $\mathcal{P} = \text{conv}(\text{spt}(f))$

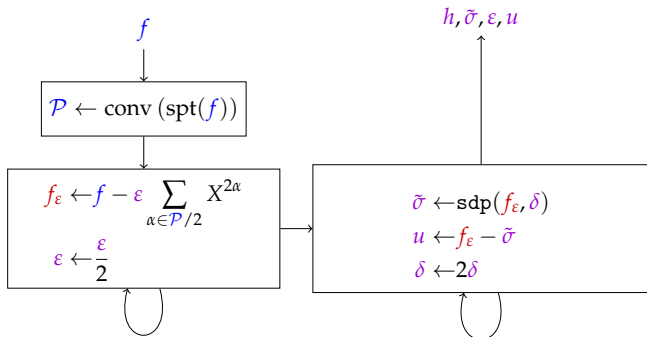


Squares in SOS decomposition $\subseteq \frac{\mathcal{P}}{2} \cap \mathbb{N}^n$
[Reznick 78]



Algorithm intsos

- **Input:** $f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ of degree d , $\varepsilon \in \mathbb{Q}^{>0}$, $\delta \in \mathbb{N}^{>0}$
- **Output:** SOS decomposition with coefficients in \mathbb{Q}



while
 $f_\varepsilon \leq 0$

while
 $u + \varepsilon \sum_{\alpha \in P/2} X^{2\alpha} \notin \Sigma$

Algorithm intsos

Theorem (Exact Certification Cost in $\mathring{\Sigma}$)

$f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ with $\deg f = d = 2k$ and bit size τ

\implies intsos terminates with SOS output of bit size $\tau d^{d^{\mathcal{O}(n)}}$

Algorithm intsos

Theorem (Exact Certification Cost in $\mathring{\Sigma}$)

$f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ with $\deg f = d = 2k$ and bit size τ

\implies intsos terminates with SOS output of bit size $\tau d^{d^{\mathcal{O}(n)}}$

Proof.

💡 # Coefficients in SOS output = $\text{size}(\mathcal{P}/2) = \binom{n+k}{n} \leq d^n$

💡 Ellipsoid algorithm for SDP [Grötschel-Lovász-Schrijver 93] \square

Deciding Non-negativity

Exact SOS Representations

Exact Reznick's Representations

Exact Putinar's Representations

Benchmarks

Conclusion and Perspectives

Algorithm Polyasos

positive definite form f has **Reznick's** representation:

$$f = \frac{\sigma}{(X_1^2 + \cdots + X_n^2)^D} \quad \text{with } \sigma \in \Sigma[X]$$

Algorithm Polyasos

positive definite form f has **Reznick's** representation:

$$f = \frac{\sigma}{(X_1^2 + \cdots + X_n^2)^D} \quad \text{with } \sigma \in \Sigma[X]$$

Theorem

$$f \cdot (X_1^2 + \cdots + X_n^2)^D \in \Sigma[X] \implies f \cdot (X_1^2 + \cdots + X_n^2)^{D+1} \in \overset{\circ}{\Sigma}[X]$$

Algorithm Polyasos

positive definite form f has **Reznick's** representation:

$$f = \frac{\sigma}{(X_1^2 + \cdots + X_n^2)^D} \quad \text{with } \sigma \in \Sigma[X]$$

Theorem

$$f \cdot (X_1^2 + \cdots + X_n^2)^D \in \Sigma[X] \implies f \cdot (X_1^2 + \cdots + X_n^2)^{D+1} \in \overset{\circ}{\Sigma}[X]$$

💡 Apply Algorithm intsos on $f \cdot (X_1^2 + \cdots + X_n^2)^{D+1}$

Algorithm Polyasos

positive definite form f has **Reznick's** representation:

$$f = \frac{\sigma}{(X_1^2 + \dots + X_n^2)^D} \quad \text{with } \sigma \in \Sigma[X]$$

Theorem

$$f \cdot (X_1^2 + \dots + X_n^2)^D \in \Sigma[X] \implies f \cdot (X_1^2 + \dots + X_n^2)^{D+1} \in \overset{\circ}{\Sigma}[X]$$

💡 Apply Algorithm `intsos` on $f \cdot (X_1^2 + \dots + X_n^2)^{D+1}$

Theorem (Exact Certification Cost of Reznick's representations)

$f \in \mathbb{Q}[X]$ positive definite form with $\deg f = d$ and bit size τ

$$\implies D \leq 2^{\tau d^{\mathcal{O}(n)}} \quad \text{OUTPUT BIT SIZE} = \boxed{2^{2^{\tau \mathcal{O}(1)} \cdot (4d+6)^{\mathcal{O}(n)}}}$$

Deciding Non-negativity

Exact SOS Representations

Exact Reznick's Representations

Exact Putinar's Representations

Benchmarks

Conclusion and Perspectives

Algorithm Putinarsos

$f > 0$ on compact $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geq 0\} \subseteq [-1, 1]^n$

Putinar's representation:

$$f = \sigma_0 + \sum_j \sigma_j g_j \quad \text{with } \sigma_j \in \Sigma[X], \deg \sigma_j \leq 2D$$

Algorithm Putinar's

$f > 0$ on compact $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geq 0\} \subseteq [-1, 1]^n$

Putinar's representation:

$$f = \sigma_0 + \sum_j \sigma_j g_j \quad \text{with } \sigma_j \in \Sigma[X], \deg \sigma_j \leq 2D$$

Theorem

$$f = \check{\sigma}_0 + \sum_j \check{\sigma}_j g_j + \sum_{|\alpha| \leq D} c_\alpha (1 - X^{2\alpha})$$

$$\text{with } \check{\sigma}_j \in \check{\Sigma}[X], \deg \check{\sigma}_j \leq 2D, c_\alpha > 0$$

Algorithm Putinarsos

$f > 0$ on compact $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geq 0\} \subseteq [-1, 1]^n$


Putinar's representation:

$$f = \sigma_0 + \sum_j \sigma_j g_j \quad \text{with } \sigma_j \in \Sigma[X], \deg \sigma_j \leq 2D$$

Theorem

$$f = \check{\sigma}_0 + \sum_j \check{\sigma}_j g_j + \sum_{|\alpha| \leq D} c_\alpha (1 - X^{2\alpha})$$

$$\text{with } \check{\sigma}_j \in \check{\Sigma}[X], \deg \check{\sigma}_j \leq 2D, c_\alpha > 0$$

 **ABSORPTION** as in Algorithm intsos:

$$u = f_\varepsilon - \check{\sigma}_0 - \sum_j \check{\sigma}_j g_j - \sum_{|\alpha| \leq D} \check{c}_\alpha (1 - X^{2\alpha})$$

Algorithm Putinarsos

$f > 0$ on compact $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geq 0\} \subseteq [-1, 1]^n$

Putinar's representation:

$$f = \sigma_0 + \sum_j \sigma_j g_j \quad \text{with } \sigma_j \in \Sigma[X], \deg \sigma_j \leq 2D$$

Theorem

$$f = \check{\sigma}_0 + \sum_j \check{\sigma}_j g_j + \sum_{|\alpha| \leq D} c_\alpha (1 - X^{2\alpha})$$

$$\text{with } \check{\sigma}_j \in \check{\Sigma}[X], \deg \check{\sigma}_j \leq 2D, c_\alpha > 0$$

💡 **ABSORPTION** as in Algorithm intsos:

$$u = f_\varepsilon - \check{\sigma}_0 - \sum_j \check{\sigma}_j g_j - \sum_{|\alpha| \leq D} \check{c}_\alpha (1 - X^{2\alpha})$$

$$\text{OUTPUT BIT SIZE} = D^{D^{\mathcal{O}(n)}} \text{ with } \log D = \mathcal{O}(2^{\tau d^n C_K})$$

Deciding Non-negativity

Exact SOS Representations

Exact Reznick's Representations

Exact Putinar's Representations

Benchmarks

Conclusion and Perspectives

RealCertify library

- Maple 16, Intel Core i7-5600U CPU (2.60 GHz)
- Averaging over five runs
- 1 Newton Polytope with `convex` Maple package [Franz 99]
- 2 arbitrary precision SDPA-GMP solver [Nakata 10] \rightsquigarrow `sdp`
- 3 Cholesky's decomposition with Maple's `LUdecomposition`

Benchmarks: Reznick

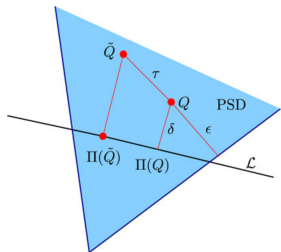
RoundProject [Peyrl-Parrilo 08]

RAGLib [Safey El Din] & CAD [Moreno Maza]

↪ exact but no certificate

Bad choice of $\varepsilon, \delta \implies$ intsos fails when

$$f \in \mathring{\Sigma}$$



Id	n	d	multivsos		RoundProject		RAGLib	CAD
			τ_1 (bits)	t_1 (s)	τ_2 (bits)	t_2 (s)	t_3 (s)	t_4 (s)
f_{20}	2	20	745 419	110.	78 949 497	141.	0.16	0.03
M	3	8	17 232	0.35	18 831	0.29	0.15	0.03
f_2	2	4	1 866	0.03	1 031	0.04	0.09	0.01
f_6	6	4	56 890	0.34	475 359	0.54	623.	—
f_1	10	4	344 347	2.45	8 374 082	4.59	—	—

Benchmarks: Nonnegative polynomials $\notin \Sigma$

S_i from Shapiro conjecture V_i from computational geometry

M_i from monotone permanent conjecture

\rightsquigarrow solved by Kaltofen, Yang & Zhi with SOS certificates

\implies **limitations** of multivsos!

Id	n	d	multivsos		RAGLib	CAD
			τ_1 (bits)	t_1 (s)	t_2 (s)	t_3 (s)
S_1	4	24	—	—	1788.	—
S_2	4	24	—	—	1840.	—
V_1	6	8	—	—	5.00	—
V_2	5	18	—	—	1180.	—
M_1	8	8	—	—	351.	—
M_2	8	8	—	—	82.0	—
M_3	8	8	—	—	120.	—
M_4	8	8	—	—	84.0	—

Benchmarks: Putinar

Id	n	d	multivsos			RAGLib	CAD
			k	τ_1 (bits)	t_1 (s)	t_2 (s)	t_3 (s)
f_{260}	6	3	2	114 642	2.72	4.19	—
f_{491}	6	3	2	108 359	9.65	6.40	0.05
f_{752}	6	2	2	10 204	0.26	0.27	—
f_{859}	6	7	4	6 355 724	303.	0.05	—
f_{863}	4	2	1	5 492	0.14	0.01	0.01
f_{884}	4	4	3	300 784	25.1	113.	—
butcher	6	3	2	247 623	1.32	231.	—
heart	8	4	2	618 847	2.94	24.7	—

Deciding Non-negativity

Exact SOS Representations

Exact Reznick's Representations

Exact Putinar's Representations

Benchmarks

Conclusion and Perspectives

Conclusion and Perspectives

SINGLY EXP ALGORITHMS in $D =$ representation degree

Conclusion and Perspectives

SINGLY EXP ALGORITHMS in D = representation degree




- 💡 Can give explicit constant $\mathcal{O}(n)$? Improve bounds on D ?
- 💡 Better arbitrary-precision SDP solvers
- 💡 When $f \in \partial\Sigma$?
- 💡 Extension to other linear/geometric/SDP relaxations

End

Thank you for your attention!

[gricad-gitlab:RealCertify](#)

<http://homepages.laas.fr/vmagron>

-  Magron, Safey El Din & Schweighofer. Algorithms for Weighted Sums of Squares Decomposition of Non-negative Univariate Polynomials, *JSC*. arxiv:1706.03941
-  Magron & Safey El Din. On Exact Polya and Putinar's Representations, *ISSAC'18*. arxiv:1802.10339
-  Magron & Safey El Din. RealCertify: a Maple package for certifying non-negativity, *ISSAC'18*. arxiv:1805.02201