On Exact Reznick & Putinar's Representations

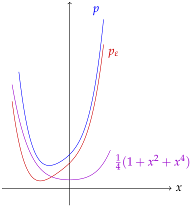
Victor Magron, CNRS

Joint work with

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

ISSAC

17th July 2018



Deciding Non-negativity

$X = (X_1, \dots, X_n)$ **co-NP hard problem: check $f \geqslant 0$ on $\mathbf{K}$**

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

Deciding Non-negativity

$X = (X_1, \ldots, X_n)$ **co-NP hard problem: check $f \geqslant 0$ on $\mathbf{K}$**

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

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

2. Constrained
$\rightsquigarrow \mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\} \quad g_j \in \mathbb{Q}[X]$

$\deg f, \deg g_j \leqslant d$

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

[Grigoriev-Vorobjov 88, Basu-Pollack-Roy 98]
Critical points **singly exponential time** $(m+1)\, \tau\, d^{\mathcal{O}(n)}$

Certifying Non-negativity

Sums of squares (SOS)

$\sigma = {h_1}^2 + \cdots + {h_p}^2$

Certifying Non-negativity

Sums of squares (SOS)

$\sigma = {h_1}^2 + \cdots + {h_p}^2$

HILBERT 17TH PROBLEM: f SOS of rational functions?

[Artin 27] **YES**!

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

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

$$f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$$
$$f \simeq \sigma = (2X_1^2 + X_1X_2 - \tfrac{8}{3}X_2^2)^2 + (\tfrac{4}{3}X_1X_2 + \tfrac{3}{2}X_2^2)^2 + (\tfrac{2}{7}X_2^2)^2$$

Certifying Non-negativity

Sums of squares (SOS)

$\sigma = {h_1}^2 + \cdots + {h_p}^2$

HILBERT 17TH PROBLEM: f SOS of rational functions?

[Artin 27] **YES**!

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

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

$f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$

$f \simeq \sigma = (2X_1^2 + X_1X_2 - \frac{8}{3}X_2^2)^2 + (\frac{4}{3}X_1X_2 + \frac{3}{2}X_2^2)^2 + (\frac{2}{7}X_2^2)^2$

$f = \sigma + \frac{8}{9}X_1^2X_2^2 - \frac{2}{3}X_1X_2^3 + \frac{983}{1764}X_2^4$

Certifying Non-negativity

💡 Sums of squares (SOS)

$\sigma = {h_1}^2 + \cdots + {h_p}^2$

HILBERT 17TH PROBLEM: f SOS of rational functions?

[Artin 27] **YES**!

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

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

$$f = 4X_1^4 + 4X_1^3 X_2 - 7X_1^2 X_2^2 - 2X_1 X_2^3 + 10X_2^4$$
$$f \simeq \sigma = (2X_1^2 + X_1 X_2 - \tfrac{8}{3} X_2^2)^2 + (\tfrac{4}{3} X_1 X_2 + \tfrac{3}{2} X_2^2)^2 + (\tfrac{2}{7} X_2^2)^2$$
$$f = \sigma + \tfrac{8}{9} X_1^2 X_2^2 - \tfrac{2}{3} X_1 X_2^3 + \tfrac{983}{1764} X_2^4$$

$$\boxed{\simeq \quad \to \quad =}$$

The Question of Exact Certification

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

Certifying Non-negativity

1. **Reznick**'s representation $f = \frac{\sigma}{(X_1 + \cdots + X_n)^{2D}}$
   positive definite form f
   [Reznick 95]

2. **Putinar**'s representation
   $f = \sigma_0 + \sigma_1 g_1 + \cdots + \sigma_m g_m$ $f > 0$ on compact K
   $\deg \sigma_i \leqslant 2D$
   [Putinar 93]

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

Hybrid **SYMBOLIC/NUMERIC** methods

[Peyrl-Parrilo 08] [Kaltofen-Yang-Zhi 08]

$\leadsto$ 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 $\deg \leqslant D$

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

Hybrid **SYMBOLIC/NUMERIC** methods

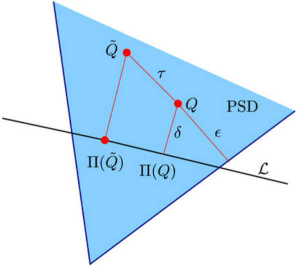
[Peyrl-Parrilo 08] [Kaltofen-Yang-Zhi 08]

$\rightsquigarrow$ 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 $\deg \leqslant D$

$$\boxed{\simeq \quad \to \quad =}$$



$\tilde{\mathbf{Q}}$ Rounding $\mathbf{Q}$ Projection $\prod(\mathbf{Q})$

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

$\prod(\mathbf{Q}) \succcurlyeq 0$ when $\varepsilon \to 0$

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

Hybrid **SYMBOLIC/NUMERIC** methods

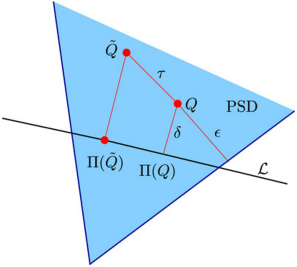
[Peyrl-Parrilo 08] [Kaltofen-Yang-Zhi 08]

$\rightsquigarrow$ 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 $\deg \leqslant D$

$$\boxed{\simeq \quad \to \quad =}$$



$\tilde{\mathbf{Q}}$ Rounding $\mathbf{Q}$ Projection $\prod(\mathbf{Q})$

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

$\prod(\mathbf{Q}) \succcurlyeq 0$ when $\varepsilon \to 0$

COMPLEXITY?

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

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 $\mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geqslant 0\}$

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

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

$\boxed{\simeq \quad \to \quad =}$

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

$\min_{\mathbf{K}} f \geqslant \varepsilon$ when $\varepsilon \to 0$

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. $f = \sum_i c_i \, {h_i}^2$?

$$\boxed{n = 1 \quad \deg f = d}$$

- $f = c_1 \, {h_1}^2 + c_2 \, {h_2}^2 + c_3 \, {h_3}^2 + c_4 \, {h_4}^2 + c_5 \, {h_5}^2$ [Pourchet 72]
- $f = c_1 \, {h_1}^2 + \cdots + c_d \, {h_d}^2$ [Schweighofer 99]
- $f = c_1 \, {h_1}^2 + \cdots + c_{d+3} \, {h_{d+3}}^2$ [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]
- $f = c_1 {h_1}^2 + \cdots + c_d {h_d}^2$ [Schweighofer 99]
- $f = c_1 {h_1}^2 + \cdots + c_{d+3} {h_{d+3}}^2$ [Chevillard et. al 11]

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

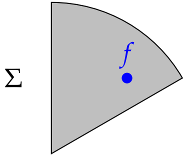
SOS with Exact LMIs $f = \mathbf{v}_d{}^T(X)\, \mathbf{G}\, \mathbf{v}_d{}^T(X)$ $\quad \mathbf{G} \succcurlyeq 0$

- 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 $\quad \deg f = d$



Complexity Question(s)

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

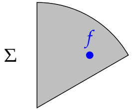
1. **Reznick**'s representation $\quad f = \frac{\sigma}{(X_1 + \cdots + X_n)^{2D}}$
   positive definite form f

2. **Putinar**'s representation
   $f = \sigma_0 + \sigma_1 \, g_1 + \cdots + \sigma_m \, g_m$
   $f > 0$ on compact $\mathbf{K}$ $\quad \deg \sigma_i \leqslant 2D$

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

Contributions

$f \in \mathbb{Q}[\mathbf{X}] \cap \mathring{\Sigma}[X]$ (interior of the SOS cone)
bit size τ $\quad \deg f = d$



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. **Putinar**'s representation — Algorithm `Putinarsos`

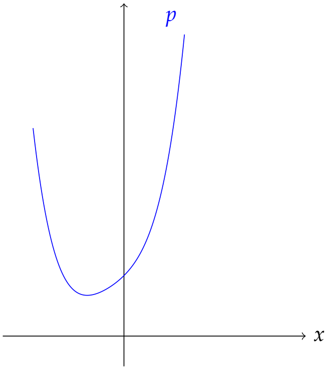
   $f > 0$ on compact $\mathbf{K}$

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

intsos with $n = 1$ and Root Approximation

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

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



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

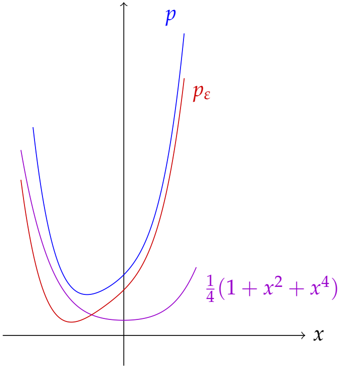
`intsos` with $n = 1$ and Root Approximation

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

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

💡 **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 Root Approximation

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

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

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

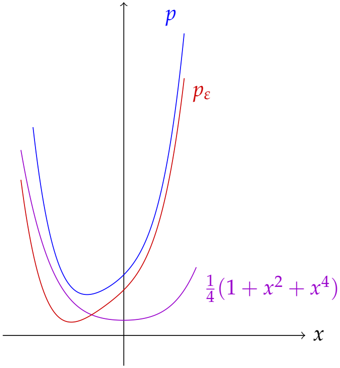
$$p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$$

Root isolation:

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

ABSORB: small enough u_i

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



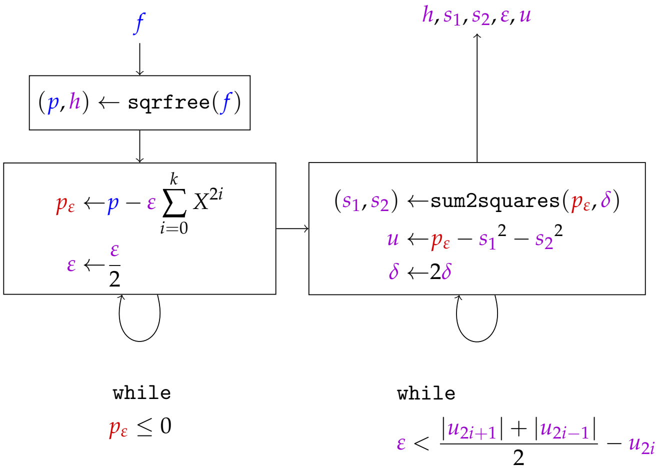
$$p = 1 + X + X^2 + X^3 + X^4$$

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

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

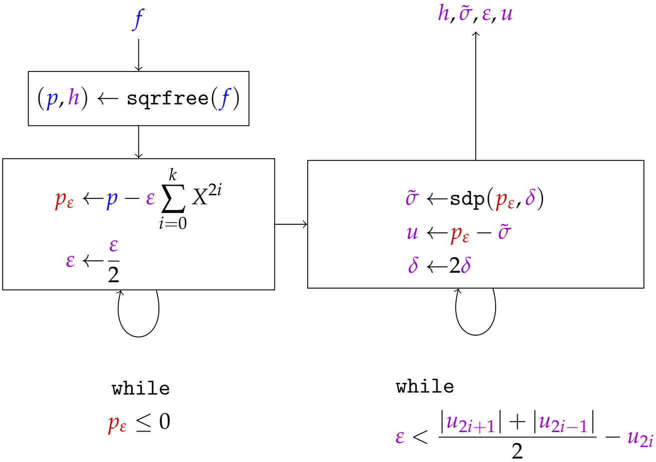
intsos with $n = 1$ and Root Approximation

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



intsos with $n = 1$ and SDP Approximation

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



intsos with $n = 1$: Absorbtion

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

`intsos` with $n = 1$: Absorbtion

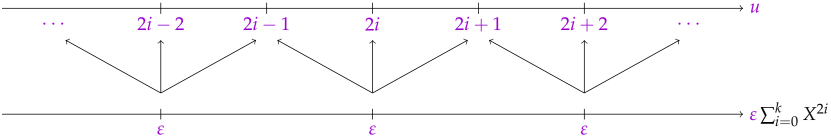
- $X = \frac{1}{2}\left[(X+1)^2 - 1 - X^2\right]$
- $-X = \frac{1}{2}\left[(X-1)^2 - 1 - X^2\right]$

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

intsos with $n = 1$: Absorbtion

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

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

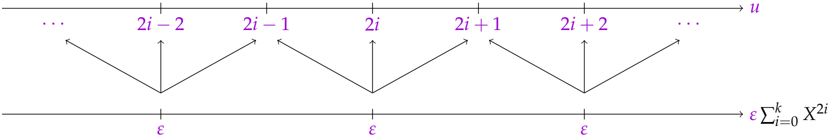


intsos with $n = 1$: Absorbtion

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

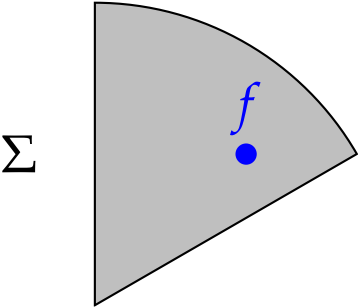
$-X = \frac{1}{2}\left[(X-1)^2 - 1 - X^2\right]$

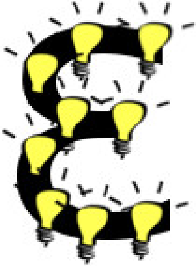
$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2}\left[(X^{i+1} + \operatorname{sgn}(u_{2i+1}) X^i)^2 - X^{2i} - X^{2i+2}\right]$$



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

intsos with $n \geqslant 1$: Perturbation





PERTURBATION idea

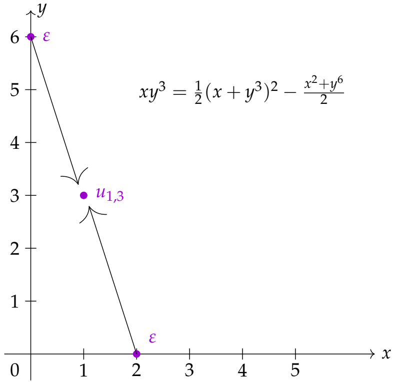
Approximate SOS Decomposition

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

intsos with $n \geqslant 1$: Absorbtion

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

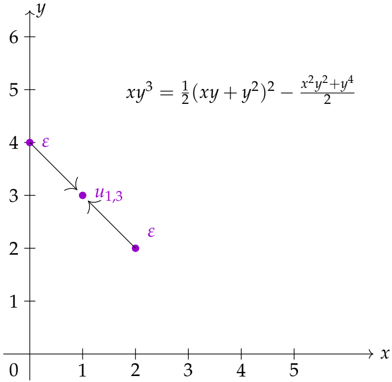
Choice of $\mathcal{P}$?



intsos with $n \geqslant 1$: Absorbtion

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

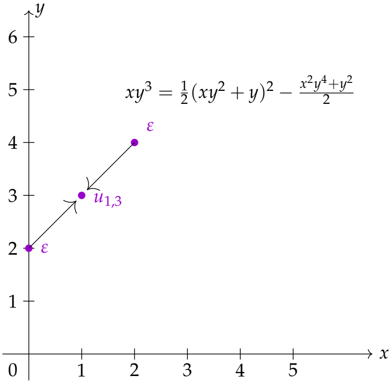
Choice of $\mathcal{P}$?



$\texttt{intsos}$ with $n \geqslant 1$: Absorbtion

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

Choice of $\mathcal{P}$?

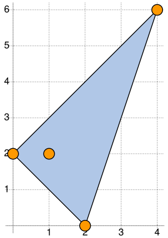


intsos with $n \geqslant 1$: Absorbtion

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

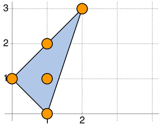
Choice of $\mathcal{P}$?

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



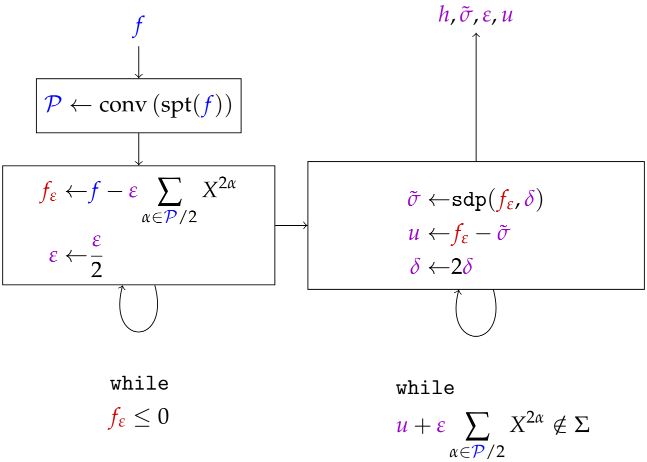
Newton Polytope $\mathcal{P} = \mathrm{conv}\,(\text{spt}(f))$

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



Algorithm `intsos`

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



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

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

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 $\boxed{\tau\, d^{d^{\mathcal{O}(n)}}}$

Proof.

- \# Coefficients in SOS output = size($\mathcal{P}/2$) = $\binom{n+k}{n} \leqslant d^n$
- Ellipsoid algorithm for SDP [Grötschel-Lovász-Schrijver 93] □

Algorithm `Polyasos`

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

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

Algorithm `Polyasos`

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

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

Theorem

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

Algorithm `Polyasos`

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

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

Theorem

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

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

Algorithm `Polyasos`

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

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

Theorem

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

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

Theorem (Exact Certification Cost of Reznick's representations)

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

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

Algorithm `Putinarsos`

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

Putinar's representation:

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

Algorithm `Putinarsos`

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

Putinar's representation:

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

Theorem

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

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

Algorithm `Putinarsos`

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

Putinar's representation:

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

Theorem

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

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

Absorbtion as in Algorithm `intsos`:

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

Algorithm `Putinarsos`

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

Putinar's representation:

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

Theorem

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

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

💡 **Absorbtion** as in Algorithm `intsos`:

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

Output Bit Size $= D^{D^{\mathcal{O}(n)}}$ with $\log D = \mathcal{O}(2^{\tau \, d^n C_{\mathbf{K}}})$

Benchmarks

RealCertify library

- Maple 16, Intel Core i7-5600U CPU (2.60 GHz 16Gb RAM)
- Averaging over five runs

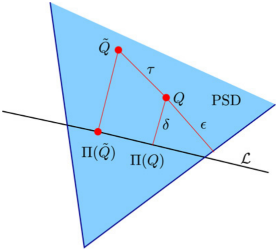
1. Newton Polytope with `convex` Maple package [Franz 99]
2. arbitrary precision SDPA-GMP solver [Nakata 10] $\rightsquigarrow$ `sdp`
3. Cholesky's decomposition with Maple's `LUDecomposition`

Benchmarks: Reznick

RoundProject [Peyrl-Parrilo 08]

RAGLib [Safey El Din] & CAD [Moreno Maza]
$\rightsquigarrow$ exact but no certificate

Bad choice of $\varepsilon, \delta \implies$ intsos fails when $f \in \mathring{\Sigma}$



Id	n	d	multivsos τ_1 (bits)	multivsos t_1 (s)	RoundProject τ_2 (bits)	RoundProject t_2 (s)	RAGLib t_3 (s)	CAD 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	598.	–
f_1	10	4	344 347	2.45	8 374 082	4.59	–	–

Benchmarks: Putinar

Id	n	d	multivsos k	multivsos τ_1 (bits)	multivsos t_1 (s)	RAGLib t_2 (s)	CAD 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	–

Conclusion and Perspectives

Input f on $\mathbf{K}$ with $\deg f = d$ and bit size τ

Algo	Input	$\mathbf{K}$	OUTPUT BIT SIZE
`intsos`	$\mathring{\Sigma}$	$\mathbb{R}^n$	$\tau\, d^{d^{\mathcal{O}\,(n)}}$

SINGLY EXP ALGORITHMS in D = representation degree

Conclusion and Perspectives

Input f on $\mathbf{K}$ with $\deg f = d$ and bit size τ

Algo	Input	$\mathbf{K}$	OUTPUT BIT SIZE
`intsos`	$\mathring{\Sigma}$	$\mathbb{R}^n$	$\tau\, d^{d^{\mathcal{O}(n)}}$

SINGLY EXP ALGORITHMS in D = representation degree

- In practice, explain why `intsos` fails when $f \in \mathring{\Sigma}$
- Better arbitrary-precision SDP solvers

End

Thank you for your attention!

gricad-gitlab:RealCertify

http://www-verimag.imag.fr/~magron

- 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