On Exact Polynomial Optimization

Victor Magron, CNRS

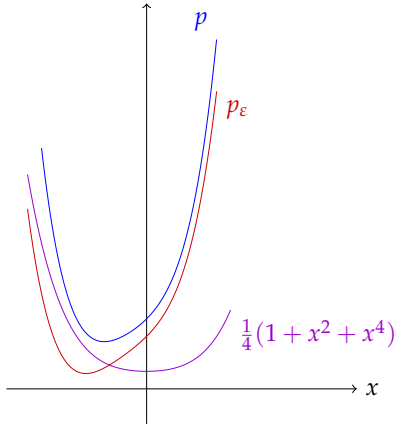
Joint work with

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

Markus Schweighofer (Konstanz University)

Institut für Mathematik, TU Berlin

25th April 2018



Certify Polynomial Non-negativity

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

co-NP hard problem: decide if $f \geqslant 0$ on $\mathbf{K}$

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

Certify Polynomial Non-negativity

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

co-NP hard problem: decide if $f \geqslant 0$ on $\mathbf{K}$

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

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

2. Constrained $\rightsquigarrow \mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geqslant 0\}$ $\qquad g_j \in \mathbb{R}[X]$

 [Collins 75]  Quantifier elimination

 [Basu-Pollack-Roy 98]  CAD **Decide in simply exp. time**

Certify Polynomial Non-negativity

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

co-NP hard problem: decide if $f \geqslant 0$ on $\mathbf{K}$

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

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

2. Constrained $\rightsquigarrow \mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geqslant 0\}$ $\qquad g_j \in \mathbb{R}[X]$

 [Collins 75]  Quantifier elimination

 [Basu-Pollack-Roy 98]  CAD **Decide in simply exp. time**

 Sums of squares (SOS) $\qquad \sigma = {h_1}^2 + \cdots + {h_p}^2$

Certify Polynomial Non-negativity

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

co-NP hard problem: decide if $f \geqslant 0$ on $\mathbf{K}$

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

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

2. Constrained $\rightsquigarrow \mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geqslant 0\}$ $\qquad g_j \in \mathbb{R}[X]$

 [Collins 75]  Quantifier elimination

 [Basu-Pollack-Roy 98]  CAD **Decide in simply exp. time**

 Sums of squares (SOS) $\qquad \sigma = {h_1}^2 + \cdots + {h_p}^2$

HILBERT 17TH PROBLEM: f SOS of rational functions?

 [Artin 27] **YES**!

Motivation

Positivity certificates

- Stability proofs of critical control systems (Lyapunov)
- Certified function evaluation [Chevillard et. al 11]
- Formal verification of real inequalities [Hales et. al 15]:

 COQ  HOL-LIGHT

Certify with SOS Representations

1. **Reznick**'s representation (positive definite forms) [Reznick 95]

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

2. **Putinar**'s representation ($f > 0$ + **K** compact) [Putinar 93]

$$f = \sigma_0 + \sigma_1\, g_1 + \cdots + \sigma_m\, g_m$$
$$\deg \sigma_i \leqslant 2D$$

The Question(s): $n = 1$

- Let $f \in \mathbb{R}[X]$ and $f \geqslant 0$ on $\mathbb{R}$

Theorem [Hilbert 1888]

There exist $f_1, f_2 \in \mathbb{R}[X]$ s.t. $f = {f_1}^2 + {f_2}^2$.

The Question(s): $n = 1$

- Let $f \in \mathbb{R}[X]$ and $f \geqslant 0$ on $\mathbb{R}$

Theorem [Hilbert 1888]

There exist $f_1, f_2 \in \mathbb{R}[X]$ s.t. $f = {f_1}^2 + {f_2}^2$.

Proof.

$f = h^2(q + ir)(q - ir)$ □

The Question(s): $n = 1$

- Let $f \in \mathbb{R}[X]$ and $f \geqslant 0$ on $\mathbb{R}$

Theorem [Hilbert 1888]

There exist $f_1, f_2 \in \mathbb{R}[X]$ s.t. $f = {f_1}^2 + {f_2}^2$.

Proof.

$f = h^2(q + ir)(q - ir)$ □

Examples

$$1 + X + X^2 = \left(X + \frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2$$

$$1 + X + X^2 + X^3 + X^4 = \left(X^2 + \frac{1}{2}X + \frac{1+\sqrt{5}}{4}\right)^2 + \left(\frac{\sqrt{10+2\sqrt{5}} + \sqrt{10-2\sqrt{5}}}{4}X + \frac{\sqrt{10-2\sqrt{5}}}{4}\right)^2$$

The Question(s): $n = 1$

- $f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ (interior of the SOS cone) with bit size τ

Existence Question

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

The Question(s): $n = 1$

- $f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ (interior of the SOS cone) with bit size τ

Existence Question

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

Examples

$$1 + X + X^2 = \left(X + \frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2 = 1\left(X + \frac{1}{2}\right)^2 + \frac{3}{4}(1)^2$$

$$1 + X + X^2 + X^3 + X^4 = \left(X^2 + \frac{1}{2}X + \frac{1+\sqrt{5}}{4}\right)^2 + \left(\frac{\sqrt{10+2\sqrt{5}} + \sqrt{10-2\sqrt{5}}}{4}X + \frac{\sqrt{10-2\sqrt{5}}}{4}\right)^2 = ???$$

The Question(s): $n \geqslant 1$

[Lasserre/Parrilo 01] **Numerical** solvers compute σ_i
Semidefinite programming (SDP) $\rightsquigarrow$ **approximate** certificates

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

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

The Question(s): $n \geqslant 1$


[Lasserre/Parrilo 01] **Numerical** solvers compute σ_i
Semidefinite programming (SDP) $\rightsquigarrow$ **approximate** certificates

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

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

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

The Question(s): $n \geqslant 1$

[Lasserre/Parrilo 01] **Numerical** solvers compute σ_i
Semidefinite programming (SDP) $\rightsquigarrow$ **approximate** certificates

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

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

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

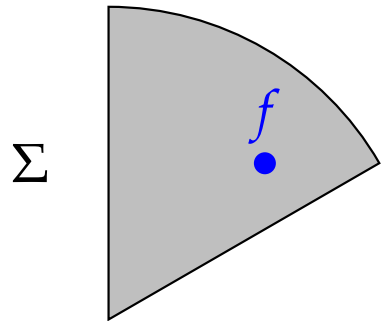
$$\boxed{\simeq \quad \rightarrow \quad =}$$

The Question of Exact Certification

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

The Question(s): $n \geqslant 1$

$f \in \mathbb{Q}[\mathbf{X}] \cap \mathring{\Sigma}[X]$ (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 (positive definite forms)
   $$f = \frac{\sigma}{(X_1+\cdots+X_n)^{2D}}$$

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

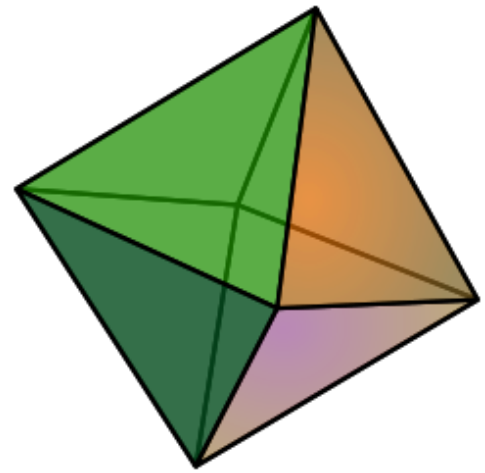
   Bounds on D, $\tau(\sigma_i)$?

SDP for Polynomial Optimization

- Linear Programming (LP):

$$\min_{\mathbf{z}} \quad \mathbf{c}^\top \mathbf{z}$$
$$\text{s.t.} \quad \mathbf{A}\,\mathbf{z} \geqslant \mathbf{d} \ .$$

  - Linear cost $\mathbf{c}$
  - Linear inequalities "$\sum_i A_{ij} z_j \geqslant d_i$"

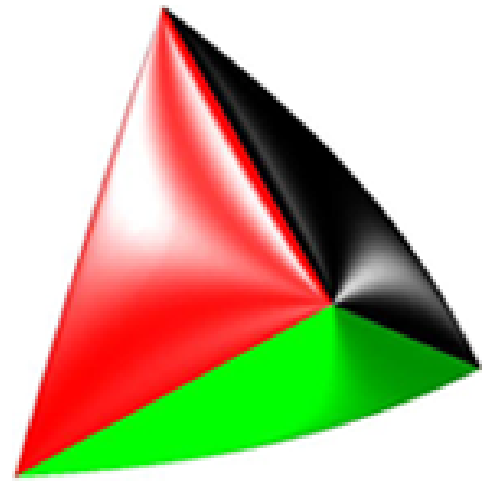


Polyhedron

SDP for Polynomial Optimization

- Semidefinite Programming (SDP):

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



Spectrahedron

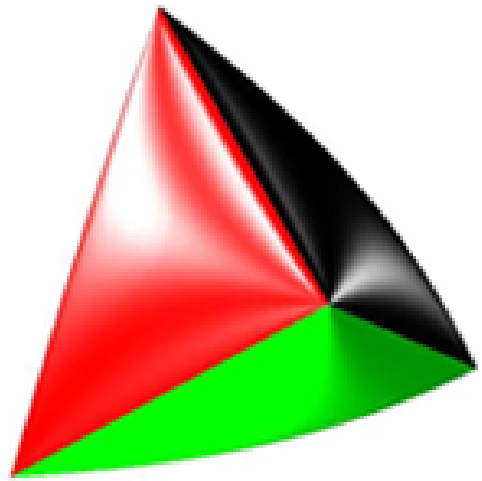
  - Linear cost $\mathbf{c}$
  - Symmetric matrices $\mathbf{F}_0, \mathbf{F}_i$
  - Linear matrix inequalities "$\mathbf{F} \succcurlyeq 0$" ($\mathbf{F}$ has non-negative eigenvalues)

SDP for Polynomial Optimization

- Semidefinite Programming (SDP):

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

  - Linear cost $\mathbf{c}$
  - Symmetric matrices $\mathbf{F}_0, \mathbf{F}_i$
  - Linear matrix inequalities "$\mathbf{F} \succcurlyeq 0$" ($\mathbf{F}$ has non-negative eigenvalues)



Spectrahedron

SDP for Polynomial Optimization

- Prove **polynomial inequalities** with SDP:

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

- Find $\mathbf{z}$ s.t.

$$f(a,b) = \begin{pmatrix} a & b \end{pmatrix} \underbrace{\begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix}}_{\succcurlyeq 0} \begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{v}_1{}^T(a,b)\, \mathbf{Q}\, \mathbf{v}_1(a,b)\,.$$

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

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

SDP for Polynomial Optimization

- 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)

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

- Solving **SDP** $\Longrightarrow$ Finding **SUMS OF SQUARES** certificates

SDP for Polynomial Optimization

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

- Semialgebraic set
  $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

SDP for Polynomial Optimization

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

- Semialgebraic set
  $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

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

SDP for Polynomial Optimization

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

- Semialgebraic set
  $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

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

$$\overbrace{x_1 x_2}^{f} + \frac{1}{8} = \overbrace{\frac{1}{2}\left(x_1 + x_2 - \frac{1}{2}\right)^2}^{\sigma_0} + \overbrace{\frac{1}{2}}^{\sigma_1} \overbrace{x_1(1-x_1)}^{g_1} + \overbrace{\frac{1}{2}}^{\sigma_2} \overbrace{x_2(1-x_2)}^{g_2}$$

SDP for Polynomial Optimization

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

- Semialgebraic set
  $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

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

$$\overbrace{x_1 x_2}^{f} + \frac{1}{8} = \overbrace{\frac{1}{2}\left(x_1 + x_2 - \frac{1}{2}\right)^2}^{\sigma_0} + \overbrace{\frac{1}{2}}^{\sigma_1} \overbrace{x_1(1-x_1)}^{g_1} + \overbrace{\frac{1}{2}}^{\sigma_2} \overbrace{x_2(1-x_2)}^{g_2}$$

- Sums of squares (SOS) σ_i

SDP for Polynomial Optimization

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

- Semialgebraic set
  $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

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

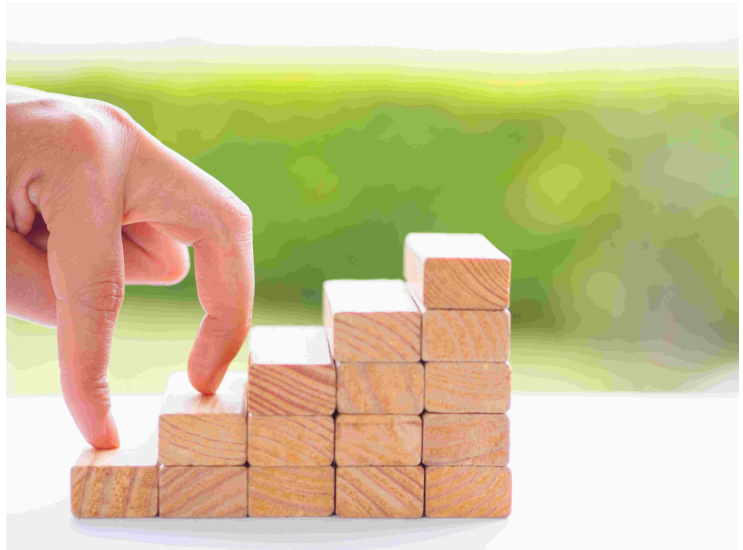
$$\overbrace{x_1 x_2}^{f} + \frac{1}{8} = \overbrace{\frac{1}{2}\left(x_1 + x_2 - \frac{1}{2}\right)^2}^{\sigma_0} + \overbrace{\frac{1}{2}}^{\sigma_1} \overbrace{x_1(1-x_1)}^{g_1} + \overbrace{\frac{1}{2}}^{\sigma_2} \overbrace{x_2(1-x_2)}^{g_2}$$

- Sums of squares (SOS) σ_i

- Bounded degree:
  $\mathcal{Q}_k(\mathbf{K}) := \left\{ \sigma_0 + \sum_{j=1}^m \sigma_j g_j, \text{ with } \deg \sigma_j g_j \leqslant 2k \right\}$

SDP for Polynomial Optimization

- **Hierarchy of SDP relaxations**:
  $\lambda_k := \sup_{\lambda} \left\{ \lambda : f - \lambda \in \mathcal{Q}_k(\mathbf{K}) \right\}$



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

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

Hybrid **SYMBOLIC/NUMERIC** methods

 [Peyrl-Parrilo 08] [Kaltofen et. al 08]

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

$$0 \preccurlyeq \tilde{\mathbf{Q}} \in \mathbb{R}^{D \times D}$$

$$\mathbf{v}_D(X) = (1, X_1, \ldots, X_n, X_1^2, \ldots, X_n^D)$$

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

Hybrid **SYMBOLIC/NUMERIC** methods

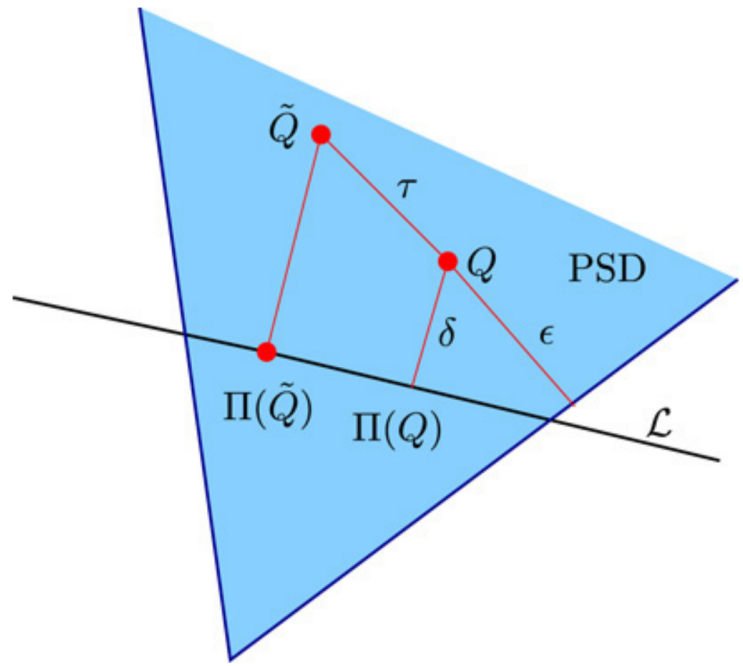
[Peyrl-Parrilo 08] [Kaltofen et. al 08]

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

$$0 \preccurlyeq \tilde{\mathbf{Q}} \in \mathbb{R}^{D \times D}$$

$$\mathbf{v}_D(X) = (1, X_1, \ldots, X_n, X_1^2, \ldots, X_n^D)$$

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



$\tilde{\mathbf{Q}}$ 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 $\varepsilon \rightarrow 0$

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

Hybrid **SYMBOLIC/NUMERIC** methods

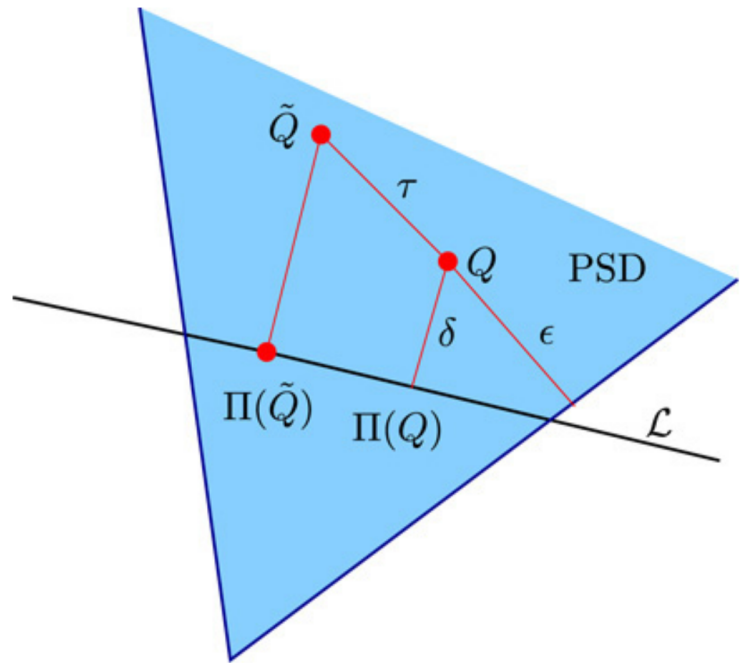
[Peyrl-Parrilo 08] [Kaltofen et. al 08]

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

$$0 \preccurlyeq \tilde{\mathbf{Q}} \in \mathbb{R}^{D \times D}$$

$$\mathbf{v}_D(X) = (1, X_1, \ldots, X_n, X_1^2, \ldots, X_n^D)$$

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



$\tilde{\mathbf{Q}}$ 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 $\varepsilon \rightarrow 0$

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

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

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

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

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

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

COMPLEXITY?

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

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

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

- $f = c_1 \, {h_1}^2 + c_2 \, {h_2}^2 + c_3 \, {h_3}^2 + c_4 \, {h_4}^2 + c_5 \, {h_5}^2$ [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]

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

- SOS with Exact LMIs $f(X) = \mathbf{v}_d{}^T(X) \, \mathbf{G} \, \mathbf{v}_d{}^T(X) \qquad \mathbf{G} \succcurlyeq 0$
- Critical point methods [Greuet et. al 11]
- CAD [Iwane 13] $\rightsquigarrow \tau d^{\mathcal{O}(n)}$
- Solving over the rationals [Guo et. al 13]
- Determinantial varieties [Henrion et. al 16]

Contribution: $n = 1$

- $f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ (interior of the SOS cone) with bit size τ

Existence Question

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

Complexity Question

What is the output bitsize of $\sum_i c_i f_i^2$?

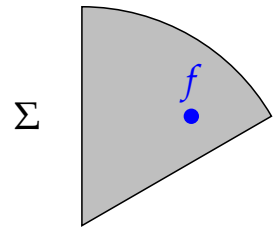
Contribution: $n = 1$

Two methods answering the questions:

- $f = c_1 {h_1}^2 + \cdots + c_d {h_d}^2$ [Schweighofer 99]
  $\rightsquigarrow$ Algorithm `univsos1` with output size $\tau_1 = \mathcal{O}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}} \tau\right)$
- $f = c_1 {h_1}^2 + \cdots + c_{d+3} {h_{d+3}}^2$ [Chevillard et. al 11]
  $\rightsquigarrow$ Algorithm `univsos2` with output size $\tau_2 = \mathcal{O}\left(d^4 \tau\right)$
  - Maple package `https://github.com/magronv/univsos`

Contribution: $n \geqslant 1$

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



Complexity Cost

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

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

Algorithm `Polyasos` $\rightsquigarrow$ **OUTPUT BIT SIZE** $= 2^{2^{\tau^{\mathcal{O}(1)}\cdot(4d+6)^{\mathcal{O}(n)}}}$

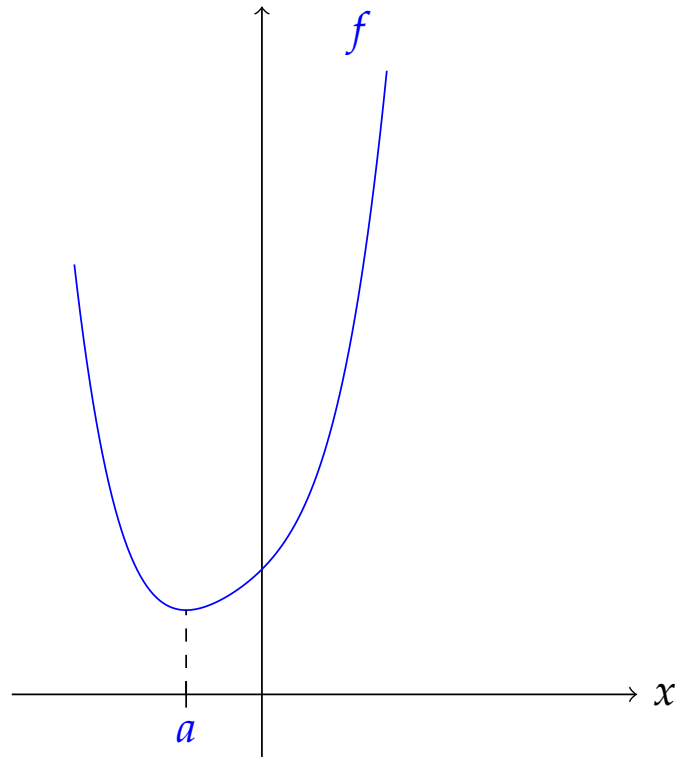
2. **Putinar**'s representation ($f > 0$ + $\mathbf{K}$ compact)
$$f = \sigma_0 + \sigma_1\, g_1 + \cdots + \sigma_m\, g_m \qquad \deg \sigma_i \leqslant 2D$$

Algorithm `Putinarsos` $\rightsquigarrow$

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

univsos1: Outline [Schweighofer 99]

$f \in \mathbb{Q}[X]$ and $f > 0$
Minimizer a may not be in $\mathbb{Q}$ . . .



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

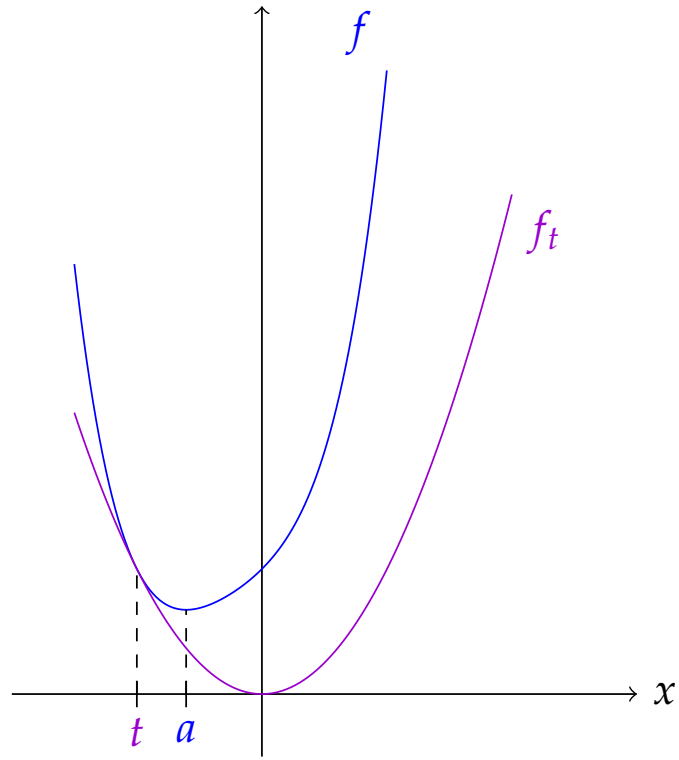
$$a = \frac{5}{4(135+60\sqrt{6})^{1/3}} - \frac{4(135+60\sqrt{6})^{1/3}}{12} - \frac{1}{4}$$

univsos1: Outline [Schweighofer 99]

$f \in \mathbb{Q}[X]$ and $f > 0$
Minimizer a may not be in $\mathbb{Q}$ . . .

Find $f_t \in \mathbb{Q}[X]$ s.t. :

- $\deg f_t \leqslant 2$
- $f_t \geqslant 0$
- $f \geqslant f_t$
- $f - f_t$ has a root $t \in \mathbb{Q}$



$f = 1 + X + X^2 + X^3 + X^4$
$a = \frac{5}{4(135+60\sqrt{6})^{1/3}} - \frac{4(135+60\sqrt{6})^{1/3}}{12} - \frac{1}{4}$
$f_t = X^2$
$t = -1$

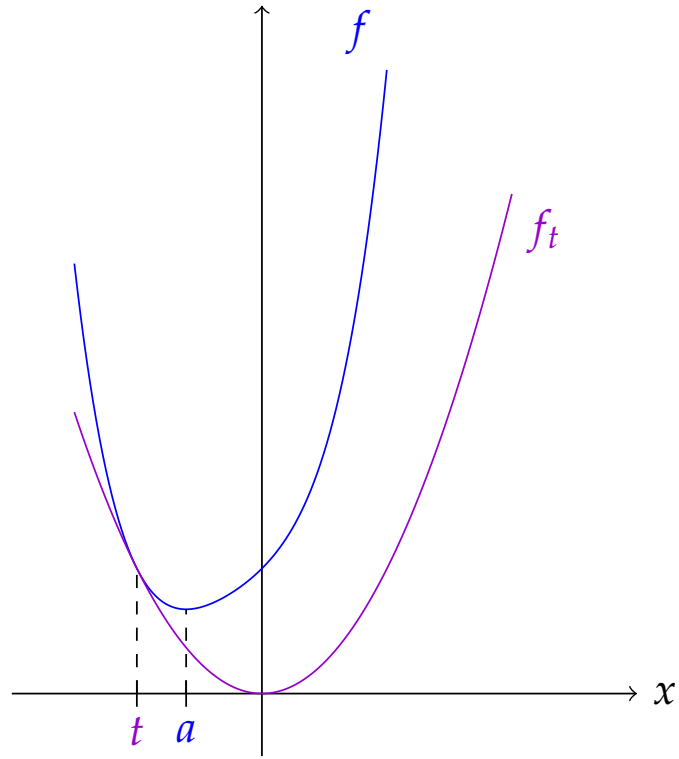
univsos1: Outline [Schweighofer 99]

$f \in \mathbb{Q}[X]$ and $f > 0$
Minimizer a may not be in $\mathbb{Q}$ ...

Square-free decomposition:

$$f - f_t = gh^2$$

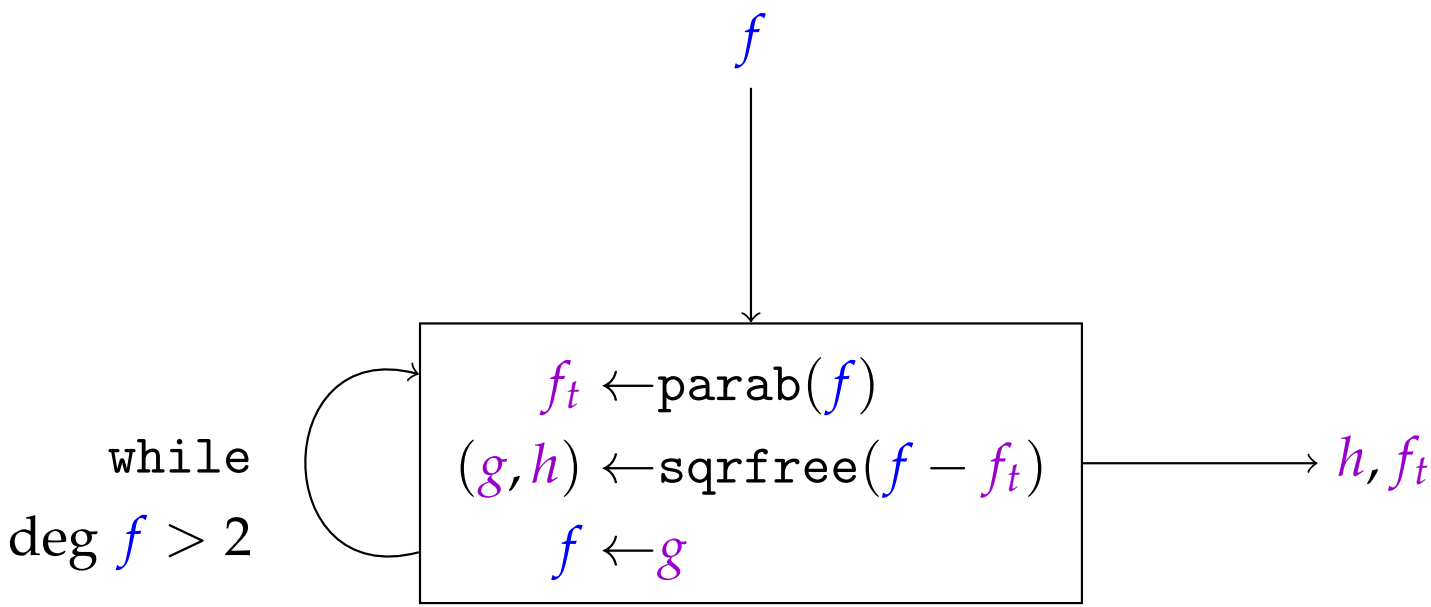
- $\deg g \leqslant \deg f - 2$
- $g > 0$
- Do it again on g



$f = 1 + X + X^2 + X^3 + X^4$
$f_t = X^2$
$f - f_t = (X^2 + 2X + 1)(X + 1)^2$

univsos1: Algorithm [Schweighofer 99]

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



univsos1: Local Inequality

Lemma [Schweighofer 99]

$$f > 0, \quad f_t := f(t) + f'(t)(X - t) + \frac{f'(t)^2}{4\,f(t)}(X - t)^2 \in \mathbb{Q}[X]\,.$$

$$\exists \text{ neighborhood } U \text{ of local min } a \text{ s.t.}$$

$$f_t(x) \leqslant f(x) \quad \forall\, t, x \in U$$

univsos1: Local Inequality

Lemma [Schweighofer 99]

$$f > 0, \quad f_t := f(t) + f'(t)(X - t) + \frac{f'(t)^2}{4\,f(t)}(X - t)^2 \in \mathbb{Q}[X]\,.$$

$$\exists \text{ neighborhood } U \text{ of local min } a \text{ s.t.}$$

$$f_t(x) \leqslant f(x) \quad \forall\, t, x \in U$$

Proof.

$\boxed{d = 2}$ Rolle's Theorem

$\boxed{d \geqslant 4}$ Taylor decomposition of f at t

□

`univsos1`: Global Inequality

Lemma [Schweighofer 99]

$$f > 0, \quad f_t := f(t) + f'(t)(X-t) + \frac{f'(t)^2}{4\,f(t)}(X-t)^2 \in \mathbb{Q}[X]\,.$$

$\exists$ neighborhood U of smallest global min a s.t.

$$f_t(x) \leqslant f(x) \quad \forall\, t \in U\,, \quad \forall\, x \in \mathbb{R}$$

univsos1: Global Inequality

Lemma [Schweighofer 99]

$$f > 0, \quad f_t := f(t) + f'(t)(X - t) + \frac{f'(t)^2}{4f(t)}(X - t)^2 \in \mathbb{Q}[X]\,.$$

$$\exists \text{ neighborhood } U \text{ of smallest global min } a \text{ s.t.}$$

$$f_t(x) \leqslant f(x) \quad \forall\, t \in U\,, \quad \forall\, x \in \mathbb{R}$$

Proof.

$\boxed{d = 2}$ $\quad f_t'' = \frac{f'(t)^2}{2f(t)}$

- Taylor Decomposition of f at t
- Negative discriminant of f: $f'(t)^2 - 4f(t)\frac{f''(t)}{2} < 0$

□

univsos1: Global Inequality

Lemma [Schweighofer 99]

$$f > 0, \quad f_t := f(t) + f'(t)(X-t) + \frac{f'(t)^2}{4f(t)}(X-t)^2 \in \mathbb{Q}[X]\,.$$

$$\exists \text{ neighborhood } U \text{ of smallest global min } a \text{ s.t.}$$

$$f_t(x) \leqslant f(x) \quad \forall\, t \in U\,, \quad \forall\, x \in \mathbb{R}$$

Proof.

$\boxed{d \geqslant 4}$ $f - f_t = \sum_{i=0}^{n} a_{it} X^i$ $U = [a-\epsilon, a+\epsilon]$ (Local Ineq)

Cauchy bound: $C_t := \max\left\{1, \frac{|a_{0t}|}{|a_{dt}|}, \ldots, \frac{|a_{(d-1)t}|}{|a_{dt}|}\right\} \leqslant C$

Smallest global min a:

$\rightsquigarrow$ 5 cases $(-\infty, C]$ $[-C, a-\epsilon]$ $[a-\epsilon, a)$ $[a, C)$ $[C, \infty)$

`univsos1`: Nichtnegativstellensätz

Theorem [Schweighofer 99]

Let $f \in \mathbb{Q}[X]$, $\deg f = d$.

$$f \geqslant 0 \text{ on } \mathbb{R} \Leftrightarrow \exists c_i \in \mathbb{Q}^{\geqslant 0}, f_i \in \mathbb{Q}[X] \text{ s.t. } f = c_1 {f_1}^2 + \cdots + c_d {f_d}^2$$

univsos1: Nichtnegativstellensätz

Theorem [Schweighofer 99]

Let $f \in \mathbb{Q}[X]$, $\deg f = d$.

$$f \geqslant 0 \text{ on } \mathbb{R} \Leftrightarrow \exists c_i \in \mathbb{Q}^{\geqslant 0}, f_i \in \mathbb{Q}[X] \text{ s.t. } f = c_1 {f_1}^2 + \cdots + c_d {f_d}^2$$

Proof by induction.

$\boxed{d = 2}$

$$f = a_2 X^2 + a_1 X + a_0 = a_2 (X + \tfrac{a_1}{2a_2})^2 + (a_0 - \tfrac{{a_1}^2}{4a_2})$$

Discriminant ${a_1}^2 - 4\, a_2\, a_0 \leqslant 0$

□

univsos1: Nichtnegativstellensätz

Theorem [Schweighofer 99]

Let $f \in \mathbb{Q}[X]$, $\deg f = d$.

$$f \geqslant 0 \text{ on } \mathbb{R} \Leftrightarrow \exists c_i \in \mathbb{Q}^{\geqslant 0}, f_i \in \mathbb{Q}[X] \text{ s.t. } f = c_1 {f_1}^2 + \cdots + c_d {f_d}^2$$

Proof by induction.

$\boxed{d \geqslant 4}$

- f not square-free $\implies f = g\, h^2$
- f square-free $\implies f > 0, \exists f_t \geqslant 0$ s.t. $f - f_t = g\,(X - t)^2$

□

`univsos1`: Bitsize of t

Lemma

Let $0 < f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.

Let $t \in \mathbb{Q}$, $f_t := f(t) + f'(t)(X-t) + \frac{f'(t)^2}{4f(t)}(X-t)^2$ s.t. $f - f_t > 0$.

Then

$$\tau(t) = \mathcal{O}\left(d^2\tau\right)$$

`univsos1`: Bitsize of t

Lemma

Let $0 < f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.
Let $t \in \mathbb{Q}$, $f_t := f(t) + f'(t)(X-t) + \frac{f'(t)^2}{4f(t)}(X-t)^2$ s.t. $f - f_t > 0$.
Then

$$\tau(t) = \mathcal{O}\left(d^2\tau\right)$$

Proof.

Bitsize B of polynomials describing:

$$\{t \in \mathbb{Q} \mid \forall x \in \mathbb{R}, f(t)^2 + f'(t)f(t)(x-t) + f'(t)^2(x-t)^2 \leqslant 4f(t)f(x)\}$$

Quantifier elimination/CAD [BPR 06]: $B = \mathcal{O}\left(d^2\tau\right)$

□

univsos1: Bitsize of Square-free Part

Lemma

Let $0 < f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.
Let $t \in \mathbb{Q}$, $f_t := f(t) + f'(t)(X-t) + \frac{f'(t)^2}{4f(t)}(X-t)^2$ s.t. $f - f_t > 0$.
Then

$$\exists\, \hat{f}, \hat{f}_t, g \in \mathbb{Z}[X] \text{ s.t. } \hat{f} - \hat{f}_t = (X-t)^2 g$$
$$\tau(f_t) = \tau(g) = \mathcal{O}\left(d^3\tau\right)$$

`univsos1`: Bitsize of Square-free Part

Lemma

Let $0 < f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.
Let $t \in \mathbb{Q}$, $f_t := f(t) + f'(t)(X-t) + \frac{f'(t)^2}{4f(t)}(X-t)^2$ s.t. $f - f_t > 0$.
Then

$$\exists\, \hat{f}, \hat{f}_t, g \in \mathbb{Z}[X] \text{ s.t. } \hat{f} - \hat{f}_t = (X-t)^2 g$$
$$\tau(f_t) = \tau(g) = \mathcal{O}(d^3\tau)$$

Proof.

$$t = \frac{t_1}{t_2} \quad \hat{f} := t_2^{2d} f(t) f(X) \quad \hat{f}_t := t_2^{2d} f(t) f_t(X)$$

Square-free part: $\tau(g) \leqslant d - 2 + \tau(\hat{f} - \hat{f}_t) + \log_2(d+1)$

`univsos1`: Output Bitsize

Theorem

Let $0 < f \in \mathbb{Q}[X]$ with bitsize τ, $\deg f = d$.
The output bitsize τ_1 of `univsos1` on f is $\mathcal{O}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}}\tau\right)$.

`univsos1`: Output Bitsize

Theorem

Let $0 < f \in \mathbb{Q}[X]$ with bitsize τ, $\deg f = d$.
The output bitsize τ_1 of `univsos1` on f is $\mathcal{O}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}}\tau\right)$.

Proof.

- Worst-case: $k = d/2$ induction steps

$$\Longrightarrow \quad \tau_1 = \mathcal{O}\left(\tau + k^3\tau + (k-1)^3k^3\tau + \cdots + (k!)^3\tau\right)$$

□

`univsos1`: Bit Complexity

Theorem

Let $0 < f \in \mathbb{Q}[X]$ with bitsize τ, $\deg f = d$.

The bit complexity of `univsos1` on f is $\widetilde{\mathcal{O}}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}}\tau\right)$.

`univsos1`: Bit Complexity

Theorem

Let $0 < f \in \mathbb{Q}[X]$ with bitsize τ, $\deg f = d$.

The bit complexity of `univsos1` on f is $\widetilde{\mathcal{O}}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}}\tau\right)$.

All involved polynomials have a global min in $\mathbb{Z}$

$\Longrightarrow$ the bit complexity is $\widetilde{\mathcal{O}}\left(d^4 + d^3\tau\right)$.

`univsos1`: Bit Complexity

Theorem

Let $0 < f \in \mathbb{Q}[X]$ with bitsize τ, $\deg f = d$.

The bit complexity of `univsos1` on f is $\widetilde{\mathcal{O}}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}}\tau\right)$.

All involved polynomials have a global min in $\mathbb{Z}$

$\Longrightarrow$ the bit complexity is $\widetilde{\mathcal{O}}\left(d^4 + d^3\tau\right)$.

Proof.

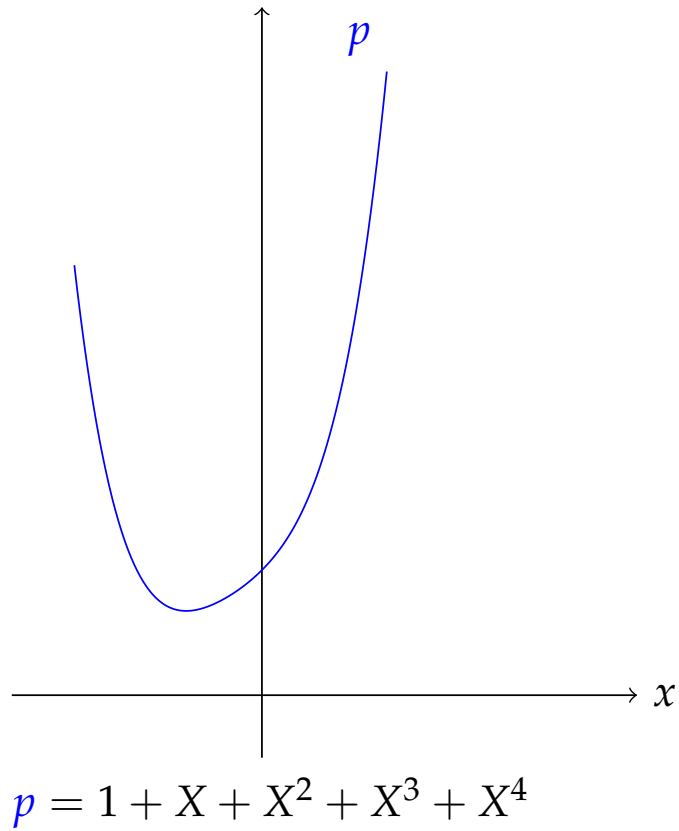
- Root bitsize: $\tau(t) = \mathcal{O}(\tau)$
- Square-free part: $\tau(g) = \mathcal{O}(d + \tau(f - f_t)) = \mathcal{O}(d + \tau)$
- Output bisize: $\tau_1 = \mathcal{O}(d^3 + d\tau)$

□

univsos2: Outline [Chevillard et. al 11]

Algorithm from [Chevillard et. al 11]

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



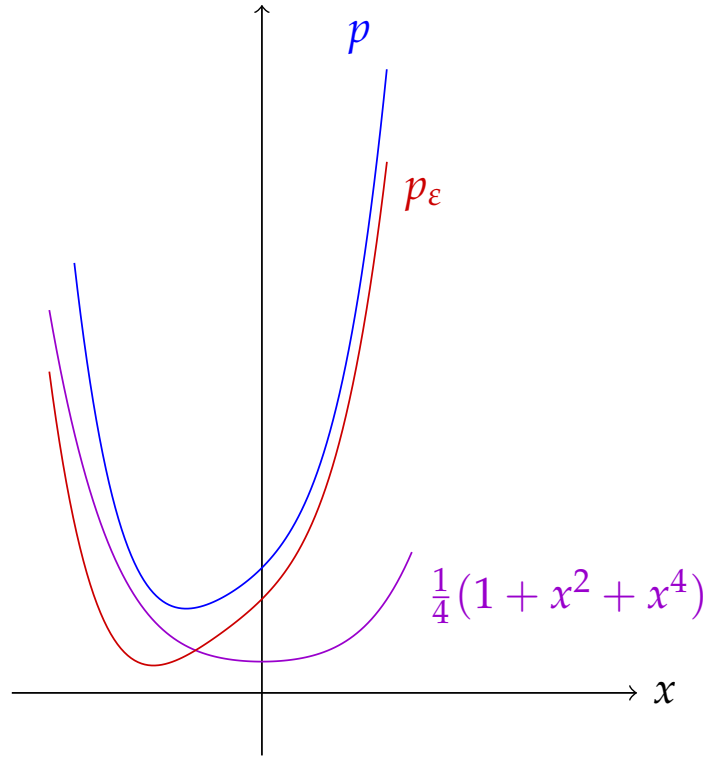
univsos2: Outline [Chevillard et. al 11]

Algorithm from [Chevillard et. al 11]

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

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

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



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

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

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

`univsos2`: Outline [Chevillard et. al 11]

Algorithm from [Chevillard et. al 11]

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

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

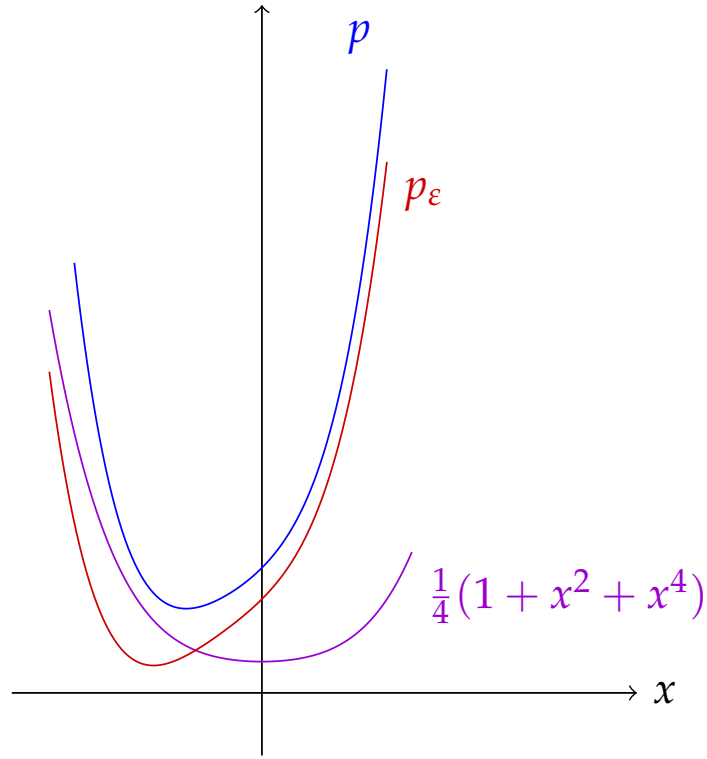
$$p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$$

- Root isolation:

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

- **ABSORB**: small enough u_i

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



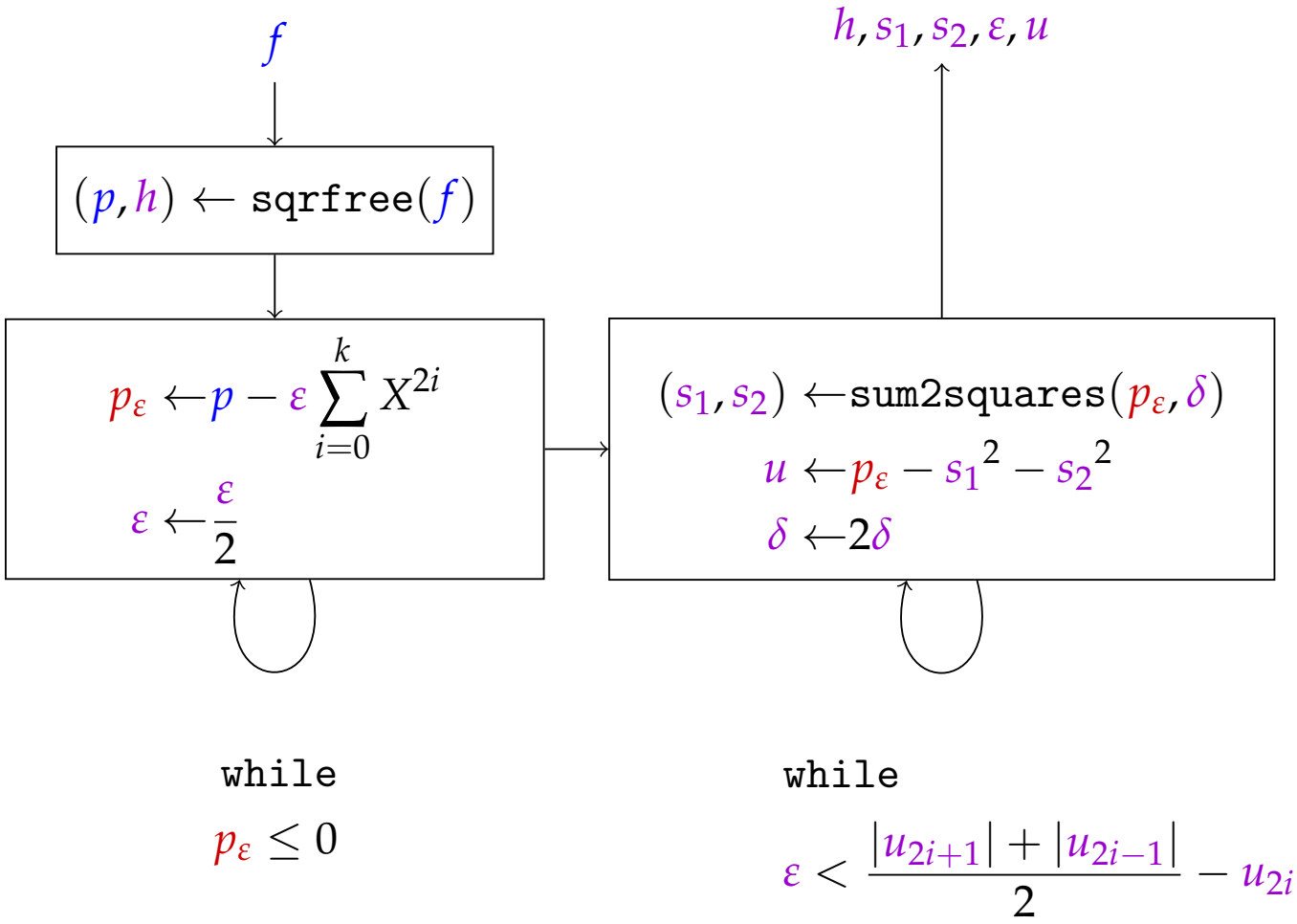
$$p = 1 + X + X^2 + X^3 + X^4$$

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

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

univsos2: Outline [Chevillard et. al 11]

- **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 $\mathbb{Q}$



univsos2: Absorbtion

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

univsos2: Absorbtion

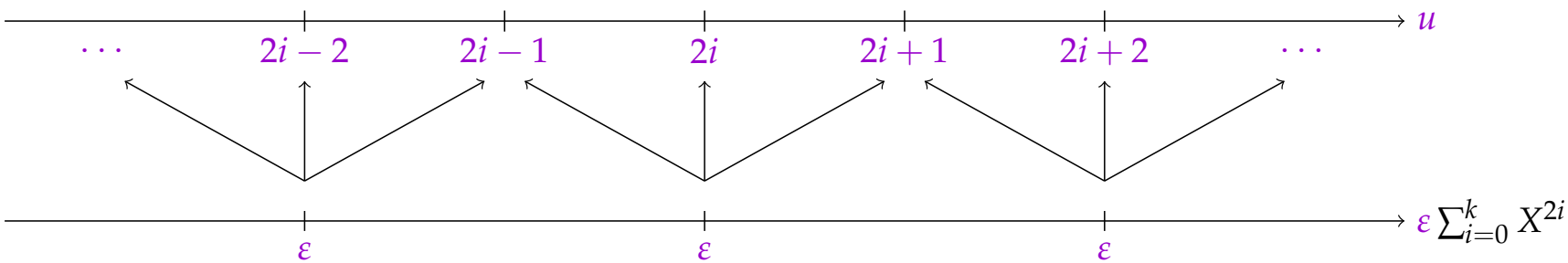
- $X = \frac{1}{2}\left[(X+1)^2 - 1 - X^2\right]$
- $-X = \frac{1}{2}\left[(X-1)^2 - 1 - X^2\right]$

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

univsos2: Absorbtion

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

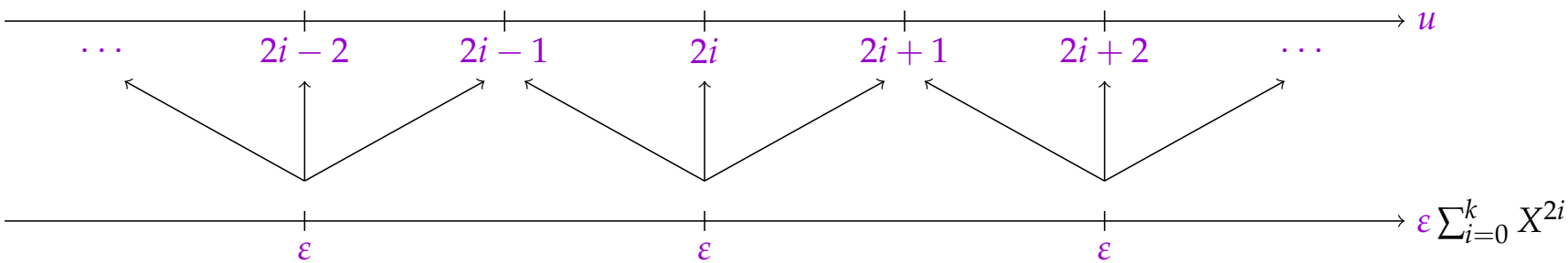
$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2}\left[(X^{i+1} + \operatorname{sgn}(u_{2i+1}) X^i)^2 - X^{2i} - X^{2i+2}\right]$$



univsos2: Absorbtion

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

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



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

univsos2: Nichtnegativstellensätz

Theorem [Chevillard et. al 11]

Let $0 \leqslant f \in \mathbb{Z}[X]$, $\deg f = d$.

$$f \geqslant 0 \text{ on } \mathbb{R} \Leftrightarrow \exists c_i \in \mathbb{Q}^{\geqslant 0}, f_i \in \mathbb{Q}[X] \text{ s.t. } f = c_1 {f_1}^2 + \cdots + c_{d+3} {f_{d+3}}^2$$

univsos2: Nichtnegativstellensätz

Theorem [Chevillard et. al 11]

Let $0 \leqslant f \in \mathbb{Z}[X]$, $\deg f = d$.

$$f \geqslant 0 \text{ on } \mathbb{R} \Leftrightarrow \exists c_i \in \mathbb{Q}^{\geqslant 0}, f_i \in \mathbb{Q}[X] \text{ s.t. } f = c_1 {f_1}^2 + \cdots + c_{d+3} {f_{d+3}}^2$$

Proof.

$f = p\,h^2 \implies 0 < p \in \mathbb{Z}[X]$, $\deg p = 2k$,
$p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$
Root isolation: $p = {ls_1}^2 + {ls_2}^2 + \varepsilon \sum_{i=0}^{k} X^{2i} + u$ at precision δ

$X^{2j+1} = (X^{j+1} + \frac{X^j}{2})^2 - (X^{2j+2} + \frac{X^{2j}}{4}) = -(X^{j+1} - \frac{X^j}{2})^2 + (X^{2j+2} + \frac{X^{2j}}{4})$

Smallest δ s.t. $\varepsilon \geqslant \frac{|u_{2i+1}|}{4} - u_{2i} + |u_{2i-1}|$
$\implies$ weighted SOS decomposition of $\varepsilon \sum_{i=0}^{k} X^{2i} + u$

univsos2: Bitsize of Perturbed Polynomials

Lemma

Let $0 < p \in \mathbb{Z}[X]$ with bitsize τ, $\deg p = d = 2k$.
Then

$$\exists\, \varepsilon \text{ s.t. } p_\varepsilon > 0 \text{ and } \tau(\varepsilon) = d \log_2 d + d\tau$$

univsos2: Bitsize of Perturbed Polynomials

Lemma

Let $0 < p \in \mathbb{Z}[X]$ with bitsize τ, $\deg p = d = 2k$.
Then

$$\exists\, \varepsilon \text{ s.t. } p_\varepsilon > 0 \text{ and } \tau(\varepsilon) = d \log_2 d + d\tau$$

Proof.

$\varepsilon := 1/2 \implies \exists\, R$ s.t. $p_\varepsilon(x) > 0$ for $|x| > R = 2d2^\tau$(Cauchy)

- Smallest N s.t. $\varepsilon = \frac{1}{2^N} < \frac{\inf_{|x| \leqslant R} p}{1+R^2 \cdots + R^{2k}}$
- $R > 1 \implies 1 + R^2 + \cdots + R^{2k} < kR^{2k}$
- $\inf_{x \in \mathbb{R}} p(x) > (d2^\tau)^{-d+2} 2^{-d \log_2 d - d\tau}$ [Melczer et. al 16] □

univsos2: Bitsize of Remainder

Lemma

Let $0 < p \in \mathbb{Z}[X]$ with bitsize τ, $\deg p = d = 2k$.
Then

$$\exists\, \varepsilon, s_1, s_2, u \text{ s.t. } p = ls_1{}^2 + ls_2{}^2 + \varepsilon \sum_{i=0}^{k} X^{2i} + u \text{ SOS}$$

with approx. root precision δ of p_ε s.t. $\tau(\delta) = d^2 + d\tau$

univsos2: Bitsize of Remainder

Lemma

Let $0 < p \in \mathbb{Z}[X]$ with bitsize τ, $\deg p = d = 2k$.
Then

$$\exists\, \varepsilon, s_1, s_2, u \text{ s.t. } p = l{s_1}^2 + l{s_2}^2 + \varepsilon \sum_{i=0}^{k} X^{2i} + u \text{ SOS}$$

with approx. root precision δ of p_ε s.t. $\tau(\delta) = d^2 + d\tau$

Proof.

$p_\varepsilon = \sum_{i=0}^{d} a_i X^i = \prod_{i=1}^{d}(X - z_i) \quad e = 2^{-\delta} \quad |\hat{z}_i| \leqslant z_i(1+e)$

Vieta's formula: $\sum_{1 \leqslant i_1 < \cdots < i_j \leqslant d} z_{i_1} \ldots z_{i_j} = (-1)^j \frac{a_{d-j}}{l}$

Smallest δ s.t. $\varepsilon \geqslant \frac{|u_{2i+1}|}{4} - u_{2i} + |u_{2i-1}|$

`univsos2`: Output Bitsize

Theorem

Let $0 \leqslant f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.
The max coeff bitsize τ_2 of `univsos2` on f is $\mathcal{O}\left(d^3 + d^2\tau\right)$.

univsos2: Output Bitsize

Theorem

Let $0 \leqslant f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.
The max coeff bitsize τ_2 of univsos2 on f is $\mathcal{O}\left(d^3 + d^2\tau\right)$.

Proof.

$p_\varepsilon = \sum_{i=0}^{d} a_i X^i = \prod_{i=1}^{d}(X - z_i) \quad e = 2^{-\delta} \quad |\hat{z}_i| \leqslant z_i(1+e)$

- Square-free part: $\tau(p) = \mathcal{O}\left(d + \tau\right)$
- $|\hat{z}_j| = |z_j|(1 + 2^{-\delta}) \geqslant \frac{1}{2^{\tau(p_\varepsilon)+1}}(1 + 2^{-\delta})|$ [Melczer et.al 16]

□

`univsos2`: Bit Complexity

Theorem

Let $0 \leqslant f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.

The bit complexity of `univsos2` on f is $\widetilde{\mathcal{O}}\left(d^4 + d^3\tau\right)$.

univsos2: Bit Complexity

Theorem

Let $0 \leqslant f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = d$.

The bit complexity of univsos2 on f is $\widetilde{\mathcal{O}}\left(d^4 + d^3\tau\right)$.

Proof.

- Root isolation with radius $\mathcal{O}\left(\delta + \tau(p_\varepsilon)\right)$ [Melczer et.al 16]:

$$\widetilde{\mathcal{O}}\left(d^3 + d^2\tau(p_\varepsilon) + d(\delta + \tau(p_\varepsilon))\right)$$

□

Benchmarks

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

1. `univsos1`: `sqrfree`, real root isolation in Maple
2. `univsos2`: PARI/GP implementation [Chevillard et. al 11]
   $\rightsquigarrow$ `sqrfree`, `sturm`, `polroots` (interface Maple-PARI/GP)
3. `univsos3`: SDPA-GMP solver (arbitrary precision)
   $\rightsquigarrow$ `sqrfree`, `sturm`, `sdp`

Benchmarks: [Chevillard et. al 11]

Approximation $f \in \mathbb{Q}[X]$ of mathematical function f_{math}

Validation of sup norm $\|f_{\text{math}} - f\|_\infty$ on a rational interval

Id	d	τ (bits)	`univsos1`		`univsos2`	
			τ_1 (bits)	t_1 (ms)	τ_2 (bits)	t_2 (ms)
# 1	13	22 682	3 403 023	2 352	51 992	824
# 5	34	117 307	7 309 717	82 583	265 330	5 204
# 7	43	67 399	18 976 562	330 288	152 277	11 190
# 9	20	30 414	641 561	928	68 664	1 605

Benchmarks: [Chevillard et. al 11]

Approximation $f \in \mathbb{Q}[X]$ of mathematical function f_{math}

Validation of sup norm $\|f_{\text{math}} - f\|_\infty$ on a rational interval

Id	d	τ (bits)	`univsos1`		`univsos2`	
			τ_1 (bits)	t_1 (ms)	τ_2 (bits)	t_2 (ms)
# 1	13	22 682	3 403 023	2 352	51 992	824
# 5	34	117 307	7 309 717	82 583	265 330	5 204
# 7	43	67 399	18 976 562	330 288	152 277	11 190
# 9	20	30 414	641 561	928	68 664	1 605

$$\Longrightarrow \tau_1 > \tau_2 \quad t_1 > t_2$$

Benchmarks: Power Sums

$$f = 1 + X + X^2 + \cdots + X^d$$

$$f = \prod_{j=1}^{k}((X - \cos\theta_j)^2 + \sin^2\theta_j), \text{ with } \theta_j := \frac{2j\pi}{d+1}$$

d	univsos1		univsos2	
	τ_1 (bits)	t_1 (ms)	τ_2 (bits)	t_2 (ms)
10	823	8	567	264
20	9 003	16	1 598	485
40	91 903	45	6 034	2 622
60	301 841	92	12 326	6 320
100	1 717 828	516	31 823	19 466
200	146 140 792	130 200	120 831	171 217
500	2 263 423 520	5 430 000	–	–

Benchmarks: Power Sums

$$f = 1 + X + X^2 + \cdots + X^d$$

$$f = \prod_{j=1}^{k}((X - \cos\theta_j)^2 + \sin^2\theta_j), \text{ with } \theta_j := \frac{2j\pi}{d+1}$$

d	univsos1		univsos2	
	τ_1 (bits)	t_1 (ms)	τ_2 (bits)	t_2 (ms)
10	823	8	567	264
20	9 003	16	1 598	485
40	91 903	45	6 034	2 622
60	301 841	92	12 326	6 320
100	1 717 828	516	31 823	19 466
200	146 140 792	130 200	120 831	171 217
500	2 263 423 520	5 430 000	–	–

$$\Longrightarrow \tau_1 > \tau_2 \quad t_1 < t_2$$

Benchmarks: Modified Wilkinson Polynomials

$$f = 1 + \prod_{j=1}^{k} (X - j)^2$$

$$a = t = 1 \quad f_t = 1 \quad f - f_t = \prod_{j=1}^{k} (X - j)^2$$

Relatively closed roots $1, \ldots, k$

Benchmarks: Modified Wilkinson Polynomials

$$f = 1 + \prod_{j=1}^{k} (X - j)^2$$

$$a = t = 1 \quad f_t = 1 \quad f - f_t = \prod_{j=1}^{k} (X - j)^2$$

Relatively closed roots $1, \ldots, k$

d	τ (bits)	`univsos1`		`univsos2`	
		τ_1 (bits)	t_1 (ms)	τ_2 (bits)	t_2 (ms)
10	140	47	17	2 373	751
20	737	198	31	12 652	3 569
40	3 692	939	35	65 404	47 022
100	29 443	7 384	441	–	–
500	1 022 771	255 767	73 522		

Benchmarks: Modified Wilkinson Polynomials

$$f = 1 + \prod_{j=1}^{k} (X - j)^2$$

$$a = t = 1 \quad f_t = 1 \quad f - f_t = \prod_{j=1}^{k} (X - j)^2$$

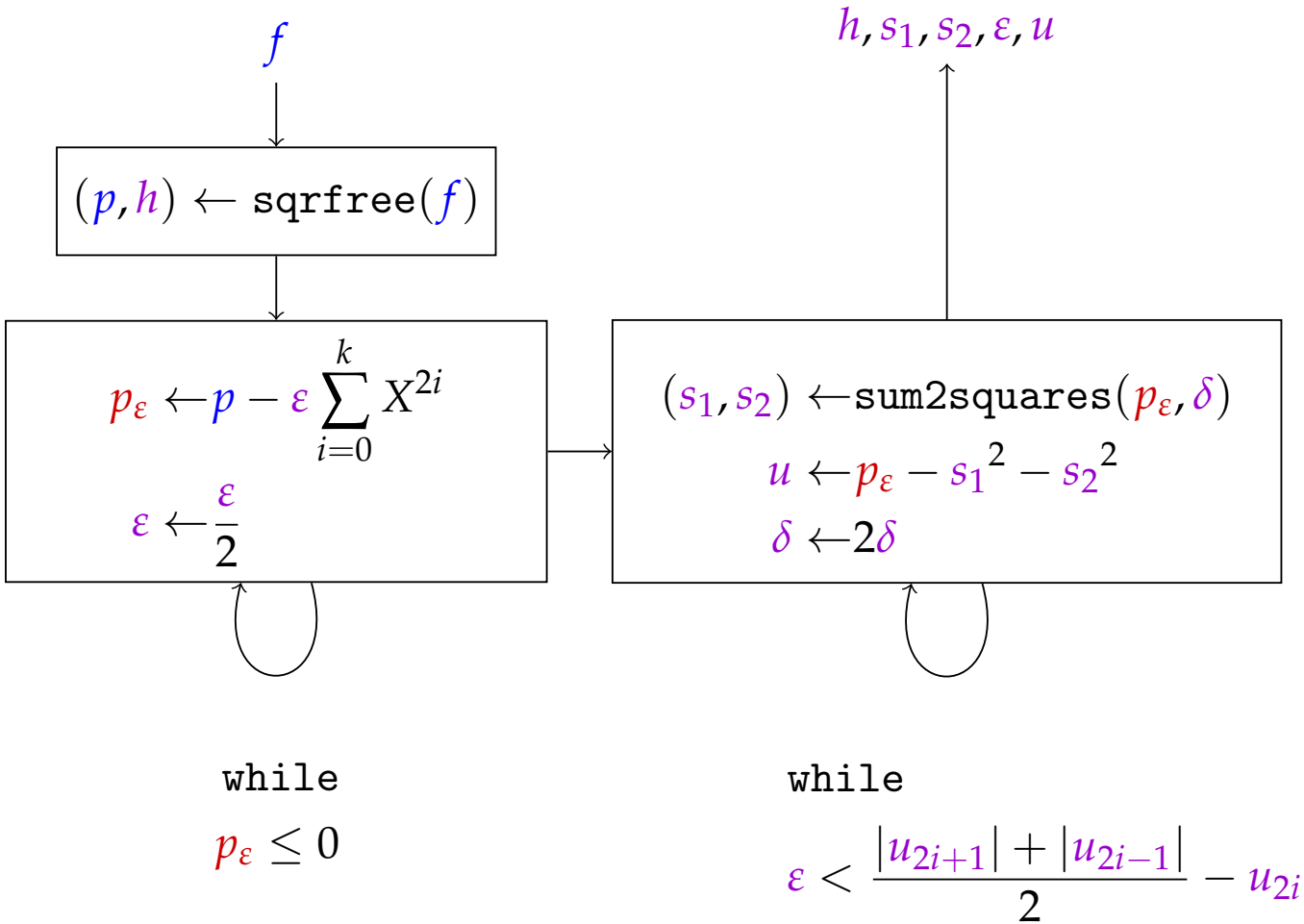
Relatively closed roots $1, \ldots, k$

d	τ (bits)	`univsos1`		`univsos2`	
		τ_1 (bits)	t_1 (ms)	τ_2 (bits)	t_2 (ms)
10	140	47	17	2 373	751
20	737	198	31	12 652	3 569
40	3 692	939	35	65 404	47 022
100	29 443	7 384	441	–	–
500	1 022 771	255 767	73 522		

$$\Longrightarrow \tau_1 < \tau_2 \quad t_1 < t_2$$

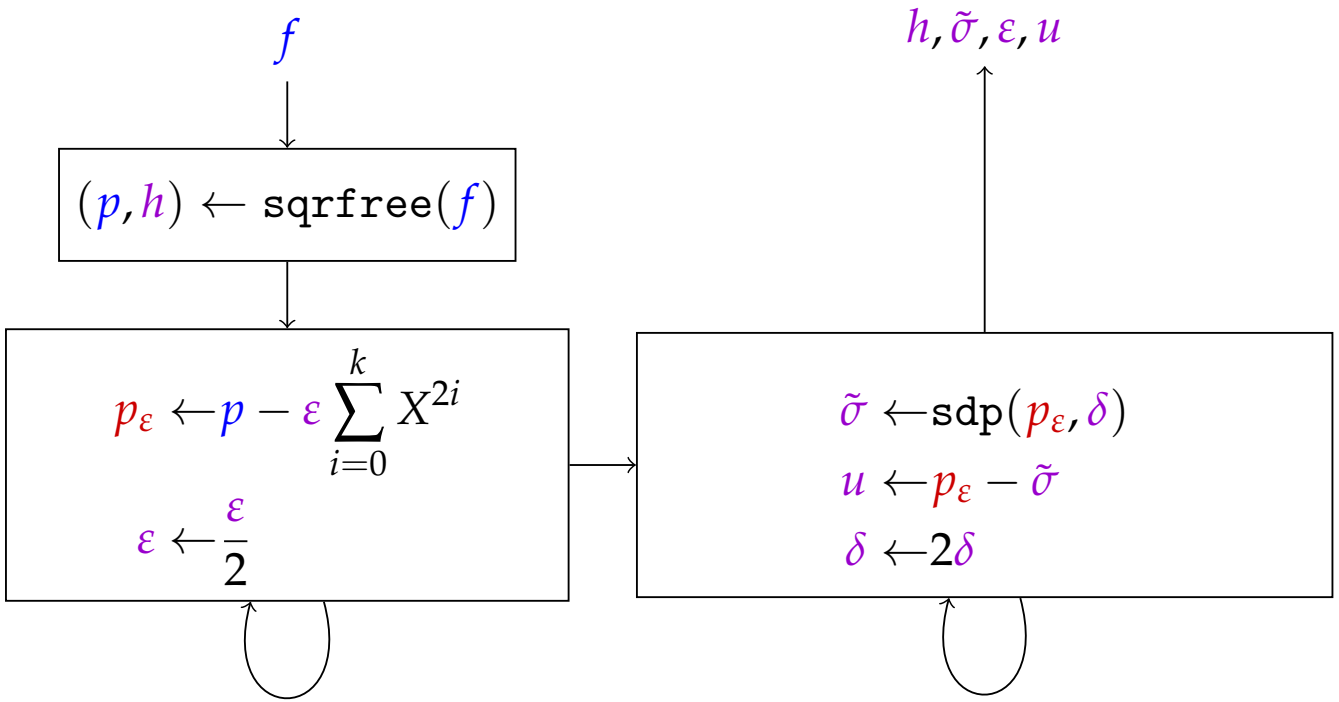
`intsos` $n = 1$ & Root Approximation: `univsos2`

- **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` $n = 1$ & SDP Approximation

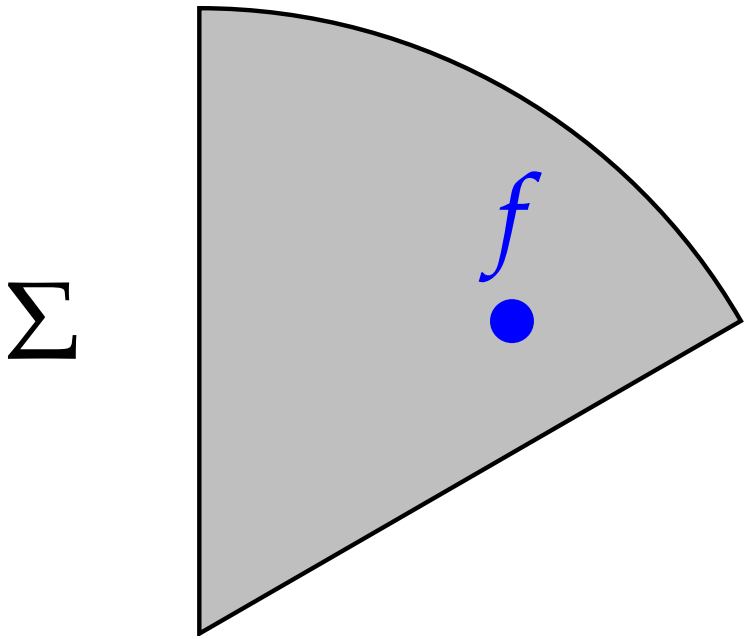
- **Input**: $f \geqslant 0 \in \mathbb{Q}[X]$ of degree $d \geqslant 2$, $\varepsilon \in \mathbb{Q}^{>0}$, $\delta \in \mathbb{N}^{>0}$
- **Output**: SOS decomposition with coefficients in $\mathbb{Q}$



`while` $p_\varepsilon \leq 0$

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

`intsos` with $n \geqslant 1$: Perturbation



PERTURBATION idea

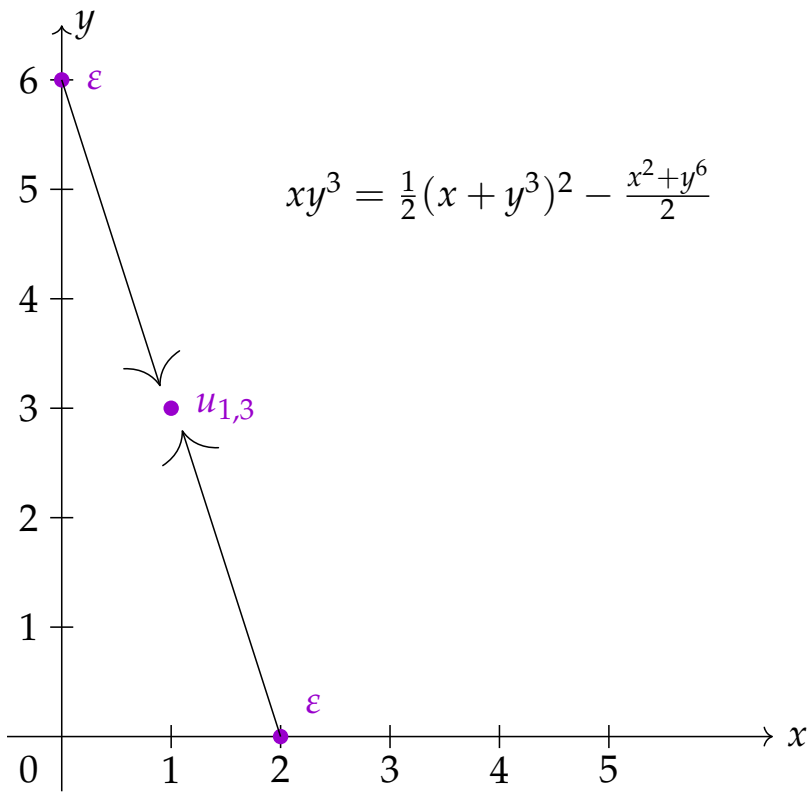
Approximate SOS Decomposition

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

`intsos` with $n \geqslant 1$: Absorbtion

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

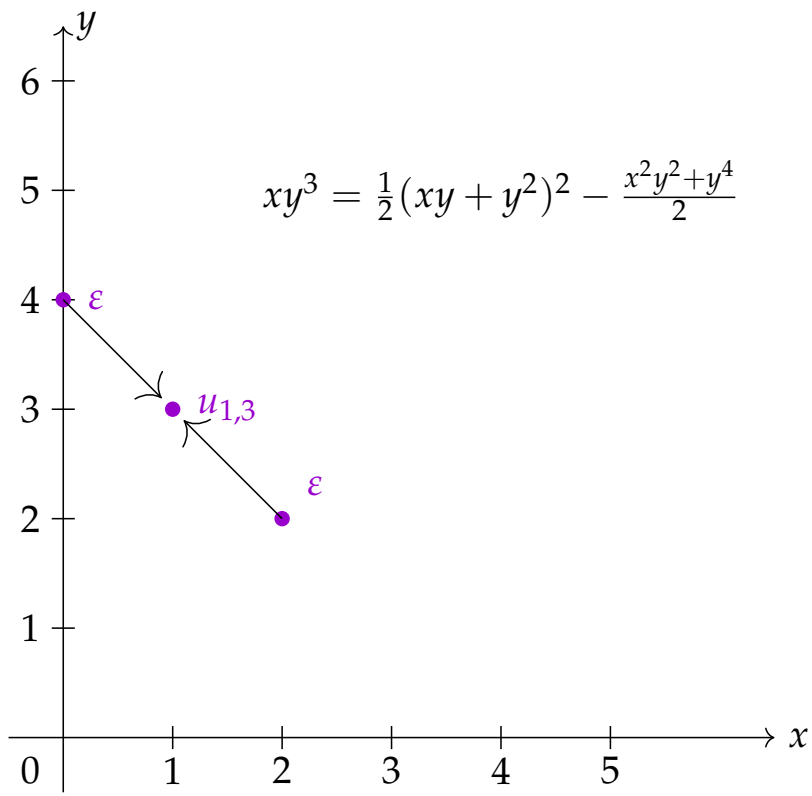
Choice of $\mathcal{P}$?



`intsos` with $n \geqslant 1$: Absorbtion

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

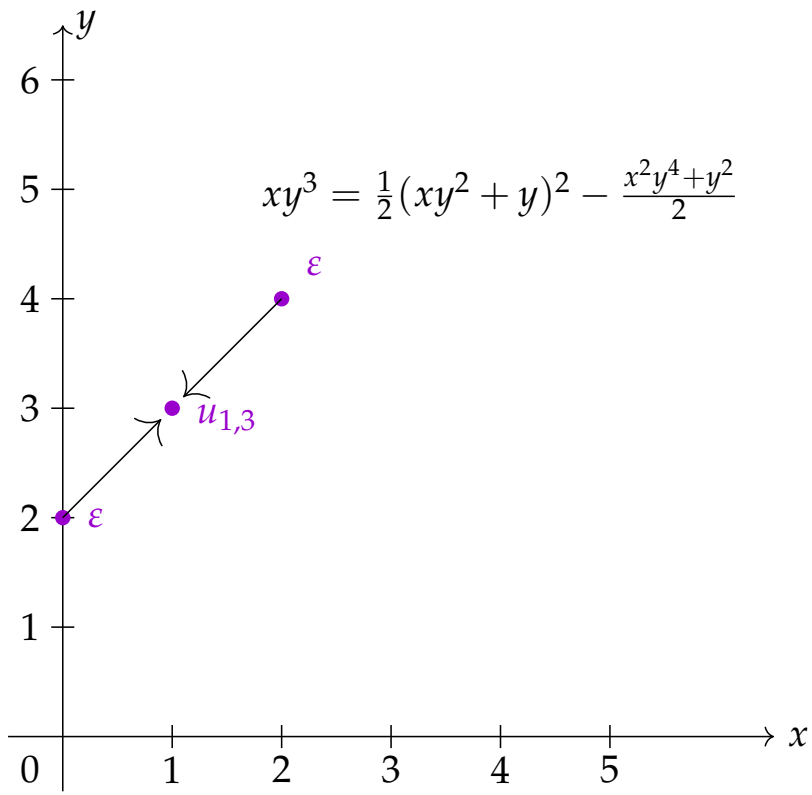
Choice of $\mathcal{P}$?



`intsos` with $n \geqslant 1$: Absorbtion

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

Choice of $\mathcal{P}$?

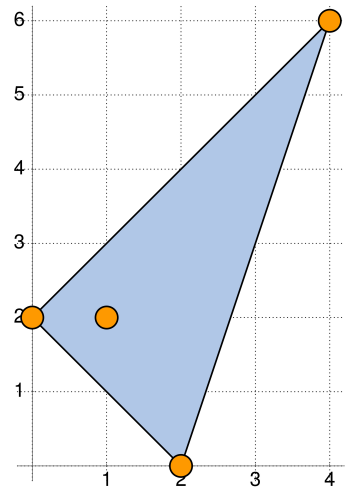


`intsos` with $n \geqslant 1$: Absorbtion

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

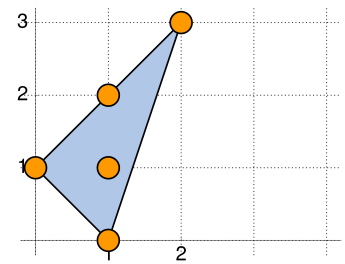
Choice of $\mathcal{P}$?

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



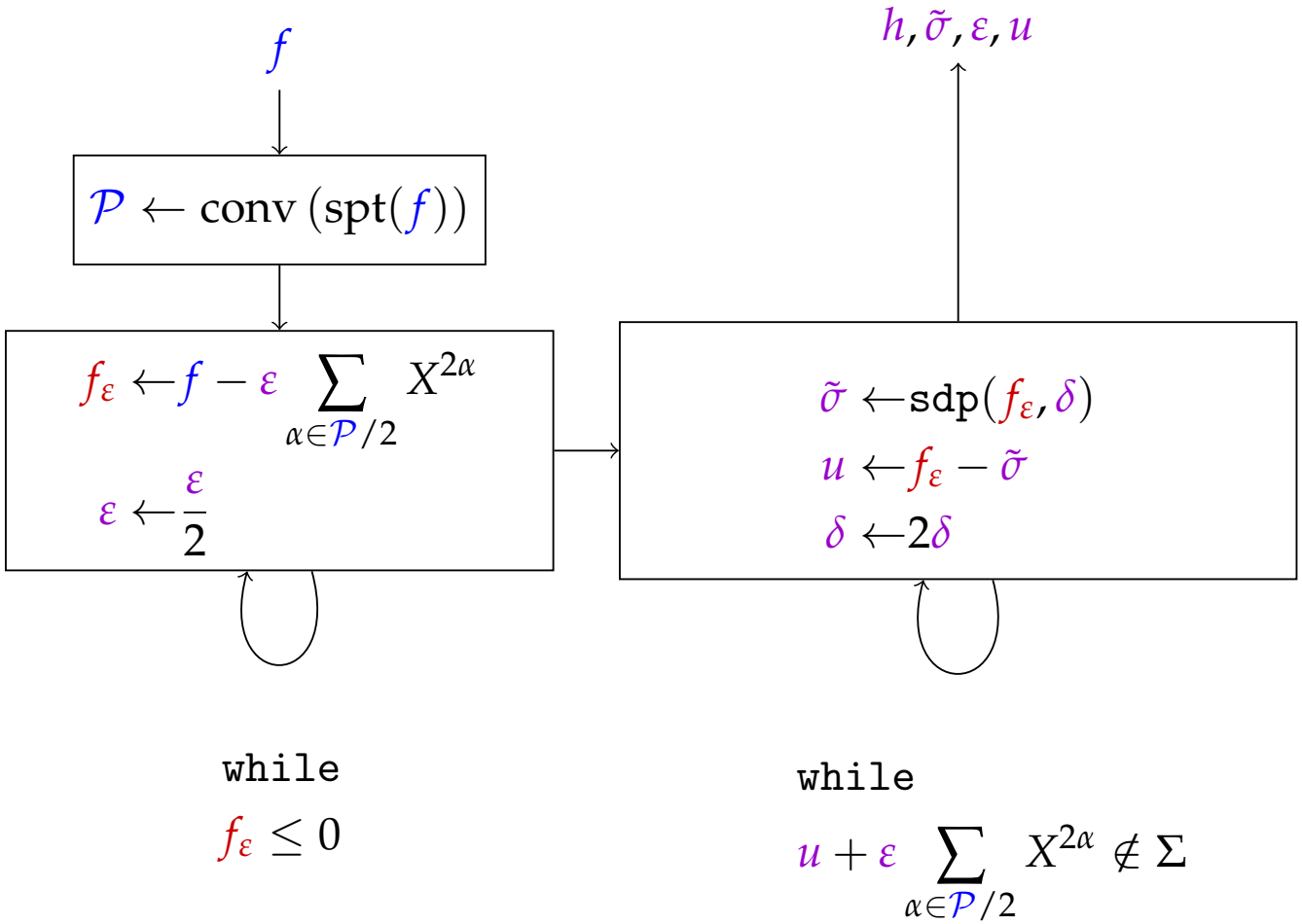
Newton Polytope $\mathcal{P} = \text{conv}\,(\text{spt}(f))$

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



Algorithm `intsos`

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



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

$\Longrightarrow$ `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 et. al 93] $\square$

Algorithm `Polyasos`

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

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

Algorithm `Polyasos`

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

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

Theorem

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

Algorithm `Polyasos`

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

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

Theorem

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

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

Algorithm `Polyasos`

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

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

Theorem

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

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

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

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

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

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

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

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

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 $\log D = \mathcal{O}\left(2^{\tau\, d^n\, C_{\mathbf{K}}}\right)$

Benchmarks

`multivsos` libary

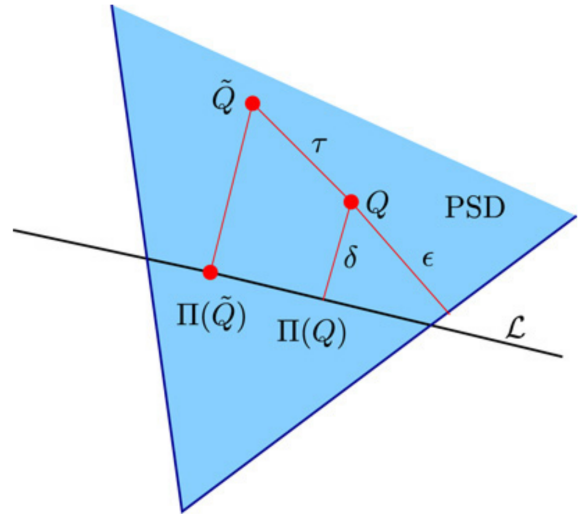
- Maple version 16, Intel Core i7-5600U CPU (2.60 GHz)
- Averaging over five runs

1. Newton Polytope with `convex` Maple package
2. SDPA-GMP solver (arbitrary precision) $\rightsquigarrow$ `sdp`
3. Cholesky's decomposition with Maple's `LUDecomposition`

Benchmarks: Reznick

`RoundProject` [Peyrl-Parrilo 08]

`RAGLib` & `CAD`: exact but no certificate



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
r_2	2	4	1 866	0.03	1 031	0.04	0.09	0.01
r_6	6	4	56 890	0.34	475 359	0.54	623.	–
r_{10}	10	4	344 347	2.45	8 374 082	4.59	–	–
r_6^2	6	8	1 283 982	13.8	146 103 466	106.	10.9	–

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	0.12	–
f_{491}	6	3	2	108 359	9.65	0.01	0.05
f_{752}	6	2	2	10 204	0.26	0.07	–
f_{859}	6	7	4	6 355 724	303.	5896.	–
f_{863}	4	2	1	5 492	0.14	0.01	0.01
f_{884}	4	4	3	300 784	25.1	0.21	–
butcher	6	3	2	247 623	1.32	47.2	–
heart	8	4	2	618 847	2.94	0.54	–

Conclusion and Perspectives

SINGLY EXP ALGORITHMS in D = representation degree

Conclusion and Perspectives

SINGLY EXP ALGORITHMS in D = representation degree

 How to improve bounds on D?

 Apply Perturb/Absorb on other relaxations?

End

Thank you for your attention!

`https://github.com/magronv/univsos`

`https://github.com/magronv/multivsos`

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


V. Magron, M. Safey El Din and M. Schweighofer. Algorithms for Weighted Sums of Squares Decomposition of Non-negative Univariate Polynomials, arxiv:1706.03941.


V. Magron and M. Safey El Din. On Exact Polya and Putinar's Representations, arxiv:1802.10339.