RealCertify: a Maple package for certifying non-negativity

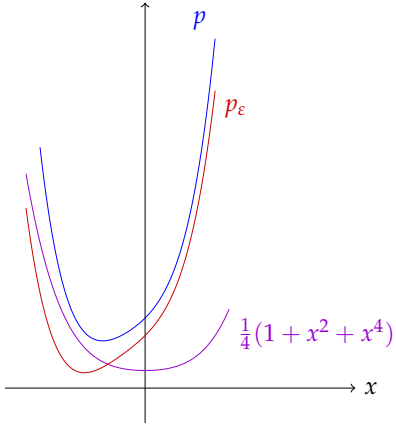
Victor Magron, CNRS

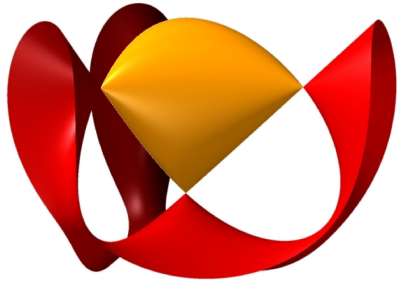
Joint work with

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

ISSAC

17th July 2018





`RealCertify`: Certify Non-negativity

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

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

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

`RealCertify`: Certify 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 $\rightsquigarrow \mathbf{K} = \mathbb{R}^n$

$$\boxed{n = 1} \quad f = 1 + X + X^2 + X^3 + X^4$$

$$\boxed{n > 1} \quad f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$$

RealCertify: Certify 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 $\rightsquigarrow \mathbf{K} = \mathbb{R}^n$

   $\boxed{n = 1}$ $\quad f = 1 + X + X^2 + X^3 + X^4$

   $\boxed{n > 1}$ $\quad f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$

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

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

   $f = -X_1^2 - 2X_1X_2 - 2X_2^2 + 6 \quad \mathbf{K} = \{1 - X_1^2 \geqslant 0, 1 - X_2^2 \geqslant 0\}$

RealCertify: Certify 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 $\rightsquigarrow \mathbf{K} = \mathbb{R}^n$

   $\boxed{n = 1}$ $\quad f = 1 + X + X^2 + X^3 + X^4$

   $\boxed{n > 1}$ $\quad f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$

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

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

   $f = -X_1^2 - 2X_1X_2 - 2X_2^2 + 6 \quad \mathbf{K} = \{1 - X_1^2 \geqslant 0, 1 - X_2^2 \geqslant 0\}$

1. $f \in \Sigma$ = sums of squares (SOS)

   $f = \sigma = {h_1}^2 + \cdots + {h_p}^2 \geqslant 0$

2. Weighted SOS $\quad f = \sigma_0 + \sigma_1 g_1 + \cdots + \sigma_m g_m \geqslant 0$ on $\mathbf{K}$

Exact Certification

Approximate solutions

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

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

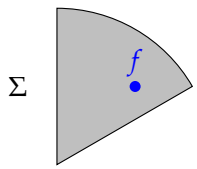
$$a^2 - 2ab + b^2 \simeq (1.00001a - 0.99998b)^2$$

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

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

Exact Certification

Win TWO-PLAYER GAME

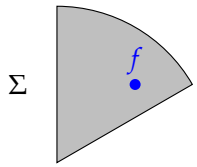


sum of squares of f?

$\simeq$ Output!

Exact Certification

Win TWO-PLAYER GAME



Hybrid Symbolic/Numeric Algorithms

sum of squares of $f + \varepsilon$?

Error Compensation

$\simeq \quad \rightarrow \quad =$

$\simeq$ Output!

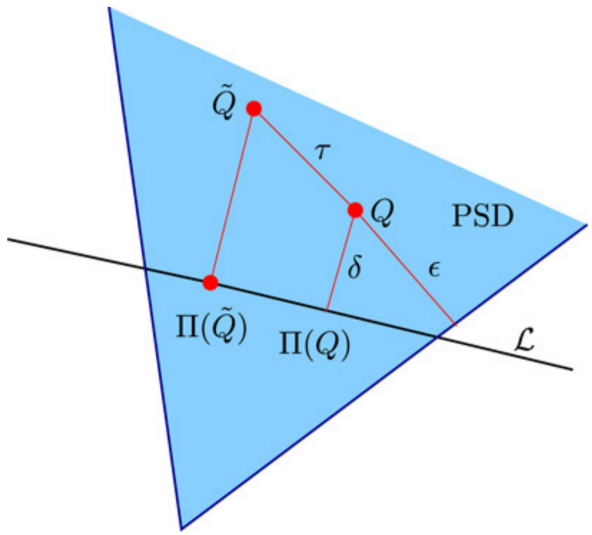
Existing Frameworks

- project & round [Peyrl-Parrilo 08] [Kaltofen-Yang-Zhi 08]
  $f \in \mathring{\Sigma}$ with $\deg f = 2D$

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

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

Find $\tilde{\mathbf{Q}}$ with semidefinite programming



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

$\rightsquigarrow$ Can handle degenerate situations!

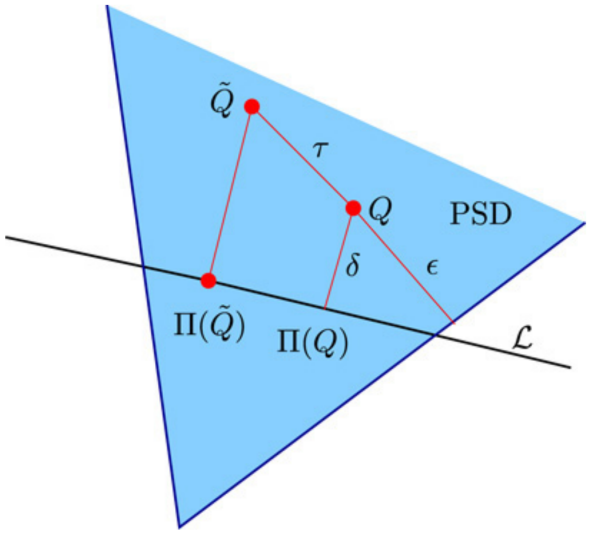
Existing Frameworks

- project & round [Peyrl-Parrilo 08] [Kaltofen-Yang-Zhi 08]
  $f \in \mathring{\Sigma}$ with $\deg f = 2D$

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

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

Find $\tilde{\mathbf{Q}}$ with semidefinite programming



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

$\rightsquigarrow$ Can handle degenerate situations!

- `RAGLib` (critical points) [Safey El Din]

- `SamplePoints` (CAD) [Moreno Maza-Alvandi-Chen-Marcus-Schost-Vrbik]

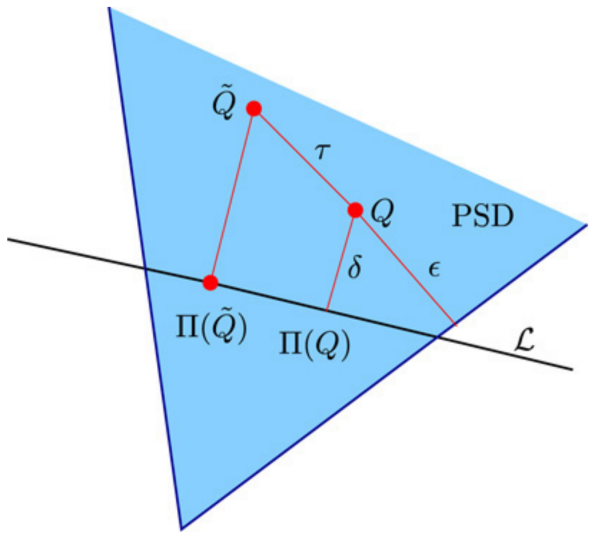
Existing Frameworks

- project & round [Peyrl-Parrilo 08] [Kaltofen-Yang-Zhi 08]
  $f \in \mathring{\Sigma}$ with $\deg f = 2D$

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

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

Find $\tilde{\mathbf{Q}}$ with semidefinite programming



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

$\rightsquigarrow$ Can handle degenerate situations!

- `RAGLib` (critical points) [Safey El Din]

- `SamplePoints` (CAD) [Moreno Maza-Alvandi-Chen-Marcus-Schost-Vrbik]

Demo 1

Modules & Install

gricad-gitlab:RealCertify

Depends on Maple &

`univsos` $\boxed{n = 1}$

- Square free decomposition with `sqrfree`
- PARI/GP for complex zero isolation

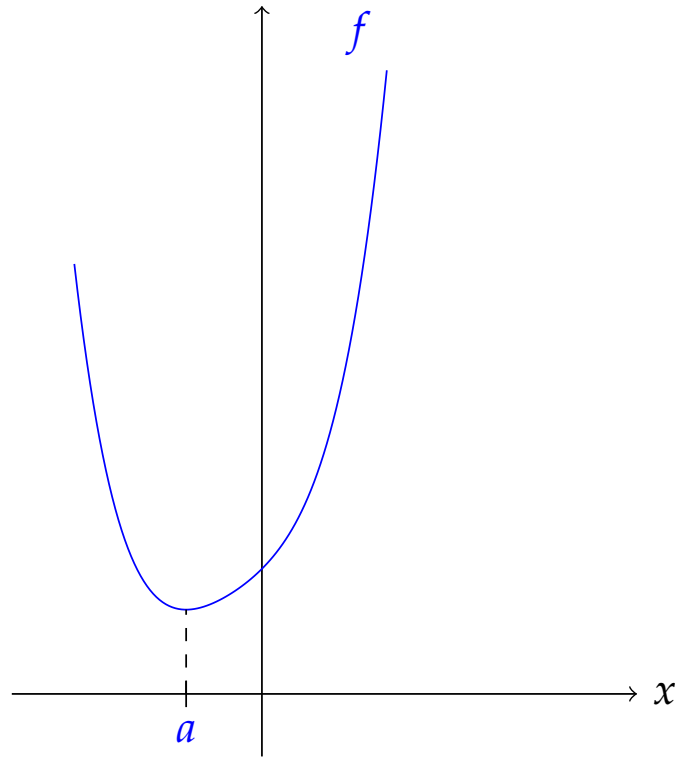
`multivsos` $\boxed{n > 1}$

- arbitrary precision SDP solver SDPA-GMP [Nakata 10]
- Newton Polytope with `convex` package [Franz 99]
- Cholesky's decomposition with `LUDecomposition`

`univsos1` [Schweighofer 99]

$f \in \mathbb{Q}[X]$ and $f > 0$

Minimizer a may not be in $\mathbb{Q}$ . . .



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

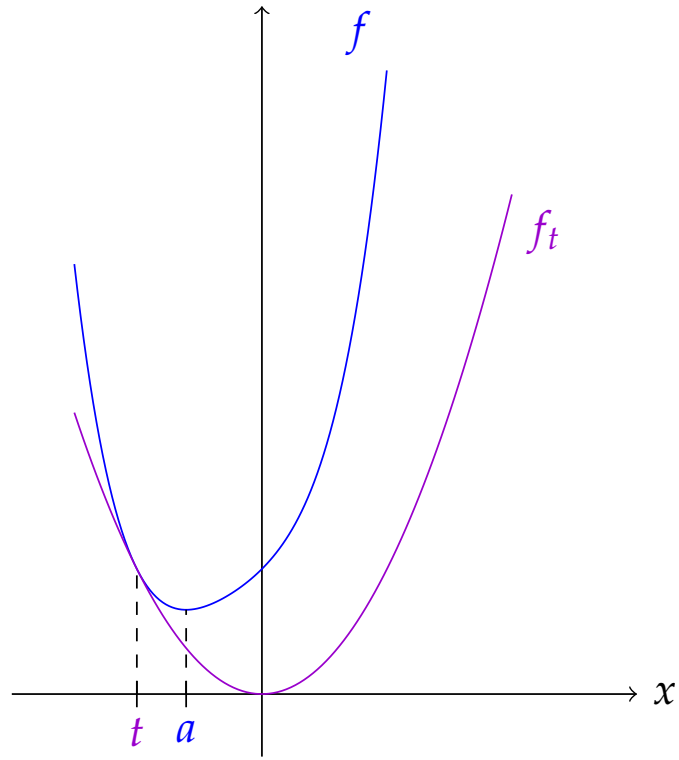
$$a = \frac{5}{4(135+60\sqrt{6})^{1/3}} - \frac{4(135+60\sqrt{6})^{1/3}}{12} - \frac{1}{4}$$

`univsos1` [Schweighofer 99]

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

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 $t \in \mathbb{Q}$



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

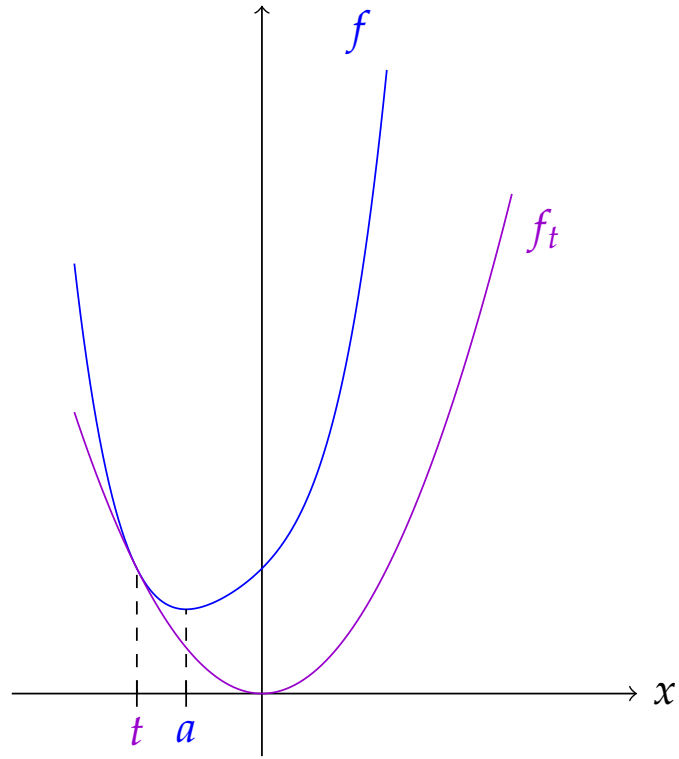
`univsos1` [Schweighofer 99]

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

Square-free decomposition:

$$f - f_t = gh^2$$

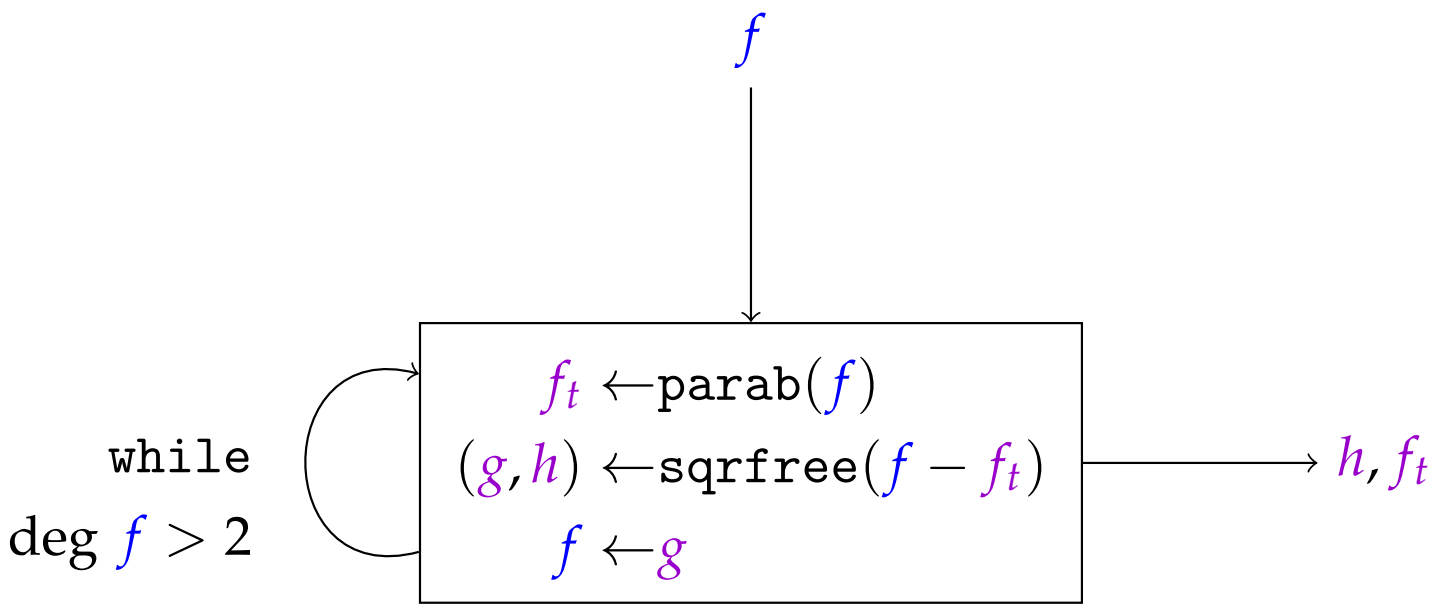
- $\deg g \leqslant \deg f - 2$
- $g > 0$
- Do it again on g



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

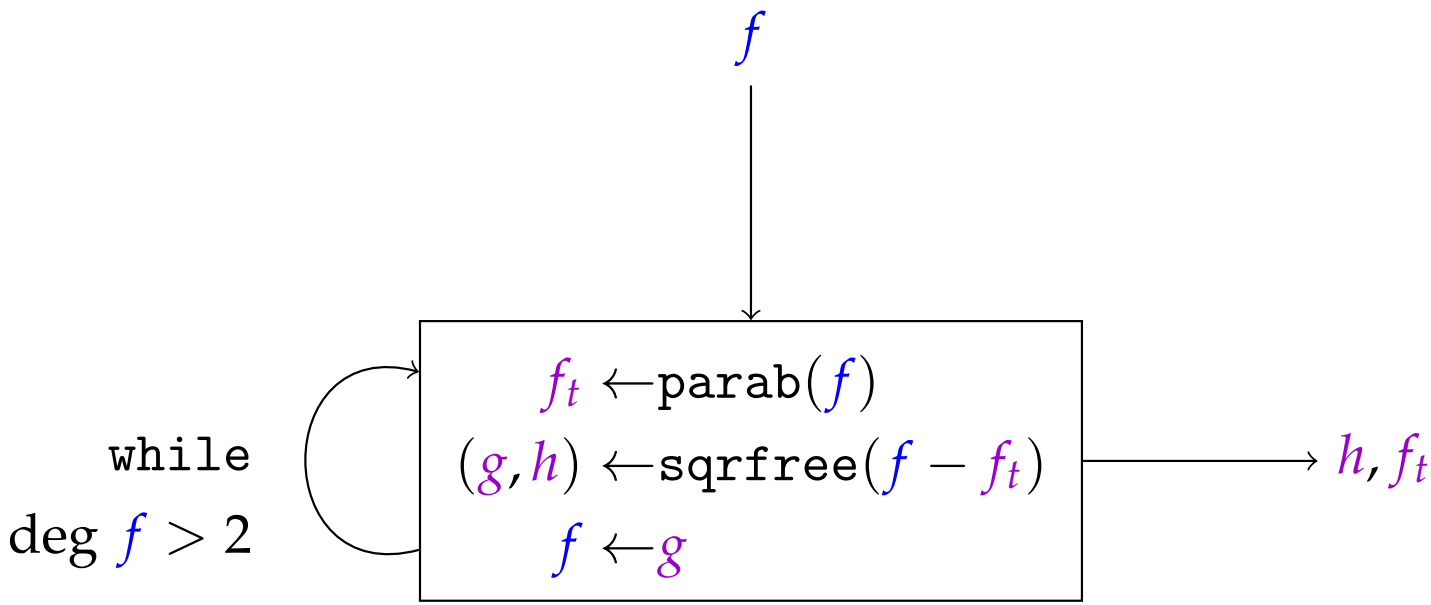
`univsos1` [Schweighofer 99]

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



`univsos1` [Schweighofer 99]

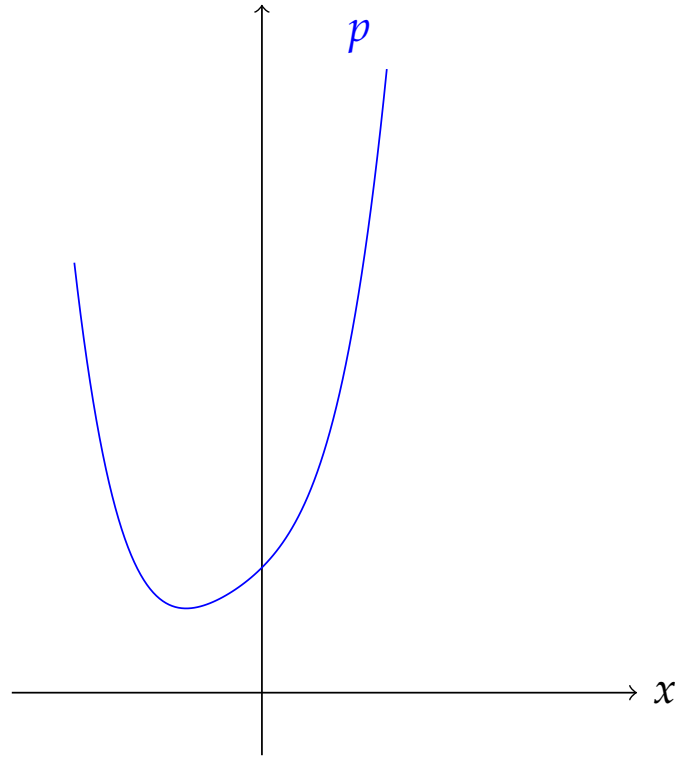
- **Input**: $f \geqslant 0 \in \mathbb{Q}[X]$ of degree $d \geqslant 2$
- **Output**: SOS decomposition with coefficients in $\mathbb{Q}$



Demo 2

`univsos2` [Chevillard et. al 11]

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



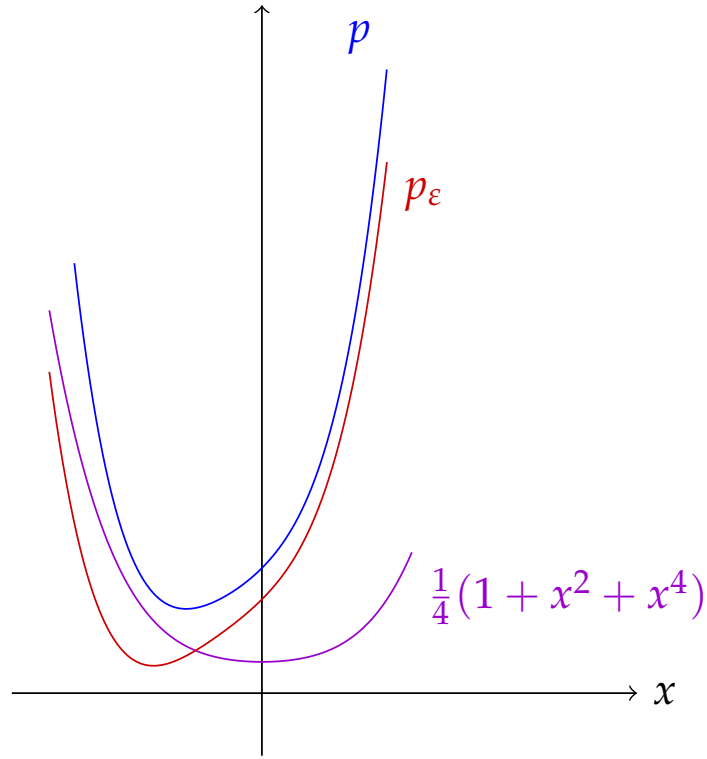
$p = 1 + X + X^2 + X^3 + X^4$

`univsos2` [Chevillard et. al 11]

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

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

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



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

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

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

`univsos2` [Chevillard et. al 11]

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

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

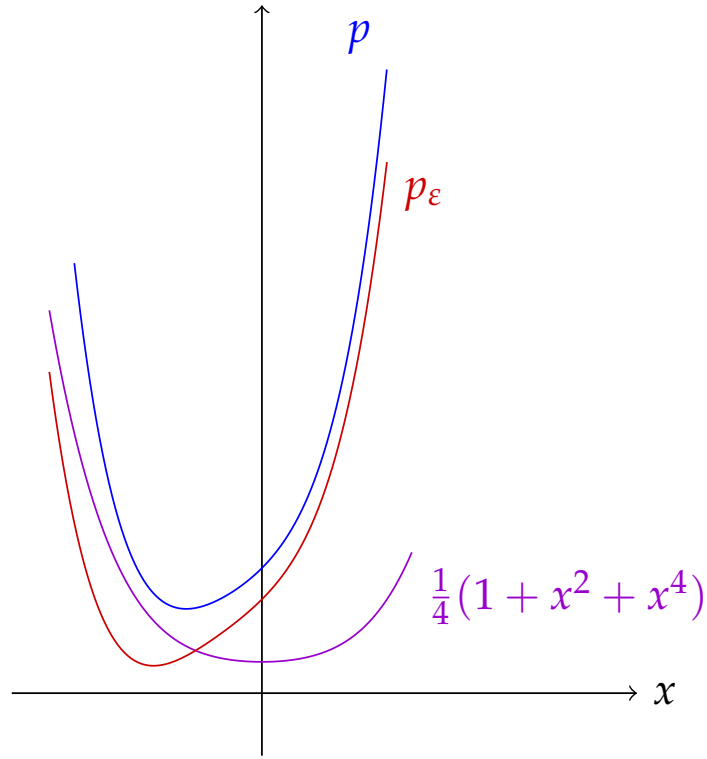
$$p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$$

- Root isolation:

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

- **ABSORB**: small enough u_i

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



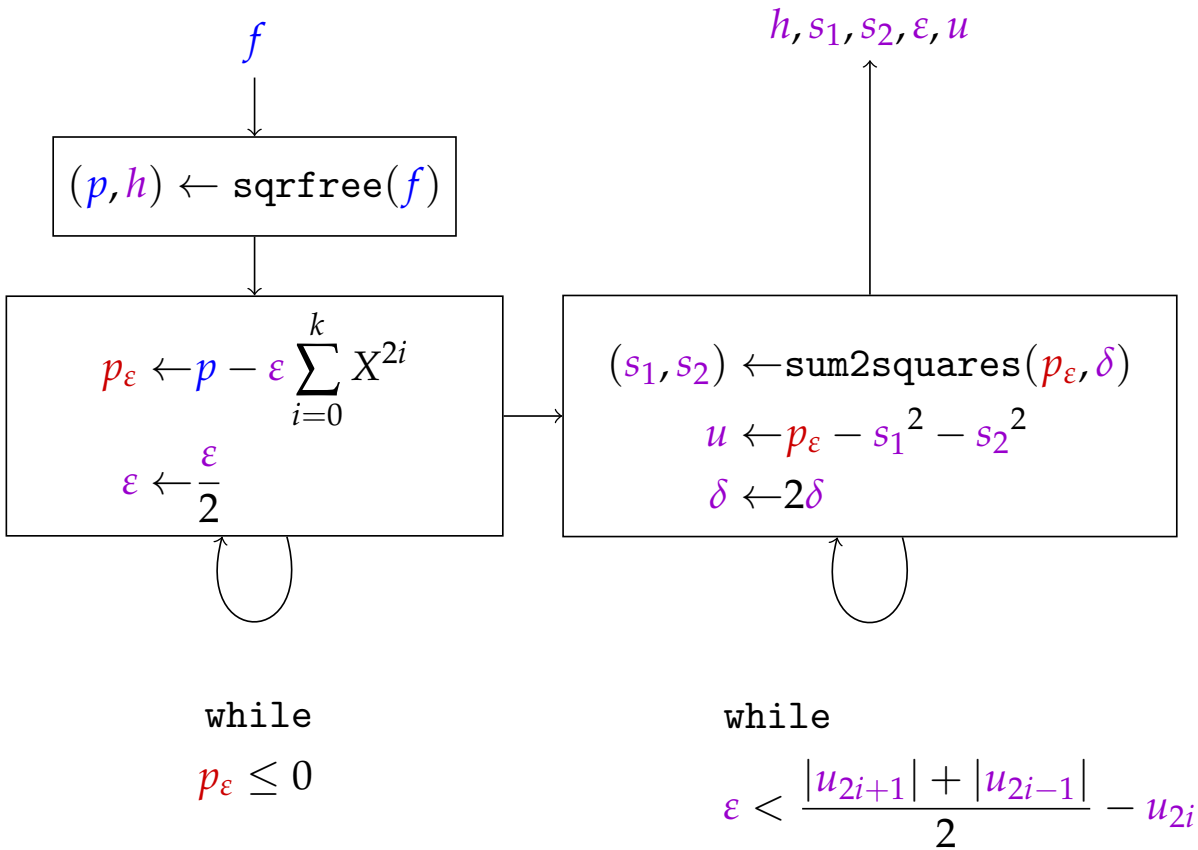
$$p = 1 + X + X^2 + X^3 + X^4$$

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

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

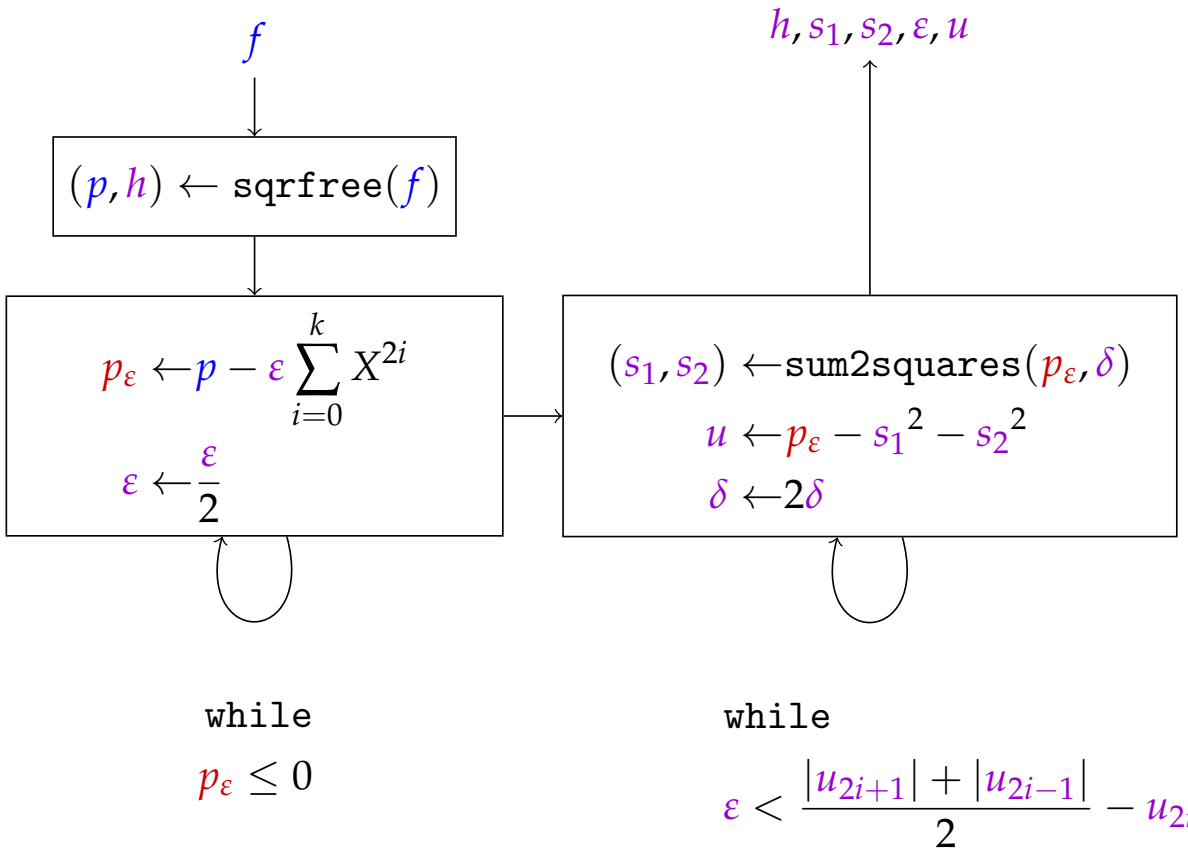
`univsos2` [Chevillard et. al 11]

- **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 [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 $\mathbb{Q}$



Demo 3

`univsos1` vs `univsos2`

Theorem [M-Safey El Din-Schweighofer 18]

Non-negative $f \in \mathbb{Q}[X]$ with bitsize τ and $\deg f = d$

$\rightsquigarrow$ `univsos1` has output bitsize $\tau_1 = \mathcal{O}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}} \tau\right)$

$\rightsquigarrow$ `univsos2` has output bitsize $\tau_2 = \mathcal{O}\left(d^4 \tau\right)$

Practice?

`univsos1` vs `univsos2`

Theorem [M-Safey El Din-Schweighofer 18]

Non-negative $f \in \mathbb{Q}[X]$ with bitsize τ and $\deg f = d$

$\rightsquigarrow$ `univsos1` has output bitsize $\tau_1 = \mathcal{O}\left(\left(\frac{d}{2}\right)^{\frac{3d}{2}} \tau\right)$

$\rightsquigarrow$ `univsos2` has output bitsize $\tau_2 = \mathcal{O}\left(d^4 \tau\right)$

Practice?

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

Demo 4

Benchmarks from [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 interval $[a, b]$

$\rightsquigarrow$ `UnivariateSumOfSquaresDecItv`

Id	d	τ	`univsos1`		`univsos2`	
			τ_1	t_1	τ_2	t_2
# 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 from [Chevillard et. al 11]

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

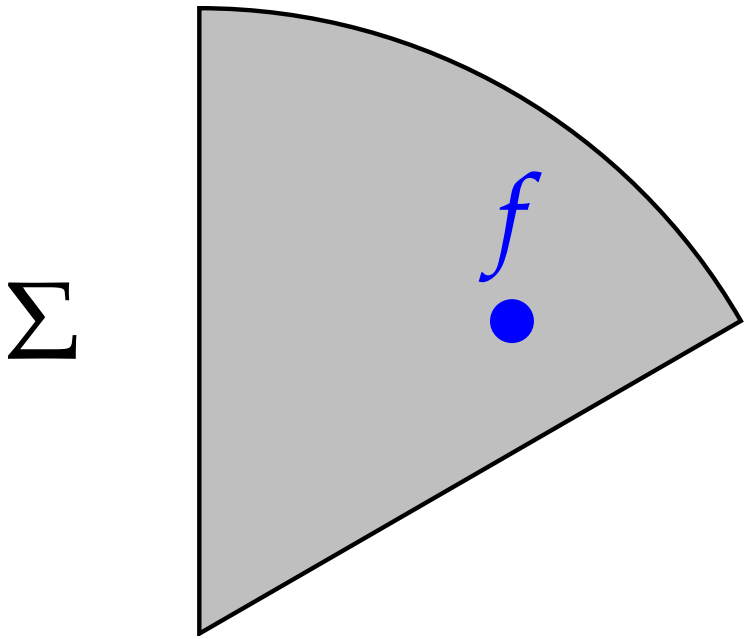
Validation of sup norm $\|f_{\text{math}} - f\|_\infty$ on interval $[a, b]$

$\rightsquigarrow$ `UnivariateSumOfSquaresDecItv`

Id	d	τ	`univsos1`		`univsos2`	
			τ_1	t_1	τ_2	t_2
# 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

$\tau_1 > \tau_2 \Longrightarrow$ same as theory prediction

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



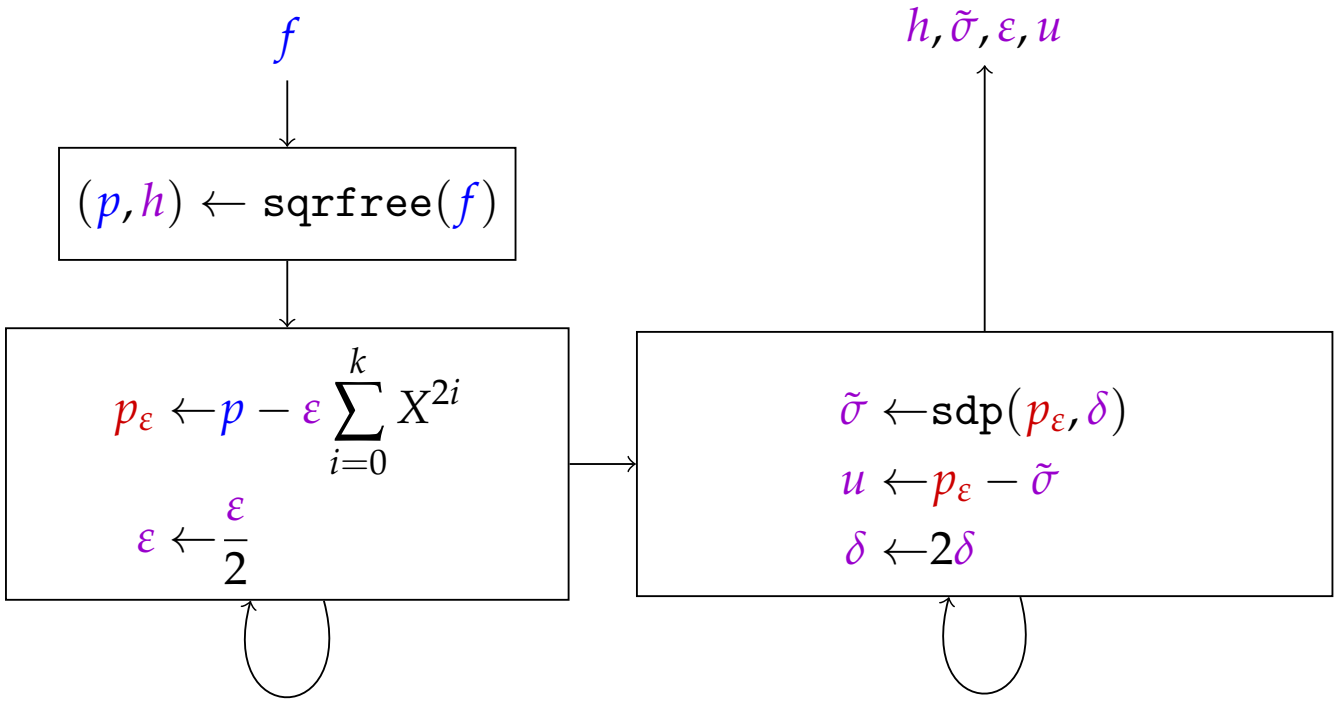
PERTURBATION idea

Approximate SOS Decomposition

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

`intsos` with $n = 1$ 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 $\mathbb{Q}$



`while` $p_\varepsilon \leq 0$

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

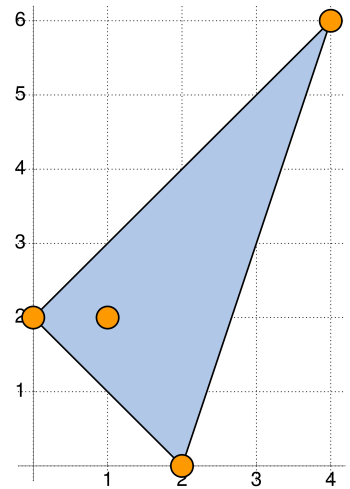
`intsos` with $n \geqslant 1$: Absorbtion

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

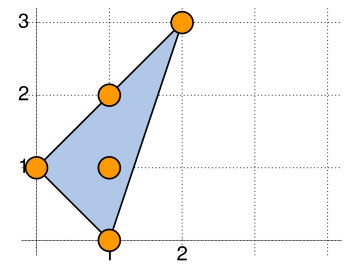
Choice of $\mathcal{P}$?

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

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

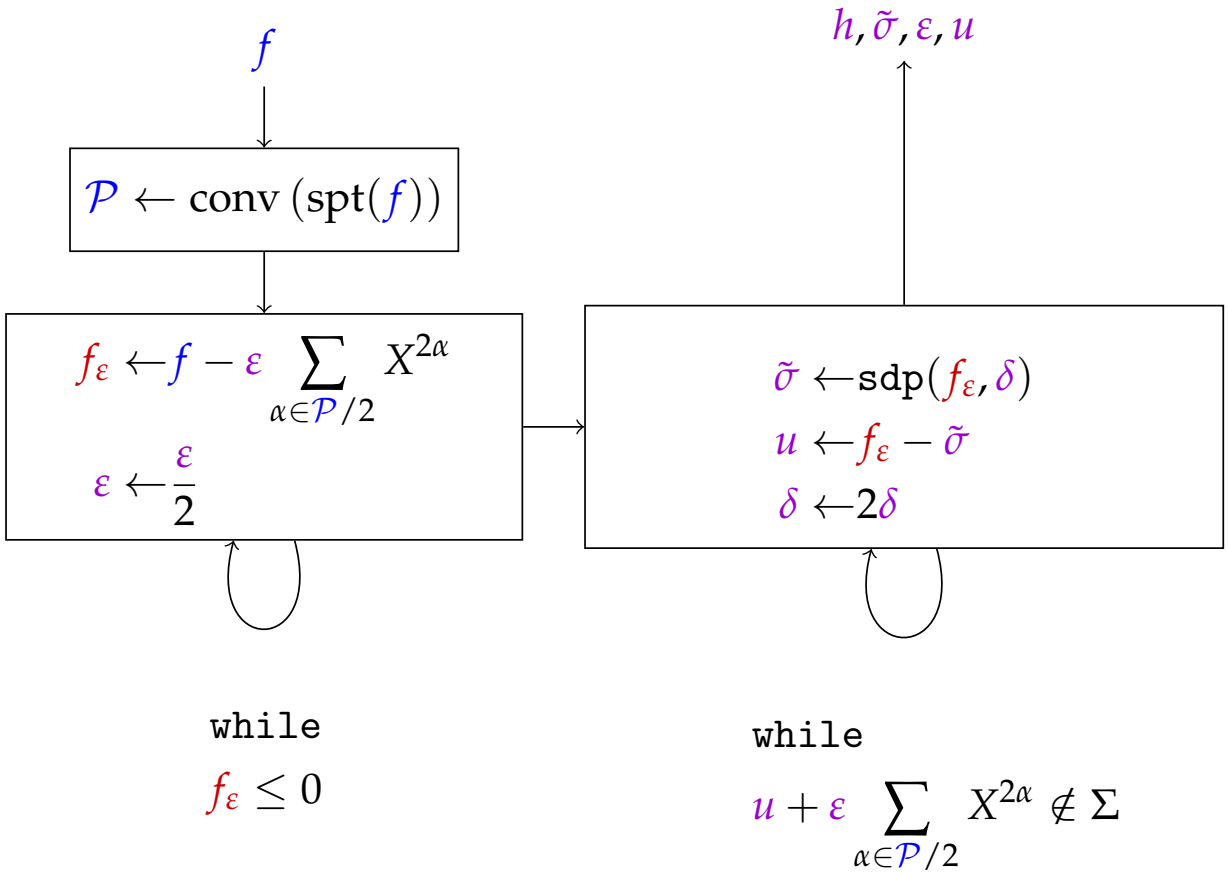


Squares in SOS decomposition $\subseteq \frac{\mathcal{P}}{2} \cap \mathbb{N}^n$
[Reznick 78]



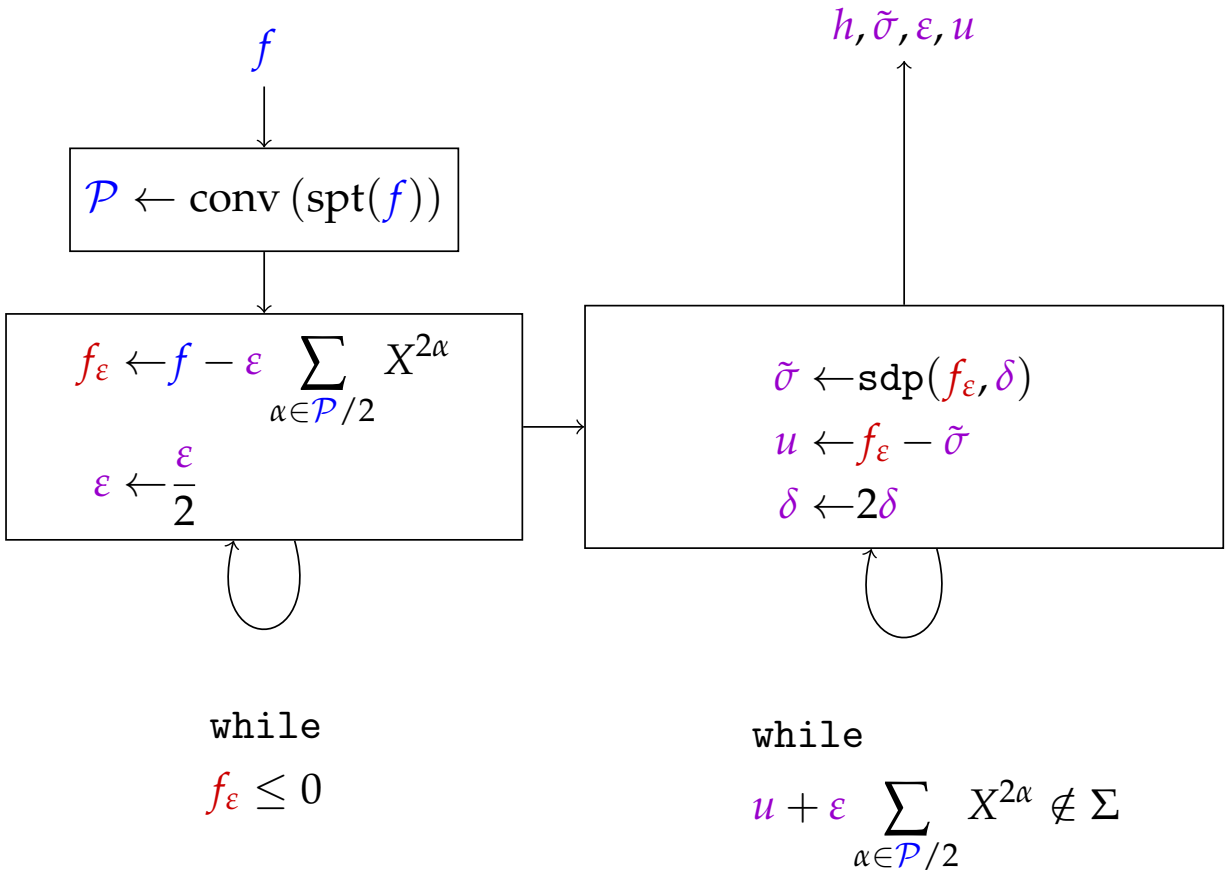
Algorithm `intsos`

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



Algorithm `intsos`

- **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 $\mathbb{Q}$



Demo 5

Algorithm `Putinarsos`

Assumption: $\exists i$ s.t. $g_i = 1 - \|X\|_2^2$

$f > 0$ 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`

Assumption: $\exists i$ s.t. $g_i = 1 - \|X\|_2^2$

$f > 0$ 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 [M.-Safey El Din 18]

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

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

Algorithm `Putinarsos`

Assumption: $\exists i$ s.t. $g_i = 1 - \|X\|_2^2$

$f > 0$ 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 [M.-Safey El Din 18]

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

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

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`

Assumption: $\exists i$ s.t. $g_i = 1 - \|X\|_2^2$

$f > 0$ 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 [M.-Safey El Din 18]

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

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

ABSORBTION as in Algorithm `intsos`:

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

Demo 6

Unconstrained Benchmarks

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	598.	–
f_1	10	4	344 347	2.45	8 374 082	4.59	–	–

Unconstrained Benchmarks

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	598.	–
f_1	10	4	344 347	2.45	8 374 082	4.59	–	–

Demo 7

Constrained Benchmarks

Id	n	d	multivsos			RAGLib	CAD
			D	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	0.01	0.05
f_{752}	6	2	2	10 204	0.26	0.07	–
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	–

Demo 8

Conclusion and Perspectives

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

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

How to handle degenerate situations?

Conclusion and Perspectives

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

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

- How to handle degenerate situations?
- Why `intsos` fails when $f \in \mathring{\Sigma}$?
- Better arbitrary-precision SDP solvers
- Extension to other relaxations, sums of hermitian squares

Crucial need for polynomial systems certification

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