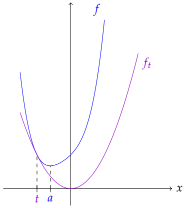
Nichtnegativstellensätze for Univariate Polynomials

Victor Magron, CNRS Verimag

Joint work with

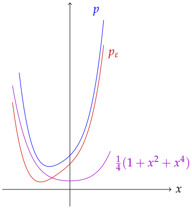
Mohab Safey El Din (INRIA/UPMC/LIP6)

Markus Schweighofer (Konstanz University)



JNCF

17 January 2017



The Question(s)

- 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)

- 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)

- 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)

- Ordered real field K
- Let $f \in K[X]$ with bitsize τ and $f \geqslant 0$ on $\mathbb{R}$

Existence Question

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

The Question(s)

- Ordered real field K
- Let $f \in K[X]$ with bitsize τ and $f \geqslant 0$ on $\mathbb{R}$

Existence Question

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

Examples

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

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

Motivation

Nichtnegativstellensätze (Nonnegativity 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

Related work

Existence Question

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

- $f = c_1 f_1^2 + c_2 f_2^2 + c_3 f_3^2 + c_4 f_4^2 + c_5 f_5^2$ [Pourchet 72]

- $f = c_1 f_1^2 + \cdots + c_n f_n^2$ [Schweighofer 99]

- $f = c_1 f_1^2 + \cdots + c_{n+3} f_{n+3}^2$ [Chevillard et. al 11]

- SOS with Exact LMIs $\quad f = (1\, x \ldots x^{\frac{n}{2}})^T \mathbf{G} (1\, x \ldots x^{\frac{n}{2}})\ \mathbf{G} \succcurlyeq 0$
  - Critical point methods [Greuet et. al 11]
  - CAD [Iwane 13]
  - Solving over the rationals [Guo et. al 13]
    $\rightsquigarrow$ output size $= \tau^{\mathcal{O}(1)} 2^{\mathcal{O}(n^3)}$
  - Determinantial varieties [Henrion et. al 16]

Contribution

- Ordered real field K
- Let $f \in K[X]$ with bitsize τ and $f \geqslant 0$ on $\mathbb{R}$

Existence Question

Does there exist $f_i \in K[X], c_i \in K^{>0}$ 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

Two methods answering the questions:

$f = c_1 f_1{}^2 + \cdots + c_n f_n{}^2$ [Schweighofer 99]
$\rightsquigarrow$ Algorithm `univsos1` with output size $\tau_1 = \mathcal{O}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}} \tau\right)$
bit complexity $\widetilde{\mathcal{O}}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}} \tau\right)$

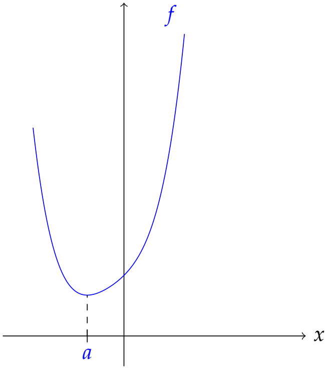
$f = c_1 f_1{}^2 + \cdots + c_{n+3} f_{n+3}{}^2$ [Chevillard et. al 11]
$\rightsquigarrow$ Algorithm `univsos2` with output size $\tau_2 = \mathcal{O}\left(n^4 \tau\right)$
bit complexity $\widetilde{\mathcal{O}}\left(n^4 \tau\right)$

- Maple package `https://github.com/magronv/univsos`
  $\rightsquigarrow$ Integration in `RAGlib`

univsos1: Outline [Schweighofer 99]

$f \in K[X]$ and $f > 0$

Minimizer a may not be in K . . .



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

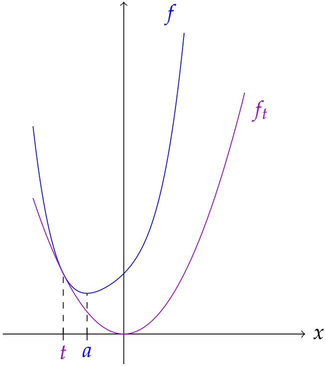
$a = \frac{5}{4(135+60\sqrt{6})^{1/3}} - \frac{4(135+60\sqrt{6})^{1/3}}{12} - \frac{1}{4}$

univsos1: Outline [Schweighofer 99]

$f \in K[X]$ and $f > 0$
Minimizer a may not be in K . . .

Find $f_t \in K[X]$ s.t. :

- $\deg f_t \leqslant 2$
- $f_t \geqslant 0$
- $f \geqslant f_t$
- $f - f_t$ has a root $t \in K$



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

`univsos1`: Outline [Schweighofer 99]

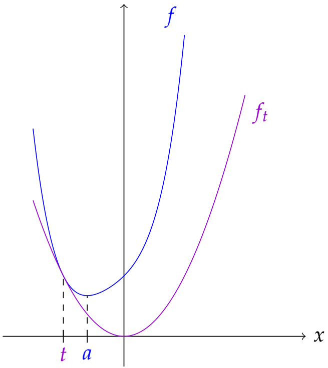
$f \in K[X]$ and $f > 0$

Minimizer a may not be in K . . .

Square-free decomposition:

$$f - f_t = g h^2$$

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



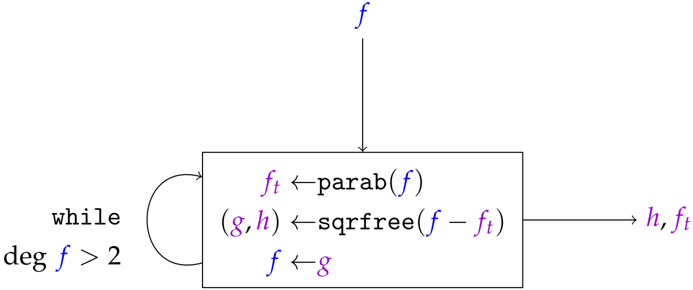
$f = 1 + X + X^2 + X^3 + X^4$

$f_t = X^2$

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

`univsos1`: Algorithm [Schweighofer 99]

- **Input**: $K, f \geqslant 0 \in K[X]$ of degree $n \geqslant 2$
- **Output**: SOS decomposition with coefficients in K



univsos1: Local Inequality

Lemma [Schweighofer 99]

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

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

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

univsos1: Local Inequality

Lemma [Schweighofer 99]

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

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

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

Proof.

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

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

□

`univsos1`: Global Inequality

Lemma [Schweighofer 99]

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

$\exists$ 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]

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

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

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

Proof.

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

- 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]

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

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

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

Proof.

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

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

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 K be an ordered real field, $f \in K[X]$, $\deg f = n$.

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

`univsos1`: Nichtnegativstellensätz

Theorem [Schweighofer 99]

Let K be an ordered real field, $f \in K[X]$, $\deg f = n$.

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

Proof by induction.

$\boxed{n = 2}$

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

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

□

`univsos1`: Nichtnegativstellensätz

Theorem [Schweighofer 99]

Let K be an ordered real field, $f \in K[X]$, $\deg f = n$.

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

Proof by induction.

$\boxed{n \geqslant 4}$

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

□

univsos1: Bitsize of t

Lemma

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

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

univsos1: Bitsize of t

Lemma

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

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

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]: $B = \mathcal{O}\left(n^2\tau\right)$

□

univsos1: Bitsize of Square-free Part

Lemma

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

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

`univsos1`: Bitsize of Square-free Part

Lemma

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

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

Proof.

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

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

□

`univsos1`: Output Bitsize

Theorem

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

`univsos1`: Output Bitsize

Theorem

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

Proof.

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

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

□

`univsos1`: Bit Complexity

Theorem

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

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

univsos1: Bit Complexity

Theorem

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

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

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

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

`univsos1`: Bit Complexity

Theorem

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

All involved polynomials have a global min in $\mathbb{Z}$
$\implies$ the bit complexity is $\widetilde{\mathcal{O}}\left(n^4 + n^3\tau\right)$.

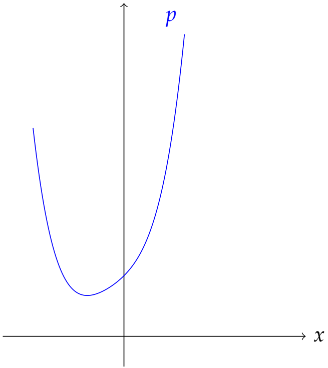
Proof.

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

□

univsos2: Outline [Chevillard et. al 11]

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



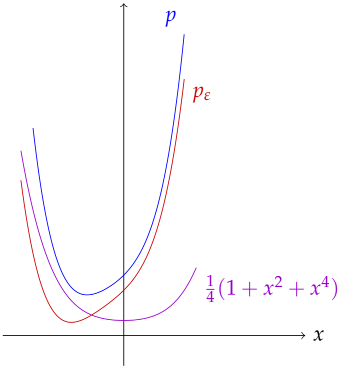
$p = 1 + X + X^2 + X^3 + X^4$

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

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

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

- $\varepsilon < l = lc(p)$
- $p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$



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

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

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

univsos2: Outline [Chevillard et. al 11]

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

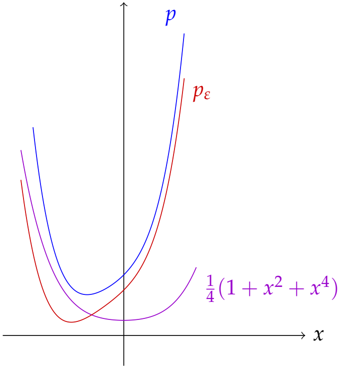
Find $\varepsilon \in \mathbb{Q}$ s.t. :

- $\varepsilon < l = lc(p)$
- $p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$

Root isolation:

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

- Small enough coefficients of u $\implies \varepsilon \sum_{i=0}^{k} X^{2i} + u$ SOS



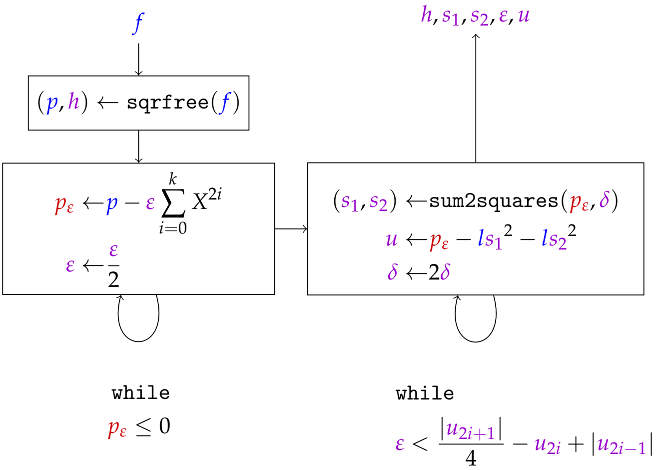
$$p = 1 + X + X^2 + X^3 + X^4$$

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

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

univsos2: Algorithm [Chevillard et. al 11]

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



`univsos2`: Perturbation

Lemma [Chevillard et. al 11]

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

Then

$$\exists\, N \in \mathbb{N}^{>0}, \varepsilon := \frac{1}{2^N} \text{ s.t. } p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0\,.$$

univsos2: Perturbation

Lemma [Chevillard et. al 11]

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

Then

$$\exists\, N \in \mathbb{N}^{>0}, \varepsilon := \frac{1}{2^N} \text{ s.t. } p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0\,.$$

Proof.

$$\varepsilon := 1/2 \implies \exists\, R \text{ s.t. } p_\varepsilon(x) > 0 \text{ for } |x| > R$$

Smallest N s.t. $\varepsilon = \frac{1}{2^N} < \frac{\inf_{|x| \leqslant R} p}{\sup_{|x| \leqslant R} 1 + x^2 \cdots + x^{2k}}$

□

univsos2: Nichtnegativstellensätz

Theorem [Chevillard et. al 11]

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

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

univsos2: Nichtnegativstellensätz

Theorem [Chevillard et. al 11]

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

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

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: $p = l{s_1}^2 + l{s_2}^2 + \varepsilon \sum_{i=0}^k X^{2i} + u$ 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, $\deg p = n = 2k$.
Then

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

univsos2: Bitsize of Perturbed Polynomials

Lemma

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

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

Proof.

$\varepsilon := 1/2 \implies \exists\, R \text{ s.t. } p_\varepsilon(x) > 0 \text{ for } |x| > R = 2n2^\tau$ (Cauchy)

- Smallest N s.t. $\varepsilon = \frac{1}{2^N} < \frac{\inf_{|x| \leqslant R} p}{1 + R^2 \cdots + R^{2k}}$

- $R > 1 \implies 1 + R^2 + \cdots + R^{2k} < kR^{2k}$

- $\inf_{x \in \mathbb{R}} p(x) > (n2^\tau)^{-n+2} 2^{-n \log_2 n - n\tau}$ [Melczer et. al 16] □

univsos2: Bitsize of Remainder

Lemma

Let $0 < p \in \mathbb{Z}[X]$ with bitsize τ, $\deg p = n = 2k$.
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. $\tau(\delta) = n \log_2 n + n\tau$

univsos2: Bitsize of Remainder

Lemma

Let $0 < p \in \mathbb{Z}[X]$ with bitsize τ, $\deg p = n = 2k$.
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. $\tau(\delta) = n \log_2 n + n\tau$

Proof.

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

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

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, $\deg f = n$.
The output bitsize τ_2 of `univsos2` on f is $\mathcal{O}(n^4 + n^3 \tau)$.

univsos2: Output Bitsize

Theorem

Let $0 \leqslant f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = n$.
The output bitsize τ_2 of univsos2 on f is $\mathcal{O}\left(n^4 + n^3\tau\right)$.

Proof.

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

💡 Square-free part: $\tau(p) = \mathcal{O}\left(n + \tau\right)$

💡 $|\hat{z}_j| = |z_j|(1 + 2^{-\delta}) \geqslant \frac{1}{2^{\tau(p_\varepsilon)+1}}(1 + 2^{-\delta})|$ [Melczer et.al 16]

□

`univsos2`: Bit Complexity

Theorem

Let $0 \leqslant f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = n$.
The bit complexity of `univsos2` on f is $\widetilde{\mathcal{O}}\,(n^4 + n^3\tau)$.

univsos2: Bit Complexity

Theorem

Let $0 \leqslant f \in \mathbb{Z}[X]$ with bitsize τ, $\deg f = n$.
The bit complexity of `univsos2` on f is $\widetilde{\mathcal{O}}(n^4 + n^3\tau)$.

Proof.

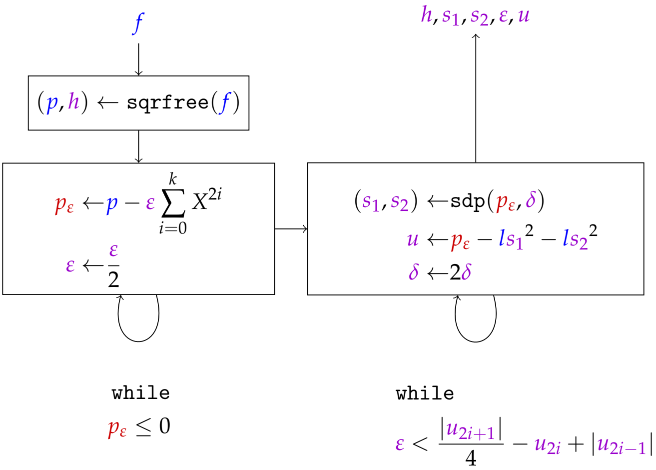
Root isolation with radius $\mathcal{O}(\delta + \tau(p_\varepsilon))$ [Melczer et.al 16]:

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

□

`univsos3`: SDP instead of Root Approximation

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



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	n	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	n	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

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

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

n	`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

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

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

n	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 complex roots $1 \pm i, \ldots, k \pm i$

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 complex roots $1 \pm i, \dots, k \pm i$

n	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 complex roots $1 \pm i, \ldots, k \pm i$

n	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	−	−

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

Conclusion and Perspectives

- Ordered real field K
- Let $f \in K[X]$ with bitsize τ, $\deg f = n$ and $f \geqslant 0$

$$f = c_1 {f_1}^2 + \cdots + c_s {f_s}^2$$

Algo	s	Output Size	Bit Complexity
`univsos1`	n	$\mathcal{O}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}} \tau\right)$	$\widetilde{\mathcal{O}}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}} \tau\right)$
`univsos2`	$n+3$	$\mathcal{O}\left(n^4 \tau\right)$	$\widetilde{\mathcal{O}}\left(n^4 \tau\right)$

Conclusion and Perspectives

- Ordered real field K
- Let $f \in K[X]$ with bitsize τ, $\deg f = n$ and $f \geqslant 0$

$$f = c_1 {f_1}^2 + \cdots + c_s {f_s}^2$$

Algo	s	Output Size	Bit Complexity
`univsos1`	n	$\mathcal{O}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}}\tau\right)$	$\widetilde{\mathcal{O}}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}}\tau\right)$
`univsos2`	$n+3$	$\mathcal{O}(n^4\tau)$	$\widetilde{\mathcal{O}}(n^4\tau)$
SDP	$n+3$	?	?
[Pourchet72]	5	?	?

$\rightsquigarrow$ SDP promising for small τ e.g. power sums for $n \leqslant 1000$

Conclusion and Perspectives

- Ordered real field K
- Let $f \in K[X]$ with bitsize τ, $\deg f = n$ and $f \geqslant 0$

$$f = c_1 {f_1}^2 + \cdots + c_s {f_s}^2$$

Algo	s	Output Size	Bit Complexity
`univsos1`	n	$\mathcal{O}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}} \tau\right)$	$\widetilde{\mathcal{O}}\left(\left(\frac{n}{2}\right)^{\frac{3n}{2}} \tau\right)$
`univsos2`	$n+3$	$\mathcal{O}\left(n^4 \tau\right)$	$\widetilde{\mathcal{O}}\left(n^4 \tau\right)$
SDP	$n+3$	?	?
[Pourchet72]	5	?	?

$\rightsquigarrow$ SDP promising for small τ e.g. power sums for $n \leqslant 1000$

💡 $\min_{x \in \mathbb{R}} f(x)$?

💡 Extension to complex variables, non-polynomial f?

End

Thank you for your attention!

https://github.com/magronv/univsos

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