An effective Positivstellensatz over the rational numbers for finite semialgebraic sets

Teresa Krick
Universidad de Buenos Aires & CONICET

with Lorenzo Baldi and Bernard Mourrain

VUB – February 28, 2025

A little history : Real polynomials

- Real univariate polynomials:

$$f \in \mathbb{R}[x]: \quad f \geq 0 \text{ on } \mathbb{R} \iff f = q_1^2 + q_2^2 \text{ for some } q_1, q_2 \in \mathbb{R}[x]$$

- Hilbert, 1888: Not every non-negative multivariate pol is a SOS of real pols
- Hilbert's 17th Problem, 1900: Is every non-negative pol a SOS of rational fns ?
- Artin, 1927: **YES!**
- Motzkin, 1967: First effective example of $f \geq 0$ on $\mathbb{R}[x,y]$ but not SOS

$$x^4y^2 + x^2y^4 + 1 - 3x^2y^2 = \frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2)^2 + (x^2-y^2)^2}{(x^2+y^2)^2}$$

A little history : Rational polynomials

- Landau, 1905 - Pourchet, 1971: Rational univariate polynomials

$$f \in \mathbb{Q}[x] : \quad f \geq 0 \text{ on } \mathbb{R} \iff f = \sum_{k=1}^{\not{8}5} \omega_k q_k^2 \text{ for some } \omega_k \in \mathbb{Q}_{\geq 0},\ q_k \in \mathbb{Q}[x]$$

A little history : Rational polynomials

- Landau, 1905 - Pourchet, 1971: Rational univariate polynomials

$$f \in \mathbb{Q}[x] : \quad f \geq 0 \text{ on } \mathbb{R} \iff f = \sum_{k=1}^{\not{8}5} \omega_k q_k^2 \text{ for some } \omega_k \in \mathbb{Q}_{\geq 0},\ q_k \in \mathbb{Q}[x]$$

- Sturmfels' question, 2007: Rational multivariate polynomials

$$f \in \mathbb{Q}[\boldsymbol{x}] : \ f \text{ SOS of } \boxed{\text{real}} \text{ pols} \Rightarrow f \text{ SOS of } \boxed{\text{rational}} \text{ pols ?}$$

A little history : Rational polynomials

- Landau, 1905 - Pourchet, 1971: Rational univariate polynomials

$$f \in \mathbb{Q}[x] : \quad f \geq 0 \ \text{ on } \mathbb{R} \quad \Longleftrightarrow \quad f = \sum_{k=1}^{\not{8}5} \omega_k q_k^2 \ \text{ for some } \ \omega_k \in \mathbb{Q}_{\geq 0}, \ q_k \in \mathbb{Q}[x]$$

- Sturmfels' question, 2007: Rational multivariate polynomials

$$f \in \mathbb{Q}[\boldsymbol{x}] : \ f \ \text{ SOS of } \boxed{\text{real}} \text{ pols } \Rightarrow \ f \text{ SOS of } \boxed{\text{rational}} \text{ pols ?}$$

- Peyrl-Parrilo, 2008: Under some strict feasibility condition **YES**

A little history : Rational polynomials

- Landau, 1905 - Pourchet, 1971: Rational univariate polynomials

$$f \in \mathbb{Q}[x] : \quad f \geq 0 \text{ on } \mathbb{R} \iff f = \sum_{k=1}^{\not{8}\,5} \omega_k q_k^2 \text{ for some } \omega_k \in \mathbb{Q}_{\geq 0},\ q_k \in \mathbb{Q}[x]$$

- Sturmfels' question, 2007: Rational multivariate polynomials

$$f \in \mathbb{Q}[\boldsymbol{x}] : \ f \ \text{SOS of } \boxed{\text{real}} \text{ pols} \Rightarrow f \text{ SOS of } \boxed{\text{rational}} \text{ pols ?}$$

- Peyrl-Parrilo, 2008: Under some strict feasibility condition **YES**
- Scheiderer, 2013: In general **NO!**

Nonnegativity on basic closed semialgebraic sets and SOS

$g_1, \ldots, g_r \in \mathbb{R}[\boldsymbol{x}]$ and $I \subset \mathbb{R}[\boldsymbol{x}]$ ideal

$$\boxed{S = \{\, \xi \in \mathbb{R}^n : \; g_i(\xi) \geq 0, \; 1 \leq i \leq r \,\} \cap V_{\mathbb{R}}(I) \quad \subset \; \mathbb{R}[\boldsymbol{x}]}$$

- Schmüdgen, 1991 – Putinar, 1993: If S is "compact" and $f > 0$ on S then

$$f \equiv \sum_k q_{0,k}^2 + \sum_{i=1}^{r} \left(\sum_k q_{i,k}^2 \right) g_i \mod I \qquad \text{for some } q_{i,k} \in \mathbb{R}[\boldsymbol{x}]$$

Nonnegativity on basic closed semialgebraic sets and SOS

$g_1, \ldots, g_r \in \mathbb{R}[\boldsymbol{x}]$ and $I \subset \mathbb{R}[\boldsymbol{x}]$ ideal

$$\boxed{S = \{\, \xi \in \mathbb{R}^n : g_i(\xi) \geq 0,\ 1 \leq i \leq r \,\} \cap V_{\mathbb{R}}(I) \quad \subset \ \mathbb{R}[\boldsymbol{x}]}$$

- Schmüdgen, 1991 – Putinar, 1993: If S is "compact" and $f > 0$ on S then

$$f \equiv \sum_k q_{0,k}^2 + \sum_{i=1}^r \left(\sum_k q_{i,k}^2 \right) g_i \mod I \qquad \text{for some } q_{i,k} \in \mathbb{R}[\boldsymbol{x}]$$

- Parrilo, 2003: If I is a radical zero-dimensional ideal and $f \geq 0$ on S, then

$$f \equiv \sum_{k=1}^D q_{0,k}^2 + \sum_{i=1}^r \left(\sum_{k=1}^D q_{i,k}^2 \right) g_i \mod I \qquad \text{for some } q_{i,k} \in \mathbb{R}[\boldsymbol{x}]$$

with $D \leq \# V_{\mathbb{C}}(I)$ and $\deg(q_{i,k}) \leq \deg(B)$ for B a basis of $\mathbb{R}[\boldsymbol{x}]/I$

Rational setting : Our results - I

$K \subset \mathbb{R}$, $g_1, \ldots, g_r \in K[\boldsymbol{x}]$ and $I \subset K[\boldsymbol{x}]$ zero-dimensional ideal

$$S = \{\xi \in \mathbb{R}^n : g_i(\xi) \geq 0,\ 1 \leq i \leq r\} \cap V_{\mathbb{R}}(I) \quad \subset \mathbb{R}[\boldsymbol{x}]$$

For $f \in K[\boldsymbol{x}]$, if $f > 0$ on S

then

$$f \equiv \sum_{k=1}^{D} \omega_{0,k} q_{0,k}^2 + \sum_{i=1}^{r} \left(\sum_{k=1}^{D} \omega_{i,k} q_{i,k}^2 \right) g_i \mod I \quad \text{for some } \omega_{i,k} \in K_{\geq 0} \text{ and } q_{i,k} \in K[\boldsymbol{x}]$$

with $D \leq \# V_{\mathbb{C}}(I)$ and $\deg(q_{i,k}) \leq \deg(B)$ for B a basis of $\mathbb{R}[\boldsymbol{x}]/I$

Rational setting : Our results - I

$K \subset \mathbb{R}$, $g_1, \ldots, g_r \in K[\boldsymbol{x}]$ and $I \subset K[\boldsymbol{x}]$ zero-dimensional ideal

$$S = \{\xi \in \mathbb{R}^n : g_i(\xi) \geq 0,\ 1 \leq i \leq r\} \cap V_{\mathbb{R}}(I) \quad \subset \mathbb{R}[\boldsymbol{x}]$$

For $f \in K[\boldsymbol{x}]$, if $f > 0$ on S or $f \geq 0$ on S with $(f) + (I : f) = (1)$

then

$$f \equiv \sum_{k=1}^{D} \omega_{0,k} q_{0,k}^2 + \sum_{i=1}^{r} \left(\sum_{k=1}^{D} \omega_{i,k} q_{i,k}^2 \right) g_i \mod I \quad \text{for some } \omega_{i,k} \in K_{\geq 0} \text{ and } q_{i,k} \in K[\boldsymbol{x}]$$

with $D \leq \# V_{\mathbb{C}}(I)$ and $\deg(q_{i,k}) \leq \deg(B)$ for B a basis of $\mathbb{R}[\boldsymbol{x}]/I$

On the assumption $(f) + (I : f) = (1)$ for $f \geq 0$ on S

$S = V_{\mathbb{R}}(I)$ with $I = (x^2)$, $f = x$ which satisfies $f(\xi) \geq 0$ for all $\xi \in V_{\mathbb{R}}(I)$

- $(f) + (I : f) = (x) + (x) = (x) \neq (1)$
- $x \equiv$ SOS $\mod (x^2)$? $\quad x = q_1^2(x) + \cdots + q_D^2(x) + q(x)x^2$?

On the assumption $(f) + (I : f) = (1)$ for $f \geq 0$ on S

$S = V_{\mathbb{R}}(I)$ with $I = (x^2)$, $f = x$ which satisfies $f(\xi) \geq 0$ for all $\xi \in V_{\mathbb{R}}(I)$

- $(f) + (I : f) = (x) + (x) = (x) \neq (1)$
- $x \equiv$ SOS $\mod (x^2)$? $x = q_1^2(x) + \cdots + q_D^2(x) + q(x)x^2$? **NO !**

On the assumption $(f)+(I:f)=(1)$ for $f \geq 0$ on S

$S = V_{\mathbb{R}}(I)$ with $I = (x^2)$, $f = x$ which satisfies $f(\xi) \geq 0$ for all $\xi \in V_{\mathbb{R}}(I)$

- $(f)+(I:f) = (x)+(x) = (x) \neq (1)$
- $x \equiv$ SOS $\mod (x^2)$? $\quad x = q_1^2(x) + \cdots + q_D^2(x) + q(x)x^2$? **NO !**

Notes:

- $(f)+(I:f) = (1) \iff f \in I + (f^2)$
- I 0-dimensional and **radical** $\implies (f)+(I:f) = (1)$

Rational setting : Our results - II

$g_1, \dots, g_r, h_1, \dots, h_s \in \mathbb{Z}[\boldsymbol{x}]$ with $\deg(g_i), \deg(h_j) \leq d,\ \mathrm{h}(g_i), \mathrm{h}(h_j) \leq \tau$

$I = (h_1, \dots, h_s) \subset \mathbb{Q}[\boldsymbol{x}]$ **radical** zero-dimensional ideal

$$S = \{\, \xi \in \mathbb{R}^n : \ g_i(\xi) \geq 0,\ 1 \leq i \leq r \,\} \cap V_{\mathbb{R}}(I) \quad \subset \mathbb{R}[\boldsymbol{x}]$$

For $f \in \mathbb{Z}[\boldsymbol{x}]$ with $\mathrm{h}(f) \leq \tau$, if $f \geq 0$ on S then

$$f \equiv \sum_{k=1}^{D} \frac{1}{\nu_{0,k}} q_{0,k}^2 + \frac{1}{\nu} \sum_{i=1}^{r} \left(\sum_{k=1}^{D} \omega_{i,k} q_{i,k}^2 \right) g_i \quad \bmod I$$

for some $\nu_{0,k},\ \nu,\ \omega_{i,k} \in \mathbb{N}$ and $q_{i,k} \in \mathbb{Z}[\boldsymbol{x}]$
with $D \leq \#V_{\mathbb{C}}(I),\ \deg(q_{i,k}) \leq \deg(f) + \deg(B)$ for B a basis of $\mathbb{R}[\boldsymbol{x}]/I$ and
$\mathrm{h}(\nu_{0,k}),\ \mathrm{h}(\nu),\ \mathrm{h}(\omega_{i,k}), \mathrm{h}(q_{i,k}) \leq c\, n \log\big((n+1)d\big)\, d^{3n}\, \delta\, \tau$ for $\delta := \max\{\deg(f), \deg(B)\}$

Some related work on rational sums of squares

- Peyrl-Parrilo, 2008: Computing sum of squares decompositions with rational coefficients *(global + condition)*
- Powers, 2011: Rational certificates of positivity on compact semialgebraic sets *(local + condition)*
- Magron-Safey El Din-Schweighofer, 2019: Algorithms for weighted sum of squares decomposition of non-negative univariate polynomials *(global)*
- Magron-Safey El Din, 2021: On exact Reznick, Hilbert-Artin and Putinar's representations *(global and local + condition)*
- Davis-Papp, 2022: Dual certificates and efficient rational sum-of-squares decompositions for polynomial optimization over compact sets *(local + cond.)*
- Magron-Safey El Din-Vu, 2023: Sum of squares decompositions of polynomials over their gradient ideals with rational coefficients *(local, 0-dim, radical)*
- K.-Mourrain-Szanto, 2023: Univariate rational sums of squares *(local)*

Proof strategy over $K \subset \mathbb{R}$

1. Step 1: $f > 0$ on $V_{\mathbb{R}}(I)$ for I a **radical** zero-dimensional ideal
2. Step 2: $f > 0$ on $V_{\mathbb{R}}(I)$ for I a zero-dimensional ideal
3. Step 3: $f > 0$ on $S = \{g_1 \geq 0, \dots, g_r \geq 0\} \cap V_{\mathbb{R}}(I)$
4. Step 4: $f \geq 0$ on S with $1 \in (f) + (I : f)$

Step 1: $f > 0$ on $V_{\mathbb{R}}(I)$ with I 0-dim and radical

$$S = V_{\mathbb{R}}(I) = \{\xi\} \text{ with } V_{\mathbb{C}}(I) = \{\xi, \zeta, \overline{\zeta}\}$$

Set $u_\xi \in \mathbb{R}[\boldsymbol{x}]$, $u_\zeta, u_{\overline{\zeta}} = \overline{u}_\zeta \in \mathbb{C}[\boldsymbol{x}]$ for the idempotents of $V_{\mathbb{C}}(I)$

- Parrilo's method, 2002:

$$\begin{aligned} f &\equiv f(\xi)u_\xi^2 + f(\zeta)u_\zeta^2 + f(\overline{\zeta})\overline{u}_\zeta^2 \mod I \\ &\equiv f(\xi)u_\xi^2 + \left(f(\zeta)u_\zeta^2 + f(\overline{\zeta})\overline{u}_\zeta^2 + 2|f(\zeta)|u_\zeta\overline{u}_\zeta\right) \mod I \\ &\equiv \underbrace{(\sqrt{f(\xi)}u_\xi)}_{\in \mathbb{R}[\boldsymbol{x}]}{}^2 + \Big(\underbrace{\sqrt{f(\zeta)}u_\zeta + \sqrt{f(\overline{\zeta})}\overline{u}_\zeta}_{\in \mathbb{R}[\boldsymbol{x}]}\Big)^2 \mod I \end{aligned}$$

Step 1: $f > 0$ on $V_{\mathbb{R}}(I)$ with I 0-dim and radical

$$\boxed{S = V_{\mathbb{R}}(I) = \{\xi\} \text{ with } V_{\mathbb{C}}(I) = \{\xi, \zeta, \overline{\zeta}\}}$$

Set $u_\xi \in \mathbb{R}[\boldsymbol{x}]$, $u_\zeta, u_{\overline{\zeta}} = \overline{u}_\zeta \in \mathbb{C}[\boldsymbol{x}]$ for the idempotents of $V_{\mathbb{C}}(I)$

- Parrilo's method, 2002:

$$\begin{aligned} f &\equiv f(\xi)u_\xi^2 + f(\zeta)u_\zeta^2 + f(\overline{\zeta})\overline{u}_\zeta^2 \quad \mod I \\ &\equiv f(\xi)u_\xi^2 + \left(f(\zeta)u_\zeta^2 + f(\overline{\zeta})\overline{u}_\zeta^2 + 2|f(\zeta)|u_\zeta\overline{u}_\zeta\right) \quad \mod I \\ &\equiv \underbrace{\left(\sqrt{f(\xi)}u_\xi\right)^2}_{\in \mathbb{R}[\boldsymbol{x}]} + \underbrace{\left(\sqrt{f(\zeta)}u_\zeta + \sqrt{f(\overline{\zeta})}\overline{u}_\zeta\right)^2}_{\in \mathbb{R}[\boldsymbol{x}]} \quad \mod I \end{aligned}$$

- A modification [K.-Mourrain-Szanto, 2023]:

$$f \equiv \underbrace{f(\xi)u_\xi^2}_{\theta_1^2} + \underbrace{\left(f(\zeta)u_\zeta^2 + f(\overline{\zeta})\overline{u}_\zeta^2 + 2\,\lambda\, u_\zeta\overline{u}_\zeta\right)}_{(\theta_2^2 \,+\, \theta_3^2)} \quad \mod I \quad \text{for } \lambda > |f(\zeta)|$$

$$\equiv \quad \theta_1^2 \quad + \quad (\theta_2^2 + \theta_3^2) \quad \mod I \quad \text{with } \{\theta_i\} \subset \mathbb{R}[\boldsymbol{x}] \text{ **basis** of } \mathbb{R}[\boldsymbol{x}]/I$$

Step 1: SOS and psd matrices - A standard translation

$f = \sum_k \theta_k^2$ with $\theta_k \in \mathbb{R}[\boldsymbol{x}]$ l.i.

$Q = \Theta\Theta^t$ $\downarrow$

$$f = B \underbrace{Q}_{\textbf{psd}} B^t$$

where

- B is a basis of monomials up to $\deg(f)/2$
- Θ is the coefficient matrix of $(\theta_k)_k$ in B

Step 1: SOS and psd matrices - A standard translation

$$f = \sum_k \theta_k^2 \quad \text{with } \theta_k \in \mathbb{R}[\boldsymbol{x}] \text{ l.i.}$$

$$Q = \Theta\Theta^t \quad \downarrow$$

$$f = B \underbrace{Q}_{\textbf{psd}} B^t \quad \xrightarrow{Q = U\Delta U^t} \quad f = (BU)\Delta(BU)^t$$

where

- B is a basis of monomials up to $\deg(f)/2$
- Θ is the coefficient matrix of $(\theta_k)_k$ in B

Step 1: SOS and psd matrices - A standard translation

$f = \sum_k \theta_k^2$ with $\theta_k \in \mathbb{R}[\boldsymbol{x}]$ l.i. $\qquad$ $f = \sum_k \omega_k\, q_k^2$ with $\omega_k \in \mathbb{R}_{\geq 0}, q_k \in \mathbb{R}[\boldsymbol{x}]$

$Q = \Theta\Theta^t \quad \downarrow \qquad\qquad \uparrow \quad (q_k)_k = B\,U,\ \omega_k = \Delta_{k,k}$

$f = B \underbrace{Q}_{\textbf{psd}} B^t \qquad \overrightarrow{Q = U\Delta U^t} \qquad f = (B\,U)\Delta(B\,U)^t$

where

- B is a basis of monomials up to $\deg(f)/2$
- Θ is the coefficient matrix of $(\theta_k)_k$ in B

Step 1: SOS and psd matrices - A standard translation

$f = \sum_k \theta_k^2$ with $\theta_k \in \mathbb{R}[\boldsymbol{x}]$ l.i. $\quad \xleftarrow{\theta_k = \sqrt{\omega_k}\, q_k} \quad f = \sum_k \omega_k\, q_k^2$ with $\omega_k \in \mathbb{R}_{\geq 0}, q_k \in \mathbb{R}[\boldsymbol{x}]$

$Q = \Theta\Theta^t \; \downarrow \qquad\qquad \uparrow \; (q_k)_k = B\,U,\ \omega_k = \Delta_{k,k}$

$f = B \underbrace{Q}_{\textbf{psd}} B^t \quad \xrightarrow{Q = U\Delta U^t} \quad f = (B\,U)\Delta(B\,U)^t$

where

- B is a basis of monomials up to $\deg(f)/2$
- Θ is the coefficient matrix of $(\theta_k)_k$ in B

Step 1: SOS for $f \in \mathbb{Q}[\mathrm{x}]$ and pd matrices

$$f \equiv \sum_{k=1}^{D} \theta_k^2 \quad \mathrm{mod}\ I_{\mathbb{R}}$$ with θ_k **basis** of $\mathbb{R}[\boldsymbol{x}]/I$

$\widetilde{Q} = \Theta\Theta^t \downarrow$ in $S^D(\mathbb{R})$

$$f \equiv B \underbrace{\widetilde{Q}}_{\textbf{pd}} B^t \quad \mathrm{mod}\ I_{\mathbb{R}}$$

Step 1: SOS for $f \in \mathbb{Q}[\mathrm{x}]$ and pd matrices

$f \equiv \sum_{k=1}^{D} \theta_k^2 \quad \mathrm{mod}\ I_{\mathbb{R}}$ with θ_k **basis** of $\mathbb{R}[\boldsymbol{x}]/I$

$\widetilde{Q} = \Theta\Theta^t \Big\downarrow$ in $S^D(\mathbb{R})$

$$f \equiv B \underbrace{\widetilde{Q}}_{\textbf{pd}} B^t \quad \mathrm{mod}\ I_{\mathbb{R}}$$

Rounding $\Big\downarrow$ Projecting

$$f \equiv B \underbrace{Q}_{\textbf{pd}} B^t \quad \mathrm{mod}\ I_{\mathbb{Q}}$$

Step 1: SOS for $f \in \mathbb{Q}[\mathrm{x}]$ and pd matrices

$f \equiv \sum_{k=1}^{D} \theta_k^2 \quad \bmod I_{\mathbb{R}}$ with θ_k **basis** of $\mathbb{R}[\boldsymbol{x}]/I$

$\widetilde{Q} = \Theta\Theta^t$ $\downarrow$ in $S^D(\mathbb{R})$

$$f \equiv B \underbrace{\widetilde{Q}}_{\textbf{pd}} B^t \quad \bmod I_{\mathbb{R}}$$

Rounding $\downarrow$ Projecting

$$f \equiv B \underbrace{Q}_{\textbf{pd}} B^t \quad \bmod I_{\mathbb{Q}} \quad \xrightarrow[\text{sqf Cholesky dec.}]{} \quad f \equiv (B\,L)\Delta(B\,L)^t \quad \bmod I_{\mathbb{Q}}$$

$Q = L\Delta L^t$

sqf Cholesky dec.

Step 1: SOS for $f \in \mathbb{Q}[\mathrm{x}]$ and pd matrices

$$f \equiv \sum_{k=1}^{D} \theta_k^2 \mod I_{\mathbb{R}}$$ with θ_k **basis** of $\mathbb{R}[\boldsymbol{x}]/I$

$\widetilde{Q} = \Theta\Theta^t$ $\Big\downarrow$ in $S^D(\mathbb{R})$

$$f \equiv B \underbrace{\widetilde{Q}}_{\textbf{pd}} B^t \mod I_{\mathbb{R}}$$

$$f \equiv \sum_{k=1}^{D} \omega_k q_k^2 \mod I_{\mathbb{Q}}$$

Rounding $\Big\downarrow$ Projecting

$\Big\uparrow$ $(q_k)_k = B\,L,\ \omega_k = \Delta_{k,k}$

$$f \equiv B \underbrace{Q}_{\textbf{pd}} B^t \mod I_{\mathbb{Q}}$$

$\longrightarrow$ $Q = L\Delta L^t$

sqf Cholesky dec.

$$f \equiv (B\,L)\Delta(B\,L)^t \mod I_{\mathbb{Q}}$$

Step 1: Example - $f > 0$ on $V_{\mathbb{R}}(I)$ with I 0-dim and radical

$$S = V_{\mathbb{R}}(I) \text{ with } I = (x^3 - 2) \subset \mathbb{Q}[x], \quad f = x \in \mathbb{Q}[x]$$

- $\xi = \sqrt[3]{2},\ \lambda = 2\sqrt[3]{2} > |f(\zeta)|$
- $x \equiv \frac{1}{18}(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4})^2 + \frac{1}{6}(x^2 - \sqrt[3]{4})^2 + \frac{1}{6}(x^2 - \sqrt[3]{2}\,x)^2 \mod I_{\mathbb{R}}$
- $f \equiv (1\ x\ x^2)\,\widetilde{Q}\,(1\ x\ x^2)^t \mod I_{\mathbb{R}}$

$$\widetilde{Q} = \begin{pmatrix} \frac{4\sqrt[3]{2}}{9} & \frac{1}{9} & -\frac{\sqrt[3]{4}}{9} \\ \frac{1}{9} & \frac{2\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} \\ -\frac{\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} & \frac{7}{18} \end{pmatrix}$$

Step 1: Example - $f > 0$ on $V_{\mathbb{R}}(I)$ with I 0-dim and radical

$$S = V_{\mathbb{R}}(I) \ \text{ with } I = (x^3 - 2) \subset \mathbb{Q}[x], \quad f = x \in \mathbb{Q}[x]$$

- $\xi = \sqrt[3]{2}, \ \lambda = 2\sqrt[3]{2} > |f(\zeta)|$
- $x \equiv \frac{1}{18}(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4})^2 + \frac{1}{6}(x^2 - \sqrt[3]{4})^2 + \frac{1}{6}(x^2 - \sqrt[3]{2}\,x)^2 \mod I_{\mathbb{R}}$
- $f \equiv (1 \ x \ x^2)\, \widetilde{Q}\, (1 \ x \ x^2)^t \mod I_{\mathbb{R}}$

Rounding and projecting:

$$\widetilde{Q} = \begin{pmatrix} \frac{4\sqrt[3]{2}}{9} & \frac{1}{9} & -\frac{\sqrt[3]{4}}{9} \\ \frac{1}{9} & \frac{2\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} \\ -\frac{\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} & \frac{7}{18} \end{pmatrix} \rightsquigarrow Q = \begin{pmatrix} 0.6 & 0.1 & -0.2 \\ 0.1 & 0.4 & -0.15 \\ -0.2 & -0.15 & 0.4 \end{pmatrix}$$

Step 1: Example - $f > 0$ on $V_{\mathbb{R}}(I)$ with I 0-dim and radical

$$S = V_{\mathbb{R}}(I) \;\text{ with } I = (x^3 - 2) \subset \mathbb{Q}[x], \quad f = x \in \mathbb{Q}[x]$$

- $\xi = \sqrt[3]{2},\ \lambda = 2\sqrt[3]{2} > |f(\zeta)|$
- $x \equiv \frac{1}{18}(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4})^2 + \frac{1}{6}(x^2 - \sqrt[3]{4})^2 + \frac{1}{6}(x^2 - \sqrt[3]{2}\,x)^2 \mod I_{\mathbb{R}}$
- $f \equiv (1\ x\ x^2)\,\widetilde{Q}\,(1\ x\ x^2)^t \mod I_{\mathbb{R}}$

Rounding and projecting:

$$\widetilde{Q} = \begin{pmatrix} \frac{4\sqrt[3]{2}}{9} & \frac{1}{9} & -\frac{\sqrt[3]{4}}{9} \\ \frac{1}{9} & \frac{2\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} \\ -\frac{\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} & \frac{7}{18} \end{pmatrix} \rightsquigarrow Q = \begin{pmatrix} 0.6 & 0.1 & -0.2 \\ 0.1 & 0.4 & -0.15 \\ -0.2 & -0.15 & 0.4 \end{pmatrix}$$

- Square-root-free Cholesky decomposition:

$$f \equiv \frac{3}{5}\left(\frac{1}{3}x^2 - \frac{1}{6}x - 1\right)^2 + \frac{23}{60}\left(\frac{7}{23}x^2 - x\right)^2 + \frac{137}{460}x^4 \mod I_{\mathbb{Q}}$$

Proof strategy over $\mathbb{Q}$ for I radical

1. Step 1: $f > 0$ on $V_{\mathbb{R}}(I)$
2. Step 2: $f > 0$ on $S = \{g_1 \geq 0, \ldots, g_r \geq 0\} \cap V_{\mathbb{R}}(I)$
3. Step 3: $f \geq 0$ on S

Step 1: A crucial tool

$I \subset \mathbb{Q}[\boldsymbol{x}]$ zero-dimensional ideal with $V := V_{\mathbb{C}}(I)$

(Philippon-)Height of V*:* $\mathrm{h}(V)$ defined by means of the primitive Chow form of V

$$\mathrm{Ch}_V = a \prod_{\zeta \in V} (U_0 + U_1\zeta_1 + \cdots + U_n\zeta_n) \quad \in \ \mathbb{Z}[U_0, \dots, U_n] \quad \text{satisfies}$$

- $|\mathrm{h}(V) - \mathrm{h}(\mathrm{Ch}_V)| \leq 3\log(n+1)\deg(V)$
- $\sum_{\zeta \in V} \log\left(\|(1,\zeta)\|_2\right) \leq \mathrm{h}(V)$

- **Arithmetic Bézout Inequality (K.-Pardo-Sombra 2001):**

$$h_1, \dots, h_s \in \mathbb{Z}[\boldsymbol{x}] \quad \text{with} \quad d_j := \deg(h_j) \quad \text{and} \quad \tau_j := \mathrm{h}(h_j)$$

Assume $d := d_2 \geq \cdots \geq d_s$ and $\tau := \max\{\tau_2, \dots, \tau_s\}$. Then

$$\mathrm{h}\big(V(h_1, \dots, h_s)\big) \leq d^{n-1}\tau_1 + 2n\log(n+1)d^{n-2}d_1(d+\tau)$$

Step 1 : Arithmetic Shape Lemma (GR/RUR)

$h_1, \dots, h_s \in \mathbb{Z}[\boldsymbol{x}]$ with $d := d_2 \geq \cdots \geq d_s$ and $\tau := \max\{\tau_2, \dots, \tau_s\}$

$I = (h_1, \dots, h_s) \subset \mathbb{Q}[\boldsymbol{x}]$ **radical** zero-dimensional ideal

$$\mathbb{Q}[\boldsymbol{x}]/I \quad \xrightarrow{\simeq} \quad \mathbb{Q}[t]/(\omega_0) \ \simeq \ \langle 1, t, \dots, t^{D-1} \rangle_{\mathbb{Q}}$$

$$x_i \quad \longmapsto \quad \omega_i(t)/{\omega_0}'(t) \quad \mod \ \omega_0$$

where for $\ell(\boldsymbol{x}) = u_1 x_1 + \cdots + u_n x_n \in \mathbb{Z}[\boldsymbol{x}]$ a separating linear form for V,

$$\omega_0(t) := \mathrm{Ch}_V(t, -\ell) = a \prod_{\zeta \in V} (t - \ell(\zeta)) \quad \in \ \mathbb{Z}[t]$$

and $\omega_i(t) := \partial_{U_i} \mathrm{Ch}_V(t, -\ell) \ \in \mathbb{Z}[t]$ with

$$\deg(\omega_i) \leq D \quad \text{and} \quad \mathrm{h}(\omega_i) \leq d^{n-1}\tau_1 + c\, n \log\big((n+1)d\big) d^{n-2} d_1 (d + \tau)$$

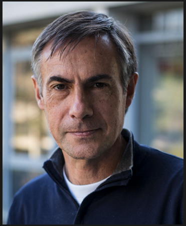
Step 1 : Consequences

- Upper and lower bounds for a polynomial $p \in \mathbb{Z}[\mathbf{x}]$ at a root $\zeta \in V$
- Upper bound for the coefficients of the remainder $\overline{p} \in \mathbb{C}[\boldsymbol{x}]/I$ of $p \in \mathbb{C}[\boldsymbol{x}]$
- Upper bound for the coefficients of the idempotents $u_\zeta \in \mathbb{C}[\boldsymbol{x}]$
- Upper bound for the coefficients of a pd matrix $\widetilde{Q} \in S^D(\mathbb{R})$ so that

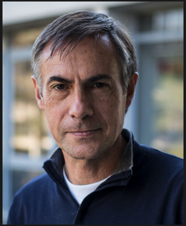
$$f \equiv B\,\widetilde{Q}\,B^t \mod I_{\mathbb{R}}$$

  and lower bound for $\sigma_{\min}(\widetilde{Q})$
- Bound for the height of the projection of a pd $\widehat{Q} \in S^D(\mathbb{Q})$ on the linear variety

$$\{\, Q \in S^D(\mathbb{Q}) \,:\, f \equiv B\,Q\,B^t \mod I \,\}$$



Thanks!



Thanks!