Certification via Symbolic-Numeric Computations

Lihong Zhi

Key Laboratory of Mathematics Mechanization
Chinese Academy of Sciences, Beijing

Joint works with F. Guo, S. Hutton, E. L. Kaltofen, B. Li, M. Safey, Z.F. Yang

SCAN'2010, Lyon, France, September 27-30

Outline

- Certification via Sums-of-Squares(SOS) of polynomials with rational coefficients.

Outline

- Certification via Sums-of-Squares(SOS) of polynomials with rational coefficients.

- Certification via SOS of rational functions with rational coefficients.

Outline

- Certification via Sums-of-Squares(SOS) of polynomials with rational coefficients.
- Certification via SOS of rational functions with rational coefficients.
- Certification via generalized critical values and SOS.

Outline

- Certification via Sums-of-Squares(SOS) of polynomials with rational coefficients.
- Certification via SOS of rational functions with rational coefficients.
- Certification via generalized critical values and SOS.
- Certification via a dual of Seidenberg's method and SOS.

Rational Function Optimization Problem

$$r = \min_{\xi \in \mathbb{R}^n} \frac{f(\xi)}{g(\xi)} \quad (\text{where } g(\xi) > 0 \text{ for all } \xi \in \mathbb{R}^n)$$

Rational Function Optimization Problem

$$r = \min_{\xi \in \mathbb{R}^n} \frac{f(\xi)}{g(\xi)} \quad (\text{where } g(\xi) > 0 \text{ for all } \xi \in \mathbb{R}^n)$$

It can be transformed as the SOS relaxation [Nie et al. 2008]:

$$\left.\begin{array}{ll} r^* := \sup\limits_{r \in \mathbb{R}, W} & r \\ \text{s. t.} & f(\mathbf{X}) - r g(\mathbf{X}) = m_d(\mathbf{X})^T \cdot W \cdot m_d(\mathbf{X}) \\ & W \succeq 0,\ W^T = W \end{array}\right\}$$

where $m_d(\mathbf{X})$ is the column vector of all terms in $\mathbf{X}_1, \ldots, \mathbf{X}_n$ up to degree d.

Rational Function Optimization Problem

$$r = \min_{\xi \in \mathbb{R}^n} \frac{f(\xi)}{g(\xi)} \quad (\text{where } g(\xi) > 0 \text{ for all } \xi \in \mathbb{R}^n)$$

It can be transformed as the SOS relaxation [Nie et al. 2008]:

$$\left.\begin{array}{lll} r^* := \sup\limits_{r \in \mathbb{R}, W} & r & \\ \text{s. t.} & f(\mathbf{X}) - rg(\mathbf{X}) = m_d(\mathbf{X})^T \cdot W \cdot m_d(\mathbf{X}) \\ & W \succeq 0,\ W^T = W \end{array}\right\}$$

where $m_d(\mathbf{X})$ is the column vector of all terms in $\mathbf{X}_1, \ldots, \mathbf{X}_n$ up to degree d.

Software: SeDuMi, YALMIP, SOSTOOLS, SparsePOP, SDPT3, VSDP, GloptiPoly

Exact Certification of Optima via Rational SOS

Problems with sum-of-squares certificates:

- Numerical sum-of-squares yields **“ $\geq$ 0” approximately**!
- **Exact** optimum is **high-degree/large-height** algebraic number.

Exact Certification of Optima via Rational SOS

Problems with sum-of-squares certificates:

- Numerical sum-of-squares yields **“ $\geq$ 0” approximately**!
- **Exact** optimum is **high-degree/large-height** algebraic number.

We certify a **rational** lower bound $\tilde{\mathbf{r}} \lessapprox \mathbf{r} \leq \frac{\mathbf{f}}{\mathbf{g}}$ via **rational** matrix $\widetilde{W}$ so that the following conditions hold **exactly**:

$$f(\mathbf{X}) - \tilde{r}g(\mathbf{X}) = m_d(\mathbf{X})^T \cdot \widetilde{W} \cdot m_d(\mathbf{X}),\ \widetilde{W} \succeq 0$$

Main Steps

1. Compute an approximate SOS with high accuracy

$$f(\mathbf{X}) - r^* g(\mathbf{X}) \approx m_d(\mathbf{X})^T \cdot W \cdot m_d(\mathbf{X}),\ W \gtrapprox 0$$

- SDP in Matlab + Gauss-Newton Refinement in Maple
- Multiple precision SDP solver in Maple

Main Steps

1. Compute an approximate SOS with high accuracy

$$f(\mathbf{X}) - r^* g(\mathbf{X}) \approx m_d(\mathbf{X})^T \cdot W \cdot m_d(\mathbf{X}),\ W \succsim 0$$

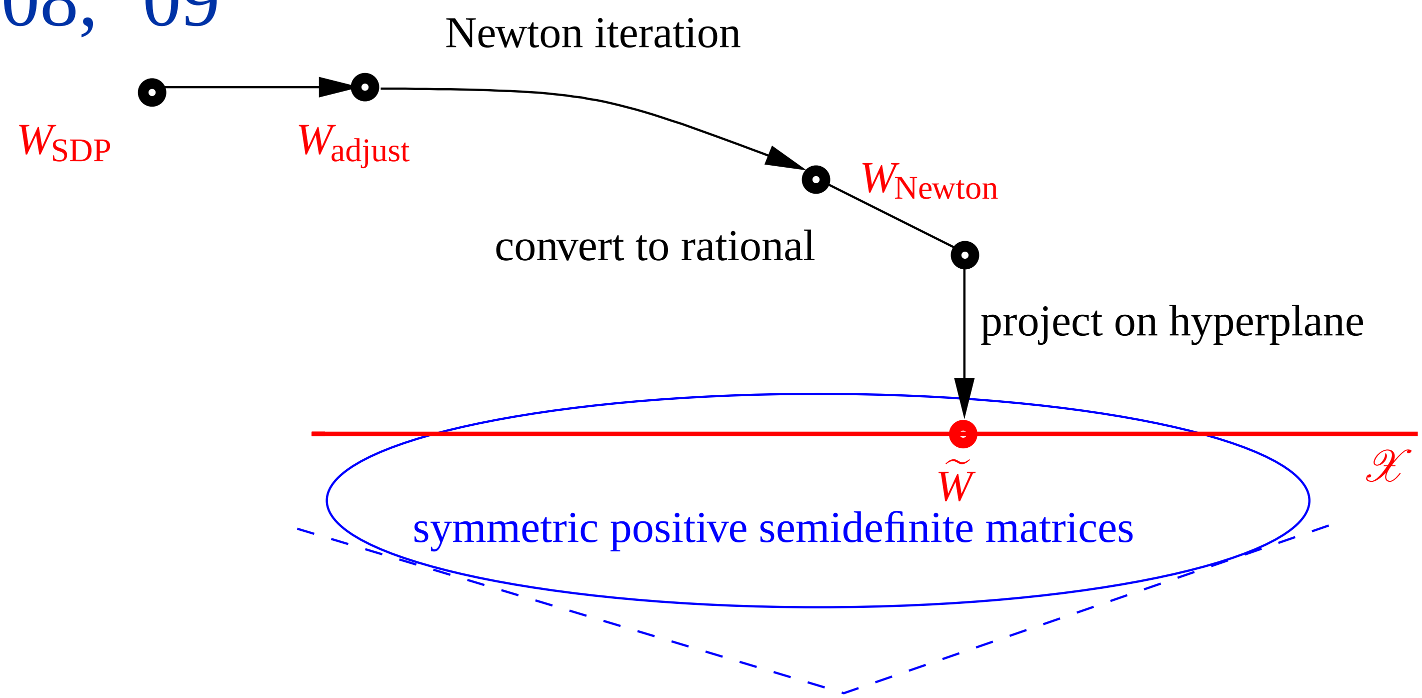
- SDP in Matlab + Gauss-Newton Refinement in Maple
- Multiple precision SDP solver in Maple

2. Convert it into an exact rational SOS

$$f(\mathbf{X}) - \tilde{r} g(\mathbf{X}) = m_d(\mathbf{X})^T \cdot \widetilde{W} \cdot m_d(\mathbf{X}),\ \widetilde{W} \succeq 0$$

- Orthogonal projection
- Rational coefficient vector recovery, e.g., LLL algorithm

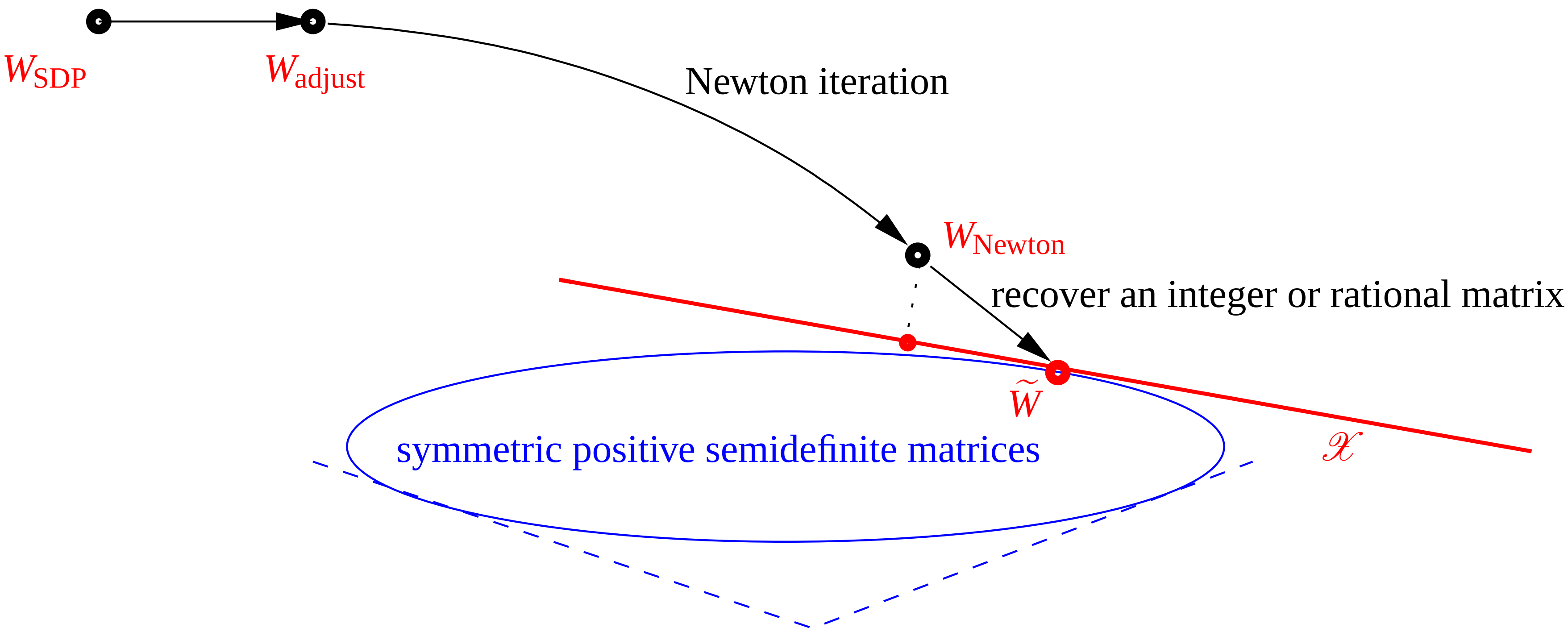
Rationalizing Sum-Of-Squares: "Easy Case" Harrison'07; Peyrl, Parrilo'07, '08; Kaltofen, Li, Yang, Zhi,'08, '09



where the affine linear hyperplane is given by

$$\mathscr{X} = \{A \mid A^T = A, f(\mathbf{X}) - \tilde{r}g(\mathbf{X}) = m_{\mathscr{G}}(\mathbf{X})^T \cdot A \cdot m_{\mathscr{G}}(\mathbf{X})\}$$

Rationalizing a Sum-Of-Squares: “Hard Case”



where the affine linear hyperplane is **tangent** to the cone boundary

singular $\widetilde{W}$: **real optimizers, fewer squares, missing terms**

A "Hard Case" Example

Voronoi2(a,α,β,X,Y) [Everett et al.'07] has 253 monomials

$$a^{12}\alpha^6 + a^{12}\alpha^4 - 4a^{11}\alpha^5 Y + 10a^{11}\alpha^4\beta X + \underbrace{\cdots}_{248\text{ terms}} + 20a^{10}\alpha^2X^2.$$

Voronoi2 is nonnegative and the global minimum zero is reached on two manifolds defined by

$$\{Y + a\alpha, 2a\beta X + 4a^3\beta X + 4a^4\alpha^2 + 4a^4 + 4a^2\alpha^2 + 4a^2 - a^2X^2 - \beta^2\}$$

and

$$\{aX + \beta, -4\beta^2 - 4 - 2a^3\alpha Y - 4a\alpha Y + a^4\alpha^2 + a^2Y^2 - 4a^2\beta^2 - 4a^2\}.$$

It is not hard!

- The singular values of the computed Gram matrix $W_{118\times 118}$:

  $196, 152.78, 152.29, 107.36, 68.64, 61.48, \mathbf{43.05}, 42.58, 25.06, \cdots$

It is not hard!

- The singular values of the computed Gram matrix $W_{118\times 118}$:

  $196, 152.78, 152.29, 107.36, 68.64, 61.48, \mathbf{43.05}, 42.58, 25.06, \cdots$

- Compute the truncated Cholesky decomposition of $W \approx \hat{L}\hat{L}^T$ w.r.t. tolerance **43** and obtain

$$\mathit{Voronoi2} \approx \mathbf{g_1^2} + \mathbf{g_2^2} + \cdots + \mathbf{g_7^2} \qquad (*)$$

It is not hard!

- The singular values of the computed Gram matrix $W_{118\times 118}$:

  $196, 152.78, 152.29, 107.36, 68.64, 61.48, \mathbf{43.05}, 42.58, 25.06, \cdots$

- Compute the truncated Cholesky decomposition of $W \approx \hat{L}\hat{L}^T$ w.r.t. tolerance **43** and obtain

$$\mathit{Voronoi2} \approx \mathbf{g_1^2} + \mathbf{g_2^2} + \cdots + \mathbf{g_7^2} \qquad (*)$$

- Apply Gauss-Newton iterations to refine $(*)$, after 30 iterations, we obtain $\tilde{L}$.

It is not hard!

- The singular values of the computed Gram matrix $W_{118\times 118}$:

  $196, 152.78, 152.29, 107.36, 68.64, 61.48, \mathbf{43.05}, 42.58, 25.06, \cdots$

- Compute the truncated Cholesky decomposition of $W \approx \hat{L}\hat{L}^T$ w.r.t. tolerance **43** and obtain

$$Voronoi2 \approx \mathbf{g}_1^2 + \mathbf{g}_2^2 + \cdots + \mathbf{g}_7^2 \qquad (*)$$

- Apply Gauss-Newton iterations to refine $(*)$, after 30 iterations, we obtain $\tilde{L}$.
- Round $\tilde{L}\,\tilde{L}^T$ to an **integer matrix** $\widetilde{W} = LDL^T$:

$$Voronoi2 = \mathbf{f}_1^2 + \frac{\mathbf{1}}{\mathbf{16}}\mathbf{f}_2^2 + \mathbf{f}_3^2 + \frac{\mathbf{1}}{\mathbf{28}}\mathbf{f}_4^2 + \frac{\mathbf{7}}{\mathbf{27}}\mathbf{f}_5^2,$$

where $f_i \in \mathbb{Q}[a, \alpha, \beta, X, Y]$.

Siegfried Rump's 2006 Model Problem

For $n = 1, 2, 3, \ldots$ compute the global minimum μ_n:

$$\mu_n = \min_{P,Q} \frac{\|PQ\|_2^2}{\|P\|_2^2 \|Q\|_2^2} \qquad \text{(rational function)}$$

$$\text{s. t. } P(Z) = \sum_{i=1}^{n} p_i Z^{i-1}, Q(Z) = \sum_{i=1}^{n} q_i Z^{i-1} \in \mathbb{R}[Z] \setminus \{0\}$$

Siegfried Rump's 2006 Model Problem

For $n = 1, 2, 3, \ldots$ compute the global minimum μ_n:

$$\mu_n = \min_{P,Q} \frac{\|PQ\|_2^2}{\|P\|_2^2 \|Q\|_2^2} \qquad \text{(rational function)}$$

$$\text{s. t. } P(Z) = \sum_{i=1}^{n} p_i Z^{i-1}, Q(Z) = \sum_{i=1}^{n} q_i Z^{i-1} \in \mathbb{R}[Z] \setminus \{0\}$$

$$\Updownarrow$$

$$\mu_n = \min_{P,Q} \|PQ\|_2^2$$

$$\text{s. t. } \|P\|_2 = \|Q\|_2 = 1, \deg(P) \le n-1, \deg(Q) \le n-1$$

Local Minimum By Lagrangian Multipliers

Siegfried Rump's 2006 Model Problem

For $n = 1, 2, 3, \ldots$ compute the global minimum μ_n:

$$\mu_n = \min_{P,Q} \frac{\|PQ\|_2^2}{\|P\|_2^2 \|Q\|_2^2} \qquad \text{(rational function)}$$

$$\text{s. t. } P(Z) = \sum_{i=1}^{n} p_i Z^{i-1}, Q(Z) = \sum_{i=1}^{n} q_i Z^{i-1} \in \mathbb{R}[Z] \setminus \{0\}$$

$$\Updownarrow$$

$$\frac{1}{\mu_n} = \max_{P,Q} B_{n-1}$$

$$\text{s. t. } \|P(Z)\|_2^2 \cdot \|Q(Z)\|_2^2 = B_{n-1} \|P(Z) \cdot Q(Z)\|_2^2$$

$$P, Q \in \mathbb{R}[Z] \setminus \{0\}, \deg(P) \leq n-1, \deg(Q) \leq n-1$$

Mignotte's factor coefficient bound: $\frac{1}{\mu_n} \leq \binom{2n-2}{n-1}^2$

Computed Lower Bounds and Upper Bounds

n	μ_n^* from fixed prec. SDP	Mignotte's lower bounds	Rump's upper bounds
3	0.11111111111111132	0.0277777777777778	0.1111111111111113
4	0.0174291733214352	0.0025000000000000	0.0174291733214326
5	0.00233959554819155	0.000204081632653061	0.00233959554815559
6	0.00028973187528375	0.0000157470395565634	0.00028973187527968
7	0.0000341850701964797	0.00000117126740503364	0.0000341850698000828
8	0.00000390543564465773	0.0000000848995604240359	0.00000390543564975573
9	4.36004072290608e-007	6.03730207459811e-009	4.36001653918105e-007
10	4.78395278113997e-008	4.23028951593812e-010	4.78393956877097e-008
11	5.18272812166654e-009	2.92956337668845e-011	5.17874909744699e-009
12	5.54188889223539e-010	2.00950775838607e-012	5.54588183116313e-010
13	4.06299438537872e-011	1.36752890929865e-013	5.886688081186609e-011
14	2.26410681869460e-010	9.24449542685886e-015	6.20244992053905e-012

Verified Lower Bounds [Rump 2010]

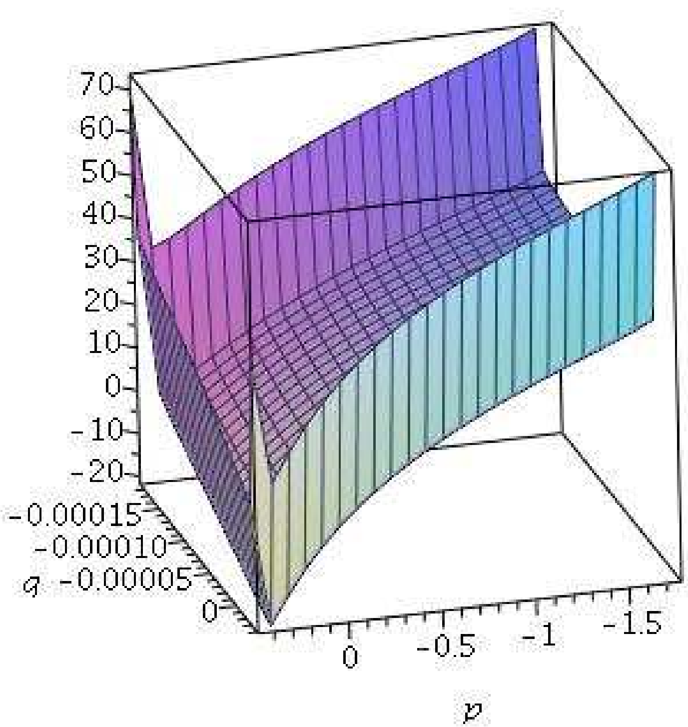
- $n \le 8$ using COSY package by Kyoko Makino.
- $n \le 12$ using SOSTOOLS and INTLAB by Siegfried Rump.
- $n \le 8$ using Gröbner bases by Mohab Safey El Din.
- $n \le 18$
  - using SOSTOOLS and rationalizing SOS by Kaltofen et al.
  - using multiple precision SDPTools and rationalizing SOS by Feng Guo.

Certified Rump Model Lower Bounds [as of Sep 2, 2009]

n	k	#iter	prec.	secs/iter	lower bound r_n	relative Δ_n	$\Delta_n^{[\text{ISSAC'08}]}$	#sq	logH
7	1	60	10×15	0.27	3.418506980e−05	2.048e−14	2.018e−14	16	2485
8	2	80	6×15	0.24	3.905435600e−06	2.561e−15	7.681e−11	16	1563
9	1	280	10×15	1.75	4.360016539e−07	3.784e−14	6.881e−08	25	3919
10	2	280	12×15	1.89	4.783939568e−08	4.517e−13	8.361e−07	25	4660
11	1	510	13×15	9.62	5.178700000e−09	9.481e−06	1.931e−04	36	7201
12	2	210	5×15	8.79	5.545390000e−10	8.869e−05	5.439e−03	36	2881
13	1	270	5×15	41.93	5.881019273e−11	9.639e−04	1.728e−02	49	4271
14	2	440	25×15	33.68	6.100000000e−12	1.679e−02	9.368e−01	49	3121
15	1	1070	25×15	162.84	6.000000000e−13	8.239e−02	—	64	5751
16	2	640	25×15	153.94	6.000000000e−14	1.273e−01	—	64	5312
17	1	1650	10×15	504.10	1.000000000e−15	6.011e+00	—	81	12984
17	1	4200	10×15	380.75	6.000000000e−15	1.685e−01	—	81	13029
18	2	6440	10×15	344.75	1.000000000e−16	6.238e+00	—	81	12570
18	2	8800	10×15	352.62	3.000000000e−16	1.413e+00	—	81	12571
18	2	26800	10×15	330.36	7.000000000e−16	3.406e−02	—	81	12578

Multiple Precision Arithmetic is Needed in SDP

$$\begin{array}{ll} \text{minimize} & (n+v\sqrt{n})\log(1+c_1p+c_2q) \\ & \qquad -\sum_{i=1}^{n}\log(1+p\mu_i)-\sum_{i=1}^{n}\log(1+q\nu_i) \\ \text{s.t.} & p_{\min}\le p\le p_{\max}, \quad q_{\min}\le q\le q_{\max} \end{array}$$

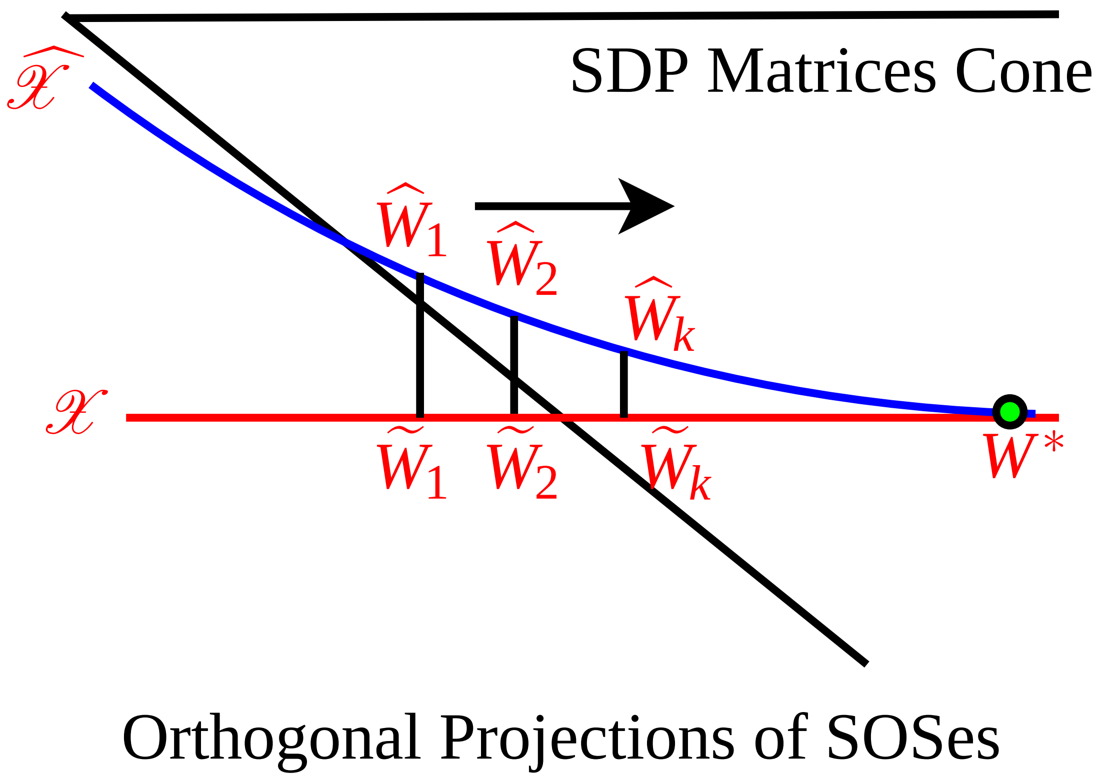


Reference: Vandenberghe and Boyd, SIAM Review 1996

A Sequence of Certified Lower Bounds

$$\widehat{\mathscr{X}} = \{A \mid A^T = A, \quad f(\mathbf{X}) - r + z(m_d(\mathbf{X})^T \cdot m_d(\mathbf{X})) = m_d(\mathbf{X})^T \cdot A \cdot m_d(\mathbf{X})\}$$

Note that $\widehat{\mathscr{X}}$ meets $\mathscr{X}(z = 0)$ at the optimizer (W^*, r^*).



Certified Lower Bounds by Multiple Precision SDP [as of Jan. 16, 2010]

n	k	# iter	prec.	secs/iter	lower bound r_n	upper bound
4	2	50	4 × 15	0.71	0.0174291733214326528	0.0174291733214326529
5	1	50	4 × 15	2.03	0.0023395955481555911 2	0.0023395955481555911 3
6	2	50	4 × 15	1.76	0.00028973187527968192	0.00028973187527968193
7	1	75	5 × 15	11.36	0.000034185069800082 84	0.000034185069800082 85
8	2	75	5 × 15	12.49	0.0000039054356497557 2	0.0000039054356497557 3
9	1	75	5 × 15	84.12	0.436001653918104846 13e–06	0.436001653918104846 13e–06
10	2	75	5 × 15	92.79	0.478393956877097593 27e–07	0.478393956877097593 27e–07
11	1	85	5 × 15	622.03	0.517874909744699053 31e–08	0.517874909744699053 31e–08
12	2	85	5 × 15	634.48	0.554588183116313476 11e–09	0.554588183116313476 12e–09
13	1	100	5 × 15	3800.0	0.588668808118660931 30e–10	0.588668808118660931 30e–10
14	2	100	5 × 15	3800.00	0.620244499205390502 19e–11	0.620244499205390502 20e–11
15	1	120	6 × 15	15000.00	0.649436541858095128 80e–12	0.649436541858095128 80e–12
16	2	120	6 × 15	23000.00	0.676360425582213790 57e–13	0.676360425582213790 58e–13
17	1	70	6 × 15	72400.00	0.70112631896355325150e–14	0.70112631970143741585e–14
18	2	50	6 × 15	95720.00	0.71154604865069396988e–15	0.72383944796943875862e–15

Theodore Motzkin's 1967 Polynomial

$$(3 \text{ arithm. mean} - 3 \text{ geom. mean})(x^4y^2, x^2y^4, z^6)$$
$$= x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2$$

is positive semidefinite (AGM inequality) but **not** a sum-of-squares.

Theodore Motzkin's 1967 Polynomial

$$(3\text{ arithm. mean} - 3\text{ geom. mean})(x^4y^2, x^2y^4, z^6)$$
$$= x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2$$

is positive semidefinite (AGM inequality) but **not** a sum-of-squares.

However,

$$(x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2)(\mathbf{x^2} + \mathbf{y^2} + \mathbf{z^2}) =$$
$$(z^4 - x^2y^2)^2 + 3\left(xyz^2 - \frac{xy^3}{2} - \frac{x^3y}{2}\right)^2 + \left(\frac{xy^3}{2} - \frac{x^3y}{2}\right)^2$$
$$+ (xz^3 - xy^2z)^2 + (yz^3 - x^2yz)^2$$

Theodore Motzkin's 1967 Polynomial

$$(3 \text{ arithm. mean} - 3 \text{ geom. mean})(x^4y^2, x^2y^4, z^6)$$
$$= x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2$$

is positive semidefinite (AGM inequality) but **not** a sum-of-squares.

However,

$$(x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2)(\mathbf{x^2} + \mathbf{z^2}) =$$
$$\left(z^4 - x^2y^2\right)^2 + \left(xyz^2 - x^3y\right)^2 + \left(xz^3 - xy^2z\right)^2$$

Certification via SOS of Rational Functions

Emil Artin's 1927 Theorem (Hilbert's 17th Problem)

$$\forall \xi_1,\dots,\xi_n \in \mathbb{R}\colon\ f(\xi_1,\dots,\xi_n) \geq 0, \qquad f \in \mathbb{Q}[X_1,\dots,X_n]$$

$$\Updownarrow$$

$$\exists u_i, v_j \in \mathbb{Q}[X_1,\dots,X_n]\colon\ f(X_1,\dots,X_n) = \frac{\sum_{i=1}^{m} u_i^2}{\sum_{j=1}^{m} v_j^2}$$

$$\Updownarrow$$

$$\exists \text{rational } W^{[1]} \succeq 0, W^{[2]} \succeq 0\colon\ f = \frac{m_d^T\, W^{[1]}\, m_d}{m_e^T\, W^{[2]}\, m_e}$$

with $m_d(X_1,\dots,X_n)$, $m_e(X_1,\dots,X_n)$ vectors of terms

Semidefinite Programming: Block Form

$A^{[i,j]}, C^{[j]}, W^{[j]}$ are real **symmetric** matrix blocks

$W =$ block diagonal$(W^{[1]}, \ldots, W^{[k]})$

$$\min_{W^{[1]},\ldots,W^{[k]}} \quad C^{[1]} \bullet W^{[1]} + \cdots + C^{[k]} \bullet W^{[k]}$$

$$\text{s. t.} \quad \begin{bmatrix} A^{[1,1]} \bullet W^{[1]} + \cdots + A^{[1,k]} \bullet W^{[k]} \\ \vdots \\ A^{[m,1]} \bullet W^{[1]} + \cdots + A^{[m,k]} \bullet W^{[k]} \end{bmatrix} = b \in \mathbb{R}^m,$$

$$\boxed{W^{[j]} \succeq 0, W^{[j]} = (W^{[j]})^T, j = 1, \ldots, k}$$

Semidefinite Programming: Block Form

$A^{[i,j]}, C^{[j]}, W^{[j]}$ are real **symmetric** matrix blocks

$W = \text{block diagonal}(W^{[1]}, \ldots, W^{[k]})$

$$\min_{W^{[1]},\ldots,W^{[k]}} \quad C^{[1]} \bullet W^{[1]} + \cdots + C^{[k]} \bullet W^{[k]}$$

$$\text{s. t.} \quad \begin{bmatrix} A^{[1,1]} \bullet W^{[1]} + \cdots + A^{[1,k]} \bullet W^{[k]} \\ \vdots \\ A^{[m,1]} \bullet W^{[1]} + \cdots + A^{[m,k]} \bullet W^{[k]} \end{bmatrix} = b \in \mathbb{R}^m,$$

$$\boxed{W^{[j]} \succeq 0, W^{[j]} = (W^{[j]})^T, j = 1, \ldots, k}$$

Software: SeDuMi, YALMIP, SOSTOOLS, SparsePOP, SDPT3, VSDP, GloptiPoly

Example 2: Monotone Column Permanent Conjecture

The permanent of an $n \times n$ matrix A is defined as

$$\operatorname{perm}(A) := \sum_{\sigma \in S_n} a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Example 2: Monotone Column Permanent Conjecture

The permanent of an $n \times n$ matrix A is defined as

$$\mathrm{perm}(A) := \sum_{\sigma \in S_n} a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Let $A \in \mathbb{R}^{n\times n}$ whose columns are weakly increasing, then all of the zeros of $\mathrm{perm}(zA + E_n) \in \mathbb{R}[z]$ are real, where E_n is the $n \times n$ matrix of all $1's$.

Example 2: Monotone Column Permanent Conjecture

The permanent of an $n \times n$ matrix A is defined as

$$\operatorname{perm}(A) := \sum_{\sigma \in S_n} a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Let $A \in \mathbb{R}^{n \times n}$ whose columns are weakly increasing, then all of the zeros of $\operatorname{perm}(zA + E_n) \in \mathbb{R}[z]$ are real, where E_n is the $n \times n$ matrix of all $1's$.

Remark: 1999 conjecture on rook polynomials by Haglund, Ono, Wagner, proven for $n = 3$ by Ray Mayer.
The MCP conjecture for arbitrary n *was proven at the end of 2009 by Branden, Haglund, Visontai, and Wagner.*

MCP continued: Joe Buhler's question [Jan 8, 2009]

Prove for all $1 \leq i \leq j \leq 3$, the following polynomials are nonnegative

$$p_{i,j} = \text{perm}([\eta_{i+1}, \eta_1, u, v])\text{perm}([\eta_{j+1}, \eta_1, u, v]) - \text{perm}([\eta_{i+1}, \eta_{j+1}, u, v])\text{perm}([\eta_1, \eta_1, u, v]) \geq 0$$

where

$u = x\eta_1 + a^2\eta_2 + b^2\eta_3 + c^2\eta_4, v = y\eta_1 + d^2\eta_2 + e^2\eta_3 + f^2\eta_4,$

and

$$\eta_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad \eta_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad \eta_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \quad \eta_4 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Implies MCP Conjecture for $n = 4$.

Proof of MCP conjecture for $n = 4$ (all rational coeff.'s)

6 polynomials of degree 8 with 8 variables:

2 polynomials are squares

1 polynomial is an SOS

3 polynomials are $\frac{\text{SOS}}{\text{weighted sum of squares of variables}}$

Examples From Literature

Example	The Denominator	#iter	prec.	#sq	secs
delzell	$2X_1^2+2X_2^2+2X_3^2$	*Null*	2×15	8	0.02
$motzkin(X_1,3X_2,3X_3)$	$4X_1^2+12X_2^2+21X_3^2$	19	1×15	5	0.304
$motzkin(X_1,3X_2,3X_3)$	$(X_1^2+X_2^2+X_3^2)^2$	96	10×15	7	17.217
leepstarr2	$15+20X_1^2+18X_2^2$	*Null*	1×15	9	0.344
laxlax	$X_1^2+X_2^2+X_3^2+X_4^2$	*Null*	2×15	7	0.52

$$
\begin{aligned}
delzell(X_1,X_2,X_3,X_4) = {} & X_1^4X_2^2X_4^2+X_2^4X_3^2X_4^2+X_1^2 \\
& X_3^4X_4^2-3\,X_1^2X_2^2X_3^2X_4^2+X_3^8.
\end{aligned}
$$

Uniform Denominators and Degree Bounds

Theorem. *(Bruce Reznick'1995) Let* $f \in H_m(\mathbb{R}^n)$ *be a homogenous polynomial of degree* m *in* n *variables. Suppose* f *is positive definite. Let*

$$\varepsilon(f) := \frac{\inf\{f(\xi) : \xi \in S^{n-1}\}}{\sup\{f(\xi) : \xi \in S^{n-1}\}}$$

which measure how close f *is to having a zero. If*

$$r \geq \frac{nm(m-1)}{(4\log 2)\varepsilon(f)} - \frac{n+m}{2},$$

then $f \cdot (X_1^2 + \cdots X_n^2)^r$ *is an SOS in* $Q[X_1, \ldots, X_n]$.

Certification via Critical Values and SOS

The gradient ideal: $\langle \nabla f \rangle := \left\langle \frac{\partial f}{\partial X_1}, \frac{\partial f}{\partial X_2}, \cdots, \frac{\partial f}{\partial X_n} \right\rangle$

The gradient variety: $V(\nabla f) := \{x \in \mathbb{C}^n \mid \nabla f(x) = 0\}$

$$f - f^*_{grad} + \varepsilon \equiv \text{SOS mod } \langle \nabla f \rangle \text{ for all } \varepsilon > 0,$$

where $f^*_{grad} := \inf\{f(x) \mid x \in V(\nabla f)\}$.

Certification via Critical Values and SOS

The gradient ideal: $\langle \nabla f \rangle := \left\langle \frac{\partial f}{\partial X_1}, \frac{\partial f}{\partial X_2}, \cdots, \frac{\partial f}{\partial X_n} \right\rangle$

The gradient variety: $V(\nabla f) := \{x \in \mathbb{C}^n \mid \nabla f(x) = 0\}$

$$f - f^*_{grad} + \varepsilon \equiv \text{SOS mod } \langle \nabla f \rangle \text{ for all } \varepsilon > 0,$$

where $f^*_{grad} := \inf\{f(x) \mid x \in V(\nabla f)\}$.

Nie, Demmel, Sturmfels'2005:

- If f attains a minimum on $\mathbb{R}^n$, $f^* = f^*_{grad}$.
- Otherwise, $f^* < f^*_{grad}$.

  Example: $f := (1 - xy)^2 + y^2$, we have $V(\nabla f) = \{(0,0)\}$
  and $f(0,0) = 1 > 0 = f^*$ ($xy \to 1,\ y \to 0,\ x \to \infty$.)

Asymptotic Value and Preordering

The set $R_\infty(f,S)$ consists of all asymptotic values of f on S,

$$\{y \in \mathbb{R} \mid \exists x_k \in S, \text{ such that } \lim_{k\to\infty} ||x_k|| = \infty, \ \lim_{k\to\infty} f(x_k) = y\}$$

The preordering generated by $g_1 \geq 0, \ldots, g_m \geq 0 \in \mathbb{R}[X]$ is denoted by

$$T(g_1,\ldots,g_m) := \left\{ \sum_{\delta\in\{0,1\}^m} s_\delta\, g_1^{\delta_1} \cdots g_m^{\delta_m} \mid s_\delta \text{ is an SOS in } \mathbb{R}[X] \right\}$$

Schweighofer, SIAM J. Optim. 2006.

Theorem. *Let* $f, g_1, \ldots, g_m \in \mathbb{R}[X]$ *and set*

$$S := \{x \in \mathbb{R}^n \mid g_1(x) \geq 0,\ g_2(x) \geq 0,\ \ldots,\ g_m(x) \geq 0\}$$

Suppose that

1. f *is bounded on* S*;*
2. $R_\infty(f, S)$ *is a finite subset of* $\mathbb{R}_{>0}$*;*
3. $f > 0$ *on* S*.*

Then $f \in T(g_1, \ldots, g_m)$*.*

Two Conditions for S

If we choose S to be a set which satisfies:

1. The set of asymptotic values:

$$(*) \quad R_\infty(f,S) \text{ is finite}$$

2. The infimums of f on $\mathbb{R}^n$ and on S coincide:

$$(**) \quad \inf\{f(x) \mid x \in \mathbb{R}^n\} = \inf\{f(x) \mid x \in S\}$$

By Schweighofer's theorem: $f - f^* + \varepsilon \in T(g_1, \ldots, g_m)$

Two Conditions for S

If we choose S to be a set which satisfies:

1. The set of asymptotic values:

$$(*) \quad R_\infty(f,S) \text{ is finite}$$

2. The infimums of f on $\mathbb{R}^n$ and on S coincide:

$$(**) \quad \inf\{f(x) \mid x \in \mathbb{R}^n\} = \inf\{f(x) \mid x \in S\}$$

By Schweighofer's theorem: $f - f^* + \varepsilon \in T(g_1, \ldots, g_m)$

Examples:

- Gradient Tentacles (Schweighofer, SIAM J. Optim. 2006.)
- Truncated Tangency Variety (Hà and Pham, SIAM J. Optim. 2008.)

Generalized Critical Values

We denote the critical values $K_0(f)$

$$\left\{ c \middle|\ \exists z \in \mathbb{R}^n \text{ s.t. } f(z) = c \text{ and } \frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0 \right\}$$

Generalized Critical Values

We denote the critical values $K_0(f)$

$$\left\{c \mid \exists z \in \mathbb{R}^n \text{ s.t. } f(z) = c \text{ and } \frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0\right\}$$

The asymptotic critical values $K_\infty(f)$ consists of c such that

- $\exists (z_l)_{l \in \mathbb{N}} \subset \mathbb{R}^n$ s.t. $\lim_{l \to \infty} f(z_l) = c$, and $\lim_{l \to \infty} ||z_l|| = +\infty$
- $\lim_{l \to \infty} ||X_i(z_l)|| \cdot ||\frac{\partial f}{\partial X_j}(z_l)|| = 0, \ 1 \leq i, j \leq n$

Generalized Critical Values

We denote the critical values $K_0(f)$

$$\left\{c \mid \exists z \in \mathbb{R}^n \text{ s.t. } f(z) = c \text{ and } \frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0\right\}$$

The asymptotic critical values $K_\infty(f)$ consists of c such that

- $\exists (z_l)_{l\in\mathbb{N}} \subset \mathbb{R}^n$ s.t. $\lim_{l\to\infty} f(z_l) = c$, and $\lim_{l\to\infty} ||z_l|| = +\infty$
- $\lim_{l\to\infty} ||X_i(z_l)|| \cdot ||\frac{\partial f}{\partial X_j}(z_l)|| = 0,\ 1 \le i, j \le n$

The set of generalized critical values is

$$K(f) = K_0(f) \cup K_\infty(f)$$

Kurdyka, Orro and Simon, J. Diff. Geom, 2000.

For all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$ and $f \in \mathbb{R}[X]$, denote $f^{\mathbf{A}} = f(\mathbf{A}X)$,

$$W_i^{\mathbf{A}} := \left\{ X_1 = \cdots = X_i = \frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0 \right\}.$$

Theorem. *(Greuet,Guo,Safey,Zhi'2010) If* $\inf_{x \in \mathbb{R}} f(x) > -\infty$, *then* $\exists$ *a Zariski-closed subset* $\mathscr{A} \subsetneq GL_n(\mathbb{C})$, $\forall\, \mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathscr{A}$,

$$f^* = \inf\{ f(x) \mid x \in \mathbb{R}^n\} = \min_i \left\{ \inf\{ f^{\mathbf{A}}(x) \mid x \in W_i^{\mathbf{A}} \cap \mathbb{R}^n\} \right\}.$$

Moreover $R_\infty(f^{\mathbf{A}}, W_i^{\mathbf{A}})$ *is a finite set.*

Certification via Generalized Critical Values and SOS

Theorem. *If* $\inf_{x\in\mathbb{R}} f(x) > -\infty$ *then* $\exists$ *a Zariski-closed subset* $\mathscr{A} \subsetneq GL_n(\mathbb{C})$, *s.t.* $\forall\, \mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathscr{A}$, $M \in f(\mathbb{R}^n)$,

$$W_{M,i}^{\mathbf{A}} := \left\{ x \in W_i^{\mathbf{A}} | M - f^{\mathbf{A}}(x) \geq 0 \right\},$$

the following conditions are equivalent:

1. $f^{\mathbf{A}} \geq 0$ *on* $\mathbb{R}^n$;
2. $f^{\mathbf{A}} \geq 0$ *on each* $W_{M,i}^{\mathbf{A}}$, $0 \leq i \leq n-1$;
3. $\forall \varepsilon > 0$, *and* $0 \leq i \leq n-1$, *there are* $\phi_{i,j}, s_i,$ *and* $t_i \in \mathbb{R}[X]$,

$$f^{\mathbf{A}} + \varepsilon = s_i + t_i \left(M - f^{\mathbf{A}} \right) + \sum_{1\leq j\leq i} \phi_{i,j} X_j + \sum_{i+2\leq j\leq n} \phi_{i,j} \frac{\partial f^{\mathbf{A}}}{\partial X_j}.$$

where s_i *and* t_i *are SOS.*

Remark

In general case, only W_0 is needed:

$$W_0 := \left\{ \frac{\partial f}{\partial X_2} = \cdots = \frac{\partial f}{\partial X_n} = 0 \right\},$$

which is simpler than the gradient variety:

$$\left\{ \frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0 \right\},$$

and the truncated tangency variety:

$$\left\{ X_j \frac{\partial f}{\partial X_i} - X_i \frac{\partial f}{\partial X_j},\ 1 \leq i < j \leq n. \right\}$$

Numerical Results

We set $\mathbf{A} := I_{n\times n}$ and $M := f^{\mathbf{A}}(0) = f(0)$

For the Motzkin's polynomial

$$f(x,y) := x^2y^4 + x^4y^2 - 3x^2y^2 + 1.$$

- $f^* = 0$ but $f^{sos} = -\infty$.
- using SOS relaxation: $f^* \approx -0.26897 \cdot 10^7$
- using our method in Matlab: $f^*_{0,0} \approx -6138.2$, and

$$f^*_{0,1} \approx -0.52508,\ f^*_{0,2} \approx -0.19588,\ f^*_{0,3} \approx 0.37327 \cdot 10^{-8}$$

Numerical Problem

Consider the polynomial $f(x,y) := (1-xy)^2 + y^2$.

- $f^{sos} = 0$ and therefore $f_k^* = 0$ for all $k \in \mathbb{N}$.

Numerical Problem

Consider the polynomial $f(x,y) := (1-xy)^2 + y^2$.

- $f^{sos} = 0$ and therefore $f_k^* = 0$ for all $k \in \mathbb{N}$.
- using *truncated tangency variety*:

$$f_0^* \approx -0.12641 \cdot 10^{-3},\ f_1^* \approx 0.12732 \cdot 10^{-1},\ f_2^* \approx 0.49626 \cdot 10^{-1}$$

Numerical Problem

Consider the polynomial $f(x,y) := (1-xy)^2 + y^2$.

- $f^{sos} = 0$ and therefore $f_k^* = 0$ for all $k \in \mathbb{N}$.
- using *truncated tangency variety*:

  $f_0^* \approx -0.12641 \cdot 10^{-3}$, $f_1^* \approx 0.12732 \cdot 10^{-1}$, $f_2^* \approx 0.49626 \cdot 10^{-1}$

- using our method:

  $f_{0,0}^* \approx 0.37874 \cdot 10^{-4}$, $f_{0,1}^* \approx 0.12018 \cdot 10^{-2}$, $f_{0,2}^* \approx 0.11063 \cdot 10^{-1}$

Unbounded Moment Matrices

Let $m_{d_1}(X) = m_{d_2}(X) := [1, x, y, x^2, xy, y^2]$, solve the problem

$$\sup_{r \in \mathbb{R}} \quad r$$

$$f(X) - r \equiv m_{d_1}(X)^T \cdot W \cdot m_{d_1}(X) + m_{d_2}(X)^T \cdot V \cdot m_{d_2}(X) \cdot (M - f) \bmod \langle \frac{\partial f}{\partial x} \rangle$$

$$W \succeq 0, \quad W^T = W, \quad V \succeq 0, \quad V^T = V.$$

It dual problem is: $\inf_{y_\alpha \in \mathbb{R}} \quad \sum_\alpha f_\alpha y_\alpha, \quad P \succeq 0, Q \succeq 0$, where

$$P = \begin{bmatrix} y_{0,0} & \cdot & \cdot & \cdot & \cdot & y_{0,2} \\ \mathbf{y_{1,0}} & \cdot & \cdot & \cdot & \cdot & y_{1,2} \\ y_{0,1} & \cdot & \cdot & \cdot & \cdot & y_{0,3} \\ \mathbf{y_{2,0}} & \cdot & \cdot & \cdot & \cdot & y_{2,2} \\ y_{1,1} & \cdot & \cdot & \cdot & \cdot & y_{1,3} \\ y_{0,2} & \cdot & \cdot & \cdot & \cdot & y_{0,4} \end{bmatrix} \quad Q = \begin{bmatrix} 4y_{0,0} + y_{1,1} - y_{0,2} & \cdot & \cdot & \cdot & 5y_{1,1} - y_{0,2} & \cdot \\ 4y_{1,0} - y_{0,1} + \mathbf{y_{2,1}} & \cdot & \cdot & \cdot & 5\mathbf{y_{2,1}} - y_{0,1} & \cdot \\ 5y_{0,1} - y_{0,3} & \cdot & \cdot & \cdot & 5y_{0,1} - y_{0,3} & \cdot \\ \mathbf{y_{3,1}} - y_{1,1} + 4\mathbf{y_{2,0}} & \cdot & \cdot & \cdot & 5\mathbf{y_{3,1}} - y_{1,1} & \cdot \\ 5y_{1,1} - y_{0,2} & \cdot & \cdot & \cdot & 5y_{1,1} - y_{0,2} & \cdot \\ 5y_{0,2} - y_{0,4} & \cdot & \cdot & \cdot & 5y_{0,2} - y_{0,4} & \cdot \end{bmatrix}$$

Unbounded Moment Matrices

Denote the optimal point $p^* = (x^*, y^*)$ of $f = (1 - xy)^2 + y^2$,

- $x^* y^* \to 1$ and $y^* \to 0 \implies {x^*}^i {y^*}^j \to \infty$ with $i > j$;
- The moment $y_{i,j} = {x^*}^i {y^*}^j$ is a minimizer of the dual problem;
- $\mathbf{y_{i,j}} \to \infty$ with $\mathbf{i} > \mathbf{j}$;
- The moment matrices P and Q are **unbounded** at the minimizer.

Exploit the Sparsity Structure

- Reduce to $m_{d_1} = [1, y, xy, y^2]$, $m_{d_2} = [1, y, xy]$

$$P = \begin{bmatrix} y_{0,0} & y_{0,1} & y_{1,1} & y_{0,2} \\ y_{0,1} & y_{0,2} & y_{1,2} & y_{0,3} \\ y_{1,1} & y_{1,2} & y_{2,2} & y_{1,3} \\ y_{0,2} & y_{0,3} & y_{1,3} & y_{0,4} \end{bmatrix}, \quad Q = \begin{bmatrix} 4y_{0,0} + y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \\ 5y_{0,1} - y_{0,3} & 5y_{0,2} - y_{0,4} & 5y_{0,1} - y_{0,3} \\ 5y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \end{bmatrix}$$

Exploit the Sparsity Structure

- Reduce to $m_{d_1} = [1, y, xy, y^2]$, $m_{d_2} = [1, y, xy]$

$$P = \begin{bmatrix} y_{0,0} & y_{0,1} & y_{1,1} & y_{0,2} \\ y_{0,1} & y_{0,2} & y_{1,2} & y_{0,3} \\ y_{1,1} & y_{1,2} & y_{2,2} & y_{1,3} \\ y_{0,2} & y_{0,3} & y_{1,3} & y_{0,4} \end{bmatrix}, \quad Q = \begin{bmatrix} 4y_{0,0} + y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \\ 5y_{0,1} - y_{0,3} & 5y_{0,2} - y_{0,4} & 5y_{0,1} - y_{0,3} \\ 5y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \end{bmatrix}$$

- All $y_{i,j}$ with $i > j$ are removed, P, Q are bounded at (x^*, y^*);

Exploit the Sparsity Structure

- Reduce to $m_{d_1} = [1, y, xy, y^2]$, $m_{d_2} = [1, y, xy]$

$$P = \begin{bmatrix} y_{0,0} & y_{0,1} & y_{1,1} & y_{0,2} \\ y_{0,1} & y_{0,2} & y_{1,2} & y_{0,3} \\ y_{1,1} & y_{1,2} & y_{2,2} & y_{1,3} \\ y_{0,2} & y_{0,3} & y_{1,3} & y_{0,4} \end{bmatrix}, \quad Q = \begin{bmatrix} 4y_{0,0} + y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \\ 5y_{0,1} - y_{0,3} & 5y_{0,2} - y_{0,4} & 5y_{0,1} - y_{0,3} \\ 5y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \end{bmatrix}$$

- All $y_{i,j}$ with $i > j$ are removed, P, Q are bounded at (x^*, y^*);
- The lower bound computed is

$$f_2^* \approx 4.029500408 \times 10^{-24}$$

Exploit the Sparsity Structure

- Reduce to $m_{d_1} = [1, y, xy, y^2]$, $m_{d_2} = [1, y, xy]$

$$P = \begin{bmatrix} y_{0,0} & y_{0,1} & y_{1,1} & y_{0,2} \\ y_{0,1} & y_{0,2} & y_{1,2} & y_{0,3} \\ y_{1,1} & y_{1,2} & y_{2,2} & y_{1,3} \\ y_{0,2} & y_{0,3} & y_{1,3} & y_{0,4} \end{bmatrix}, \quad Q = \begin{bmatrix} 4y_{0,0} + y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \\ 5y_{0,1} - y_{0,3} & 5y_{0,2} - y_{0,4} & 5y_{0,1} - y_{0,3} \\ 5y_{1,1} - y_{0,2} & 5y_{0,1} - y_{0,3} & 5y_{1,1} - y_{0,2} \end{bmatrix}$$

- All $y_{i,j}$ with $i > j$ are removed, P, Q are bounded at (x^*, y^*);
- The lower bound computed is

$$f_2^* \approx 4.029500408 \times 10^{-24}$$

- The certified lower bound is

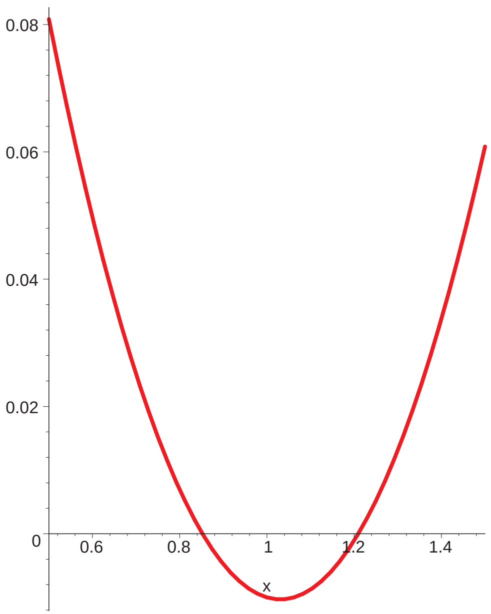
$$f_2^* = 4.0293412063831573555202295686125106 32 \times 10^{-24}$$

Inequalities with Floating Point Scalars

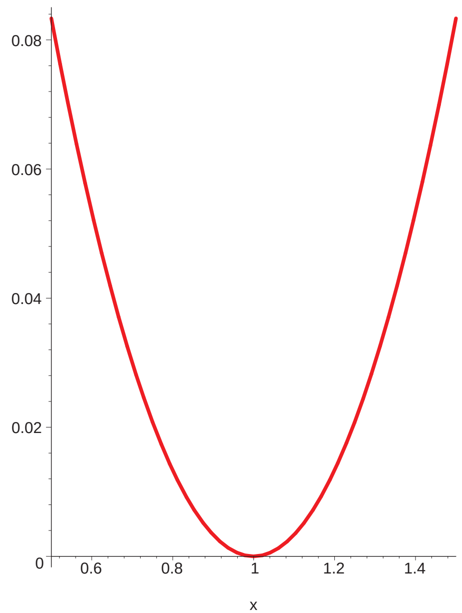
$$\forall x \in \mathbb{R}:\ 0.34x^2 - 0.66x + 0.33 > 0.009 \quad ???$$

Inequalities with Floating Point Scalars

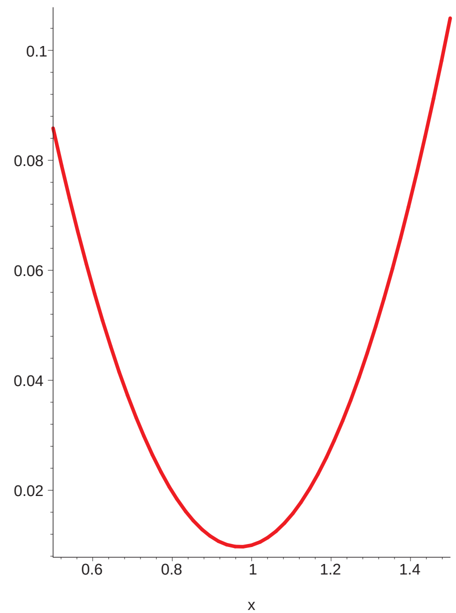
$$\forall x \in \mathbb{R}:\ 0.34x^2 - 0.66x + 0.33 > 0.009 \quad ???$$



$$\left(\tfrac{1}{3} - \tfrac{1}{100}\right)x^2 - \tfrac{2}{3}x + \tfrac{1}{3}$$



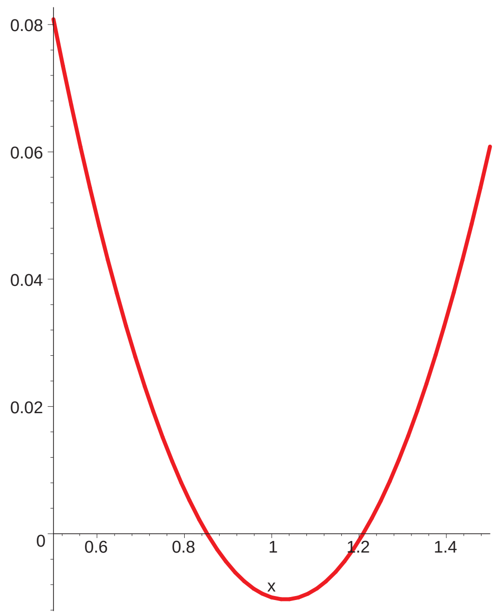
$$\tfrac{1}{3}x^2 - \tfrac{2}{3}x + \tfrac{1}{3}$$



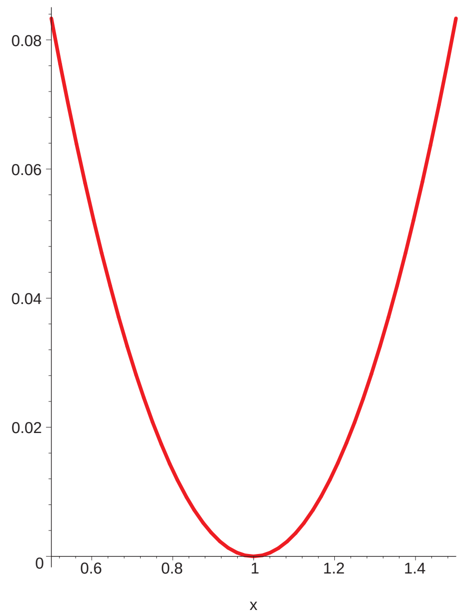
$$\left(\tfrac{1}{3} + \tfrac{1}{100}\right)x^2 - \tfrac{2}{3}x + \tfrac{1}{3}$$

Inequalities with Floating Point Scalars

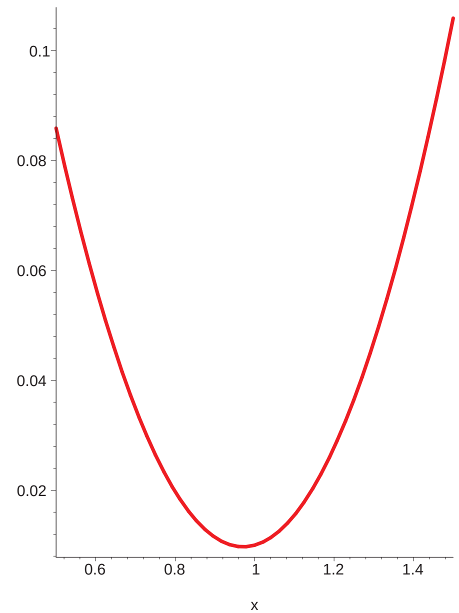
$$\forall x \in \mathbb{R}:\ 0.34x^2 - 0.66x + 0.33 > 0.009 \quad ???$$



$$\left(\frac{1}{3} - \frac{1}{100}\right)x^2 - \frac{2}{3}x + \frac{1}{3}$$



$$\frac{1}{3}x^2 - \frac{2}{3}x + \frac{1}{3}$$



$$\left(\frac{1}{3} + \frac{1}{100}\right)x^2 - \frac{2}{3}x + \frac{1}{3}$$

A. Seidenberg 1954: decide whether a given polynomial $f(x,y) \in \mathbb{R}[x,y]$ has a real root.

Radius of Positive Semidefinitenes (unconstrained coeff's)

$$\rho_2(f) = \inf_{\tilde{f} \in \mathbb{R}[X_1,\ldots,X_n]} \|f - \tilde{f}\|_2^2 \quad \text{(coeff. vector 2-norm)}$$

$$\text{s. t. } \exists \alpha \in \mathbb{R}^n\colon\ \tilde{f}(\alpha) = 0,$$

$$\deg(\tilde{f}) \le \deg(f), \quad \text{(any degree notion)}$$

Radius of Positive Semidefinitenes (unconstrained coeff's)

$$\rho_2(f) = \inf_{\tilde{f} \in \mathbb{R}[X_1,\ldots,X_n]} \| f - \tilde{f} \|_2^2 \quad \text{(coeff. vector 2-norm)}$$

$$\text{s. t. } \exists \alpha \in \mathbb{R}^n \colon \tilde{f}(\alpha) = 0,$$

$$\deg(\tilde{f}) \le \deg(f), \quad \text{(any degree notion)}$$

- $\rho_2(x^2 + 1) = 1, \ \tilde{f} = x^2$
- $\rho_2(x^2 + (1 - xy)^2) = 0$ as $\varepsilon^2 + (1 - \varepsilon \frac{1}{\varepsilon})^2 - \varepsilon^2 = 0$

Main Theorem [Corless, Hitz, Hutton, Kaltofen, Karmarkar, Lakshman, Ruatta, Stetter, Szanto, Zhi]

Let $\alpha \in \mathbb{R}^n$: $\mathcal{N}_2^{[f]}(\alpha) = \inf_{\tilde{f} \in \mathbb{R}[X_1,\ldots,X_n]} \|f - \tilde{f}\|_2^2$

s. t. $\tilde{f}(\alpha) = 0,$

$\deg(\tilde{f}) \le \deg(f)$

$$\boxed{= \frac{f(\alpha)^2}{\|\tau\|_2^2}},$$

where $\tau = [1, \alpha_1, \ldots, \alpha_n, \ldots, \alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}, \ldots]_{(i_1,\ldots,i_n)\le\deg(f)}$

The coefficient vector $\vec{\tilde{f}}$ of the minimizer is $\boxed{\vec{\tilde{f}} = \vec{f} - \frac{\tau^T \vec{f}}{\|\tau\|_2^2}\tau}$

Main Theorem [Corless, Hitz, Hutton, Kaltofen, Karmarkar, Lakshman, Ruatta, Stetter, Szanto, Zhi]

Let $\alpha \in \mathbb{R}^n$: $\mathcal{N}_2^{[f]}(\alpha) = \inf_{\tilde{f} \in \mathbb{R}[X_1,\ldots,X_n]} \|f - \tilde{f}\|_2^2$

s. t. $\tilde{f}(\alpha) = 0$,

$\deg(\tilde{f}) \leq \deg(f)$

$$\boxed{= \frac{f(\alpha)^2}{\|\tau\|_2^2}},$$

where $\tau = [1, \alpha_1, \ldots, \alpha_n, \ldots, \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}, \ldots]_{(i_1,\ldots,i_n) \leq \deg(f)}$

The coefficient vector $\vec{\tilde{f}}$ of the minimizer is $\boxed{\vec{\tilde{f}} = \vec{f} - \frac{\tau^T \vec{f}}{\|\tau\|_2^2} \tau}$

Corollary:

$$\rho_2(f) = \inf_{(\alpha_1,\ldots,\alpha_n) \in \mathbb{R}^n} \frac{f(\alpha_1, \ldots, \alpha_n)^2}{\sum_{(i_1,\ldots,i_n) \leq \deg(f)} \alpha_1^{2i_1} \cdots \alpha_n^{2i_n}}$$

Weighted norms $\|\vec{f}\|_{2,w}^2 = \sum_j w_j (\vec{f})_j^2$ for weights $w_i > 0$

$$\mathcal{N}_{2,w}^{[f]}(\alpha) = \frac{f(\alpha_1, \ldots, \alpha_n)^2}{\sum_{(i_1,\ldots,i_n)\leq \deg(f)} \frac{1}{w_{i_1,\ldots,i_n}} \alpha_1^{2i_1} \cdots \alpha_n^{2i_n}}$$

$$\vec{\tilde{f}} = \vec{f} - \frac{\tau^T \vec{f}}{\tau^T \mathrm{Diag}(w)^{-1} \tau} \mathrm{Diag}(w)^{-1} \tau,$$

Weighted norms $\|\vec{f}\|_{2,w}^2 = \sum_j w_j (\vec{f})_j^2$ for weights $w_i > 0$

$$\mathcal{N}_{2,w}^{[f]}(\alpha) = \frac{f(\alpha_1, \ldots, \alpha_n)^2}{\sum_{(i_1,\ldots,i_n)\le \deg(f)} \frac{1}{w_{i_1,\ldots,i_n}} \alpha_1^{2i_1} \cdots \alpha_n^{2i_n}}$$

$$\vec{\tilde{f}} = \vec{f} - \frac{\tau^T \vec{f}}{\tau^T \mathrm{Diag}(w)^{-1} \tau} \mathrm{Diag}(w)^{-1} \tau,$$

$w_j \to \infty$: coefficient remains fixed, e.g., 0

$w_j \to 0$: coefficient is a don't care

$$\tilde{f}(x) = f(x) - \frac{f(\alpha)}{\alpha^i} x^i, \quad \alpha \neq 0$$

A Motzkin-like Example

$Mot(x,y) = x^4y^2 + x^2y^4 - 3x^2y^2 + 2 \geq 1, \forall x,y \in \mathbb{R}$ is **not** an SOS.

Let $\tau = [1, x^2y^4, y^2x^4, x^2y^2]$.

- Run SOS solver in Matlab to obtain

$$Mot^2 - 0.12854802625946718 00\,\tau^T\tau \approx SOS$$

A Motzkin-like Example

$Mot(x,y) = x^4y^2 + x^2y^4 - 3x^2y^2 + 2 \geq 1, \forall x,y \in \mathbb{R}$ is **not** an SOS.

Let $\tau = [1, x^2y^4, y^2x^4, x^2y^2]$.

- Run SOS solver in Matlab to obtain

$$Mot^2 - 0.12854802625946718000\,\tau^T\tau \approx SOS$$

- Use rational SOS solver in Maple:

$$Mot^2 - \frac{1285480262594283}{10000000000000000}\,\tau^T\tau = SOS \text{ (10 squares)}$$

$\Longrightarrow Mot(x,y) > 0,\ \forall x,y \in \mathbb{R}$.

$\Longrightarrow Mot(x,y)$ has no real root (Seidenberg's Problem).

A Motzkin-like Example

$Mot(x,y) = x^4y^2 + x^2y^4 - 3x^2y^2 + 2 \geq 1, \forall x,y \in \mathbb{R}$ is **not** an SOS.

Let $\tau = [1, x^2y^4, y^2x^4, x^2y^2]$.

- Run SOS solver in Matlab to obtain

$$Mot^2 - 0.12854802625946718 00\,\tau^T\tau \approx SOS$$

- Use rational SOS solver in Maple:

$$Mot^2 - \frac{1285480262594283 3}{10000000000000000 0}\,\tau^T\tau = SOS \text{ (10 squares)}$$

$\Longrightarrow Mot(x,y) > 0,\ \forall x,y \in \mathbb{R}$.

$\Longrightarrow Mot(x,y)$ has no real root (Seidenberg's Problem).

Conjecture: If $\tilde{\rho}_2(f) > 0$ then $f^2 - \tilde{\rho}_2(f)\|\tau\|_2^2$ is SOS **for all** f.

Nearest Consistent System

$f_1(x,y) = x^4 + y^4 + 1$ and $f_2(x,y) = x^2 + x^2y^2 - 2xy + 1$

Compute

$$\rho_2(f_1, f_2) = \inf_{\alpha,\beta\in\mathbb{R}} \frac{f_1(\alpha,\beta)^2 + f_2(\alpha,\beta)^2}{\sum_{0\le i+j\le 4} \alpha^{2i}\beta^{2j}}$$

Use $\partial_\alpha, \partial_\beta$ and Gröbner bases

cf. [Becker, Powers, and Wörmann 2000] $z^2F(x,y)+1=0$

and Mohab Safey El Din's RAGlib package

Nearest Consistent System

$f_1(x,y) = x^4 + y^4 + 1$ and $f_2(x,y) = x^2 + x^2y^2 - 2xy + 1$

Compute

$$\rho_2(f_1, f_2) = \inf_{\alpha,\beta\in\mathbb{R}} \frac{f_1(\alpha,\beta)^2 + f_2(\alpha,\beta)^2}{\sum_{0\le i+j\le 4} \alpha^{2i}\beta^{2j}}$$

Use $\partial_\alpha, \partial_\beta$ and Gröbner bases

cf. [Becker, Powers, and Wörmann 2000] $z^2F(x,y) + 1 = 0$
and Mohab Safey El Din's RAGlib package

- 20 digits: $x = 2.5645$, $y = -0.2751$, $\rho_2(f_1, f_2) = 0.9180$.
- 25 digits: $x = -0.9202$ $y = -1.1947$, $\rho_2(f_1, f_2) = 0.64598$.

Nearest Consistent System

$f_1(x,y) = x^4 + y^4 + 1$ and $f_2(x,y) = x^2 + x^2y^2 - 2xy + 1$

Compute

$$\rho_2(f_1, f_2) = \inf_{\alpha,\beta\in\mathbb{R}} \frac{f_1(\alpha,\beta)^2 + f_2(\alpha,\beta)^2}{\sum_{0\le i+j\le 4} \alpha^{2i}\beta^{2j}}$$

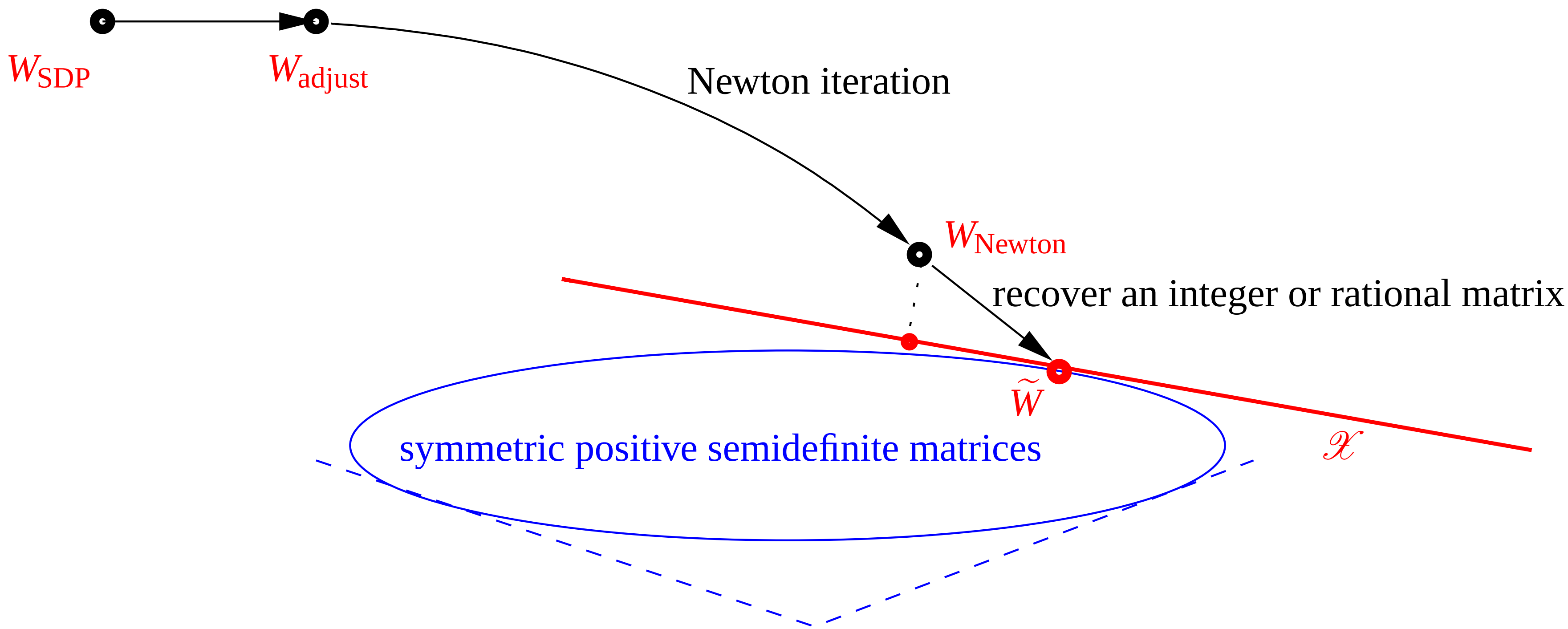
Use $\partial_\alpha, \partial_\beta$ and Gröbner bases

cf. [Becker, Powers, and Wörmann 2000] $z^2F(x,y)+1=0$

and Mohab Safey El Din's RAGlib package

Exact SOS certificate for $\rho_2(f_1, f_2) > \frac{6459730699807810 8}{10000000000000000 00}$.

Concluding Observations: “Hard Case”



Sturmfels’ Conjecture: Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ s.t. $f = \sum_{i=1}^{s} g_i^2$, $g_i \in \mathbb{R}[X_1, \ldots, X_n]$, then there exists $f_1, \ldots, f_p$ in $\mathbb{Q}[X_1, \ldots, X_n]$ s.t. $f = f_1^2 + \cdots + f_p^2$.

C. Hillar’09: It is true when coefficients of g_i in $\mathbb{K}$ which is a totally real number field. See also Kaltofen’09, Quarez’09.

Bound the Height of the Rational SOS

Theorem. *(Safey and Zhi'2010) Let* $f \in \mathbb{Z}[X_1,\ldots,X_n]$ *with coefficients of bit size* $\leq \tau$ *and* $\deg(f) = 2D$. *One can decide if* $f = \sum f_i^2, f_i \in \mathbb{Q}[X_1,\ldots,X_n]$ *within*

$$\tau^{\mathbf{O(1)}}\mathbf{D}^{\mathbf{O(n^3)}}$$

bit operations. The bit lengths of rational coefficients of the f_i*'s are bounded by*

$$\tau\delta^{\mathbf{O(N^3)}}$$

with $\delta = \binom{n+D}{n}$ *and* $N \leq \frac{1}{2}\delta(\delta+1) - \binom{n+2D}{n}$.

Proof: Using quantifier elimination over the reals, sampling points in semi-algebraic sets, etc.

Concluding Remarks

- Exact SOS is an alternative to symbolic critical values computations in RAG and interval computations in INTALAB.

- Huge amount of works to develop at the interface of numerical global optimization and symbolic computations.

Concluding Remarks

- Exact SOS is an alternative to symbolic critical values computations in RAG and interval computations in INTALAB.

- Huge amount of works to develop at the interface of numerical global optimization and symbolic computations.

Announcements:

- SIAM / MSRI Workshop on Hybrid Methodologies for Symbolic-Numeric Computation, Nov. 17-19, 2010. `http://www.scg.uwaterloo.ca/siam-msri-hybrid`

- The 4th International Workshop on Symbolic-Numeric Computation, June, 2010.

Thanks to

- the organizers
- the Arènaire project team, LIP
- all my collaborators of these works
  - NCSU: E.L. Kaltofen, S. Hutton
  - LIP6: M. Safey, A. Greuet
  - CNEU: Z.F. Yang
  - KLMM: B. Li, F. Guo