

Validating Numerical Semidefinite Programming Solvers for Polynomial Invariants

Pierre Roux

ONERA, Toulouse

October 24th 2017

Joint work with Érik Martin-Dorel

Numerical Optimization

Powerful tool to infer numerical invariants

```
(x1, x2) ∈ {x1, x2 | x12 + x22 ≤ 1.52}  
while (1) {  
    // Find Inv. p(x1, x2) ≥ 0  
    x1 = x1 * x2;  
    x2 = -x1;  
}
```

Numerical Optimization

Powerful tool to infer numerical invariants

```
(x1, x2) ∈ {x1, x2 | x12 + x22 ≤ 1.52}  
while (1) {  
    // Find Inv. p(x1, x2) ≥ 0  
    x1 = x1 * x2;  
    x2 = -x1;  
}
```

encoded as an optimization problem

"*polynomial_expr*(p) ≥ 0"

Numerical Optimization

Powerful tool to infer numerical invariants

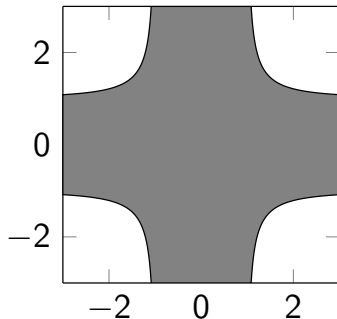
```
(x1, x2) ∈ {x1, x2 | x12 + x22 ≤ 1.52}  
while (1) {  
    // Find Inv. p(x1, x2) ≥ 0  
    x1 = x1 * x2;  
    x2 = -x1;  
}
```

encoded as an optimization problem

"*polynomial_expr*(p) ≥ 0"

optimization procedure gives

$$p(x_1, x_2) = 1 + 2.46x_1^2 + 2.46x_2^2 - 5 \times 10^{-7}x_1^4 \\ - 2.46x_1^2x_2^2 - 5 \times 10^{-7}x_2^4$$



Numerical Optimization

Powerful tool to infer numerical invariants

```
(x1, x2) ∈ {x1, x2 | x12 + x22 ≤ 1.52}  
while (1) {  
    // Find Inv. p(x1, x2) ≥ 0  
    x1 = x1 * x2;  
    x2 = -x1;  
}
```

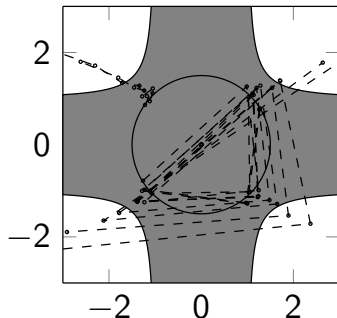
encoded as an optimization problem

“*polynomial_expr*(p) ≥ 0”

optimization procedure gives

$$p(x_1, x_2) = 1 + 2.46x_1^2 + 2.46x_2^2 - 5 \times 10^{-7}x_1^4 \\ - 2.46x_1^2x_2^2 - 5 \times 10^{-7}x_2^4$$

Can yield **incorrect results** without warning.



Polynomial Invariants

In a very nice SAS'15 paper, Adjé, Garoche and Magron offer for

```
(x1, x2) ∈ [0.9, 1.1] × [0, 0.2]
while (1) {
  pre_x1 = x1; pre_x2 = x2;
  if (x1^2 + x2^2 <= 1) {
    x1 = pre_x1^2 + pre_x2^3;
    x2 = pre_x1^3 + pre_x2^2;
  } else {
    x1 = 0.5 * pre_x1^3 + 0.4 * pre_x2^2;
    x2 = -0.6 * pre_x1^2 + 0.3 * pre_x2^2;
  }
}
```

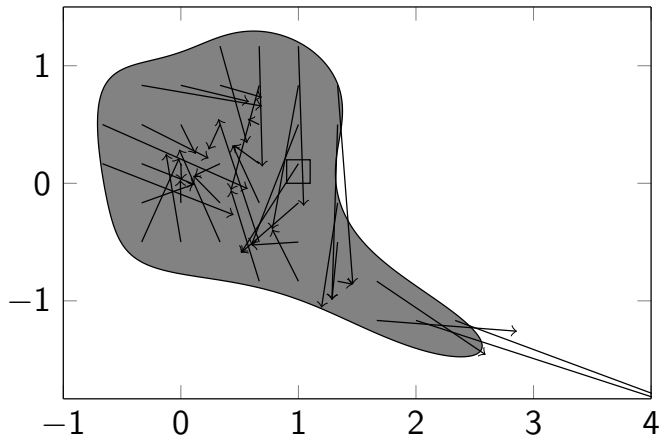
the inductive invariant $2.510902467 + 0.0050x_1 + 0.0148x_2 - 3.0998x_1^2 + 0.8037x_2^3 + 3.0297x_1^3 - 2.5924x_2^2 - 1.5266x_1x_2 + 1.9133x_1^2x_2 + 1.8122x_1x_2^2 - 1.6042x_1^4 - 0.0512x_1^3x_2 + 4.4430x_1^2x_2^2 + 1.8926x_1x_2^3 - 0.5464x_2^4 + 0.2084x_1^5 - 0.5866x_1^4x_2 - 2.2410x_1^3x_2^2 - 1.5714x_1^2x_2^3 + 0.0890x_1x_2^4 + 0.9656x_2^5 - 0.0098x_1^6 + 0.0320x_1^5x_2 + 0.0232x_1^4x_2^2 - 0.2660x_1^3x_2^3 - 0.7746x_1^2x_2^4 - 0.9200x_1x_2^5 - 0.6411x_2^6 \geq 0$.

Should we trust such results ?

- ▶ Some are correct (we'll prove it formally).

Should we trust such results ?

- ▶ Some are correct (we'll prove it formally).
- ▶ Others aren't (previous degree 6 polynomial)



Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Cholesky Decomposition

Experiments

Demo

Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Cholesky Decomposition

Experiments

Demo

In Adjé et al. paper

Look for a polynomial p s.t.

$$\begin{array}{ll} p - \sigma q \geq 0, & \sigma \geq 0 \quad \text{initial condition } (\forall x, q(x) \geq 0 \Rightarrow p(x) \geq 0) \\ p \circ f - p \geq 0 & \text{inductiveness } (\forall x, p(x) \geq 0 \Rightarrow p(f(x)) \geq 0) \end{array}$$

with $\{x \mid q(x) \geq 0\}$ initial set and f loop body.

Then $p \geq 0$ is an invariant.

In Adjé et al. paper

Look for a polynomial p s.t.

$$\begin{array}{ll} p - \sigma q \geq 0, & \sigma \geq 0 \quad \text{initial condition } (\forall x, q(x) \geq 0 \Rightarrow p(x) \geq 0) \\ p \circ f - p \geq 0 & \text{inductiveness } (\forall x, p(x) \geq 0 \Rightarrow p(f(x)) \geq 0) \end{array}$$

with $\{x \mid q(x) \geq 0\}$ initial set and f loop body.

Then $p \geq 0$ is an invariant.

Need to verify **polynomial positivity**.

demo.v

Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Cholesky Decomposition

Experiments

Demo

Sum of Squares (SOS) Polynomials

Definition (SOS Polynomial)

A polynomial p is SOS if there are polynomials q_1, \dots, q_m s.t.

$$p = \sum_i q_i^2.$$

- If p SOS then $p \geq 0$

Sum of Squares (SOS) Polynomials

Definition (SOS Polynomial)

A polynomial p is SOS if there are polynomials q_1, \dots, q_m s.t.

$$p = \sum_i q_i^2.$$

- ▶ If p SOS then $p \geq 0$
- ▶ p SOS iff there exist $z := [1, x_0, x_1, x_0x_1, \dots, x_n^d]$
and $Q \succeq 0$ (i.e., for all $x, x^T Q x \geq 0$) s.t.

$$p = z^T Q z.$$

⇒ SOS can be encoded as semi-definite programming (SDP).

SOS: Example

Example

Is $p(x, y) := 2x^4 + 2x^3y - x^2y^2 + 5y^4$ SOS ?

$$p(x, y) = \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix}^T \begin{bmatrix} q_{11} & q_{12} & q_{13} \\ q_{12} & q_{22} & q_{23} \\ q_{13} & q_{23} & q_{33} \end{bmatrix} \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix}$$

that is

$$p(x, y) = q_{11}x^4 + 2q_{13}x^3y + 2q_{23}xy^3 + (2q_{12} + q_{33})x^2y^2 + q_{22}y^4$$

SOS: Example

Example

Is $p(x, y) := 2x^4 + 2x^3y - x^2y^2 + 5y^4$ SOS ?

$$p(x, y) = \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix}^T \begin{bmatrix} q_{11} & q_{12} & q_{13} \\ q_{12} & q_{22} & q_{23} \\ q_{13} & q_{23} & q_{33} \end{bmatrix} \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix}$$

that is

$$p(x, y) = q_{11}x^4 + 2q_{13}x^3y + 2q_{23}xy^3 + (2q_{12} + q_{33})x^2y^2 + q_{22}y^4$$

hence $q_{11} = 2$, $2q_{13} = 2$, $2q_{23} = 0$, $2q_{12} + q_{33} = -1$, $q_{22} = 5$.

SOS: Example

Example

Is $p(x, y) := 2x^4 + 2x^3y - x^2y^2 + 5y^4$ SOS ?

$$p(x, y) = \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix}^T \begin{bmatrix} q_{11} & q_{12} & q_{13} \\ q_{12} & q_{22} & q_{23} \\ q_{13} & q_{23} & q_{33} \end{bmatrix} \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix}$$

that is

$$p(x, y) = q_{11}x^4 + 2q_{13}x^3y + 2q_{23}xy^3 + (2q_{12} + q_{33})x^2y^2 + q_{22}y^4$$

hence $q_{11} = 2, 2q_{13} = 2, 2q_{23} = 0, 2q_{12} + q_{33} = -1, q_{22} = 5$.

For instance

$$Q = \begin{bmatrix} 2 & -3 & 1 \\ -3 & 5 & 0 \\ 1 & 0 & 5 \end{bmatrix} = L^T L \quad L = \frac{1}{\sqrt{2}} \begin{bmatrix} 2 & -3 & 1 \\ 0 & 1 & 3 \end{bmatrix}$$

$$\text{hence } p(x, y) = \frac{1}{2} (2x^2 - 3y^2 + xy)^2 + \frac{1}{2} (y^2 + 3xy)^2.$$

Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Cholesky Decomposition

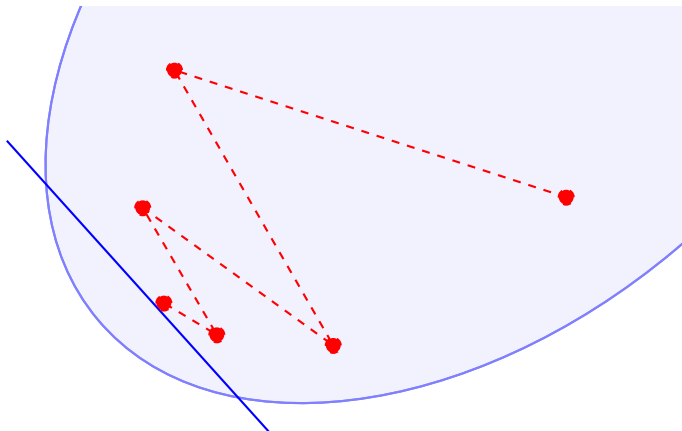
Experiments

Demo

Inaccuracy in Solving SDPs

SDP solvers only yield **approximate** solutions due to

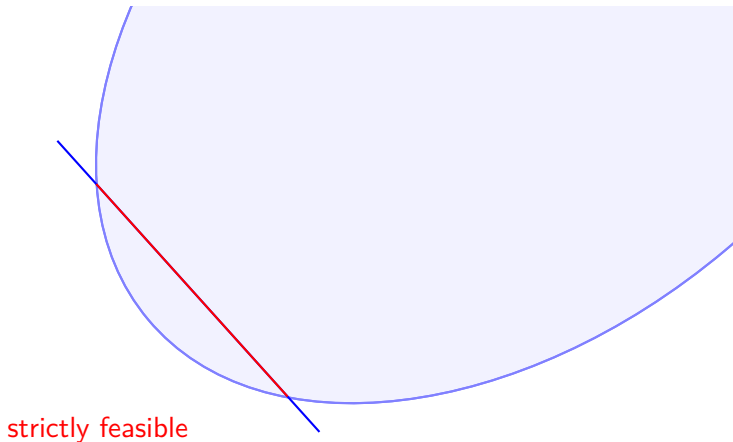
- ▶ inexact termination



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

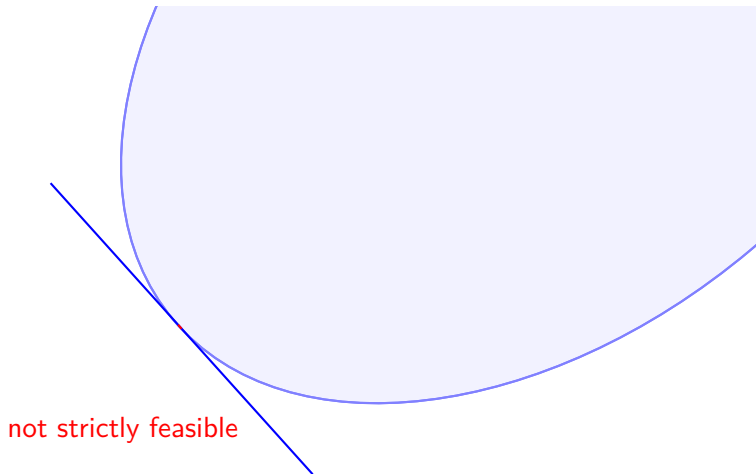
- ▶ inexact termination
- ▶ failure of strict feasibility



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

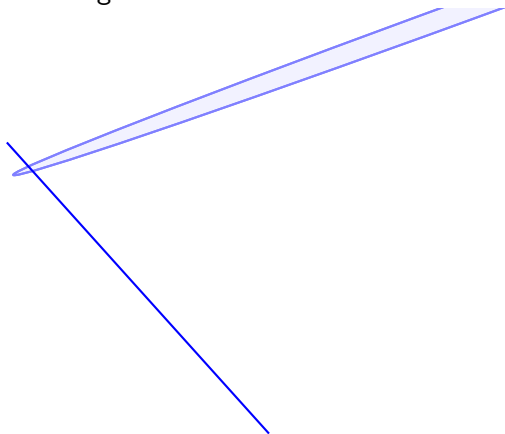
- ▶ inexact termination
- ▶ failure of strict feasibility



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

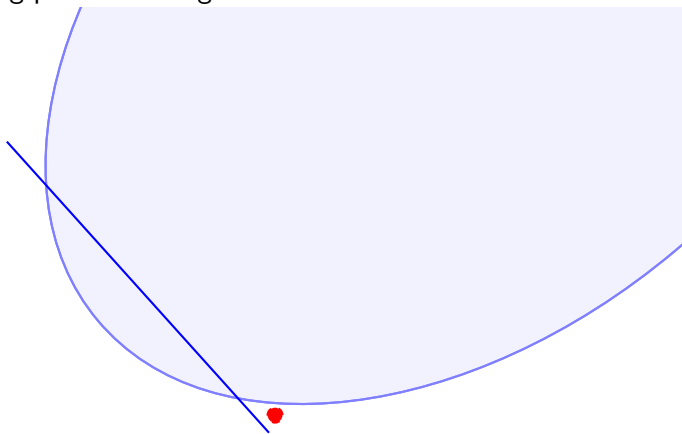
- ▶ inexact termination
- ▶ failure of strict feasibility
- ▶ ill conditioning



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

- ▶ inexact termination
- ▶ failure of strict feasibility
- ▶ ill conditioning
- ▶ floating-point rounding errors



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

- ▶ inexact termination
- ▶ failure of strict feasibility
- ▶ ill conditioning
- ▶ floating-point rounding errors

State of the art [Harrison, Peyrl and Parrilo,
Monniaux and Corbineau, Kaltofen et al., Magron et al.]

- ▶ round to exact rational solution (heuristic)
- ▶ proofs in rational arithmetic (expensive).

SOS: Using approximate SDP solvers

Result Q from SDP solver will only satisfy equality constraints up to some ϵ

$$p = z^T Q z + z^T E z, \quad \forall i, j, |E_{i,j}| \leq \epsilon.$$

SOS: Using approximate SDP solvers

Result Q from SDP solver will only satisfy equality constraints up to some ϵ

$$p = z^T Q z + z^T E z, \quad \forall i, j, |E_{i,j}| \leq \epsilon.$$

If $Q + E \succeq 0$ then $p = z^T (Q + E) z$ is SOS.

SOS: Using approximate SDP solvers

Result Q from SDP solver will only satisfy equality constraints up to some ϵ

$$p = z^T Q z + z^T E z, \quad \forall i, j, |E_{i,j}| \leq \epsilon.$$

If $Q + E \succeq 0$ then $p = z^T (Q + E) z$ is SOS.

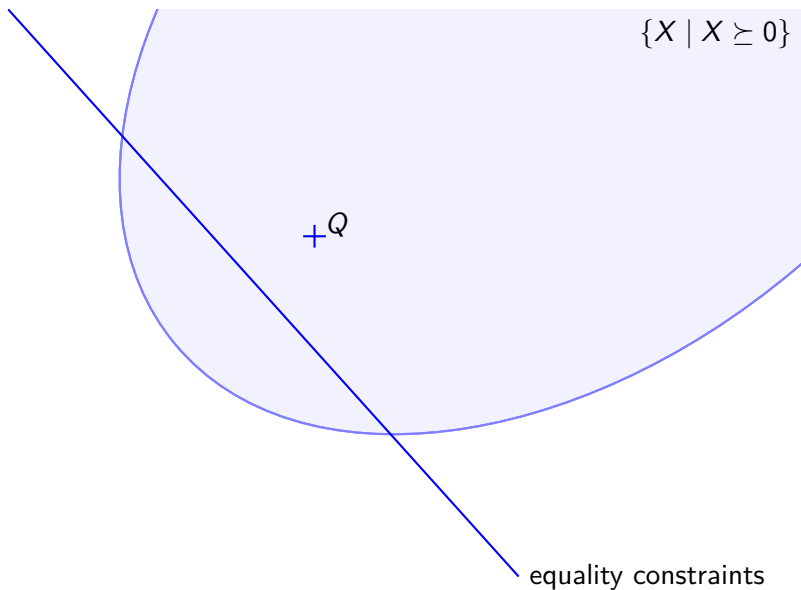
- ▶ Hence the validation method: given $p \simeq z^T Q z$
 1. Check that all monomials of p are in $z z^T$.
 2. Bound difference ϵ between coefficients of p and $z^T Q z$.
 3. If $Q - s \epsilon I \succeq 0$ ($s := \text{size of } Q$), then p is proved SOS.
 - ▶ 2 can be done with interval arithmetic
and 3 with a Cholesky decomposition ($\Theta(s^3)$ flops).
- ⇒ Efficient validation method using just floats.

Intuitively

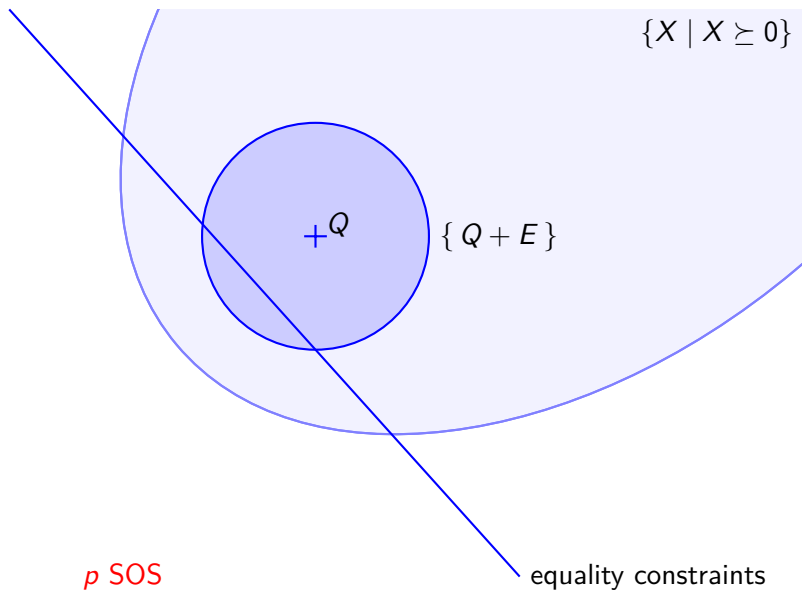
$$\{X \mid X \succeq 0\}$$

equality constraints

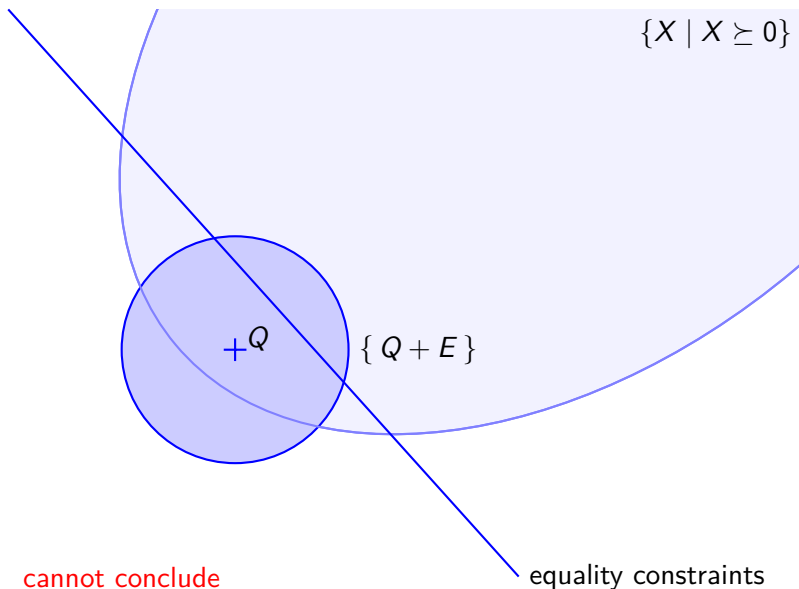
Intuitively



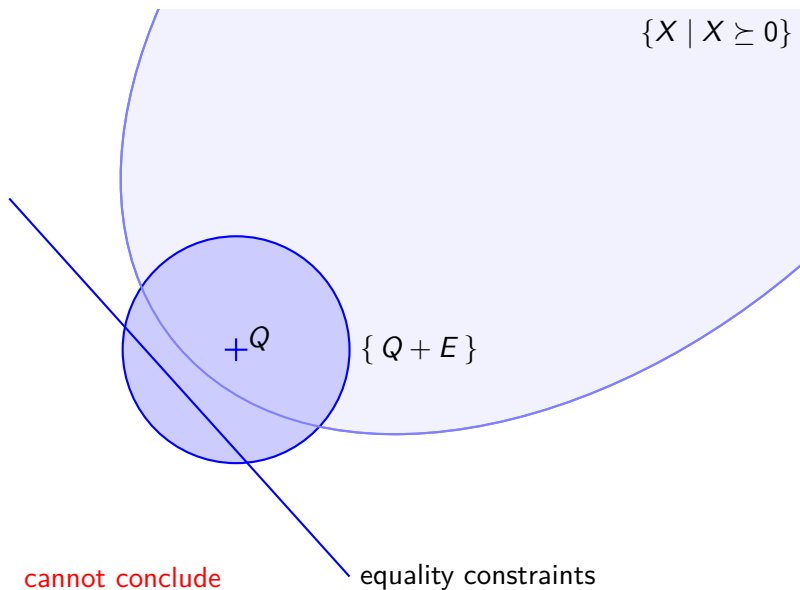
Intuitively



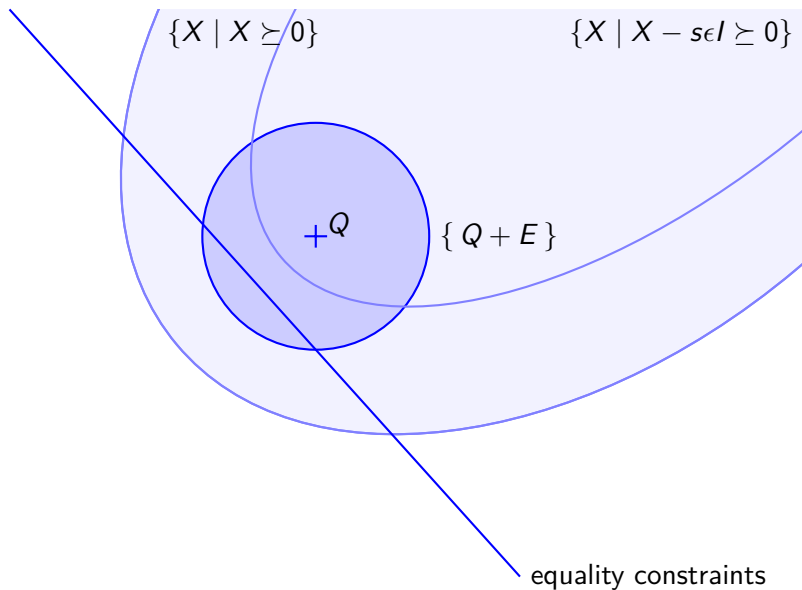
Intuitively



Intuitively



Padding



Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Cholesky Decomposition

Experiments

Demo

Cholesky Decomposition

- ▶ To prove that $a \in \mathbb{R}$ is non negative,
we can exhibit r such that $a = r^2$ (typically $r = \sqrt{a}$).

Cholesky Decomposition

- ▶ To prove that $a \in \mathbb{R}$ is non negative, we can exhibit r such that $a = r^2$ (typically $r = \sqrt{a}$).
- ▶ To prove that a matrix $A \in \mathbb{R}^{n \times n}$ is positive semi-definite we can similarly expose R such that $A = R^T R$ (since $x^T (R^T R) x = (Rx)^T (Rx) = \|Rx\|_2^2 \geq 0$).

Cholesky Decomposition

- ▶ To prove that $a \in \mathbb{R}$ is non negative, we can exhibit r such that $a = r^2$ (typically $r = \sqrt{a}$).
- ▶ To prove that a matrix $A \in \mathbb{R}^{n \times n}$ is positive semi-definite we can similarly expose R such that $A = R^T R$ (since $x^T (R^T R) x = (Rx)^T (Rx) = \|Rx\|_2^2 \geq 0$).
- ▶ The Cholesky decomposition computes such a matrix R :

```
 $R := 0;$   
for  $j$  from 1 to  $n$  do  
  for  $i$  from 1 to  $j - 1$  do  
     $R_{i,j} := \left( A_{i,j} - \sum_{k=1}^{i-1} R_{k,i} R_{k,j} \right) / R_{i,i};$   
  od  
   $R_{j,j} := \sqrt{M_{j,j} - \sum_{k=1}^{j-1} R_{k,j}^2};$   
od
```

- ▶ If it succeeds (no $\sqrt{\text{ of negative or div. by 0}}$) then $A \succeq 0$.

Cholesky Decomposition (end)

With rounding errors $A \neq R^T R$, Cholesky can succeed while $A \not\geq 0$.

Cholesky Decomposition (end)

With rounding errors $A \neq R^T R$, Cholesky can succeed while $A \not\succeq 0$.

But error is bounded and for some (tiny) $c \in \mathbb{R}$:
if Cholesky succeeds on A then $A + c I \succeq 0$.

Hence:

Theorem

If Cholesky succeeds on $A - c I$ then $A \succeq 0$

holds for any $c \geq \frac{(s+1)\varepsilon}{1-(2s+2)\varepsilon} \text{tr}(A) + 4(s+1) \left(2(s+2) + \max_i(A_{i,i}) \right) \eta$
(ε and η relative and absolute precision of floating-point format).

Proved in Coq (paper proof: 6 pages, Coq: 5.1 kloc)

Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Cholesky Decomposition

Experiments

Demo

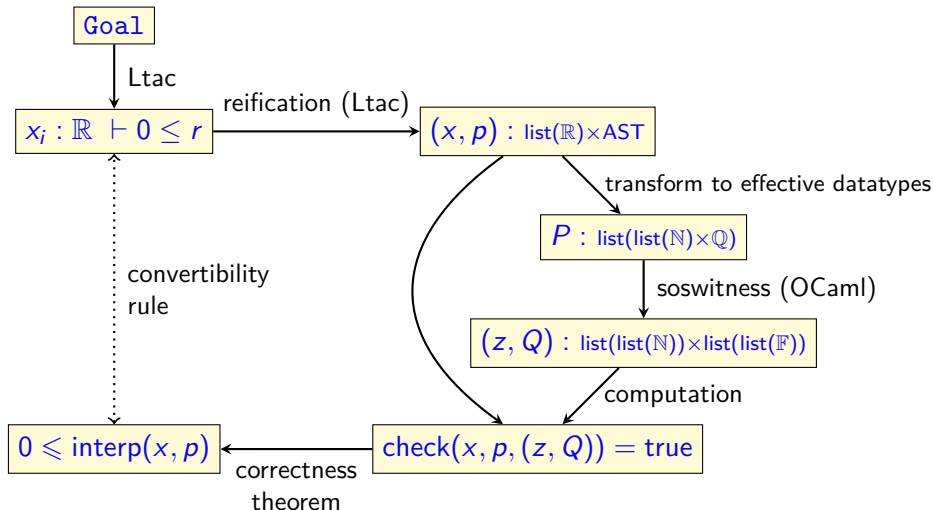
OCAML Implementation

- ▶ OPAM package: `opam install osdp`
- ▶ Available at <https://cavale.enseeiht.fr/osdp/>
- ▶ LGPL license
- ▶ Interface to SDP solvers CSDP, Mosek and SDPA
- ▶ 6.2 kloc of OCaml code + 1.2 kloc of C code

Coq Implementation

- ▶ Available at <https://sourcesup.renater.fr/validsdp/>
- ▶ LGPL license
- ▶ uses libraries
 - ▶ CoqEAL [Cano, Cohen, Dénès, Mörtberg, Rouhling, Siles]
for refinement proofs
(based on SSReflect and MathComp [Gonthier et al.])
 - ▶ SSrMultinomials [Strub]
for multivariate polynomials
 - ▶ CoqInterval [Melquiond] and Flocq [Boldo, Melquiond]
for floating-point numbers
- ▶ 15 kloc of Coq + 0.3 kloc of OCaml code

The validsdp tactic – the big picture



Benchmarks (1/3)

Setup:

- ▶ A desktop PC under Debian GNU/Linux Jessie
- ▶ Core i5-4460S CPU clocked at 2.9 GHz
- ▶ All timings are total elapsed time (in seconds)
- ▶ Timeout of 900s
- ▶ ValidSDP version: d60c663
- ▶ library versions: Coq 8.5.2, MathComp 1.6, Flocq 2.5.1, Coquelicot 2.1.1, CoqInterval 3.1.0, OSDP 0.5.2 and dev. version of other libs

Benchmarks (2/3)

Problem	n	d	OSDP (not verified)	MonniauxC11 (not verified)	NLCertify (not verified)	QEPCAD (not verified)	ValidSDP	PVS/Bernstein	NLCertify	HOL Light/ Taylor
adaptiveLV	4	4	0.75	2.67	1.12	3.29	5.16	14.93	2.61	12.31
butcher	6	4	1.58	—	1.05	—	9.40	48.44	8.36	15.62
caprasse	4	4	0.41	1.82	0.88	4.33	5.19	25.89	2.63	17.68
heart	8	4	3.18	268.75	—	—	16.67	131.13	—	26.15
magnetism	7	2	1.11	2.04	1.64	4.02	5.18	245.52	14.50	16.07
reaction	3	2	0.81	1.56	0.24	3.00	4.33	11.48	1.96	12.41
schwefel	3	4	0.95	2.45	2.76	3.26	3.70	14.72	56.13	17.46
fs260	6	4	1.25	—	—	—	5.99	—	—	—
fs461	6	4	0.70	11.18	0.87	—	5.18	621.06	7.46	22.70
fs491	6	4	0.54	21.81	—	—	5.38	—	—	—
fs745	6	4	0.98	11.74	0.94	—	5.55	623.17	6.90	22.48
fs752	6	2	0.35	1.81	0.90	—	3.80	54.52	7.88	13.34
fs8	6	2	0.43	1.53	1.48	—	3.93	52.63	6.62	13.40
fs859	6	8	—	—	—	—	—	—	—	—
fs860	6	4	1.21	10.53	1.11	—	6.08	73.65	7.34	14.28
fs861	6	4	1.09	10.48	1.20	—	5.15	69.74	7.87	14.28
fs862	6	4	1.27	79.25	1.25	—	5.37	73.54	7.58	14.14
fs863	6	2	0.94	1.50	—	—	3.85	—	—	13.85
fs864	6	2	0.56	2.05	—	—	4.05	—	—	13.28
fs865	6	2	0.76	2.11	—	—	3.68	—	—	13.76
fs867	6	2	0.21	2.09	1.74	—	4.22	—	8.04	—

Benchmarks (3/3)

Problem	n	d	OSDP (not verified)	MonniauxC11 (not verified)	NLCertify (not verified)	QEPCAD (not verified)	ValidSDP	PVS/Bernstein	NLCertify	HOL Light/ Taylor
fs868	6	4	0.94	—	—	—	6.05	—	—	—
fs884	6	4	—	—	—	—	—	—	—	—
fs890	6	4	—	7.78	—	—	—	—	—	—
ex4_d4	2	12	—	—	—	—	—	—	—	—
ex4_d6	2	18	—	—	—	—	—	—	—	—
ex4_d8	2	24	16.99	—	—	—	82.89	—	—	—
ex4_d10	2	30	—	—	—	—	—	—	—	—
ex5_d4	3	8	1.67	—	—	—	13.63	—	—	—
ex5_d6	3	12	16.10	—	—	—	66.82	—	—	—
ex5_d8	3	16	203.06	—	—	—	353.70	—	—	—
ex5_d10	3	20	—	—	—	—	—	—	—	—
ex6_d4	4	8	16.82	—	—	—	44.99	—	—	—
ex6_d6	4	12	—	—	—	—	—	—	—	—
ex7_d4	2	12	—	—	—	—	—	—	—	—
ex7_d6	2	18	1.50	—	—	—	26.78	—	—	—
ex7_d8	2	24	15.38	—	—	—	83.47	—	—	—
ex7_d10	2	30	—	—	—	—	—	—	—	—
ex8_d4	2	8	0.87	15.72	—	61.94	7.52	—	—	—
ex8_d6	2	12	—	—	—	—	—	—	—	—
ex8_d8	2	16	—	—	—	—	—	—	—	—
ex8_d10	2	20	—	—	—	—	—	—	—	—

Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Cholesky Decomposition

Experiments

Demo

OSDP (OCaml)

invariant.ml

ValidSDP (Coq)

invariant.v

Questions

Thanks for your attention!

