

Validating Numerical Semidefinite Programming Solvers for Polynomial Invariants

Pierre Roux¹ Yuen-Lam Voronin²
Sriram Sankaranarayanan²

¹ONERA, Toulouse, FRANCE

²University of Colorado, Boulder, CO, USA

September 10th 2016

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

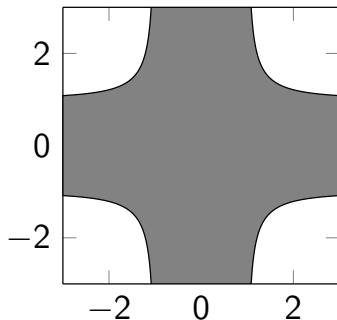
```
(x1, x2) ∈ {x1, x2 | x12 + x22 ≤ 1.52}  
while (1) {  
  // Find Inv. p(x1, x2) ≥ 0  
  x1 = x1 * x2;  
  x2 = -x1;  
}
```

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;  
}
```

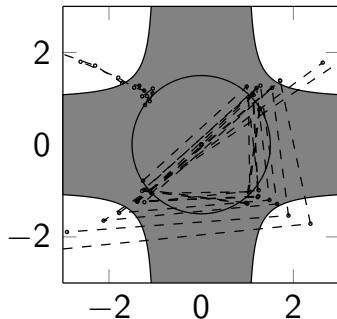
encoded as an optimization problem

“*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;
  }
}
```

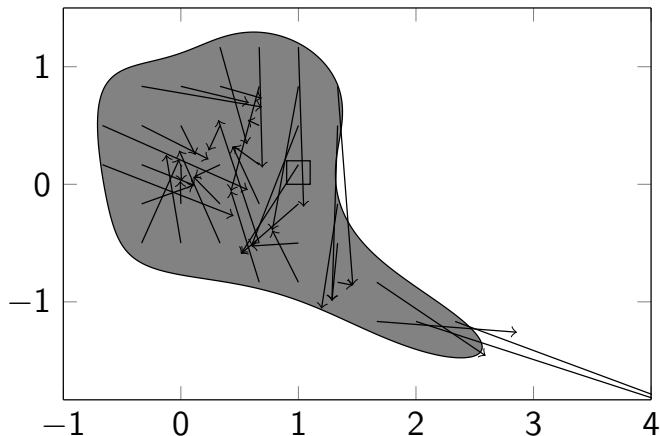
the inductive invariant $2.510902467 + 0.0050x_1 + 0.0148x_2 - 3.0998x_1^2 + 0.8037x_2^3 + 3.0297x_1^3 - 2.5924x_2^2 - 1.5266x_1x_2 + 1.9133x_1^2x_2 + 1.8122x_1x_2^2 - 1.6042x_1^4 - 0.0512x_1^3x_2 + 4.4430x_1^2x_2^2 + 1.8926x_1x_2^3 - 0.5464x_2^4 + 0.2084x_1^5 - 0.5866x_1^4x_2 - 2.2410x_1^3x_2^2 - 1.5714x_1^2x_2^3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

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).
- ▶ Other aren't (previous degree 6 polynomial)



Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Experiments

Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Experiments

In Adjé et al. paper

Look for a polynomial p

s.t.

$$\begin{aligned} p - \sigma q &\geq 0, \quad \sigma \geq 0 \\ p \circ f - p &\geq 0 \end{aligned}$$

initial condition
inductiveness

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 minimizing w s.t.

$$p - \sigma q \geq 0, \quad \sigma \geq 0$$

$$p \circ f - p \geq 0$$

$$w - \|x\|_2^2 - p \geq 0$$

initial condition

inductiveness

look for a "small" set

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 minimizing w s.t.

$$p - \sigma q \geq 0, \quad \sigma \geq 0$$

$$p \circ f - p \geq 0$$

$$w - \|x\|_2^2 - p \geq 0$$

initial condition

inductiveness

look for a "small" set

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

Then $p \geq 0$ is an invariant.

$q \geq 0$ relaxed as “ q sum of squares” and solved with SDP solvers.

Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Experiments

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

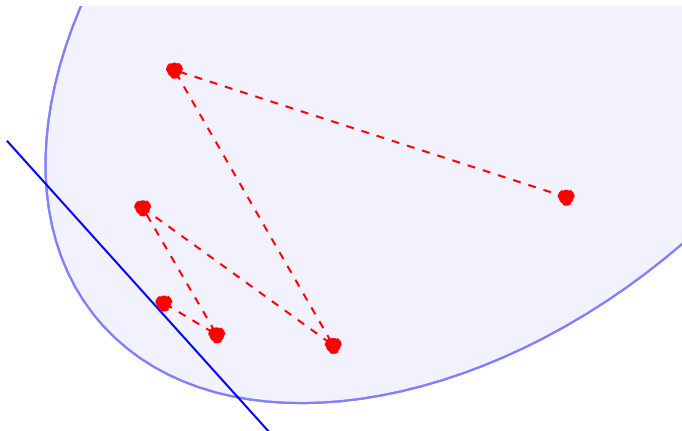
Numerical Verification of SOS

Experiments

Inaccuracy in Solving SDPs

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

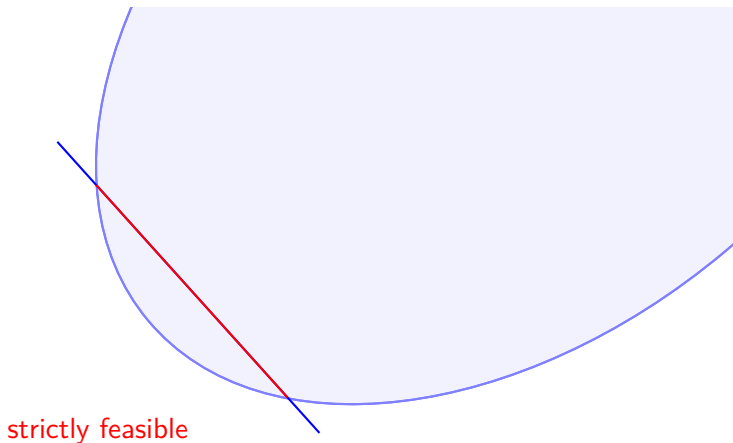
- ▶ inexact termination



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

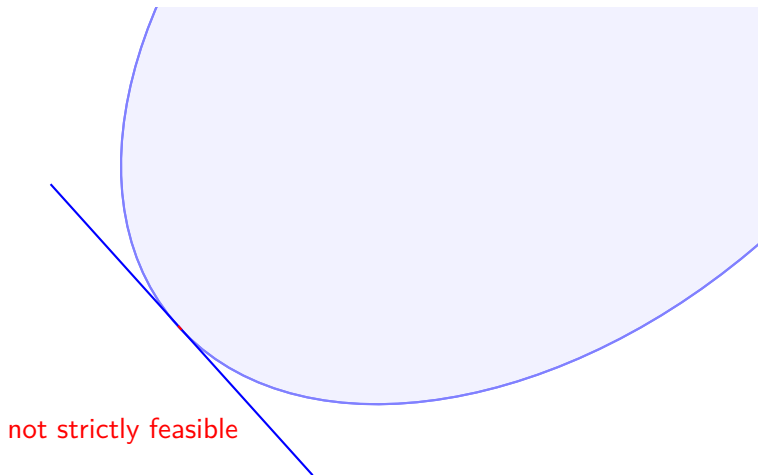
- ▶ inexact termination
- ▶ failure of strict feasibility



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

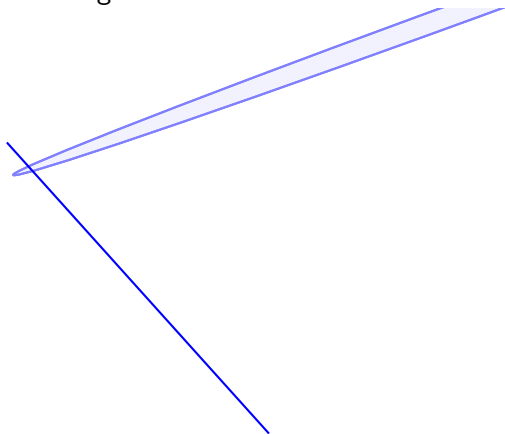
- ▶ inexact termination
- ▶ failure of strict feasibility



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

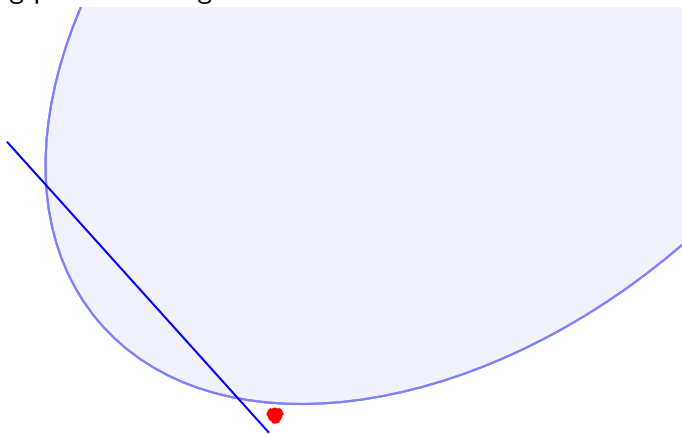
- ▶ inexact termination
- ▶ failure of strict feasibility
- ▶ ill conditioning



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

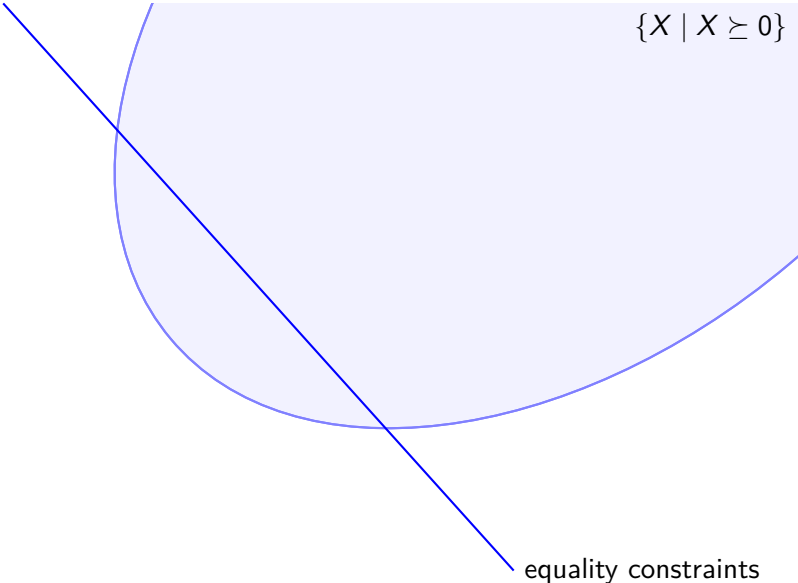
Result Q from SDP solver will only satisfy equality constraints up to some ϵ

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

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

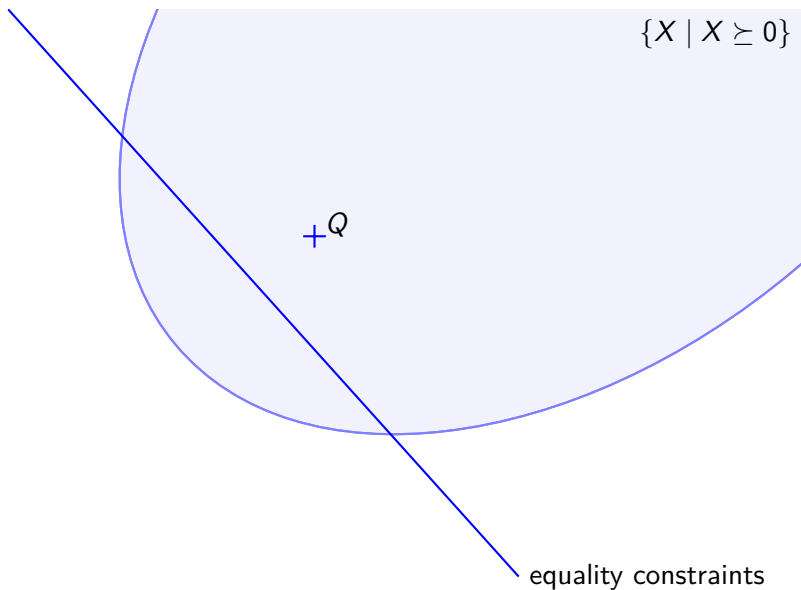
- ▶ Hence the validation method: given $p \simeq z^T Q z$
 1. Check that all monomials of p are in $z z^T$.
 2. Bound difference ϵ between coefficients of p and $z^T Q z$.
 3. If $Q - s \in I \succeq 0$ ($s :=$ size of Q), then p is proved SOS.
 - ▶ 2 can be done with interval arithmetic and 3 with a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

Intuitively

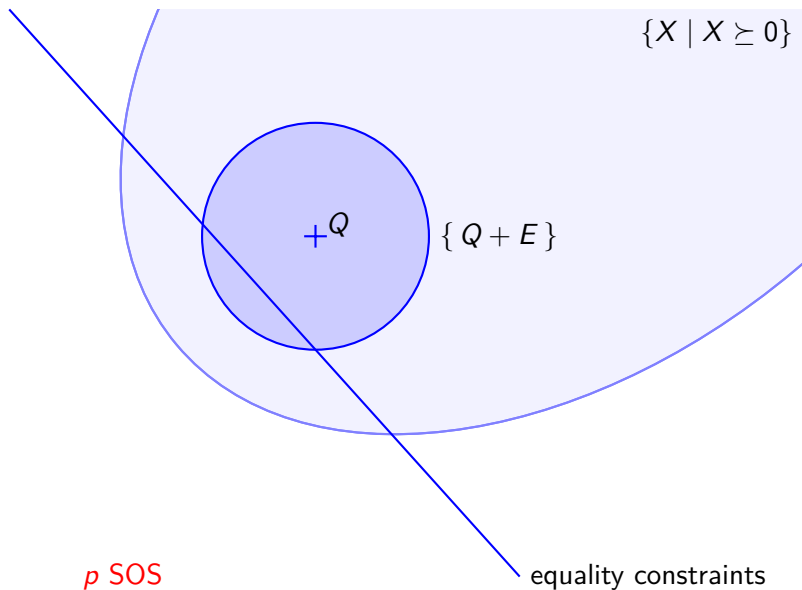
$$\{X \mid X \succeq 0\}$$


equality constraints

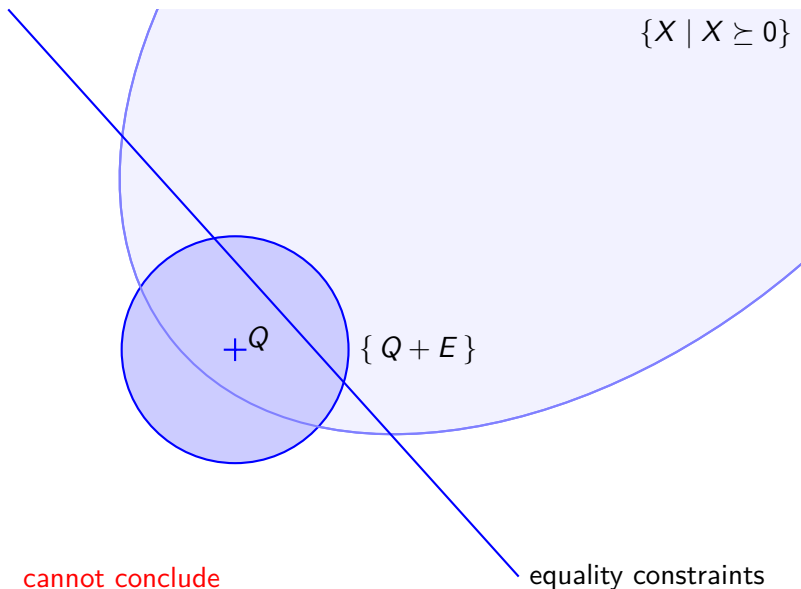
Intuitively



Intuitively



Intuitively



Intuitively

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

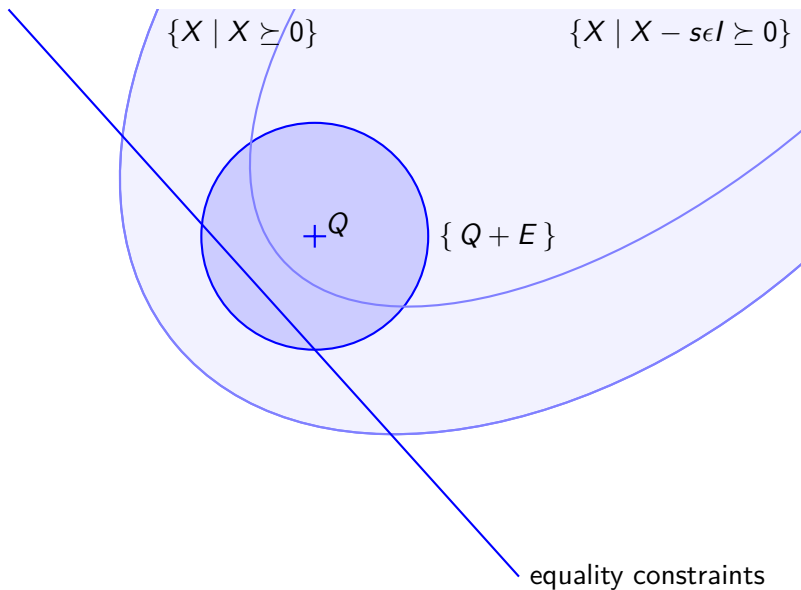
$$+Q$$

$$\{Q + E\}$$

cannot conclude

equality constraints

Padding



Polynomial Invariants

Sum of Squares (SOS) Polynomials

Numerical Verification of SOS

Experiments

Implementation

OCaml library OSDP: <http://cavale.enseeiht.fr/osdp/>

Experiments

- ▶ Reuse benchmarks from Adjé et al.
- ▶ Synthesize Invariants using their method
- ▶ Attempt proofs using rational arithmetic
- ▶ Then floating-point arithmetic

Experiments: Invariant Synthesis

Table : Time to synthesize candidate invariants for benchmarks of Adjé et al. n is the number of variables. All times are in seconds, TO means timeout (900s) and MO out of memory (4GB).

	$d = 4$	$d = 6$	$d = 8$	$d = 10$
Ex. 4 ($n = 2$)	0.25	0.95	3.31	8.85
Ex. 5 ($n = 3$)	0.48	2.83	22.75	112.37
Ex. 6 ($n = 4$)	2.12	64.07	TO	MO
Ex. 7 ($n = 2$)	0.25	0.96	3.15	10.45
Ex. 8 ($n = 2$)	0.17	0.34	0.74	1.93

Experiments: Proof using Exact Rational Arithmetic

Table : Checking the candidate invariants with the implementation of MONNIAUX and CORBINEAU. All times in seconds, NS means no proof is found, TO means timeout (900s) and MO out of memory (4GB).

		$d = 4$		$d = 6$		$d = 8$		$d = 10$	
		init	ind.	init	ind.	init	ind.	init	ind.
Ex. 4	$(n = 2)$	1.43	NS	3.35	TO	19.80	MO	142.33	MO
Ex. 5	$(n = 3)$	3.82	TO	142.49	MO	TO	MO	TO	MO
Ex. 6	$(n = 4)$	32.20	TO	TO	MO	—	—	—	—
Ex. 7	$(n = 2)$	1.48	NS	3.36	TO	18.36	MO	120.40	MO
Ex. 8	$(n = 2)$	1.93	12.81	3.78	NS	26.29	TO	193.79	TO

Experiments: Proof using Floating-Point Arithmetic

Table : Checking the candidate invariants with our method.

Counter-examples are easily found for Ex. 4, $d = 4, 6$ and Ex. 7, $d = 4$.

Whether other unproved “invariants” are inductive remains unknown.

	$d = 4$		$d = 6$		$d = 8$		$d = 10$	
	init	ind.	init	ind.	init	ind.	init	ind.
Ex. 4 ($n = 2$)	0.05	NS	0.07	NS	0.19	3.03	0.17	NS
Ex. 5 ($n = 3$)	0.08	0.33	0.23	2.20	0.74	14.55	2.50	92.15
Ex. 6 ($n = 4$)	0.22	1.52	1.26	38.94	—	—	—	—
Ex. 7 ($n = 2$)	0.05	NS	0.07	0.85	0.19	3.32	0.17	NS
Ex. 8 ($n = 2$)	0.05	0.13	0.07	NS	0.09	NS	0.15	NS

Future work

- ▶ Coq automatic tactic (almost done)
- ▶ Use in SMT solvers (prototype in Alt-Ergo)
- ▶ Use of facial reduction to alleviate strict feasibility constraint
- ▶ Applications to hybrid systems

Questions

Thanks for your attention!

