ValidSDP: Coq Proofs of Polynomial Positivity

using Numerical Solvers and Floating-Point Computations

Érik Martin-Dorel[1] Pierre Roux[2]

[1]IRIT, Université Paul Sabatier, Toulouse, France

[2]ONERA, Toulouse, France

May 25th, 2023

Certified and Symbolic-Numeric Computation, Lyon

Motivation

- Polynomial inequalities in the real field are decidable (Tarski)
- But exact algo. expensive

Motivation

- Polynomial inequalities in the real field are decidable (Tarski)
- But exact algo. expensive

$\Rightarrow$ Use incomplete numerical methods
  - off-the-shelf optimization solvers
  - a posteriori validation with exact rational arithmetic: state of the art (simple but costly)

Motivation

- Polynomial inequalities in the real field are decidable (Tarski)
- But exact algo. expensive

⇒ Use incomplete numerical methods

  - off-the-shelf optimization solvers
  - a posteriori validation with exact rational arithmetic: state of the art (simple but costly)
  - a posteriori validation with floating-point arithmetic (more efficient but non trivial)

  ⇒ We'd like formal proofs

Sum of Squares (SOS) Polynomials

Definition (SOS Polynomial)

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

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

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

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

$\Rightarrow$ 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

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

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

SOS: Using approximate SDP solvers

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

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

SOS: Using approximate SDP solvers

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

$$p = z^T Q z + z^T E z, \qquad \forall i\, j, |E_{i,j}| \le \delta.$$

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 error δ

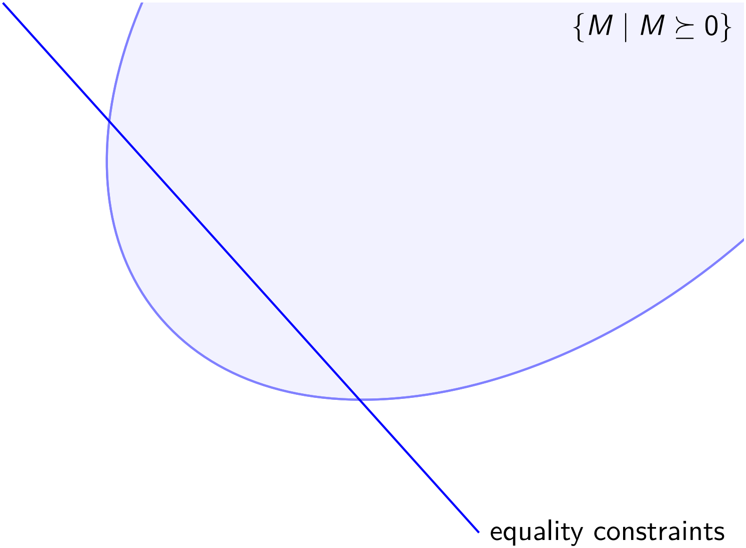
$$p = z^T Q\, z + z^T E\, z, \qquad\qquad \forall i\, j, |E_{i,j}| \leq \delta.$$

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

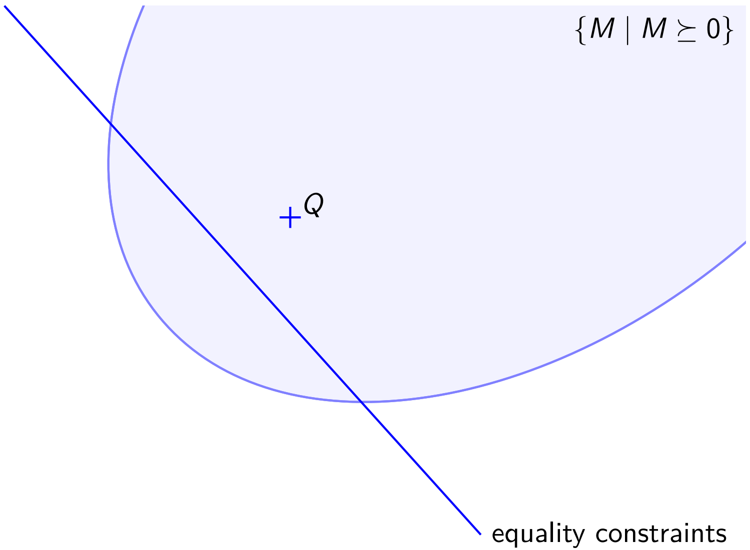
- Hence the validation method: given $p \simeq z^T Q\, z$
  1. Bound difference δ between coefficients of p and $z^T Q\, z$.
  2. If $Q - s\,\delta\, I \succeq 0$ ($s :=$ size of Q), then p is proved SOS.
- 1 can be done with interval arithmetic
  and 2 with a Cholesky decomposition ($\Theta(s^3)$ flops).

$\Rightarrow$ Efficient validation method using just floats.

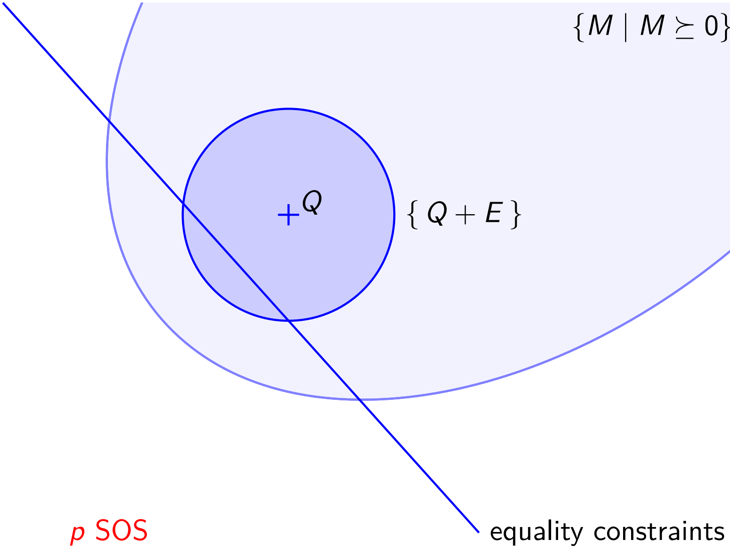
Intuitively



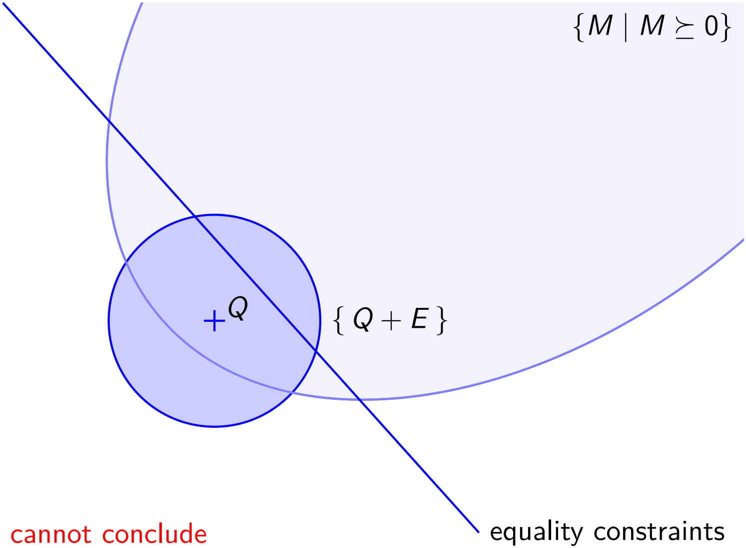
Intuitively



Intuitively

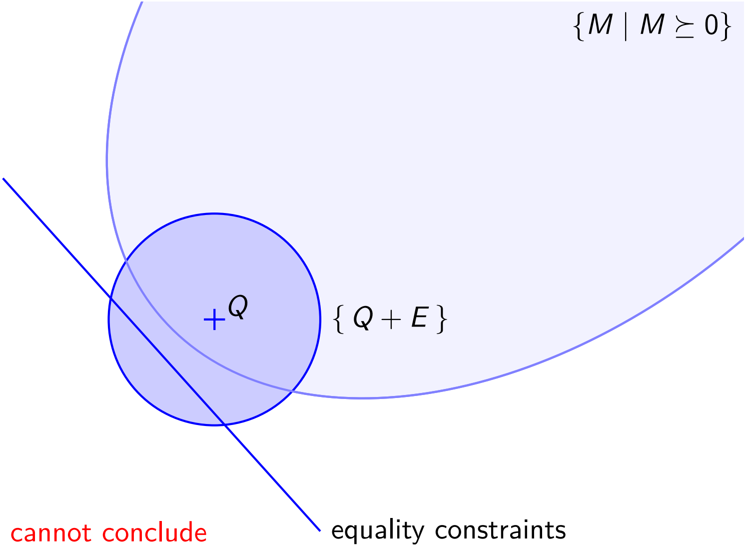


Intuitively



cannot conclude

Intuitively



cannot conclude

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 $x^T \left(R^T R\right) x = (Rx)^T (Rx) = \|Rx\|_2^2 \geq 0$).

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 $x^T \left(R^T R\right) x = (Rx)^T (Rx) = \|Rx\|_2^2 \geq 0$).
- 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 $\sqrt{}$ 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 $A \not\succeq 0$.

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 floating-point Cholesky succeeds on $A - c\,I$ then $A \succeq 0$
holds for any $c \geq \frac{(s+1)\varepsilon}{1-(s+1)\varepsilon}\mathrm{tr}(A) + 4s\left(2(s+1) + \max_i(A_{i,i})\right)\eta$
(ε and η relative and absolute precision of floating-point format).

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

Sum of Squares (SOS) Polynomials

Numerical Verification

Formalization & Reflexive Tactic

Benchmarks

Conclusion

Outline of the formalization

1. Effective multivariate polynomials
   - CoqEAL [Cano, Cohen, Dénès, Mörtberg, Rouhling, Siles]
   - ⇝ uses SSReflect and MathComp [Gonthier et al.]
   - proof: MathComp Multinomials [Strub]
   - implem.: FMapAVL from Coq stdlib
   - coefficients: $\mathbb{Q}$ as `bigQ` from Coq stdlib

Outline of the formalization

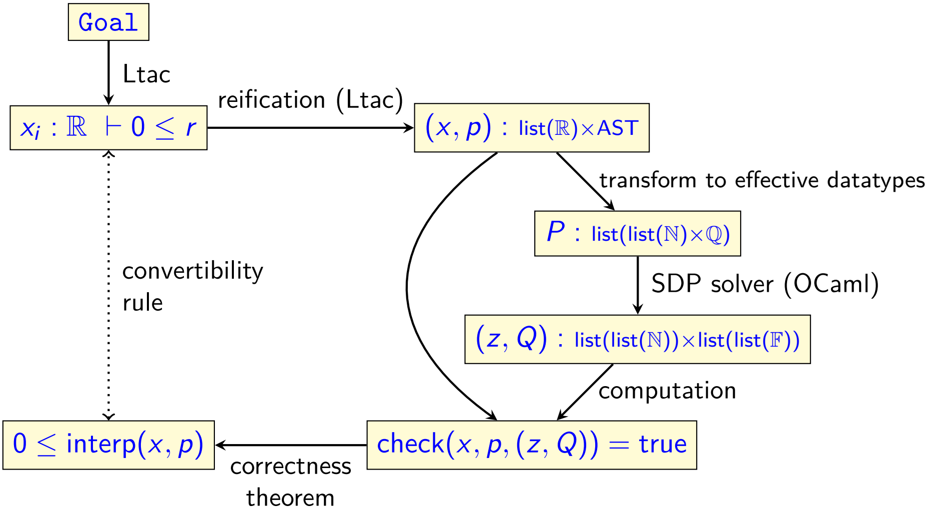
1. Effective multivariate polynomials
   - CoqEAL [Cano, Cohen, Dénès, Mörtberg, Rouhling, Siles]

   ⇝ uses SSReflect and MathComp [Gonthier et al.]
   - proof: MathComp Multinomials [Strub]
   - implem.: FMapAVL from Coq stdlib
   - coefficients: $\mathbb{Q}$ as `bigQ` from Coq stdlib
2. Effective check for positive definite matrices
   - CoqEAL
   - proof: MathComp matrices
   - implem.: lists of lists, CoqEAL
   - coefficients: floating-point from CoqInterval [Melquiond] or hardware floats (c.f., Érik tomorrow)

Outline of the formalization

1. Effective multivariate polynomials
   - CoqEAL [Cano, Cohen, Dénès, Mörtberg, Rouhling, Siles]
   - $\rightsquigarrow$ uses SSReflect and MathComp [Gonthier et al.]
   - proof: MathComp Multinomials [Strub]
   - implem.: FMapAVL from Coq stdlib
   - coefficients: $\mathbb{Q}$ as `bigQ` from Coq stdlib
2. Effective check for positive definite matrices
   - CoqEAL
   - proof: MathComp matrices
   - implem.: lists of lists, CoqEAL
   - coefficients: floating-point from CoqInterval [Melquiond] or hardware floats (c.f., Érik tomorrow)
3. Reflexive tactic
   - OCaml code as a wrapper for SDP solvers
   - Some Ltac2 code

The validsdp tactic – the big picture



Sum of Squares (SOS) Polynomials

Numerical Verification

Formalization & Reflexive Tactic

Benchmarks

Conclusion

Benchmarks (1/2)

Problem	n	d	OSDP (not verified)	MonniauxC11 (not verified)	NLCertify (not verified)	ValidSDP	PVS/Bernstein	NLCertify	HOL Light/Taylor
adaptativeLV	4	4	**0.75**	2.67	1.12	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	**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	**5.18**	245.52	14.50	16.07
reaction	3	2	**0.81**	1.56	0.24	4.33	11.48	**1.96**	12.41
schwefel	3	4	**0.95**	2.45	2.76	**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	—

Times in s with 900 s timeout

Benchmarks (2/2)

Problem	n	d	OSDP (not verified)	MonniauxC11 (not verified)	NLCertify (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	—	**7.52**	—	—	—
ex8_d6	2	12	—	—	—	—	—	—	—
ex8_d8	2	16	—	—	—	—	—	—	—
ex8_d10	2	20	—	—	—	—	—	—	—

Times in s with 900 s timeout

Conclusion

- Context: formal proof of multivariate polynomial positivity
- A Coq reflexive tactic
  - Input: polynomial goals with real variables and rational coefs
  - Use off-the-shelf SDP solvers as untrusted oracles
  - Numerical approach with formal floating-point arithmetic
  - Algorithm involving matrices (Cholesky)

Thank you!

Questions

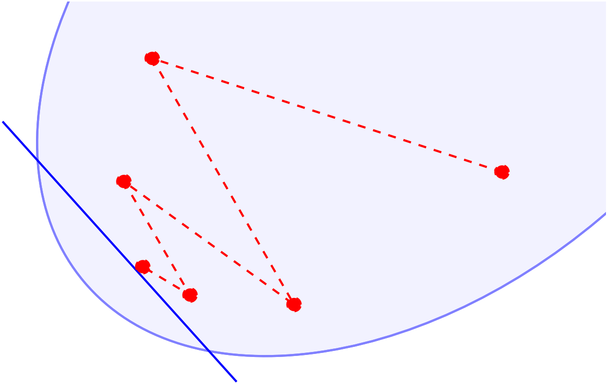
?

https://github.com/validsdp/validsdp

Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

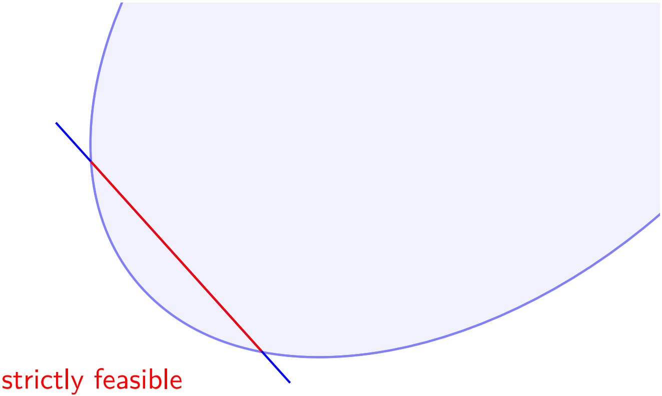
- inexact termination



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

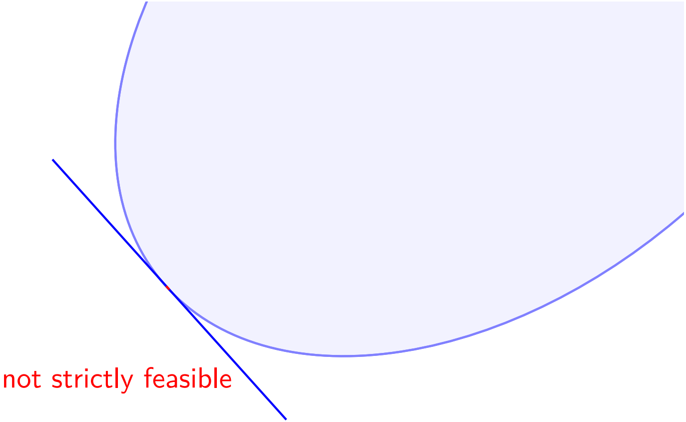
- inexact termination
- failure of strict feasibility



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

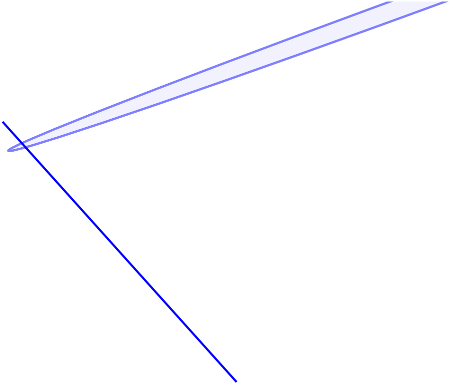
- inexact termination
- failure of strict feasibility



Inaccuracy in Solving SDPs

SDP solvers only yield approximate solutions due to

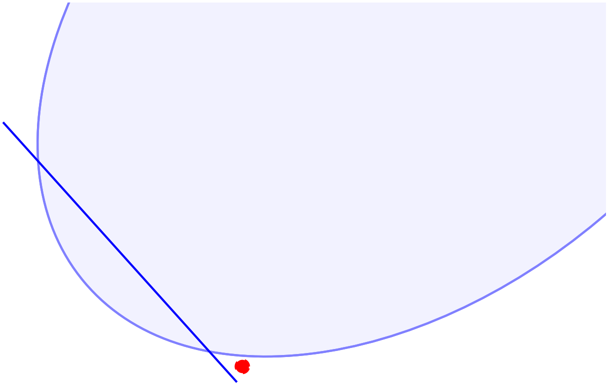
- inexact termination
- failure of strict feasibility
- ill conditioning



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

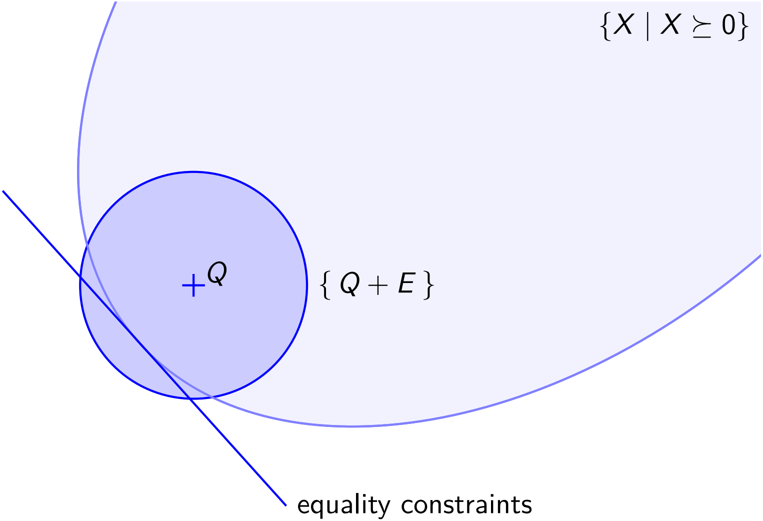
- inexact termination
- failure of strict feasibility
- ill conditioning
- floating-point rounding errors

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

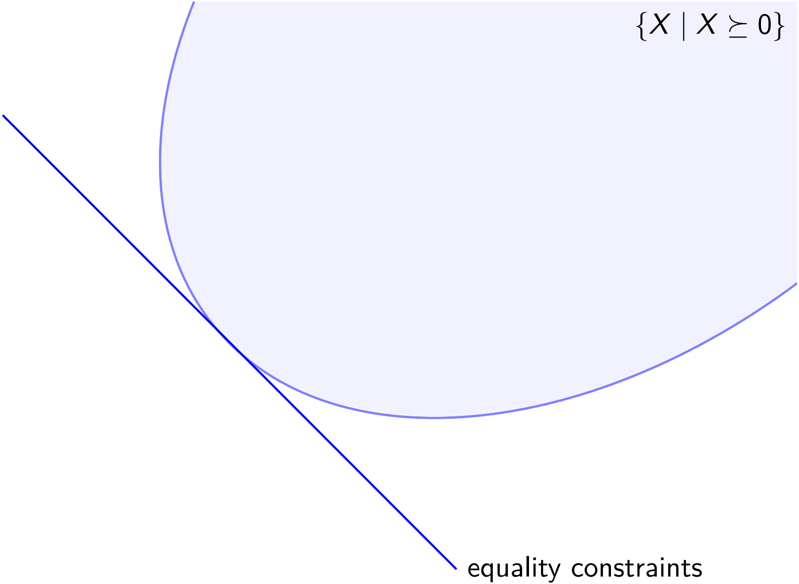
- round to exact rational solution (heuristic)
- proofs in rational arithmetic (expensive).

Incompleteness: Empty Interior SDP Problems

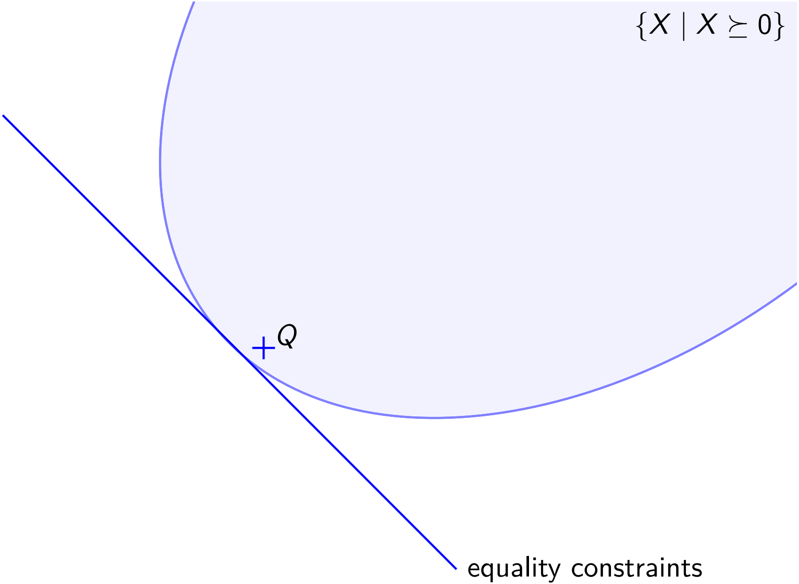
If the interior of the feasibility set of the problem is empty
(i.e., no feasible Q s.t. every Q' in a small neighborhood is feasible)
previous method almost never works.



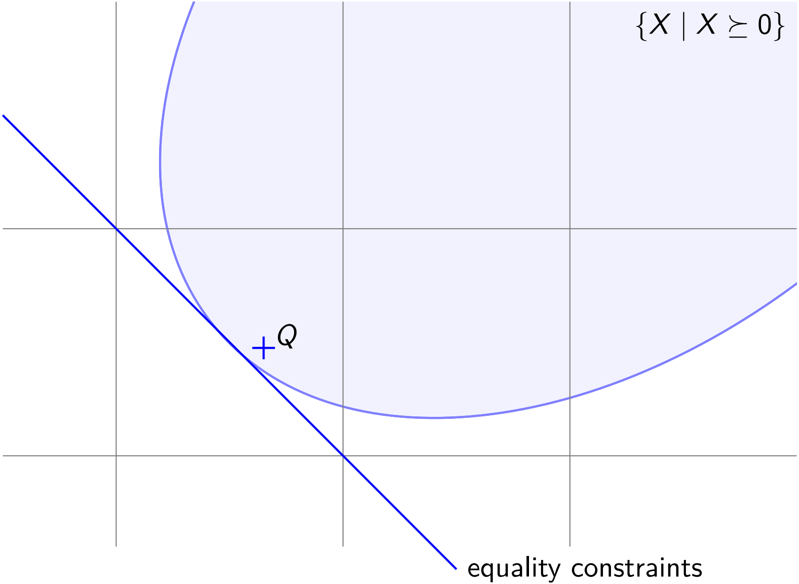
Intuitively, Rounding to an Exact Solution



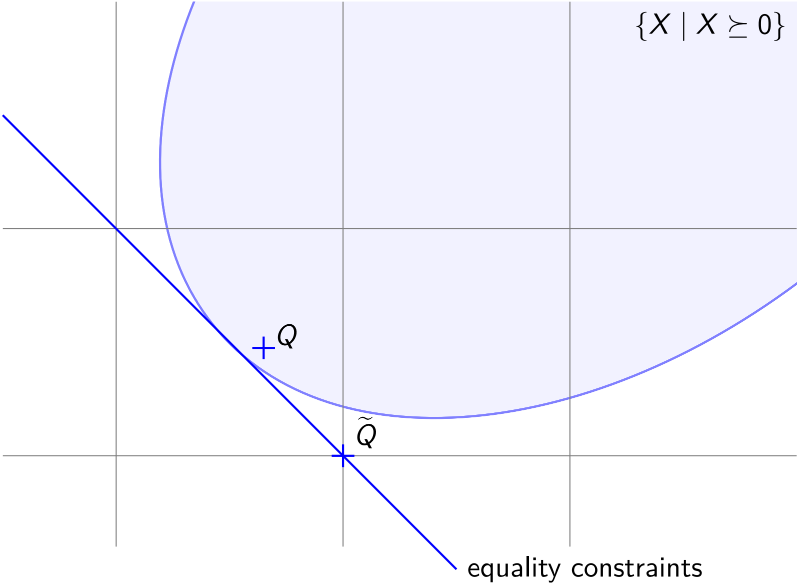
Intuitively, Rounding to an Exact Solution



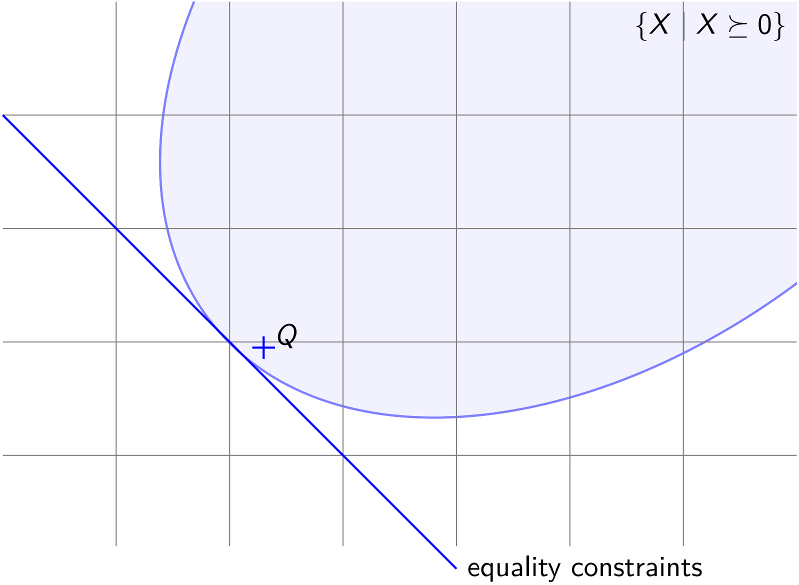
Intuitively, Rounding to an Exact Solution



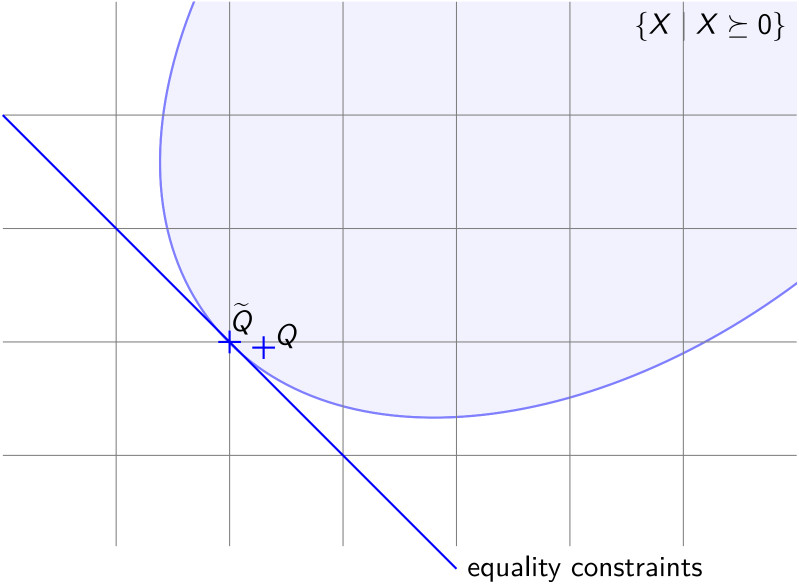
Intuitively, Rounding to an Exact Solution



Intuitively, Rounding to an Exact Solution



Intuitively, Rounding to an Exact Solution



Positivstellensatz

We want to prove that

$$p_1(x_1, \ldots, x_n) \geq 0 \wedge \ldots \wedge p_m(x_1, \ldots, x_n) \geq 0$$

is not satisfiable.

Positivstellensatz

We want to prove that

$$p_1(x_1, \ldots, x_n) \geq 0 \wedge \ldots \wedge p_m(x_1, \ldots, x_n) \geq 0$$

is not satisfiable.

Sufficient condition: there exist $r_i \in \mathbb{R}[x]$ s.t.

$$-\sum_i r_i \, p_i > 0 \quad \text{and} \quad \forall i, r_i \geq 0$$

Positivstellensatz

We want to prove that

$$p_1(x_1, \ldots, x_n) \geq 0 \wedge \ldots \wedge p_m(x_1, \ldots, x_n) \geq 0$$

is not satisfiable.

Sufficient condition: there exist $r_i \in \mathbb{R}[x]$ s.t.

$$-\sum_i r_i \, p_i > 0 \quad \text{and} \quad \forall i, r_i \geq 0$$

- equivalence under hypotheses (Putinar's Positivstellensatz)
- no practical bound on degrees of $r_i \Rightarrow$ will be arbitrarily fixed