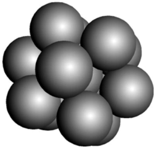
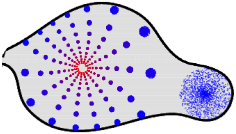
Certified Optimization for System Verification

Victor Magron, CNRS

17 Mai 2018

68nqrt Seminar, Irisa, INRIA Rennes





Research Field

Certified optimization

Input: linear problem  (LP), geometric, semidefinite  (SDP)

Output: value + numerical/symbolic/formal **certificate**

Research Field

CERTIFIED OPTIMIZATION

Input: linear problem  (LP), geometric, semidefinite  (SDP)

Output: value + numerical/symbolic/formal **certificate**

VERIFICATION OF CRITICAL SYSTEMS

Safety of embedded software/hardware

Mathematical formal proofs

CPS, robotics, analysers, . . .

Research Field

CERTIFIED OPTIMIZATION

Input: linear problem  (LP), geometric, semidefinite  (SDP)

Output: value + numerical/symbolic/formal **certificate**

VERIFICATION OF CRITICAL SYSTEMS

Safety of embedded software/hardware

Mathematical formal proofs

CPS, robotics, analysers, . . .

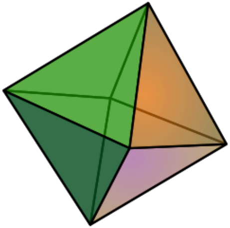
Efficient certification for nonlinear systems

- Certified optimization of polynomial systems
  analysis / synthesis / control
- Efficiency
  symmetry reduction, sparsity
- Certified approximation algorithms
  convergence, error analysis

What is Semidefinite Optimization?

- Linear Programming (LP):

$$\begin{aligned} \min_{\mathbf{z}} \quad & \mathbf{c}^\top \mathbf{z} \\ \text{s.t.} \quad & \mathbf{A}\,\mathbf{z} \geqslant \mathbf{d} \,. \end{aligned}$$



Polyhedron

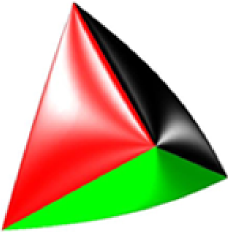
  - Linear cost $\mathbf{c}$
  - Linear inequalities "$\sum_i A_{ij}\, z_j \geqslant d_i$"

What is Semidefinite Optimization?

- Semidefinite Programming (SDP):

$$\min_{\mathbf{z}} \quad \mathbf{c}^\top \mathbf{z}$$
$$\text{s.t.} \quad \sum_i \mathbf{F}_i z_i \succcurlyeq \mathbf{F}_0 \; .$$

  - Linear cost $\mathbf{c}$
  - Symmetric matrices $\mathbf{F}_0, \mathbf{F}_i$
  - Linear matrix inequalities "$\mathbf{F} \succcurlyeq 0$" ($\mathbf{F}$ has nonnegative eigenvalues)

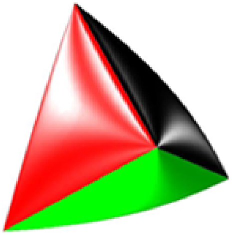


Spectrahedron

What is Semidefinite Optimization?

- Semidefinite Programming (SDP):

$$\min_{\mathbf{z}} \quad \mathbf{c}^\top \mathbf{z}$$
$$\text{s.t.} \quad \sum_i \mathbf{F}_i z_i \succcurlyeq \mathbf{F}_0 \ , \quad \mathbf{A}\,\mathbf{z} = \mathbf{d} \ .$$



Spectrahedron

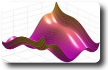
- Linear cost $\mathbf{c}$
- Symmetric matrices $\mathbf{F}_0, \mathbf{F}_i$
- Linear matrix inequalities "$\mathbf{F} \succcurlyeq 0$" ($\mathbf{F}$ has nonnegative eigenvalues)

Applications of SDP

- Combinatorial optimization
- Control theory
- Matrix completion
- Unique Games Conjecture (Khot '02) :
  "A *single concrete algorithm* provides **optimal guarantees** among all efficient algorithms for a large class of computational problems."
  (Barak and Steurer survey at ICM'14)
- Solving polynomial optimization (Lasserre '01)

SDP for Polynomial Optimization

Theoretical approach for polynomial optimization

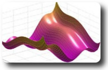
(Primal)		(Dual)
$\inf \int f \, d\mu$		$\sup \lambda$
avec μ probabilité $\Rightarrow$	LP INFINI	$\Leftarrow$ avec $f - \lambda \geqslant 0$

SDP for Polynomial Optimization

Practical approach for polynomial optimization

(Primal **Relaxation**)

moments $\int \mathbf{x}^\alpha \, d\mu$



(Dual **Strengthening**)

$f - \lambda =$ **sums of squares**

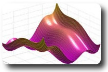
finite $\Rightarrow$ **SDP** $\Leftarrow$ **fixed** degree

SDP for Polynomial Optimization

Practical approach for polynomial optimization

(Primal **Relaxation**)

moments $\int \mathbf{x}^\alpha \, d\mu$



(Dual **Strengthening**)

$f - \lambda =$ **sums of squares**

finite $\Rightarrow$ **SDP** $\Leftarrow$ **fixed** degree

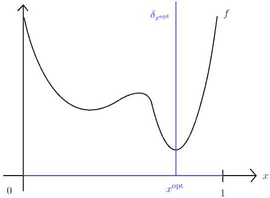
Hierarchy of **SDP** $\uparrow f^*$

degree $2k$
n vars $\Longrightarrow \binom{n+2k}{n}$ **SDP** VARIABLES

Lasserre's hierarchy

Cast polynomial optimization as *infinite-dimensional* LP over measures [Lasserre 01]

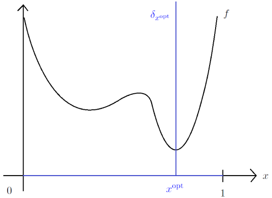
$$f^\star := \inf_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x}) = \inf_{\mu \in \mathcal{M}_+(\mathbf{K})} \int_{\mathbf{K}} f(\mathbf{x}) d\mu$$



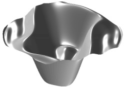
Lasserre's hierarchy

💡**Cast polynomial optimization** as *infinite-dimensional* LP over measures [Lasserre 01]

$$f^\star := \inf_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x}) = \inf_{\mu \in \mathcal{M}_+(\mathbf{K})} \int_{\mathbf{K}} f(\mathbf{x}) d\mu$$

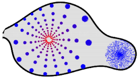


⇝ **Regions of attraction** [Henrion-Korda 14]



⇝ **Maximum invariants** [Korda et al 13]

⇝ **Reachable sets** [Magron et al 17]



SDP for Polynomial Optimization

- Prove **polynomial inequalities** with SDP:

$$f(a, b) := a^2 - 2ab + b^2 \geqslant 0 \ .$$

- Find $\mathbf{z}$ s.t. $f(a,b) = \begin{pmatrix} a & b \end{pmatrix} \underbrace{\begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix}}_{\succcurlyeq 0} \begin{pmatrix} a \\ b \end{pmatrix}$.

- Find $\mathbf{z}$ s.t. $a^2 - 2ab + b^2 = z_1 a^2 + 2 z_2 ab + z_3 b^2 \qquad (\mathbf{A}\,\mathbf{z} = \mathbf{d})$

- $\begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{\mathbf{F}_1} z_1 + \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\mathbf{F}_2} z_2 + \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{\mathbf{F}_3} z_3 \succcurlyeq \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}}_{\mathbf{F}_0}$

SDP for Polynomial Optimization

- Choose a cost $\mathbf{c}$ e.g. $(1, 0, 1)$ and solve:

$$\min_{\mathbf{z}} \quad \mathbf{c}^\top \mathbf{z}$$
$$\text{s.t.} \quad \sum_i \mathbf{F}_i z_i \succcurlyeq \mathbf{F}_0 \ , \quad \mathbf{A}\,\mathbf{z} = \mathbf{d} \ .$$

- Solution $\begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \succcurlyeq 0$ (eigenvalues 0 and 2)

- $a^2 - 2ab + b^2 = \begin{pmatrix} a & b \end{pmatrix} \underbrace{\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}}_{\succcurlyeq 0} \begin{pmatrix} a \\ b \end{pmatrix} = (a - b)^2 \, .$

- Solving **SDP** $\Longrightarrow$ Finding **Sums of Squares** certificates

SDP for Polynomial Optimization

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

SDP for Polynomial Optimization

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

- $:= [0,1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geqslant 0, \quad x_2(1 - x_2) \geqslant 0\}$

SDP for Polynomial Optimization

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

- $:= [0,1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geqslant 0, \quad x_2(1 - x_2) \geqslant 0\}$

$$\overbrace{x_1 x_2}^{f} + \frac{1}{8} = \overbrace{\frac{1}{2}\left(x_1 + x_2 - \frac{1}{2}\right)^2}^{\sigma_0} + \overbrace{\frac{1}{2}}^{\sigma_1} \overbrace{x_1(1 - x_1)}^{g_1} + \overbrace{\frac{1}{2}}^{\sigma_2} \overbrace{x_2(1 - x_2)}^{g_2}$$

SDP for Polynomial Optimization

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \dots, g_m(\mathbf{x}) \geqslant 0\}$

- $:= [0,1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geqslant 0, \quad x_2(1 - x_2) \geqslant 0\}$

$$\overbrace{x_1 x_2}^{f} + \frac{1}{8} = \overbrace{\frac{1}{2}\left(x_1 + x_2 - \frac{1}{2}\right)^2}^{\sigma_0} + \overbrace{\frac{1}{2}}^{\sigma_1} \overbrace{x_1(1 - x_1)}^{g_1} + \overbrace{\frac{1}{2}}^{\sigma_2} \overbrace{x_2(1 - x_2)}^{g_2}$$

- Sums of squares (SOS) σ_i

SDP for Polynomial Optimization

NP hard General Problem: $f^* := \min_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$

- Semialgebraic set $\mathbf{K} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$

- $:= [0,1]^2 = \{\mathbf{x} \in \mathbb{R}^2 : x_1(1 - x_1) \geqslant 0, \quad x_2(1 - x_2) \geqslant 0\}$

$$\overbrace{x_1 x_2}^{f} + \frac{1}{8} = \overbrace{\frac{1}{2}\left(x_1 + x_2 - \frac{1}{2}\right)^2}^{\sigma_0} + \overbrace{\frac{1}{2}}^{\sigma_1} \overbrace{x_1(1 - x_1)}^{g_1} + \overbrace{\frac{1}{2}}^{\sigma_2} \overbrace{x_2(1 - x_2)}^{g_2}$$

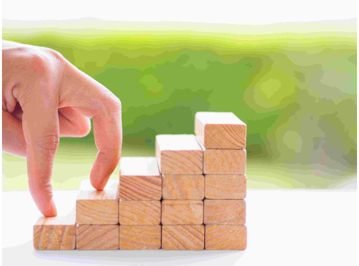
- Sums of squares (SOS) σ_i

- Bounded degree:

  $\mathcal{Q}_k(\mathbf{K}) := \left\{ \sigma_0 + \sum_{j=1}^m \sigma_j g_j, \text{ with } \deg \sigma_j \, g_j \leqslant 2k \right\}$

SDP for Polynomial Optimization

- **Hierarchy of SDP relaxations**:
  $\lambda_k := \sup_{\lambda} \Big\{ \lambda : f - \lambda \in \mathcal{Q}_k(\mathbf{K}) \Big\}$

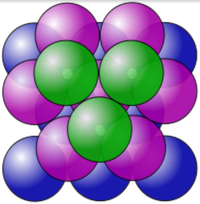


- Convergence guarantees $\lambda_k \uparrow f^*$ [Lasserre 01]
- Can be computed with SDP solvers (CSDP, SDPA)
- **"No Free Lunch" Rule**: $\binom{n+2k}{n}$ SDP variables

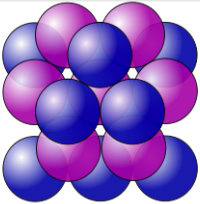
From Oranges Stack...

Kepler Conjecture (1611):

The maximal density of sphere packings in 3D-space is $\frac{\pi}{\sqrt{18}}$



Face-centered cubic Packing



Hexagonal Compact Packing

...to Flyspeck Nonlinear Inequalities

- The proof of T. Hales (1998) contains mathematical and computational parts

- Computation: check thousands of nonlinear inequalities

- **Flyspeck** [Hales 06]: **F**ormal **P**roof of **K**epler Conjecture

...to Flyspeck Nonlinear Inequalities

- The proof of T. Hales (1998) contains mathematical and computational parts
- Computation: check thousands of nonlinear inequalities
- **Flyspeck** [Hales 06]: **F**ormal **P**roof of **K**epler Conjecture
- **Project Completion on August 2014 by the Flyspeck team**

A "Simple" Example

In the computational part:

- Multivariate Polynomials:
  $\Delta\mathbf{x} := x_1x_4(-x_1 + x_2 + x_3 - x_4 + x_5 + x_6) + x_2x_5(x_1 - x_2 + x_3 + x_4 - x_5 + x_6) + x_3x_6(x_1 + x_2 - x_3 + x_4 + x_5 - x_6) - x_2(x_3x_4 + x_1x_6) - x_5(x_1x_3 + x_4x_6)$

A "Simple" Example

In the computational part:

- Semialgebraic functions: composition of polynomials with $|\cdot|, \sqrt{}, +, -, \times, /, \sup, \inf, \ldots$

$$p(\mathbf{x}) := \partial_4 \Delta \mathbf{x} \qquad q(\mathbf{x}) := 4x_1 \Delta \mathbf{x}$$
$$r(\mathbf{x}) := p(\mathbf{x}) / \sqrt{q(\mathbf{x})}$$

$$l(\mathbf{x}) := -\frac{\pi}{2} + 1.6294 - 0.2213\,(\sqrt{x_2} + \sqrt{x_3} + \sqrt{x_5} + \sqrt{x_6} - 8.0) + 0.913\,(\sqrt{x_4} - 2.52) + 0.728\,(\sqrt{x_1} - 2.0)$$

A “Simple” Example

In the computational part:

- Transcendental functions $\mathcal{T}$: composition of semialgebraic functions with arctan, exp, sin, $+, -, \times, \dots$

A "Simple" Example

In the computational part:

- Feasible set $\mathbf{K} := [4, 6.3504]^3 \times [6.3504, 8] \times [4, 6.3504]^2$

Lemma$_{9922699028}$ from Flyspeck:

$$\forall \mathbf{x} \in \mathbf{K}, \arctan\left(\frac{p(\mathbf{x})}{\sqrt{q(\mathbf{x})}}\right) + l(\mathbf{x}) \geqslant 0$$

Existing Formal Frameworks

Formal proofs for Global Optimization:

- Bernstein polynomial methods [Zumkeller's PhD 08]
- SMT methods [Gao et al. 12]
- Interval analysis and Sums of squares

Existing Formal Frameworks

Interval analysis

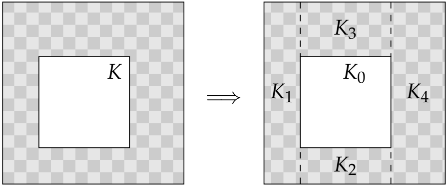
- Certified interval arithmetic in Coq [Melquiond 12]
- Taylor methods in HOL Light [Solovyev thesis 13]
  - Formal verification of floating-point operations
- robust but subject to the **Curse of Dimensionality**

Existing Formal Frameworks

Lemma$_{9922699028}$ from Flyspeck:

$$\forall \mathbf{x} \in \mathbf{K}, \arctan\left(\frac{\partial_4 \Delta \mathbf{x}}{\sqrt{4 x_1 \Delta \mathbf{x}}}\right) + l(\mathbf{x}) \geqslant 0$$

- Dependency issue using Interval Calculus:
  - One can bound $\partial_4 \Delta \mathbf{x} / \sqrt{4 x_1 \Delta \mathbf{x}}$ and $l(\mathbf{x})$ separately
  - Too coarse lower bound: -0.87
  - Subdivide $\mathbf{K}$ to prove the inequality



Existing Formal Frameworks

Sums of squares (SOS) techniques

- Formalized in HOL-LIGHT [Harrison 07] COQ [Besson 07]
- Precise methods but scalability and robustness issues (numerical)
- powerful: global optimality certificates without branching

but

- not so robust: handles moderate size problems
- Restricted to polynomials

Existing Formal Frameworks

- *Caprasse* Problem:

  $\forall \mathbf{x} \in [-0.5, 0.5]^4, -x_1 x_3^3 + 4 x_2 x_3^2 x_4 + 4 x_1 x_3 x_4^2 + 2 x_2 x_4^3 + 4 x_1 x_3 + 4 x_3^2 - 10 x_2 x_4 - 10 x_4^2 + 5.1801 \geqslant 0.$

- Decompose the polynomial as SOS of degree at most 4

- Gives a nonnegative bound!

Existing Formal Frameworks

Approximation theory: Chebyshev/Taylor models

- mandatory for non-polynomial problems
- hard to combine with SOS techniques (degree of approximation)

Existing Formal Frameworks

Can we develop a new approach with both keeping the respective strength of interval and precision of SOS?

Proving Flyspeck Inequalities is challenging: medium-size and tight

Contribution: Publications and Software

- M., Allamigeon, Gaubert, Werner.
  Formal Proofs for Nonlinear Optimization,
  Journal of Formalized Reasoning 8(1):1–24, 2015.

- Hales, Adams, Bauer, Dang, Harrison, Hoang, Kaliszyk, M., Mclaughlin, Nguyen, Nguyen, Nipkow, Obua, Pleso, Rute, Solovyev, Ta, Tran, Trieu, Urban, Vu & Zumkeller, *Forum of Mathematics, Pi*, 5 2017

Software Implementation `NLCertify`**:**

- 15 000 lines of OCAML code

- 4000 lines of COQ code

- M. NLCertify: A Tool for Formal Nonlinear Optimization, *ICMS*, 2014.

General informal Framework

Given $\mathbf{K}$ a compact set and f a transcendental function, bound $f^* = \inf_{\mathbf{x} \in \mathbf{K}} f(\mathbf{x})$ and prove $f^* \geqslant 0$

- f is under-approximated by a semialgebraic function f_{sa}
- Reduce the problem $f_{\text{sa}}^* := \inf_{\mathbf{x} \in \mathbf{K}} f_{\text{sa}}(\mathbf{x})$ to a polynomial optimization problem (POP)

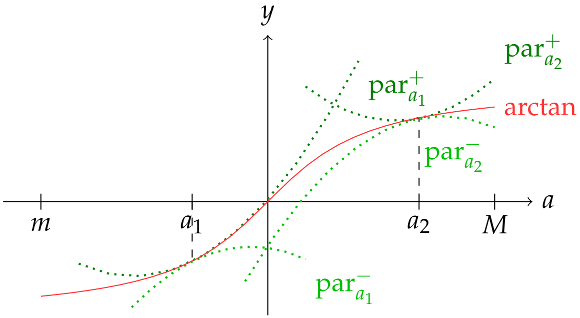
Maxplus Approximation

- Initially introduced to solve Optimal Control Problems [Fleming-McEneaney 00]
- **Curse of dimensionality** reduction [McEaneney Kluberg, Gaubert-McEneaney-Qu 11, Qu 13].
  Allowed to solve instances of dim up to 15 (inaccessible by grid methods)
- In our context: approximate transcendental functions

Maxplus Approximation

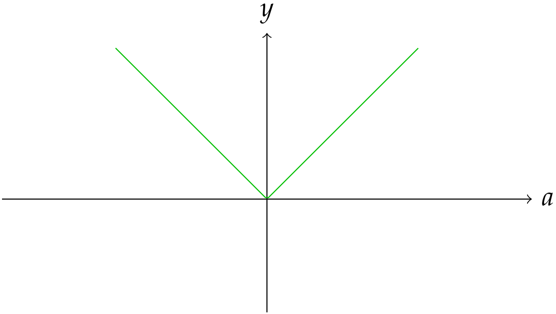
Definition

Let $\gamma \geqslant 0$. A function $\phi : \mathbb{R}^n \to \mathbb{R}$ is said to be γ-*semiconvex* if the function $\mathbf{x} \mapsto \phi(\mathbf{x}) + \frac{\gamma}{2} \|\mathbf{x}\|_2^2$ is convex.



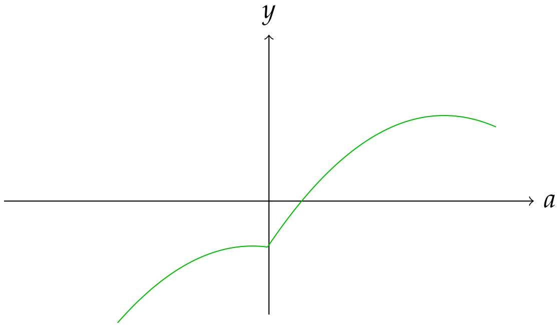
Nonlinear Function Representation

Exact parsimonious maxplus representations



Nonlinear Function Representation

Exact parsimonious maxplus representations



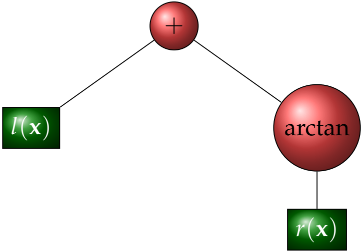
Nonlinear Function Representation

Abstract syntax tree representations of multivariate transcendental functions:

- leaves are semialgebraic functions of $\mathcal{A}$
- nodes are univariate functions of $\mathcal{D}$ or binary operations

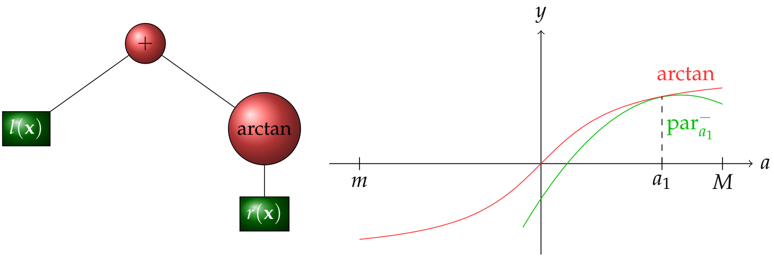
Nonlinear Function Representation

- For the “Simple” Example from Flyspeck:



Maxplus Optimization Algorithm

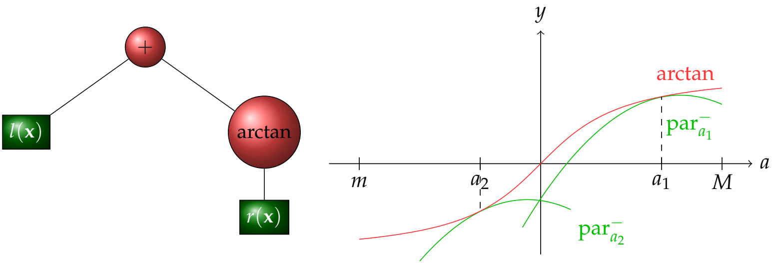
First iteration:



1 control point $\{a_1\}$: $m_1 = -4.7 \times 10^{-3} < 0$

Maxplus Optimization Algorithm

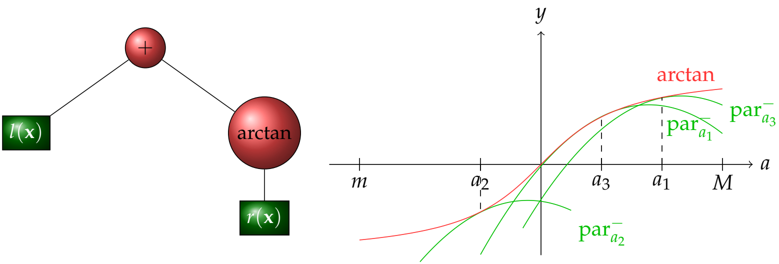
Second iteration:



2 control points $\{a_1, a_2\}$: $m_2 = -6.1 \times 10^{-5} < 0$

Maxplus Optimization Algorithm

Third iteration:



3 control points $\{a_1, a_2, a_3\}$: $m_3 = 4.1 \times 10^{-6} > 0$

OK!

SDP for Nonlinear Optimization

SDP for Characterizing Values/Curves/Sets

- Semialgebraic Maxplus Optimization
- Roundoff Error Bounds
- Pareto Curves
- Polynomial Images of Semialgebraic Sets
- Reachable Sets of Polynomial Systems
- Invariant Measures of Polynomial Systems

Exact Polynomial Optimization

Conclusion

Roundoff Error Bounds

- Exact:

$$f(\mathbf{x}) := x_1 x_2 + x_3 x_4$$

- Floating-point:

$$\hat{f}(\mathbf{x}, \mathbf{e}) := [x_1 x_2 (1 + e_1) + x_3 x_4 (1 + e_2)](1 + e_3)$$

- $\mathbf{x} \in \mathbf{X}$, $\quad | e_i | \leqslant 2^{-p} \quad p = 24$ (single) or 53 (double)

Roundoff Error Bounds

Input: exact $f(\mathbf{x})$, floating-point $\hat{f}(\mathbf{x}, \mathbf{e})$
Output: Bounds for $f - \hat{f}$

1: Error $r(\mathbf{x}, \mathbf{e}) := f(\mathbf{x}) - \hat{f}(\mathbf{x}, \mathbf{e}) = \sum_{\boldsymbol{\alpha}} r_{\boldsymbol{\alpha}}(\mathbf{e})\mathbf{x}^{\boldsymbol{\alpha}}$

2: Decompose $r(\mathbf{x}, \mathbf{e}) = l(\mathbf{x}, \mathbf{e}) + h(\mathbf{x}, \mathbf{e})$, l **linear** in $\mathbf{e}$

3: Bound $h(\mathbf{x}, \mathbf{e})$ with interval arithmetic

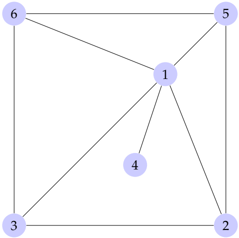
4: Bound $l(\mathbf{x}, \mathbf{e})$ with **SPARSE SUMS OF SQUARES**

Roundoff Error Bounds

Sparse SDP Optimization [Waki, Lasserre 06]

- Correlative sparsity pattern (csp) of vars

$$x_2x_5 + x_3x_6 - x_2x_3 - x_5x_6 + x_1(-x_1 + x_2 + x_3 - x_4 + x_5 + x_6)$$

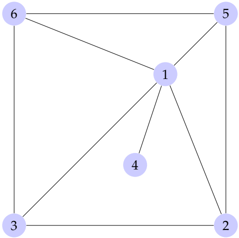


Roundoff Error Bounds

Sparse SDP Optimization [Waki, Lasserre 06]

- Correlative sparsity pattern (csp) of vars

$x_2 x_5 + x_3 x_6 - x_2 x_3 - x_5 x_6 + x_1(-x_1 + x_2 + x_3 - x_4 + x_5 + x_6)$



1. Maximal cliques $C_1, \ldots, C_l$
2. Average size $\kappa \rightsquigarrow \binom{\kappa+2k}{\kappa}$ vars

$C_1 := \{1, 4\}$

$C_2 := \{1, 2, 3, 5\}$

$C_3 := \{1, 3, 5, 6\}$

Dense SDP: 210 vars

Sparse SDP: 115 vars

Contributions

$l(\mathbf{x}, \mathbf{e}) = \sum_{i=1}^{m} s_i(\mathbf{x}) e_i$

Maximal cliques correspond to $\{\mathbf{x}, e_1\}, \dots, \{\mathbf{x}, e_m\}$

M., Constantinides, Donaldson. Certified Roundoff Error Bounds Using Semidefinite Programming, *Trans. Math. Soft.*, 2016

SDP for Nonlinear Optimization

SDP for Characterizing Values/Curves/Sets

- Semialgebraic Maxplus Optimization
- Roundoff Error Bounds
- Pareto Curves
- Polynomial Images of Semialgebraic Sets
- Reachable Sets of Polynomial Systems
- Invariant Measures of Polynomial Systems

Exact Polynomial Optimization

Conclusion

Bicriteria Optimization Problems

- Let $f_1, f_2 \in \mathbb{R}[\mathbf{x}]$ two conflicting criteria
- Let $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$ a semialgebraic set

$$(\mathbf{P}) \left\{ \min_{\mathbf{x} \in \mathbf{S}} (f_1(\mathbf{x})\, f_2(\mathbf{x}))^\top \right\}$$

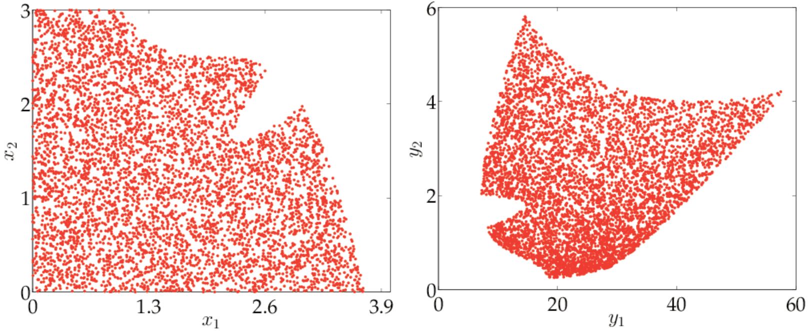
Assumption

The image space $\mathbb{R}^2$ is partially ordered in a natural way ($\mathbb{R}^2_+$ is the ordering cone).

Bicriteria Optimization Problems

$$g_1 := -(x_1 - 2)^3/2 - x_2 + 2.5 \ ,$$
$$g_2 := -x_1 - x_2 + 8(-x_1 + x_2 + 0.65)^2 + 3.85 \ ,$$
$$\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : g_1(\mathbf{x}) \geqslant 0, g_2(\mathbf{x}) \geqslant 0\} \ .$$

$$f_1 := (x_1 + x_2 - 7.5)^2/4 + (-x_1 + x_2 + 3)^2 \ ,$$
$$f_2 := (x_1 - 1)^2/4 + (x_2 - 4)^2/4 \ .$$



Parametric Sublevel Set Approximations

- Inspired by previous research on multiobjective linear optimization [Gorissen-den Hertog 12]
- Workaround: reduce **P** to a **parametric POP**

$$(\mathbf{P}_\lambda): \quad f^*(\lambda) := \min_{\mathbf{x} \in \mathbf{S}} \{ f_2(\mathbf{x}) : f_1(\mathbf{x}) \leqslant \lambda \} \;,$$

- variable $(\mathbf{x}, \lambda) \in \mathbf{K} = \mathbf{S} \times [0, 1]$

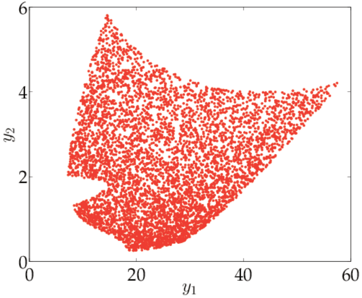
A Hierarchy of Polynomial Approximations

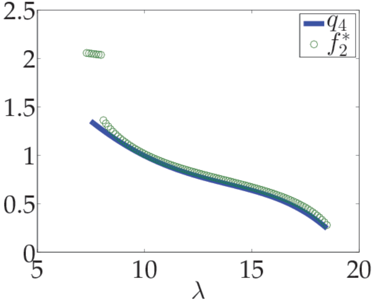
Moment-SOS approach [Lasserre 10]:

$$(D_k) \left\{ \begin{array}{ll} \max\limits_{q \in \mathbb{R}_{2k}[\lambda]} & \sum\limits_{i=0}^{2k} q_i / (1+i) \\ \text{s.t.} & f_2(\mathbf{x}) - q(\lambda) \in \mathcal{Q}_{2k}(\mathbf{K}) \end{array} \right. .$$

- The hierarchy (D_k) provides a sequence (q_k) of **polynomial under-approximations** of $f^*(\lambda)$.
- $\lim_{d \to \infty} \int_0^1 (f^*(\lambda) - q_k(\lambda)) d\lambda = 0$

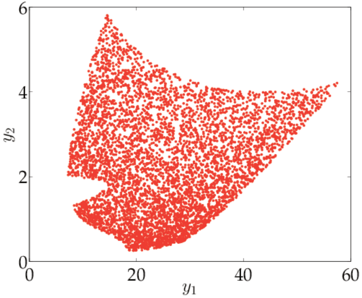
A Hierarchy of Polynomial Approximations

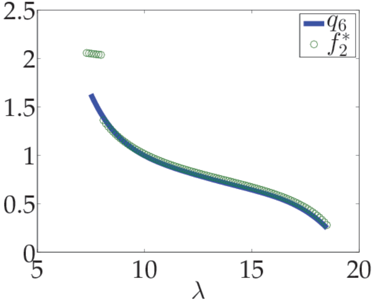




Degree 4

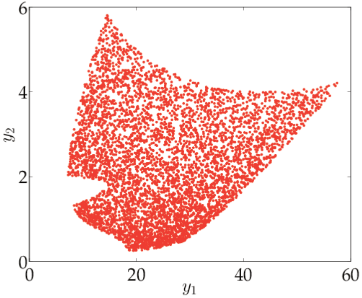
A Hierarchy of Polynomial Approximations

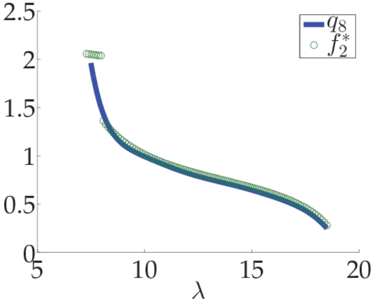




Degree 6

A Hierarchy of Polynomial Approximations





Degree 8

Contributions

- Numerical schemes that **avoid computing finitely many points**.

- Pareto curve approximation with polynomials, **convergence guarantees** in L_1-norm

M., Henrion, Lasserre. Approximating Pareto Curves using Semidefinite Relaxations. *Operations Research Letters*, 2014.

Polynomial Images of Semialgebraic Sets

- Semialgebraic set $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \dots, g_l(\mathbf{x}) \geqslant 0\}$
- A polynomial map $f : \mathbb{R}^n \to \mathbb{R}^m$,
  $\mathbf{x} \mapsto f(\mathbf{x}) := (f_1(\mathbf{x}), \dots, f_m(\mathbf{x}))$
- $\deg f = d := \max\{\deg f_1, \dots, \deg f_m\}$
- $\mathbf{F} := f(\mathbf{S}) \subseteq \mathbf{B}$, with $\mathbf{B} \subset \mathbb{R}^m$ a box or a ball
- Tractable approximations of $\mathbf{F}$?

Polynomial Images of Semialgebraic Sets

- Includes important special cases:

1. $m = 1$: **polynomial optimization**

$$\mathbf{F} \subseteq [\inf_{\mathbf{x} \in \mathbf{S}} f(\mathbf{x}), \sup_{\mathbf{x} \in \mathbf{S}} f(\mathbf{x})]$$

2. Approximate **projections** of $\mathbf{S}$ when $f(\mathbf{x}) := (x_1, \ldots, x_m)$

3. **Pareto curve** approximations

   For f_1,f_2 two conflicting criteria: $(\mathbf{P}) \left\{ \min_{\mathbf{x} \in \mathbf{S}} (f_1(\mathbf{x})\, f_2(\mathbf{x}))^\top \right\}$

Support of Image Measures

- **Pushforward** $f_{\#} : \mathcal{M}(\mathbf{S}) \to \mathcal{M}(\mathbf{B})$:

$$f_{\#}\mu_0(\mathbf{A}) := \mu_0(\{\mathbf{x} \in \mathbf{S} : f(\mathbf{x}) \in \mathbf{A}\}), \quad \forall \mathbf{A} \in \mathcal{B}(\mathbf{B}), \forall \mu_0 \in \mathcal{M}(\mathbf{S})$$

- $f_{\#}\mu_0$ is the **image measure** of μ_0 under f

Support of Image Measures

$$
\begin{aligned}
p^* := \sup_{\mu_0,\mu_1,\hat{\mu}_1} \quad & \int_{\mathbf{B}} \mu_1 \\
\text{s.t.} \quad & \mu_1 + \hat{\mu}_1 = \lambda_{\mathbf{B}} \,, \\
& \mu_1 = f_{\#}\mu_0 \,, \\
& \mu_0 \in \mathcal{M}_+(\mathbf{S}), \quad \mu_1, \hat{\mu}_1 \in \mathcal{M}_+(\mathbf{B}) \,.
\end{aligned}
$$

Lebesgue measure on $\mathbf{B}$ is $\lambda_{\mathbf{B}}(d\mathbf{y}) := \mathbf{1}_{\mathbf{B}}(\mathbf{y})\, d\mathbf{y}$

Support of Image Measures

$$
\begin{aligned}
p^* := \sup_{\mu_0,\mu_1,\hat{\mu}_1} \quad & \int_{\mathbf{B}} \mu_1 \\
\text{s.t.} \quad & \mu_1 + \hat{\mu}_1 = \lambda_{\mathbf{B}} \,, \\
& \mu_1 = f_{\#}\mu_0 \,, \\
& \mu_0 \in \mathcal{M}_+(\mathbf{S}), \quad \mu_1, \hat{\mu}_1 \in \mathcal{M}_+(\mathbf{B}) \,.
\end{aligned}
$$

Lemma

Let μ_1^* be an optimal solution of the above LP.
Then $\mu_1^* = \lambda_{\mathbf{F}}$ and $p^* = \operatorname{vol} \mathbf{F}$.

Method 2: Primal-dual LP Formulation

Primal LP

$$
\begin{aligned}
p^* := \sup_{\mu_0, \mu_1, \hat{\mu}_1} \quad & \int \mu_1 \\
\text{s.t.} \quad & \mu_1 + \hat{\mu}_1 = \lambda_{\mathbf{B}}\,, \\
& \mu_1 = f_{\#}\mu_0\,, \\
& \mu_0 \in \mathcal{M}_+(\mathbf{S})\,, \\
& \mu_1, \hat{\mu}_1 \in \mathcal{M}_+(\mathbf{B})\,.
\end{aligned}
$$

Dual LP

$$
\begin{aligned}
d^* := \inf_{v, w} \quad & \int w(\mathbf{y})\, \lambda_{\mathbf{B}}(d\mathbf{y}) \\
\text{s.t.} \quad & v(f(\mathbf{x})) \geqslant 0, \quad \forall \mathbf{x} \in \mathbf{S}\,, \\
& w(\mathbf{y}) \geqslant 1 + v(\mathbf{y}), \quad \forall \mathbf{y} \in \mathbf{B}\,, \\
& w(\mathbf{y}) \geqslant 0, \quad \forall \mathbf{y} \in \mathbf{B}\,, \\
& v, w \in \mathcal{C}(\mathbf{B})\,.
\end{aligned}
$$

Method 2: Strong Convergence Property

Strengthening of the dual LP:

$$
\begin{aligned}
d_k^* := \inf_{v,w} \quad & \sum_{\beta \in \mathbb{N}^m_{2k}} w_\beta z_\beta^{\mathbf{B}} \\
\text{s.t.} \quad & v \circ f \in \mathcal{Q}_{kd}(\mathbf{S}), \\
& w - 1 - v \in \mathcal{Q}_k(\mathbf{B}), \\
& w \in \mathcal{Q}_k(\mathbf{B}), \\
& v, w \in \mathbb{R}_{2k}[\mathbf{y}].
\end{aligned}
$$

Method 2: Strong Convergence Property

Theorem

Assuming that $\mathring{\mathbf{F}} \neq \emptyset$ and $\mathcal{Q}_k(\mathbf{S})$ is Archimedean,

1. The sequence (w_k) converges to $\mathbf{1}_{\mathbf{F}}$ w.r.t the $L_1(\mathbf{B})$-norm:

$$\lim_{k \to \infty} \int_{\mathbf{B}} |w_k - \mathbf{1}_{\mathbf{F}}| d\mathbf{y} = 0 \ .$$

Method 2: Strong Convergence Property

Theorem

Assuming that $\mathring{\mathbf{F}} \neq \emptyset$ and $\mathcal{Q}_k(\mathbf{S})$ is Archimedean,

1. The sequence (w_k) converges to $\mathbf{1}_{\mathbf{F}}$ w.r.t the $L_1(\mathbf{B})$-norm:

$$\lim_{k \to \infty} \int_{\mathbf{B}} |w_k - \mathbf{1}_{\mathbf{F}}| d\mathbf{y} = 0 \ .$$

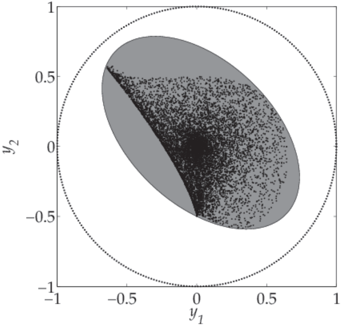
2. Let $\mathbf{F}_k := \{\mathbf{y} \in \mathbf{B} : w_k(\mathbf{y}) \geqslant 1\}$. Then,

$$\lim_{k \to \infty} \mathrm{vol}(\mathbf{F}_k \backslash \mathbf{F}) = 0 \ .$$

Polynomial Image of the Unit Ball

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (x_1 + x_1 x_2, x_2 - x_1^3)/2$$

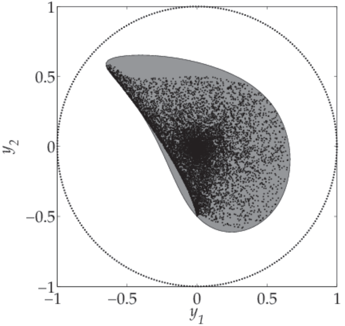


$\mathbf{F}_1$

Polynomial Image of the Unit Ball

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (x_1 + x_1 x_2, x_2 - x_1^3)/2$$

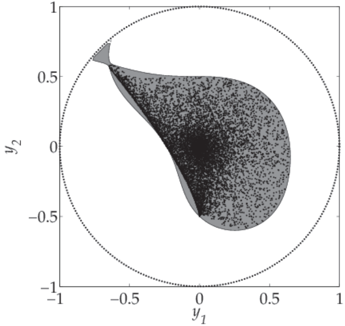


$\mathbf{F}_2$

Polynomial Image of the Unit Ball

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (x_1 + x_1 x_2, x_2 - x_1^3)/2$$

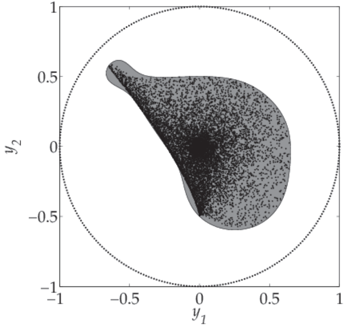


$\mathbf{F}_3$

Polynomial Image of the Unit Ball

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (x_1 + x_1 x_2, x_2 - x_1^3)/2$$

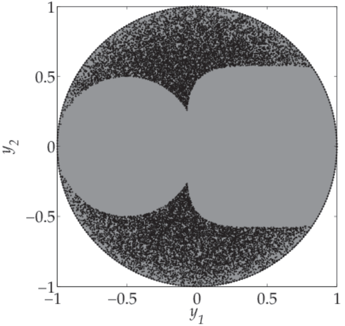


$\mathbf{F}_4$

Semialgebraic Set Projections

$f(\mathbf{x}) = (x_1, x_2)$: projection on $\mathbb{R}^2$ of the semialgebraic set

$$\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^3 : \|\mathbf{x}\|_2^2 \leqslant 1, 1/4 - (x_1 + 1/2)^2 - x_2^2 \geqslant 0, \\ 1/9 - (x_1 - 1/2)^4 - x_2^4 \geqslant 0\}$$

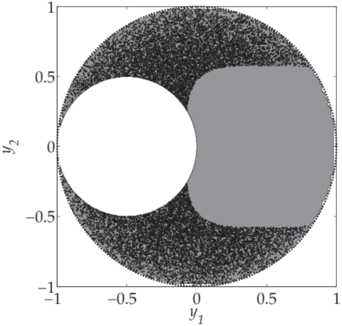


$\mathbf{F}_2$

Semialgebraic Set Projections

$f(\mathbf{x}) = (x_1, x_2)$: projection on $\mathbb{R}^2$ of the semialgebraic set

$$\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^3 : \|\mathbf{x}\|_2^2 \leqslant 1, 1/4 - (x_1 + 1/2)^2 - x_2^2 \geqslant 0, \\ 1/9 - (x_1 - 1/2)^4 - x_2^4 \geqslant 0\}$$

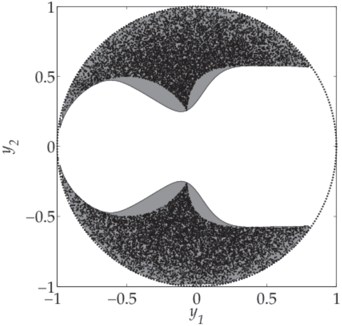


F_3

Semialgebraic Set Projections

$f(\mathbf{x}) = (x_1, x_2)$: projection on $\mathbb{R}^2$ of the semialgebraic set

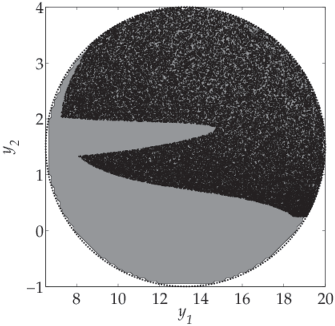
$$\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^3 : \|\mathbf{x}\|_2^2 \leqslant 1, 1/4 - (x_1 + 1/2)^2 - x_2^2 \geqslant 0, \\ 1/9 - (x_1 - 1/2)^4 - x_2^4 \geqslant 0\}$$



$\mathbf{F}_4$

Approximating Pareto Curves

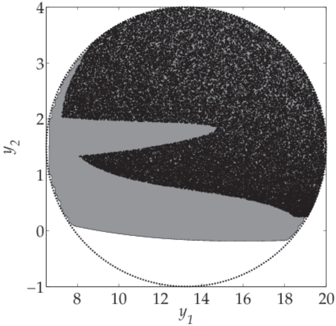
Back on our previous nonconvex example:



$\mathbf{F}_1$

Approximating Pareto Curves

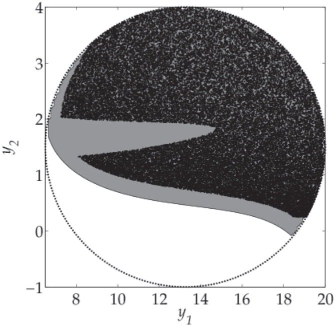
Back on our previous nonconvex example:



F_2

Approximating Pareto Curves

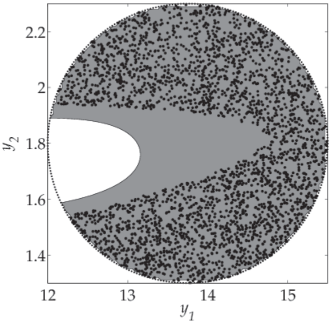
Back on our previous nonconvex example:



$\mathbf{F}_3$

Approximating Pareto Curves

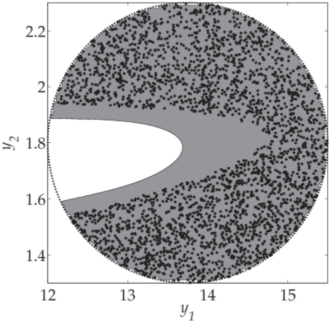
"Zoom" on the region which is hard to approximate:



$\mathbf{F_4}$

Approximating Pareto Curves

"Zoom" on the region which is hard to approximate:

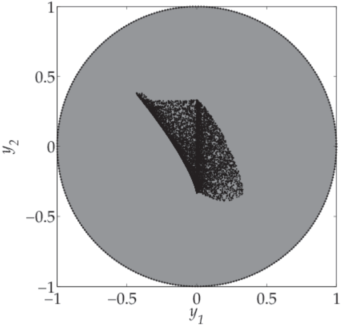


$\mathbf{F}_5$

Semialgebraic Image of Semialgebraic Sets

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (\min(x_1 + x_1 x_2, x_1^2), x_2 - x_1^3)/3$$

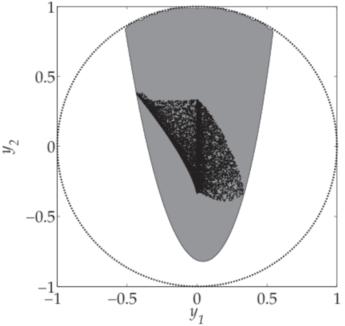


$\mathbf{F}_1$

Semialgebraic Image of Semialgebraic Sets

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (\min(x_1 + x_1 x_2, x_1^2), x_2 - x_1^3)/3$$

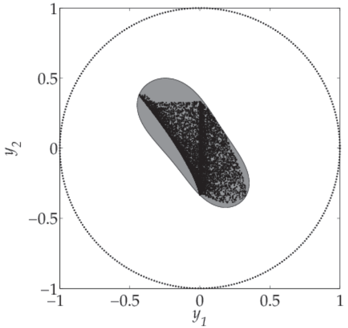


$\mathbf{F}_2$

Semialgebraic Image of Semialgebraic Sets

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (\min(x_1 + x_1 x_2, x_1^2), x_2 - x_1^3)/3$$

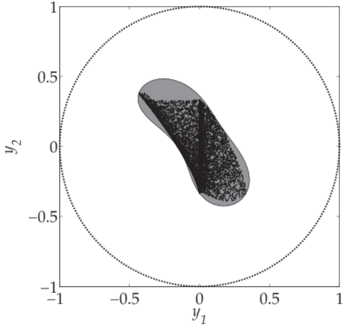


$\mathbf{F}_3$

Semialgebraic Image of Semialgebraic Sets

Image of the unit ball $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_2^2 \leqslant 1\}$ by

$$f(\mathbf{x}) := (\min(x_1 + x_1 x_2, x_1^2), x_2 - x_1^3)/3$$



$\mathbf{F}_4$

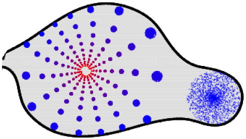
Contributions

M., Henrion, Lasserre. Semidefinite approximations of projections and polynomial images of semialgebraic sets. *SIAM Opt.* , 2015.

Reachable Sets of Polynomial Systems

Iterations $\mathbf{x}_{t+1} = f(\mathbf{x}_t)$
Uncertain $\mathbf{x}_{t+1} = f(\mathbf{x}_t, \mathbf{u})$

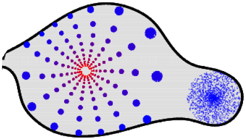
- **Converging** SDP hierarchies
- Image measure
- Liouville equation (conservation)



$$\mu_t + \mu = f_{\#}\,\mu + \mu_0$$

Reachable Sets of Polynomial Systems

Iterations $\mathbf{x}_{t+1} = f(\mathbf{x}_t)$
Uncertain $\mathbf{x}_{t+1} = f(\mathbf{x}_t, \mathbf{u})$



- **Converging** SDP hierarchies
- Image measure
- Liouville equation (conservation)

$$\mu_t + \mu = f_{\#}\, \mu + \mu_0$$

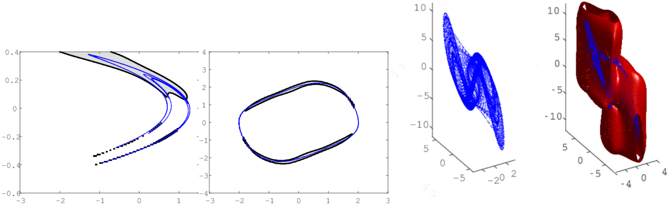
M., Garoche, Henrion, Thirioux. Semidefinite Approximations of Reachable Sets for Discrete-time Polynomial Systems, 2017.

Invariant Measures of Polynomial Systems

Discrete $\mathbf{x}_{t+1} = f(\mathbf{x}_t) \implies f_{\#}\mu - \mu = 0$

Continuous $\dot{\mathbf{x}} = f(\mathbf{x}) \implies \operatorname{div} f\,\mu = 0$

- **Converging** SDP hierarchies
- measures with density in L_p
- singular measures $\implies$ chaotic attractors

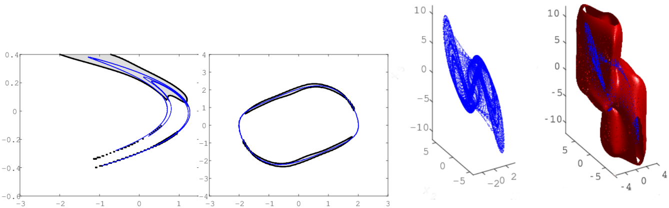


Invariant Measures of Polynomial Systems

Discrete $\mathbf{x}_{t+1} = f(\mathbf{x}_t) \implies f_{\#}\mu - \mu = 0$

Continuous $\dot{\mathbf{x}} = f(\mathbf{x}) \implies \operatorname{div} f \mu = 0$

- **Converging** SDP hierarchies
- measures with density in L_p
- singular measures $\implies$ chaotic attractors



M., Forets, Henrion. Semidefinite Characterization of Invariant Measures for Polynomial Systems. *In Progress*, 2018.

SDP for Nonlinear Optimization

SDP for Characterizing Values/Curves/Sets

Exact Polynomial Optimization

Conclusion

Exact Polynomial Optimization

💡[Lasserre/Parrilo 01] **Numerical** solvers compute σ_i
Semidefinite programming (SDP) $\rightsquigarrow$ **approximate** certificates

$$f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$$

$$f \simeq \sigma = (2X_1^2 + X_1X_2 - \tfrac{8}{3}X_2^2)^2 + (\tfrac{4}{3}X_1X_2 + \tfrac{3}{2}X_2^2)^2 + (\tfrac{2}{7}X_2^2)^2$$

Exact Polynomial Optimization

[Lasserre/Parrilo 01] **Numerical** solvers compute σ_i
Semidefinite programming (SDP) $\rightsquigarrow$ **approximate** certificates

$$f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$$

$$f \simeq \sigma = (2X_1^2 + X_1X_2 - \tfrac{8}{3}X_2^2)^2 + (\tfrac{4}{3}X_1X_2 + \tfrac{3}{2}X_2^2)^2 + (\tfrac{2}{7}X_2^2)^2$$

$$f = \sigma + \tfrac{8}{9}X_1^2X_2^2 - \tfrac{2}{3}X_1X_2^3 + \tfrac{983}{1764}X_2^4$$

Exact Polynomial Optimization

💡[Lasserre/Parrilo 01] **Numerical** solvers compute σ_i
Semidefinite programming (SDP) $\rightsquigarrow$ **approximate** certificates

$$f = 4X_1^4 + 4X_1^3X_2 - 7X_1^2X_2^2 - 2X_1X_2^3 + 10X_2^4$$

$$f \simeq \sigma = (2X_1^2 + X_1X_2 - \tfrac{8}{3}X_2^2)^2 + (\tfrac{4}{3}X_1X_2 + \tfrac{3}{2}X_2^2)^2 + (\tfrac{2}{7}X_2^2)^2$$

$$f = \sigma + \tfrac{8}{9}X_1^2X_2^2 - \tfrac{2}{3}X_1X_2^3 + \tfrac{983}{1764}X_2^4$$

$$\boxed{\simeq \quad \rightarrow \quad =}$$

The Question of Exact Certification

How to go from **approximate** to **exact** certification?

One Answer when $\mathbf{K} = \mathbb{R}^n$

Hybrid SYMBOLIC/NUMERIC methods

[Peyrl-Parrilo 08] [Kaltofen et. al 08]

$$f(X) \simeq \mathbf{v}_D{}^T(X)\, \tilde{\mathbf{Q}}\, \mathbf{v}_D(X)$$

$$0 \preccurlyeq \tilde{\mathbf{Q}} \in \mathbb{R}^{D \times D}$$

$$\mathbf{v}_D(X) = (1, X_1, \dots, X_n, X_1^2, \dots, X_n^D)$$

One Answer when $\mathbf{K} = \mathbb{R}^n$

Hybrid SYMBOLIC/NUMERIC methods

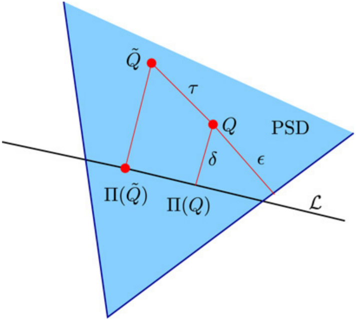
[Peyrl-Parrilo 08] [Kaltofen et. al 08]

$$f(X) \simeq \mathbf{v}_D{}^T(X)\, \tilde{\mathbf{Q}}\, \mathbf{v}_D(X)$$

$$0 \preccurlyeq \tilde{\mathbf{Q}} \in \mathbb{R}^{D \times D}$$

$$\mathbf{v}_D(X) = (1, X_1, \dots, X_n, X_1^2, \dots, X_n^D)$$

$$\boxed{\simeq \quad \rightarrow \quad =}$$



$\tilde{\mathbf{Q}}$ Rounding $\mathbf{Q}$ Projection $\prod(\mathbf{Q})$

$$f(X) = \mathbf{v}_D{}^T(X) \prod(\mathbf{Q})\, \mathbf{v}_D(X)$$

$\prod(\mathbf{Q}) \succcurlyeq 0$ when $\varepsilon \to 0$

One Answer when $\mathbf{K} = \mathbb{R}^n$

Hybrid SYMBOLIC/NUMERIC methods

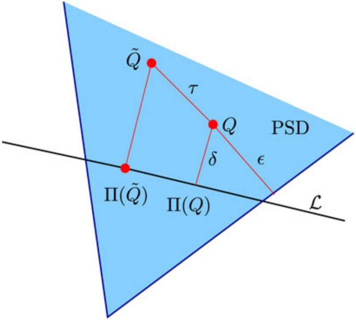
[Peyrl-Parrilo 08] [Kaltofen et. al 08]

$$f(X) \simeq \mathbf{v}_D{}^T(X)\, \tilde{\mathbf{Q}}\, \mathbf{v}_D(X)$$

$$0 \preccurlyeq \tilde{\mathbf{Q}} \in \mathbb{R}^{D \times D}$$

$$\mathbf{v}_D(X) = (1, X_1, \ldots, X_n, X_1^2, \ldots, X_n^D)$$

$$\boxed{\simeq \quad \to \quad =}$$



$\tilde{\mathbf{Q}}$ Rounding $\mathbf{Q}$ Projection $\prod(\mathbf{Q})$

$$f(X) = \mathbf{v}_D{}^T(X) \prod(\mathbf{Q})\, \mathbf{v}_D(X)$$

$\prod(\mathbf{Q}) \succcurlyeq 0$ when $\varepsilon \to 0$

COMPLEXITY?

One Answer when $\mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geqslant 0\}$

Hybrid **Symbolic/Numeric** methods

Magron-Allamigeon-Gaubert-Werner 14

$$f \simeq \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$$

$$u = f - \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$$

One Answer when $\mathbf{K} = \{\mathbf{x} \in \mathbb{R}^n : g_j(\mathbf{x}) \geqslant 0\}$

Hybrid SYMBOLIC/NUMERIC methods

Magron-Allamigeon-Gaubert-Werner 14

$f \simeq \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$

Compact $\mathbf{K} \subseteq [0,1]^n$

$u = f - \tilde{\sigma}_0 + \tilde{\sigma}_1 g_1 + \cdots + \tilde{\sigma}_m g_m$

$\simeq \quad \rightarrow \quad =$

$\forall \mathbf{x} \in [0,1]^n, u(\mathbf{x}) \leqslant -\varepsilon$

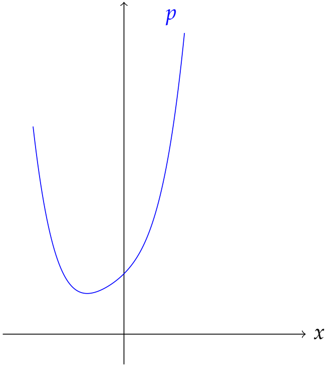
$\min_{\mathbf{K}} f \geqslant \varepsilon$ when $\varepsilon \rightarrow 0$

COMPLEXITY?

`intsos` with $n = 1$ and SDP Approximation

Algorithm from [Chevillard et. al 11]

$p \in \mathbb{Z}[X]$, $\deg p = d = 2k$, $p > 0$



$p = 1 + X + X^2 + X^3 + X^4$

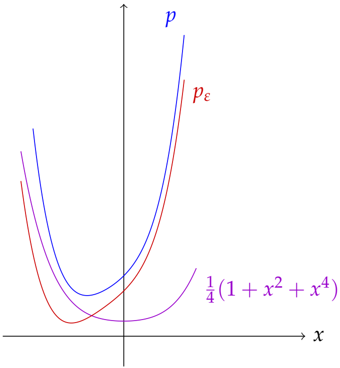
`intsos` with $n = 1$ and SDP Approximation

Algorithm from [Chevillard et. al 11]

$p \in \mathbb{Z}[X]$, $\deg p = d = 2k$, $p > 0$

Perturb: find $\varepsilon \in \mathbb{Q}$ s.t.

$$p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$$



$$p = 1 + X + X^2 + X^3 + X^4$$

$$\varepsilon = \frac{1}{4}$$

$$p > \frac{1}{4}(1 + X^2 + X^4)$$

intsos with $n = 1$ and SDP Approximation

Algorithm from [Chevillard et. al 11]

$p \in \mathbb{Z}[X]$, $\deg p = d = 2k$, $p > 0$

PERTURB: find $\varepsilon \in \mathbb{Q}$ s.t.

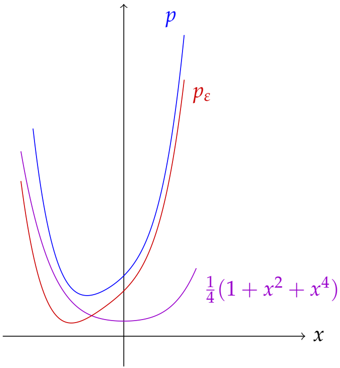
$$p_\varepsilon := p - \varepsilon \sum_{i=0}^{k} X^{2i} > 0$$

SDP Approximation:

$$p - \varepsilon \sum_{i=0}^{k} X^{2i} = \sigma + u$$

ABSORB: small enough u_i

$\implies \varepsilon \sum_{i=0}^{k} X^{2i} + u$ SOS



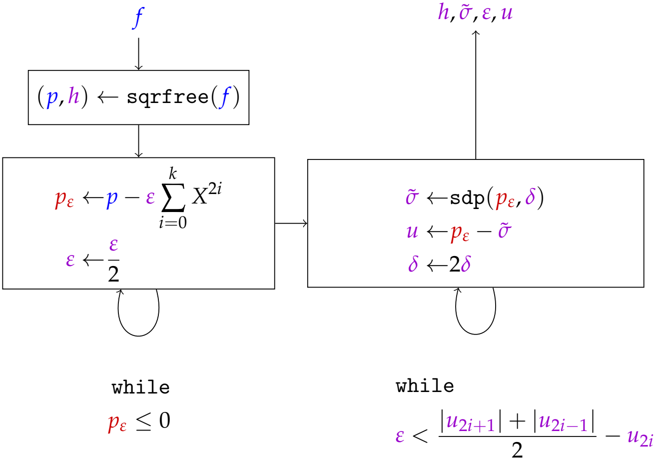
$$p = 1 + X + X^2 + X^3 + X^4$$

$$\varepsilon = \frac{1}{4}$$

$$p > \frac{1}{4}(1 + X^2 + X^4)$$

intsos with $n = 1$ and SDP Approximation

- **Input**: $f \geqslant 0 \in \mathbb{Q}[X]$ of degree $d \geqslant 2$, $\varepsilon \in \mathbb{Q}^{>0}$, $\delta \in \mathbb{N}^{>0}$
- **Output**: SOS decomposition with coefficients in $\mathbb{Q}$



intsos with $n = 1$: Absorbtion

- $X = \frac{1}{2}\left[(X+1)^2 - 1 - X^2\right]$
- $-X = \frac{1}{2}\left[(X-1)^2 - 1 - X^2\right]$

intsos with $n = 1$: Absorbtion

- $X = \frac{1}{2}\left[(X+1)^2 - 1 - X^2\right]$
- $-X = \frac{1}{2}\left[(X-1)^2 - 1 - X^2\right]$

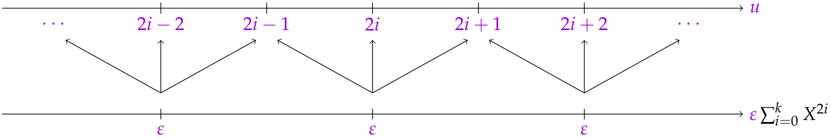
$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2}\left[(X^{i+1} + \operatorname{sgn}(u_{2i+1}) X^i)^2 - X^{2i} - X^{2i+2}\right]$$

`intsos` with $n = 1$: Absorbtion

💡 $X = \frac{1}{2}\left[(X+1)^2 - 1 - X^2\right]$

💡 $-X = \frac{1}{2}\left[(X-1)^2 - 1 - X^2\right]$

$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2}\left[(X^{i+1} + \operatorname{sgn}(u_{2i+1}) X^i)^2 - X^{2i} - X^{2i+2}\right]$$

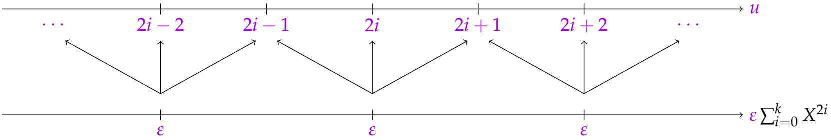


intsos with $n = 1$: Absorbtion

$$X = \frac{1}{2}\left[(X+1)^2 - 1 - X^2\right]$$

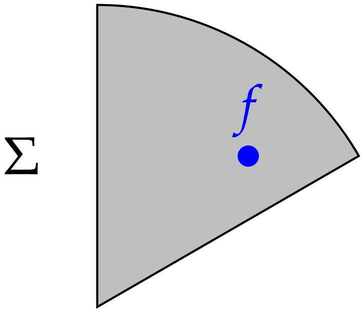
$$-X = \frac{1}{2}\left[(X-1)^2 - 1 - X^2\right]$$

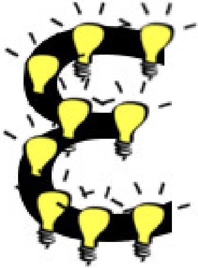
$$u_{2i+1} X^{2i+1} = \frac{|u_{2i+1}|}{2}\left[(X^{i+1} + \operatorname{sgn}(u_{2i+1}) X^i)^2 - X^{2i} - X^{2i+2}\right]$$



$$\varepsilon \geqslant \frac{|u_{2i+1}| + |u_{2i-1}|}{2} - u_{2i} \implies \varepsilon \sum_{i=0}^{k} X^{2i} + u \quad \text{SOS}$$

`intsos` with $n \geqslant 1$: Perturbation





PERTURBATION idea

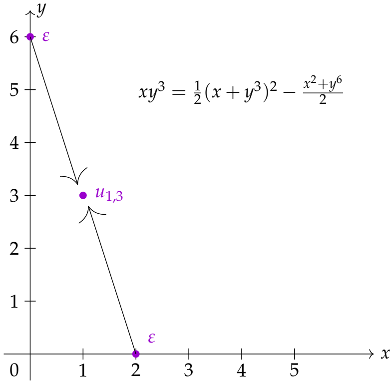
Approximate SOS Decomposition

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

intsos with $n \geqslant 1$: Absorbtion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

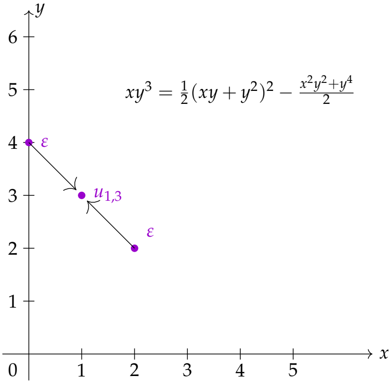
Choice of $\mathcal{P}$?



intsos with $n \geqslant 1$: Absorbtion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

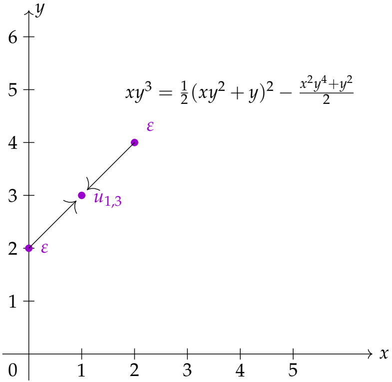
Choice of $\mathcal{P}$?



intsos with $n \geqslant 1$: Absorbtion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

Choice of $\mathcal{P}$?

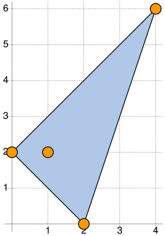


intsos with $n \geqslant 1$: Absorbtion

$$f(X) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} X^{2\alpha} = \tilde{\sigma} + u$$

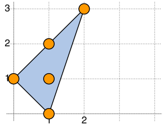
Choice of $\mathcal{P}$?

$f = 4x^4y^6 + x^2 - xy^2 + y^2$
spt(f) = $\{(4,6),(2,0),(1,2),(0,2)\}$



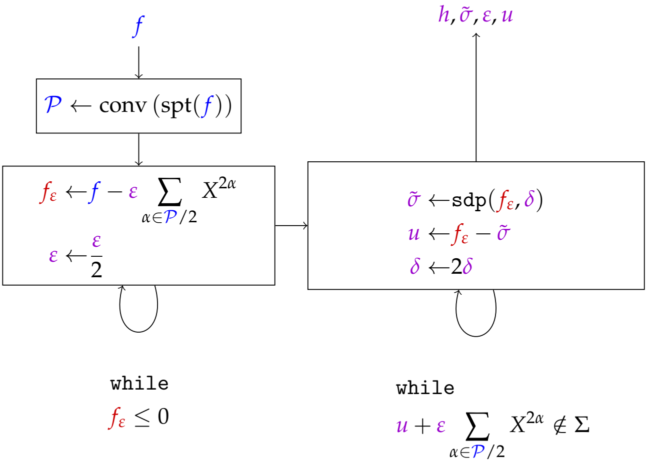
Newton Polytope $\mathcal{P} = \text{conv}\,(\text{spt}(f))$

Squares in SOS decomposition $\subseteq \frac{\mathcal{P}}{2} \cap \mathbb{N}^n$
[Reznick 78]



Algorithm `intsos`

- **Input**: $f \geqslant 0 \in \mathbb{Q}[X]$ of degree $d \geqslant 2$, $\varepsilon \in \mathbb{Q}^{>0}$, $\delta \in \mathbb{N}^{>0}$
- **Output**: SOS decomposition with coefficients in $\mathbb{Q}$



Algorithm `intsos`

Theorem (Exact Certification Cost in $\mathring{\Sigma}$)

$f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ with $\deg f = d = 2k$ and bit size τ

$\Longrightarrow$ `intsos` terminates with SOS output of bit size $\boxed{\tau\, d^{\mathcal{O}(n)}}$

Algorithm `intsos`

Theorem (Exact Certification Cost in $\mathring{\Sigma}$)

$f \in \mathbb{Q}[X] \cap \mathring{\Sigma}[X]$ with $\deg f = d = 2k$ and bit size τ

$\implies$ `intsos` terminates with SOS output of bit size $\boxed{\tau\, d^{\mathcal{O}(n)}}$

Proof.

- $\{\varepsilon \in \mathbb{R} : \forall \mathbf{x} \in \mathbb{R}^n, f(\mathbf{x}) - \varepsilon \sum_{\alpha \in \mathcal{P}/2} \mathbf{x}^{2\alpha} \geqslant 0\} \neq \emptyset$
  Quantifier Elimination [Basu et. al 06] $\implies \tau(\varepsilon) = \tau\, d^{\mathcal{O}(n)}$

- # Coefficients in SOS output = size($\mathcal{P}/2$) = $\binom{n+k}{n} \leqslant d^n$

- Ellipsoid algorithm for SDP [Grötschel et. al 93] $\square$

SDP for Nonlinear Optimization

SDP for Characterizing Values/Curves/Sets

Exact Polynomial Optimization

Conclusion

Conclusion

SDP/SOS powerful to handle **Nonlinear Verification**:

- Optimize values/curves/sets
- Formal nonlinear optimization: `NLCertify`
- Analysis of **nonlinear systems** (Reachability, Invariants)

Conclusion

SDP/SOS powerful to handle **NONLINEAR VERIFICATION**:

- Optimize values/curves/sets
- Formal nonlinear optimization: `NLCertify`
- Analysis of **NONLINEAR SYSTEMS** (Reachability, Invariants)

FUTURE:

- PDEs
- Exact methods
- Non polynomial functions

End

Thank you for your attention!

`http://www-verimag.imag.fr/~magron`