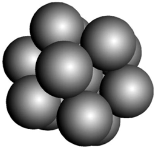
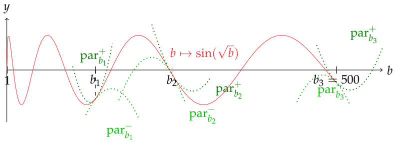
Semidefinite Optimization for System Verification

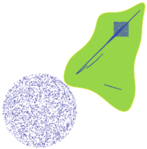
Victor Magron, CNRS

8 October 2015

Tempo Meeting, VERIMAG







Personal Background

- 2008 – 2010: Master at Tokyo University
  HIERARCHICAL DOMAIN DECOMPOSITION METHODS
  (S. Yoshimura)

- 2010 – 2013: PhD at Inria Saclay LIX/CMAP
  FORMAL PROOFS FOR NONLINEAR OPTIMIZATION
  (S. Gaubert and B. Werner)

- 2014 Jan-Sept: Postdoc at LAAS-CNRS
  MOMENT-SOS APPLICATIONS
  (D. Henrion and J.B. Lasserre)

- 2014 – 2015: Postdoc at Imperial
  SDP FOR AUTOMATED HARDWARE TUNING
  (G. Constantinides and A. Donaldson)

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

biology, 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

biology, robotics, analysers, . . .

Efficient certification for nonlinear automatic control

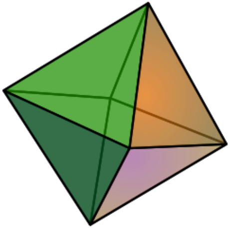
- Certified Optimization of control systems
  analysis / synthesis
- Efficiency
  symmetry reduction, sparsity
- Certified approximation algorithms
  convergence, error analysis

What is Semidefinite Optimization?

- Linear Programming (LP):

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

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

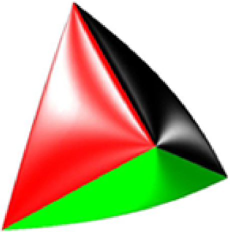


Polyhedron

What is Semidefinite Optimization?

- Semidefinite Programming (SDP):

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



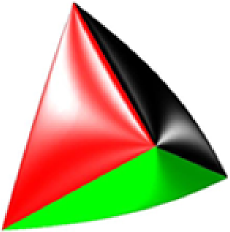
Spectrahedron

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

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

- Prove **polynomial inequalities** with SDP:

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

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

- 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 1)

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

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

SDP for Polynomial Optimization

General case:

- Semialgebraic set $\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\}$
- $p^* := \min_{\mathbf{x} \in \mathbf{S}} p(\mathbf{x})$: NP hard
- Sums of squares (SOS) $\Sigma[\mathbf{x}]$ (e.g. $(x_1 - x_2)^2$)
- $\mathcal{Q}(\mathbf{S}) := \left\{ \sigma_0(\mathbf{x}) + \sum_{j=1}^m \sigma_j(\mathbf{x}) g_j(\mathbf{x}), \text{ with } \sigma_j \in \Sigma[\mathbf{x}] \right\}$
- Fix the degree $2k$ of sums of squares
  $\mathcal{Q}_k(\mathbf{S}) := \mathcal{Q}(\mathbf{S}) \cap \mathbb{R}_{2k}[\mathbf{x}]$

SDP for Polynomial Optimization

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

- Convergence guarantees $\lambda_k \uparrow p^*$ [Lasserre 01]

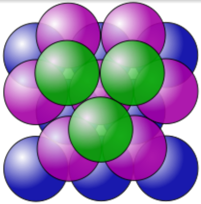
- Can be computed with SDP solvers (CSDP, SDPA)

- Extension to semialgebraic functions $r(\mathbf{x}) = p(\mathbf{x}) / \sqrt{q(\mathbf{x})}$ [Lasserre-Putinar 10]

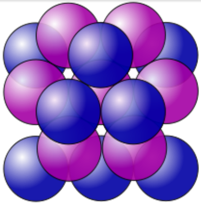
From Oranges Stack...

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 $|\cdot|, \sqrt{}, +, -, \times, /, \sup, \inf, \dots$

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

$$r(\mathbf{x}) := p(\mathbf{x}) / \sqrt{q(\mathbf{x})}$$

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

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 $\mathbf{S} := [4, 6.3504]^3 \times [6.3504, 8] \times [4, 6.3504]^2$

Lemma$_{9922699028}$ from Flyspeck:

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

New Framework (in my PhD thesis)

- Certificates for Nonlinear Optimization using SDP and:
  - Maxplus approximation (Optimal Control)
  - Nonlinear templates (Static Analysis)
- Verification of these certificates inside Coq:
  $p = \sigma_0 + \sum_j \sigma_j g_j \implies \forall \mathbf{x} \in \mathbf{S}, \quad p(\mathbf{x}) \geqslant 0\,.$

Contribution: Publications and Software

V. M., X. Allamigeon, S. Gaubert and B. Werner.
Formal Proofs for Nonlinear Optimization,
arxiv:1404.7282, 2015. *Journal of Formalized Reasoning*.

Software Implementation `NLCertify`**:**

- `https://forge.ocamlcore.org/projects/nl-certify/`

15 000 lines of OCaml code

4000 lines of Coq code

V. M. NLCertify: A Tool for Formal Nonlinear Optimization,
arxiv:1405.5668, 2014. *ICMS*.

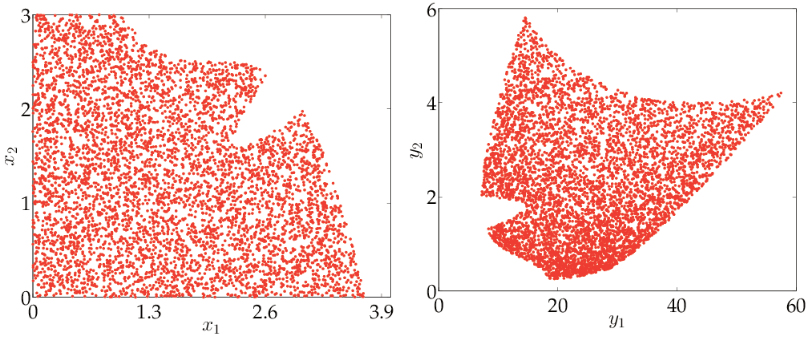
Projections of Semialgebraic Sets

- 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 $f : \mathbb{R}^n \to \mathbb{R}^m$,
  $\mathbf{x} \mapsto f(\mathbf{x}) := (f_1(\mathbf{x}), \dots, f_m(\mathbf{x}))$
- $\mathbf{F} := f(\mathbf{S}) \subseteq \mathbf{B}$, with $\mathbf{B} \subset \mathbb{R}^m$ a box or a ball
- Tractable approximations of $\mathbf{F}$?

Projections of Semialgebraic Sets

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

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



$\mathbf{S}$ $\qquad$ $\mathbf{F} = f(\mathbf{S})$

Projections of Semialgebraic Sets

- Includes important special cases:

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

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

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

Existential Quantifier Elimination

Another point of view:

$$\mathbf{F} = \{\mathbf{y} \in \mathbf{B} : \exists \mathbf{x} \in \mathbf{S} \text{ s.t. } f(\mathbf{x}) = \mathbf{y}\} \ ,$$

Existential Quantifier Elimination

Another point of view:

$$\mathbf{F} = \{\mathbf{y} \in \mathbf{B} : \exists \mathbf{x} \in \mathbf{S} \text{ s.t. } \|\mathbf{y} - f(\mathbf{x})\|_2^2 = 0\} \ ,$$

Existential Quantifier Elimination

Another point of view:

$$\mathbf{F} = \{\mathbf{y} \in \mathbf{B} : \exists \mathbf{x} \in \mathbf{S} \text{ s.t. } h_f(\mathbf{x}, \mathbf{y}) \geqslant 0\} \ ,$$

with

$$h_f(\mathbf{x}, \mathbf{y}) := -\|\mathbf{y} - f(\mathbf{x})\|_2^2 \ .$$

Define $h(\mathbf{y}) := \sup_{\mathbf{x} \in \mathbf{S}} h_f(\mathbf{x}, \mathbf{y})$

Existential Quantifier Elimination

Hierarchy of **SDP**:

$$\inf_{q}\left\{ \int_{\mathbf{B}} (q - h) d\mathbf{y} : q - h_f \in \mathcal{Q}_k(\mathbf{S} \times \mathbf{B}) \right\} \ .$$

Existential QE: approximate **F** as closely as desired [Lasserre 14]

$$\mathbf{F}_k := \{\mathbf{y} \in \mathbf{B} : q_k(\mathbf{y}) \geqslant 0\} \ ,$$

for some polynomials $q_k \in \mathbb{R}_{2k}[\mathbf{y}]$.

Existential Quantifier Elimination

Theorem

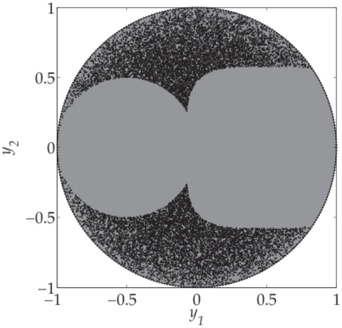
Assuming that $\mathbf{S}$ has non empty interior,

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

Approximating Projections

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

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

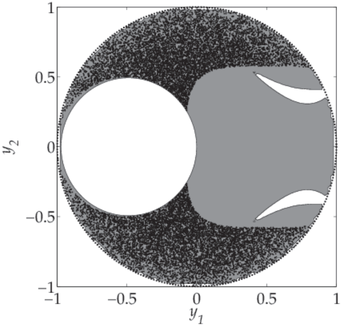


$\mathbf{F}_2$

Approximating Projections

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

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

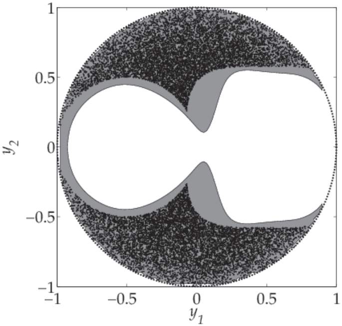


$\mathbf{F}_3$

Approximating Projections

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

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

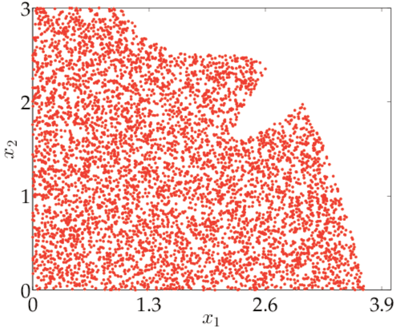


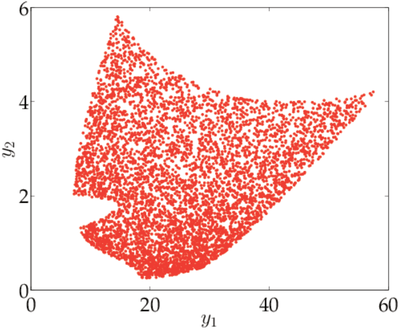
$\mathbf{F}_4$

Approximating Pareto Curves

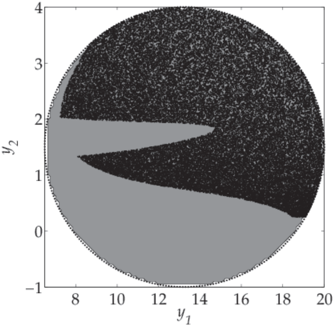
$$g_1 := -(x_1 - 2)^3/2 - x_2 + 2.5 \ ,$$
$$g_2 := -x_1 - x_2 + 8(-x_1 + x_2 + 0.65)^2 + 3.85 \ ,$$
$$\mathbf{S} := \{\mathbf{x} \in \mathbb{R}^2 : g_1(\mathbf{x}) \geqslant 0, g_2(\mathbf{x}) \geqslant 0\} \ .$$

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



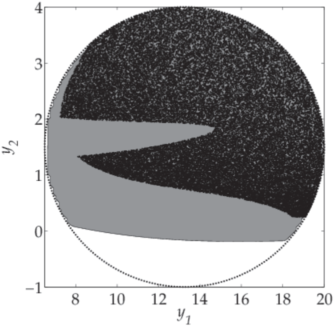


Approximating Pareto Curves



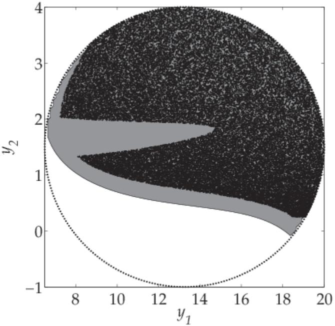
$\mathbf{F}_1$

Approximating Pareto Curves



$\mathbf{F}_2$

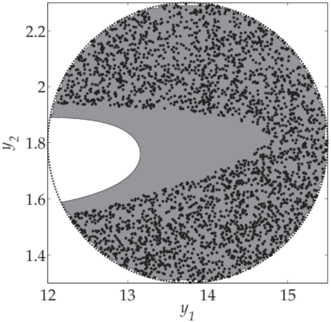
Approximating Pareto Curves



$\mathbf{F_4}$

Approximating Pareto Curves

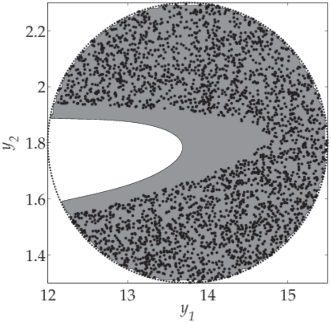
“Zoom” on the region which is hard to approximate:



$\mathbf{F}_4$

Approximating Pareto Curves

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



$\mathbf{F}_5$

Contributions

V. Magron, D. Henrion, J.B. Lasserre. Semidefinite approximations of projections and polynomial images of semialgebraic sets, 2015. *SIAM J. Optimization*.

Polynomial Programs (One-loop with Guards)

- $r, s, T^i, T^e \in \mathbb{R}[\mathbf{x}]$
- $\mathbf{x}_0 \in \mathbf{X}_0$, with $\mathbf{X}_0$ semialgebraic set

```
x = x0;
while (r(x) ⩽ 0){
   if (s(x) ⩽ 0){
         x = T^i(x);
         }
   else{
         x = T^e(x);
         }
}
```

Polynomial Inductive Invariants

Sufficient condition to get inductive invariant:

$$\alpha := \min_{q \in \mathbb{R}[\mathbf{x}]} \sup_{\mathbf{x} \in \mathbf{X}_0} q(\mathbf{x})$$

$$\text{s.t.} \quad q - q \circ T^i \geqslant 0 \ , \text{ if } s(\mathbf{x}) \leqslant 0 \text{ and } r(\mathbf{x}) \leqslant 0 \,,$$

$$q - q \circ T^e \geqslant 0 \ , \text{ if } s(\mathbf{x}) \geqslant 0 \text{ and } r(\mathbf{x}) \leqslant 0 \,,$$

$$q - \kappa \geqslant 0 \ .$$

- $\bigcup_{k \in \mathbb{N}} \mathbf{X}_k \subseteq \{\mathbf{x} \in \mathbb{R}^n : q(\mathbf{x}) \leqslant \alpha\} \subseteq \{\mathbf{x} \in \mathbb{R}^n : \kappa(\mathbf{x}) \leqslant \alpha\}$

Bounding Polynomial Invariants

Sufficient condition to get bounding inductive invariant:

$$\alpha := \min_{q \in \mathbb{R}[\mathbf{x}]} \sup_{\mathbf{x} \in \mathbf{X}_0} q(\mathbf{x})$$

$$\text{s.t.} \quad q - q \circ T^i \geqslant 0 \ , \text{ if } s(\mathbf{x}) \leqslant 0 \text{ and } r(\mathbf{x}) \leqslant 0 \ ,$$

$$q - q \circ T^e \geqslant 0 \ , \text{ if } s(\mathbf{x}) \geqslant 0 \text{ and } r(\mathbf{x}) \leqslant 0 \ ,$$

$$q - \| \cdot \|_2^2 \geqslant 0 \ .$$

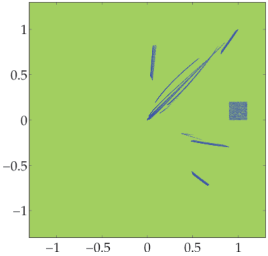
- $\bigcup_{k \in \mathbb{N}} \mathbf{X}_k \subseteq \{\mathbf{x} \in \mathbb{R}^n : q(\mathbf{x}) \leqslant \alpha\} \subseteq \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|^2 \leqslant \alpha\}$

Bounds for $\bigcup_{k\in\mathbb{N}} \mathbf{X}_k$

$\mathbf{X}_0 := [0.9, 1.1] \times [0, 0.2] \quad r(\mathbf{x}) := 1 \quad s(\mathbf{x}) := 1 - \|\mathbf{x}\|^2$

$T^i(\mathbf{x}) := (x_1^2 + x_2^3, x_1^3 + x_2^2) \quad T^e(\mathbf{x}) := (\frac{1}{2}x_1^2 + \frac{2}{5}x_2^3, -\frac{3}{5}x_1^3 + \frac{3}{10}x_2^2)$

$\kappa(\mathbf{x}) = \|\mathbf{x}\|^2$



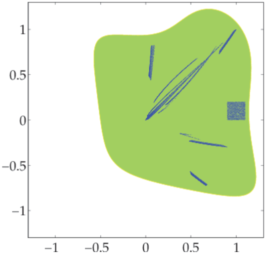
Degree 6

Bounds for $\bigcup_{k\in\mathbb{N}} \mathbf{X}_k$

$\mathbf{X}_0 := [0.9, 1.1] \times [0, 0.2] \quad r(\mathbf{x}) := 1 \quad s(\mathbf{x}) := 1 - \|\mathbf{x}\|^2$

$T^i(\mathbf{x}) := (x_1^2 + x_2^3, x_1^3 + x_2^2) \quad T^e(\mathbf{x}) := (\frac{1}{2}x_1^2 + \frac{2}{5}x_2^3, -\frac{3}{5}x_1^3 + \frac{3}{10}x_2^2)$

$\kappa(\mathbf{x}) = \|\mathbf{x}\|^2$



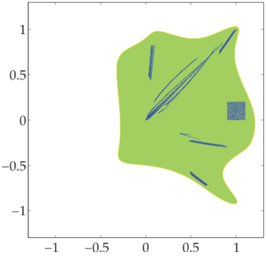
Degree 8

Bounds for $\bigcup_{k \in \mathbb{N}} \mathbf{X}_k$

$\mathbf{X}_0 := [0.9, 1.1] \times [0, 0.2] \quad r(\mathbf{x}) := 1 \quad s(\mathbf{x}) := 1 - \|\mathbf{x}\|^2$

$T^i(\mathbf{x}) := (x_1^2 + x_2^3, x_1^3 + x_2^2) \quad T^e(\mathbf{x}) := (\frac{1}{2}x_1^2 + \frac{2}{5}x_2^3, -\frac{3}{5}x_1^3 + \frac{3}{10}x_2^2)$

$\kappa(\mathbf{x}) = \|\mathbf{x}\|^2$



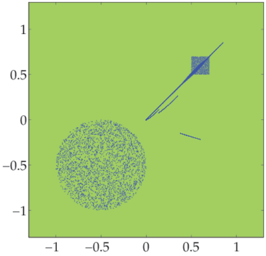
Degree 10

Does $\bigcup_{k\in\mathbb{N}} \mathbf{X}_k$ avoid unsafe region?

$\mathbf{X}_0 := [0.5, 0.7]^2 \quad r(\mathbf{x}) := 1 \quad s(\mathbf{x}) := 1 - \|\mathbf{x}\|^2$

$T^i(\mathbf{x}) := (x_1^2 + x_2^3, x_1^3 + x_2^2) \quad T^e(\mathbf{x}) := (\frac{1}{2}x_1^2 + \frac{2}{5}x_2^3, -\frac{3}{5}x_1^3 + \frac{3}{10}x_2^2)$

$\kappa(\mathbf{x}) = \frac{1}{4} - (x_1 + \frac{1}{2})^2 - (x_2 + \frac{1}{2})^2$



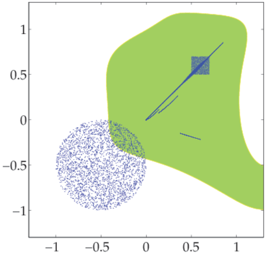
Degree 6

Does $\bigcup_{k\in\mathbb{N}} \mathbf{X}_k$ avoid unsafe region?

$$\mathbf{X}_0 := [0.5, 0.7]^2 \quad r(\mathbf{x}) := 1 \quad s(\mathbf{x}) := 1 - \|\mathbf{x}\|^2$$

$$T^i(\mathbf{x}) := (x_1^2 + x_2^3, x_1^3 + x_2^2) \quad T^e(\mathbf{x}) := (\frac{1}{2}x_1^2 + \frac{2}{5}x_2^3, -\frac{3}{5}x_1^3 + \frac{3}{10}x_2^2)$$

$$\kappa(\mathbf{x}) = \frac{1}{4} - (x_1 + \frac{1}{2})^2 - (x_2 + \frac{1}{2})^2$$



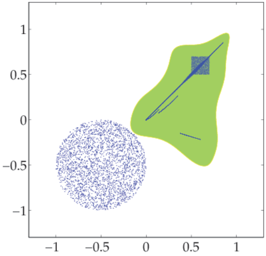
Degree 8

Does $\bigcup_{k\in\mathbb{N}} \mathbf{X}_k$ avoid unsafe region?

$$\mathbf{X}_0 := [0.5, 0.7]^2 \quad r(\mathbf{x}) := 1 \quad s(\mathbf{x}) := 1 - \|\mathbf{x}\|^2$$

$$T^i(\mathbf{x}) := (x_1^2 + x_2^3, x_1^3 + x_2^2) \quad T^e(\mathbf{x}) := (\frac{1}{2}x_1^2 + \frac{2}{5}x_2^3, -\frac{3}{5}x_1^3 + \frac{3}{10}x_2^2)$$

$$\kappa(\mathbf{x}) = \frac{1}{4} - (x_1 + \frac{1}{2})^2 - (x_2 + \frac{1}{2})^2$$



Degree 10

Contributions

A. Adjé, P-L. Garoche, V Magron. Property-based Polynomial Invariant Generation using Sums-of-Squares Optimization, 2014. *Static Analysis Symposium*.

Ongoing: Bounding Floating-point Errors

- Exact:

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

- Floating-point:

$$\hat{f}(\mathbf{x}, \boldsymbol{\epsilon}) := [x_1 x_2 (1 + \epsilon_1) + x_3 x_4 (1 + \epsilon_2)](1 + \epsilon_3)$$

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

Ongoing: Bounding Floating-point Errors

Input: exact $f(\mathbf{x})$, floating-point $\hat{f}(\mathbf{x}, \boldsymbol{\epsilon})$, $\mathbf{x} \in \mathbf{S}$, $| \epsilon_i | \leqslant 2^{-p}$
Output: Bounds for $f - \hat{f}$

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

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

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

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

Contributions

V. Magron, G. Constantinides, A. Donaldson. Certified Roundoff Error Bounds Using Semidefinite Programming, 2015.

Conclusion

SDP is powerful to handle **NONLINEARITY**:

- Optimize nonlinear (transcendental) functions
- Approximate Pareto Curves, projections of semialgebraic sets
- Analyze nonlinear systems

Conclusion

Further research:

- Flyspeck nonlinear inequalities : decrease current verification time (5000 CPU hours!!)

- Alternative polynomial bounds using geometric programming (T. de Wolff, S. Iliman)

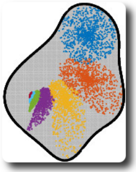
- Mixed linear/SDP certificates (trade-off CPU/precision)

- System verification:

  Loops $\mathbf{x}_{k+1} = f(\mathbf{x}_k)$ Roundoff errors $\mathbf{x}_{k+1} = f(\mathbf{x}_k, \epsilon)$

  certified/**convergent** SDP hierarchies

  image measure supports conservation eqs.



End

Thank you for your attention!

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