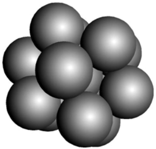
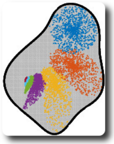
Certified Optimization for System Verification

Victor Magron, CNRS

26 Juin 2017

SMAI-MODE Meeting

Personal Background

- 2008 – 2010: Master at Tokyo University
  Hierarchical Domain Decomposition Methods
- 2010 – 2013: PhD at Inria Saclay LIX/CMAP
  Formal Proofs for Nonlinear Optimization
  (S. Gaubert, B. Werner)
- 2014 Jan-Sept: Postdoc at LAAS-CNRS
  Moment-SOS applications (D. Henrion, J.B. Lasserre)
- 2014 – 2015: Postdoc at Imperial College
  Roudoff Errors with Polynomial Optimization
  (G. Constantinides and A. Donaldson)
- 2015 – 2017: CR2 CNRS-Verimag (Tempo Team)

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, . . .

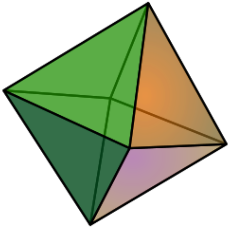
Efficient certification for nonlinear systems

- 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):

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



Polyhedron

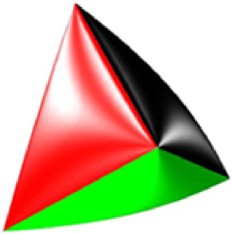
  - Linear cost $\mathbf{c}$
  - Linear inequalities "$\sum_i A_{ij} z_j \geqslant d_i$"

What is Semidefinite Optimization?

- Semidefinite Programming (SDP):

$$\begin{aligned} \min_{\mathbf{z}} \quad & \mathbf{c}^\top \mathbf{z} \\ \text{s.t.} \quad & \sum_i \mathbf{F}_i z_i \succcurlyeq \mathbf{F}_0 \, . \end{aligned}$$

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



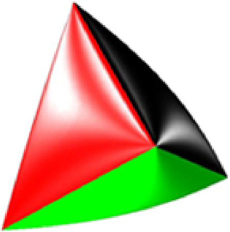
Spectrahedron

What is Semidefinite Optimization?

- Semidefinite Programming (SDP):

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

  - 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

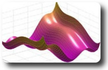
Applications of SDP

- 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)



$$\inf \int p \, d\mu \qquad\qquad \sup \lambda$$

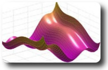
avec μ probabilité $\Rightarrow$ **LP INFINI** $\Leftarrow$ avec $p - \lambda \geqslant 0$

SDP for Polynomial Optimization

Practical approach for polynomial optimization

(Primal **Relaxation**)

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



(Dual **Strengthening**)

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

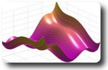
finite $\Rightarrow$ **SDP** $\Leftarrow$ **fixed** degree

SDP for Polynomial Optimization

Practical approach for polynomial optimization

(Primal **Relaxation**)

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



(Dual **Strengthening**)

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

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

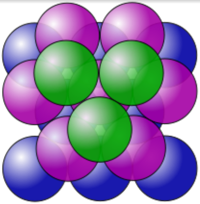
Hierarchy of **SDP** $\uparrow p^*$

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

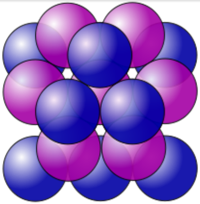
From Oranges Stack...

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**

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.

Roundoff Error Bounds

- 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)

Roundoff Error Bounds

Input: exact $f(\mathbf{x})$, floating-point $\hat{f}(\mathbf{x}, \boldsymbol{\epsilon})$
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**

Roundoff Error Bounds

Input: exact $f(\mathbf{x})$, floating-point $\hat{f}(\mathbf{x}, \boldsymbol{\epsilon})$
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 $\boldsymbol{\epsilon}$

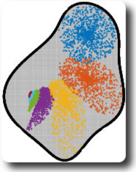
3: Bound $h(\mathbf{x}, \boldsymbol{\epsilon})$ with interval arithmetic

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

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

Reachable Sets of Polynomial Systems

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

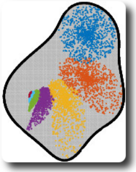


- **Converging** SDP hierarchies
- Image measure
- Liouville equation (conservation)

$$\mu_t + \mu = f_\# \mu + \mu_0$$

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., Henrion, Lasserre. Semidefinite Approximations of Projections and Polynomial Images of SemiAlgebraic Sets. SIAM J. Optim, 2015

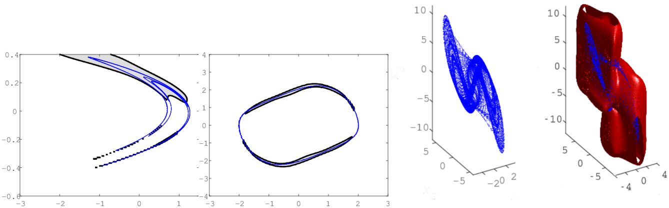
M., Garoche, Henrion, Thirioux. Semidefinite Approximations of Reachable Sets for Discrete-time Polynomial Systems, 2017.

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

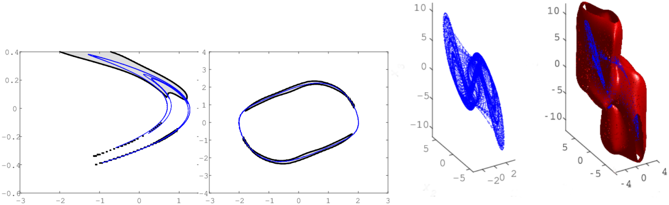


Invariant Measures of Polynomial Systems

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, 2017

Conclusion

SDP/SOS powerful to handle **NONLINEARITY**:

- Optimize nonlinear functions
- Analysis of nonlinear systems (Reachability, Invariants)

FUTURE:

- PDEs (with C. Prieur)
- Exact methods for $n = 1$ (with M. Safey, M. Schweighofer)
- Non polynomial functions

End

Thank you for your attention!

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