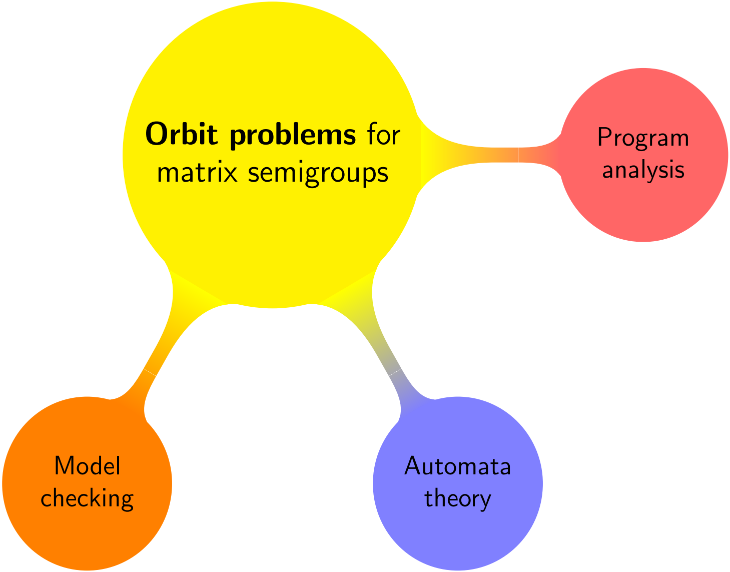
Orbit Problems for Linear Dynamical Systems

James Worrell

Department of Computer Science
Oxford University

MOVEP 2020, VERIMAG

A Landscape of Orbit Problems



Once Upon a Time in Linear Semigroups . . .

Theorem (Markov 1947)

There is a fixed set of 6×6 *integer matrices* $M_1, \ldots, M_k$ *such that the* **Membership Problem** *"*$M \in \langle M_1, \ldots, M_k \rangle$*?" is undecidable.*

Once Upon a Time in Linear Semigroups . . .

Theorem (Markov 1947)

There is a fixed set of 6×6 *integer matrices* $M_1, \ldots, M_k$ *such that the* **Membership Problem** *"*$M \in \langle M_1, \ldots, M_k \rangle$*?" is undecidable.*

Mortality Problem: Is the zero matrix contained in the semigroup generated by a given set of $n \times n$ matrices with integer entries?

Once Upon a Time in Linear Semigroups . . .

Theorem (Markov 1947)

There is a fixed set of 6×6 *integer matrices* $M_1, \ldots, M_k$ *such that the* **Membership Problem** *"*$M \in \langle M_1, \ldots, M_k \rangle$*?" is undecidable.*

Mortality Problem: Is the zero matrix contained in the semigroup generated by a given set of $n \times n$ matrices with integer entries?

Theorem (Paterson 1970)

The Mortality Problem is undecidable for 3×3 *matrices.*

Finiteness is Decidable

Theoretical Computer Science 5 (1977) 101–111.

ON FINITE SEMIGROUPS OF MATRICES*

Arnaldo MANDEL[1] and Imre SIMON[2]
Instituto de Matemática e Estatística, Universidade de São Paulo, 05508 São Paulo, SP, Brasil

Communicated by M. Nivat
Received February 1977

Abstract. Finite semigroups of n by n matrices over the naturals are characterized both by algebraic and combinatorial methods. Next we show that the cardinality of a finite semigroup S of n by n matrices over a field is bounded by a function depending only on n, the number of generators of S and the maximum cardinality of its subgroups. As a consequence, given n and k, there exist, up to isomorphism, only a finite number of finite semigroups of n by n matrices over the rationals, generated by at most k elements. Among other applications to Automaton Theory, we show that it is decidable whether the behavior of a given $\mathbf{N}-\Sigma$ automaton is bounded.

1. Introduction

The results in this paper originated from the investigation of the following question in Automaton Theory: Is it decidable whether the behavior of a given $\mathbf{N}-\Sigma$ automaton is bounded? This is answered affirmatively and it leads to the study of finite semigroups of matrices over the naturals. After obtaining effective characterizations of these semigroups, we investigate finite semigroups of matrices over a field. This enables us to generalize, to matrices over the rationals, one of the results obtained earlier.

The Commutative Case

Theorem (Babai, Beals, Cai, Ivanyos, Luks 1996)

The semigroup membership problem "$M \in \langle M_1, \ldots, M_k \rangle$?" is decidable for commuting matrices $M_1, \ldots, M_k$ and M.

The Commutative Case

Theorem (Babai, Beals, Cai, Ivanyos, Luks 1996)

The semigroup membership problem "$M \in \langle M_1, \ldots, M_k \rangle$?" is decidable for commuting matrices $M_1, \ldots, M_k$ and M.

Theorem (Kannan, Lipton 1986)

The membership problem "$M \in \langle M_1 \rangle$?" is polynomial-time decidable.

The Commutative Case

Theorem (Babai, Beals, Cai, Ivanyos, Luks 1996)

The semigroup membership problem "$M \in \langle M_1, \ldots, M_k \rangle$?" is decidable for commuting matrices $M_1, \ldots, M_k$ and M.

Theorem (Kannan, Lipton 1986)

The membership problem "$M \in \langle M_1 \rangle$?" is polynomial-time decidable.

Proof Sketch. Reduce to finding multiplicative relations:

$$\alpha_1^{n_1} \cdots \alpha_k^{n_k} = \beta \qquad n_1, \ldots, n_k \in \mathbb{Z}$$

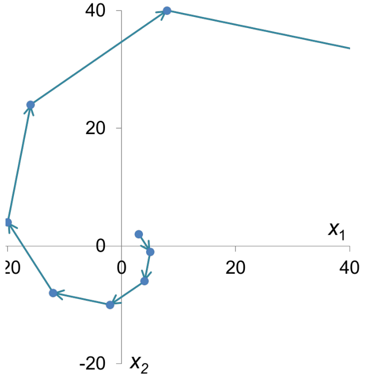
for given algebraic numbers $\alpha_1, \ldots, \alpha_k, \beta$.

Orbit Problems

Consider **orbit** $\mathcal{O} := \langle M_1, \ldots, M_k \rangle \boldsymbol{x}$:

Orbit Problems

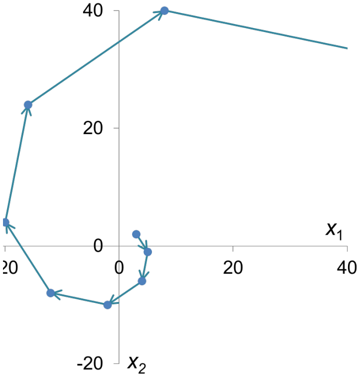
Consider **orbit** $\mathcal{O} := \langle M_1, \ldots, M_k \rangle \boldsymbol{x}$:



Orbit Problems

Consider **orbit** $\mathcal{O} := \langle M_1, \ldots, M_k \rangle \boldsymbol{x}$:

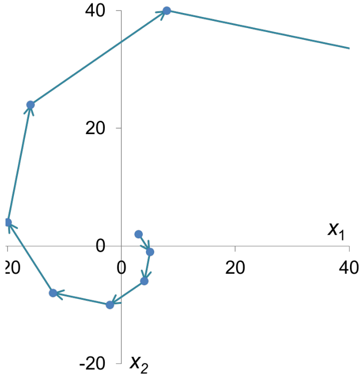
- **Reachability:** Does the orbit meet a target set (point, hyperplane, polyhedron, ...)?



Orbit Problems

Consider **orbit** $\mathcal{O} := \langle M_1, \ldots, M_k \rangle \boldsymbol{x}$:

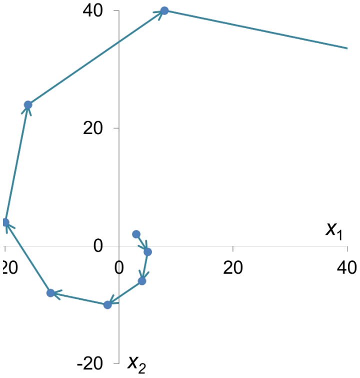
- **Reachability:** Does the orbit meet a target set (point, hyperplane, polyhedron, ...)?
- **Invariance:** Can the orbit be separated from the target?



Orbit Problems

Consider **orbit** $\mathcal{O} := \langle M_1, \ldots, M_k \rangle \boldsymbol{x}$:

- **Reachability:** Does the orbit meet a target set (point, hyperplane, polyhedron, ...)?
- **Invariance:** Can the orbit be separated from the target?
- **Termination:** Does every orbit escape a given set?



A Fundamental Orbit Problem . . .

Orbit $\mathcal{O} := \langle A \rangle \boldsymbol{x}$ reaches hyperplane normal to $\boldsymbol{y}$ iff the sequence $\langle \boldsymbol{y}^\top A^n \boldsymbol{x} : n \in \mathbb{N} \rangle$ contains a zero.

. . . that is not Easy

Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)

Skolem's Problem *"$\exists n \,.\, u_n = 0$?" is decidable for LRS (u_n) of order at most 4.*

...that is not Easy

Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)

Skolem's Problem *"$\exists n \,.\, u_n = 0$?" is decidable for LRS (u_n) of order at most 4.*

Theorem (Ouaknine, W. 2013)

The **Positivity Problem** *"$\forall n \,.\, u_n \geq 0$?" is decidable for LRS (u_n) of order at most 5.*

...that is not Easy

Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)

Skolem's Problem *"$\exists n \,.\, u_n = 0$?" is decidable for LRS (u_n) of order at most 4.*

Theorem (Ouaknine, W. 2013)

*The **Positivity Problem** "$\forall n \,.\, u_n \geq 0$?" is decidable for LRS (u_n) of order at most 5.*

Theorem (Ouaknine, W. 2014)

*The **Ultimate Positivity Problem** "$\exists N \, \forall n \geq N \,.\, u_n \geq 0$?" is decidable for simple LRS (u_n) at all orders.*

This Tutorial

1. **Polynomial invariants**:
   - Compute the Zariski closure of the orbit of a point under a matrix semigroup

This Tutorial

1. **Polynomial invariants**:
   - Compute the Zariski closure of the orbit of a point under a matrix semigroup
2. **Termination of linear loops**:
   - Decide whether all orbits escape a polyhedron?

This Tutorial

1. **Polynomial invariants**:
   - Compute the Zariski closure of the orbit of a point under a matrix semigroup
2. **Termination of linear loops**:
   - Decide whether all orbits escape a polyhedron?
3. **Continuous Skolem Problem**:
   - Decide whether the orbit of a point under a one-parameter semigroup reaches a hyperplane.

Part I: Polynomial Invariants

Programming in the Jurassic

destination (or origin) is v. An *interpretation* I of a flowchart is a mapping of its edges on propositions. Some, but not necessarily all, of the free variables of these propositions may be variables manipulated by the

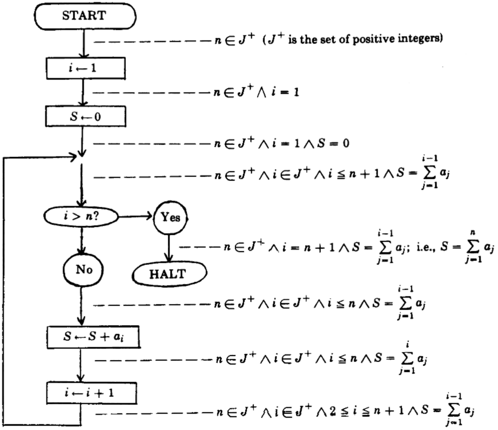


FIGURE 1. Flowchart of program to compute $S = \sum_{j=1}^{n} a_j$ $(n \geqq 0)$

Robert W. Floyd, *Assigning Meanings to Programs*, 1967

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix}\ \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$

while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix}$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix}$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$

Polynomial Invariants

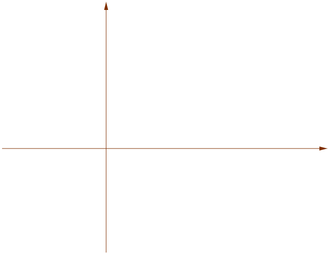
$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$

Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

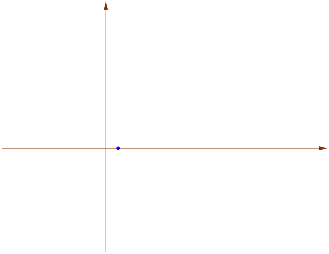
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

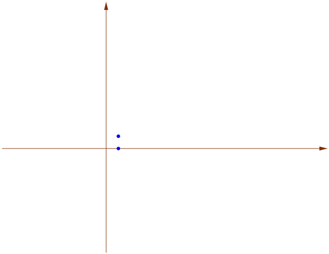
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$

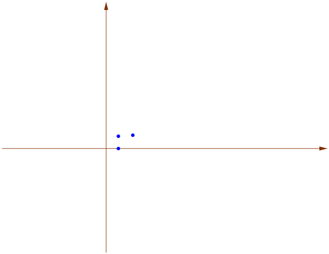


Polynomial Invariants

$x := 1;\ ;\ y := 0;$

while **true** do

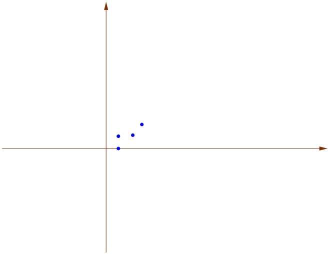
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

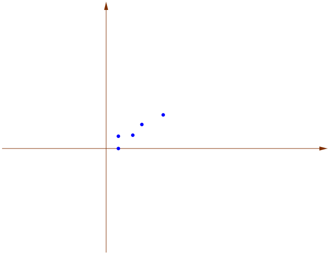
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

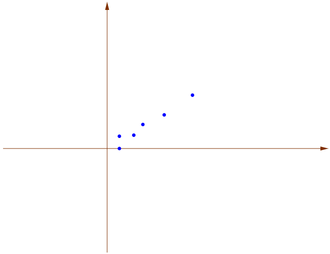
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

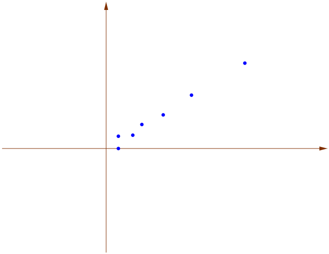
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

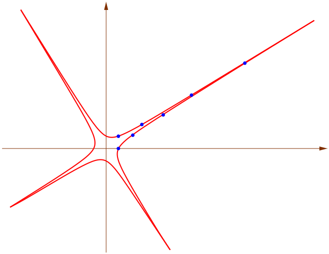
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1; \; ; \; y := 0;$
while **true** do

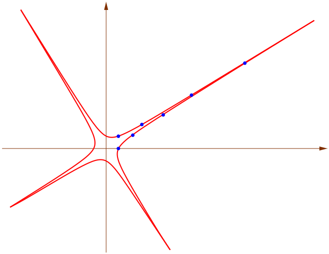
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial Invariants

$x := 1;\ ;\ y := 0;$
while **true** do

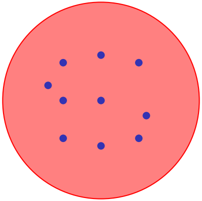
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};\quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 8 \end{pmatrix}$$



Polynomial invariant: $x^4 + y^4 - 2x^3y - x^2y^2 + 2xy^3 - 1 = 0$

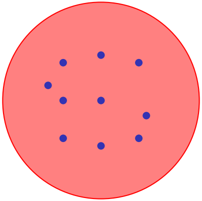
Invariants

invariant = overapproximation of the reachable states

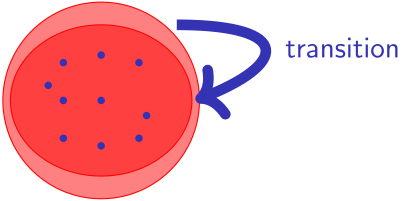


Invariants

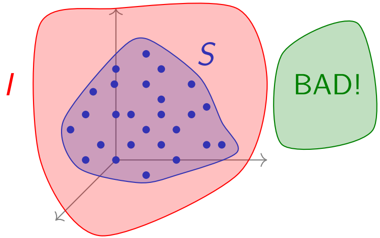
invariant = overapproximation of the reachable states



inductive invariant = invariant preserved by the transition relation



Why Invariants?



The classical approach to the verification of temporal safety properties of programs requires the construction of **inductive invariants** *[...].* **Automation of this construction is the main challenge in program verification.**

D. Beyer, T. Henzinger, R. Majumdar, and A. Rybalchenko
Invariant Synthesis for Combined Theories, 2007

Equivalence of Deterministic Top-Down Tree-to-String Transducers Is Decidable

HELMUT SEIDL, Technical University of Munich
SEBASTIAN MANETH, Universität of Bremen
GREGOR KEMPER, Technical University of Munich

“ [. . .] we introduce polynomial transducers and prove that for these, equivalence can be certified by means of an inductive polynomial invariant. This allows us to construct two semi-algorithms, one searching for an invariant and the other for a witness of non-equivalence [. . .]”

Automata-Theoretic Applications

DECIDABLE AND UNDECIDABLE PROBLEMS ABOUT QUANTUM AUTOMATA*

VINCENT D. BLONDEL†, EMMANUEL JEANDEL‡, PASCAL KOIRAN‡, AND NATACHA PORTIER‡

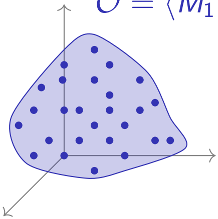
Abstract. We study the following decision problem: is the language recognized by a quantum finite automaton empty or nonempty? We prove that this problem is decidable or undecidable depending on whether recognition is defined by strict or nonstrict thresholds. This result is in contrast with the corresponding situation for probabilistic finite automata, for which it is known that strict and nonstrict thresholds both lead to undecidable problems.

Theorem (Blondel, Jeandel, Koiran, Portier 2005)

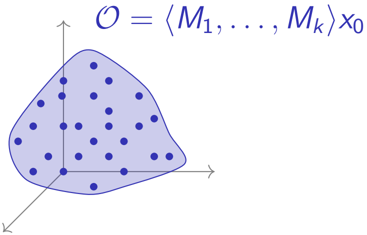
The strict threshold problem is decidable for quantum automata.

The Strongest Algebraic Invariant of an Orbit

$$\mathcal{O} = \langle M_1, \ldots, M_k \rangle x_0$$

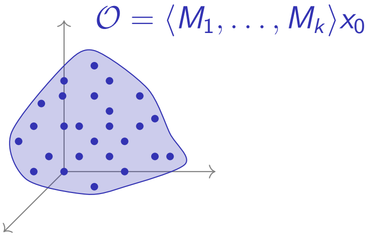


The Strongest Algebraic Invariant of an Orbit



- Compute **ideal** of polynomial relations satisfied by the orbit $\mathcal{O}$ (determines the **Zariski closure** $\overline{\mathcal{O}} \subseteq \mathbb{R}^d$)

The Strongest Algebraic Invariant of an Orbit

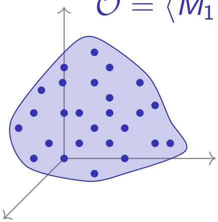


- Compute **ideal** of polynomial relations satisfied by the orbit $\mathcal{O}$ (determines the **Zariski closure** $\overline{\mathcal{O}} \subseteq \mathbb{R}^d$)
- Yields an inductive invariant:

$$M_i(\overline{\mathcal{O}}) \subseteq \overline{M_i \mathcal{O}} \subseteq \overline{\mathcal{O}}$$

The Strongest Algebraic Invariant of an Orbit

$$\mathcal{O} = \langle M_1, \ldots, M_k \rangle x_0$$



- Compute **ideal** of polynomial relations satisfied by the orbit $\mathcal{O}$ (determines the **Zariski closure** $\overline{\mathcal{O}} \subseteq \mathbb{R}^d$)
- Yields an inductive invariant:

$$M_i(\overline{\mathcal{O}}) \subseteq \overline{M_i \mathcal{O}} \subseteq \overline{\mathcal{O}}$$

- Idea is to compute Zariski closure of $\langle M_1, \ldots, M_k \rangle \subseteq \mathbb{R}^{d \times d}$, generalising [Mandel and Simon 77]

The Group Case

ELSEVIER

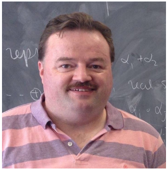
Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Symbolic Computation 39 (2005) 357–371

Journal of Symbolic Computation

www.elsevier.com/locate/jsc



Quantum automata and algebraic groups

Harm Derksen[a], Emmanuel Jeandel[b], Pascal Koiran[b,*]

[a] *Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, United States*
[b] *Laboratoire de l'Informatique du Parallélisme, Ecole Normale Supérieure de Lyon, 69364, France*

Received 15 September 2003; accepted 1 November 2004

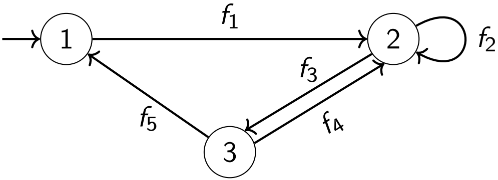
Abstract

We show that several problems which are known to be undecidable for probabilistic automata become decidable for quantum finite automata. Our main tool is an algebraic result of independent interest: we give an algorithm which, given a finite number of invertible matrices, computes the Zariski closure of the group generated by these matrices.

Keywords: Quantum automata; Probabilistic automata; Undecidability; Algebraic groups; Algebraic geometry

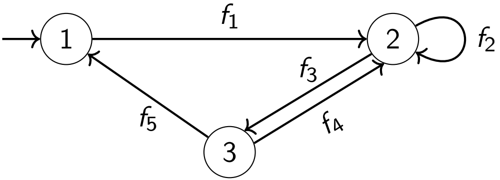
Motivation: A Problem in Program Analysis

Polynomial Programs (Muller-Olm and Seidl 2004)



Motivation: A Problem in Program Analysis

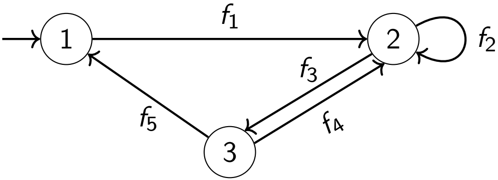
Polynomial Programs (Muller-Olm and Seidl 2004)



- Nondeterministic branching (no guards)

Motivation: A Problem in Program Analysis

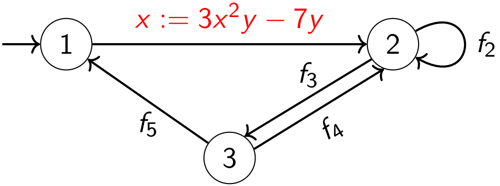
Polynomial Programs (Muller-Olm and Seidl 2004)



- Nondeterministic branching (no guards)
- Integer variables with polynomial assignments

Motivation: A Problem in Program Analysis

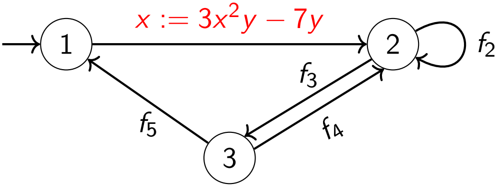
Polynomial Programs (Muller-Olm and Seidl 2004)



- Nondeterministic branching (no guards)
- Integer variables with polynomial assignments

Motivation: A Problem in Program Analysis

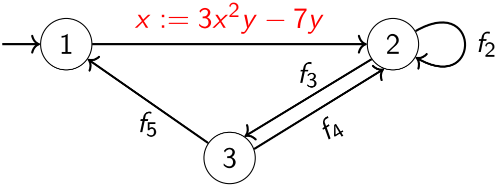
Polynomial Programs (Muller-Olm and Seidl 2004)



- Nondeterministic branching (no guards)
- Integer variables with polynomial assignments
- Compute **all valid polynomial relations** at each location

Motivation: A Problem in Program Analysis

Polynomial Programs (Muller-Olm and Seidl 2004)



- Nondeterministic branching (no guards)
- Integer variables with polynomial assignments
- Compute **all valid polynomial relations** at each location
- Represents the **Zariski closure** of the reachable set at each location

Finding all polynomial invariants

ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Information Processing Letters 91 (2004) 233–244

Information Processing Letters

www.elsevier.com/locate/ipl

Computing polynomial program invariants

Markus Müller-Olm [a,*,1], Helmut Seidl [b]

[a] *FernUniversität Hagen, LG Praktische Informatik 5, 58084 Hagen, Germany*

[b] *TU München, Informatik, I2, 85748 München, Germany*

Received 16 October 2003; received in revised form 20 April 2004

Available online 19 June 2004

Finding all polynomial invariants

ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Information Processing Letters 91 (2004) 233–244

Information Processing Letters

www.elsevier.com/locate/ipl

Computing polynomial program invariants

Markus Müller-Olm [a,*,1], Helmut Seidl [b]

[a] *FernUniversität Hagen, LG Praktische Informatik 5, 58084 Hagen, Germany*

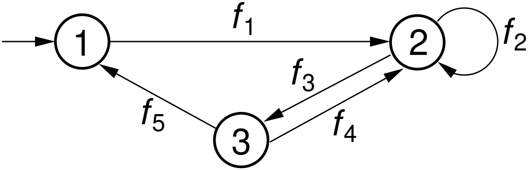
[b] *TU München, Informatik, I2, 85748 München, Germany*

Received 16 October 2003; received in revised form 20 April 2004

Available online 19 June 2004

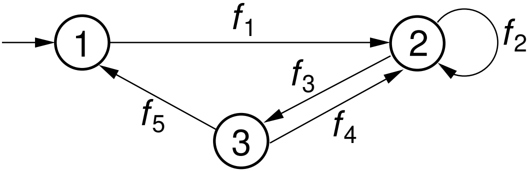
It is a challenging open problem whether or not the set of *all* valid polynomial relations can be computed not just the ones of some given form. It is not

Geometric Picture



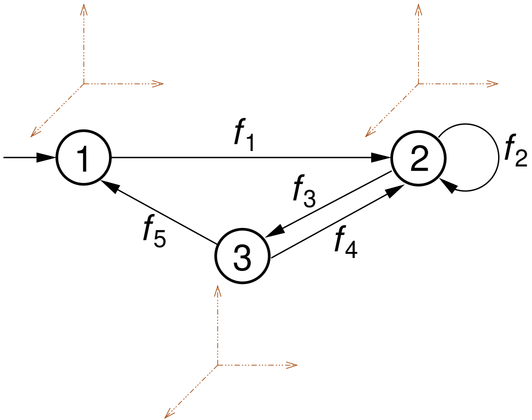
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



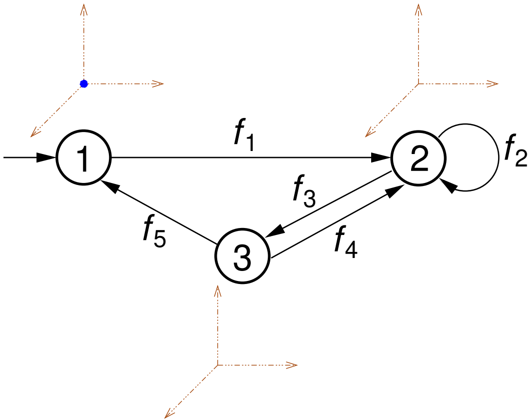
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



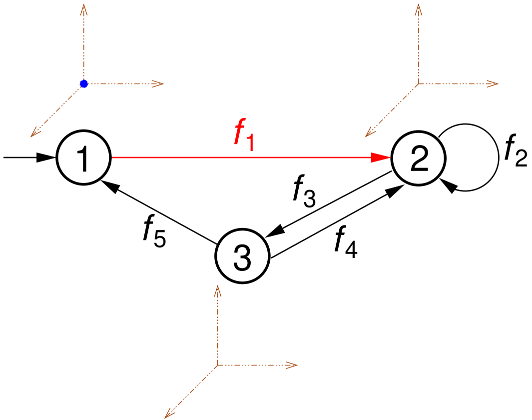
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



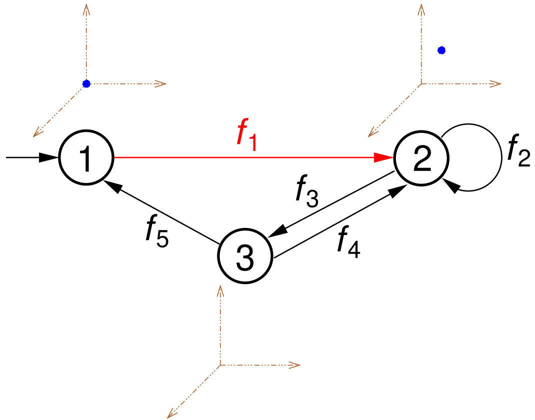
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



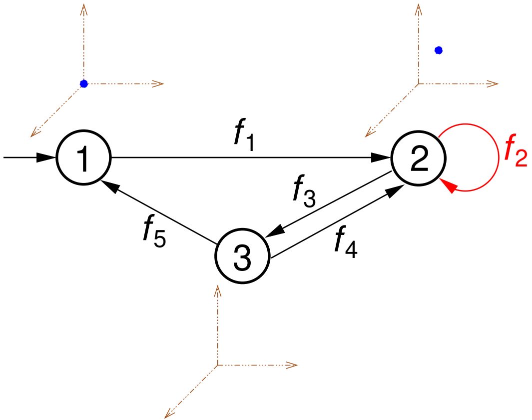
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



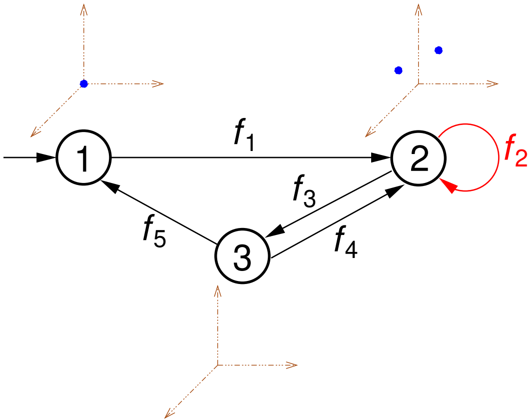
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



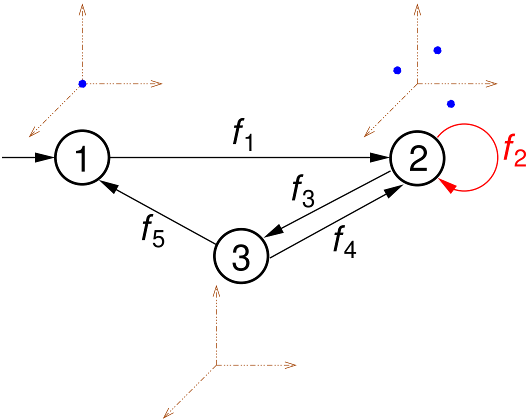
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



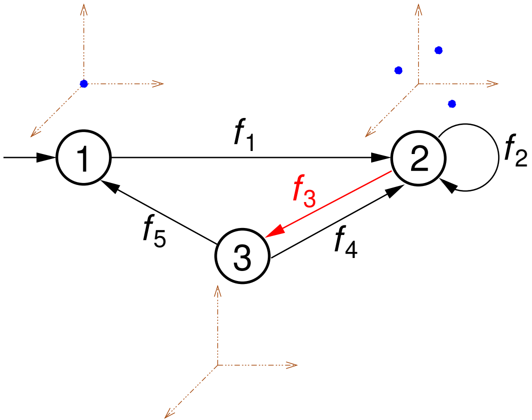
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



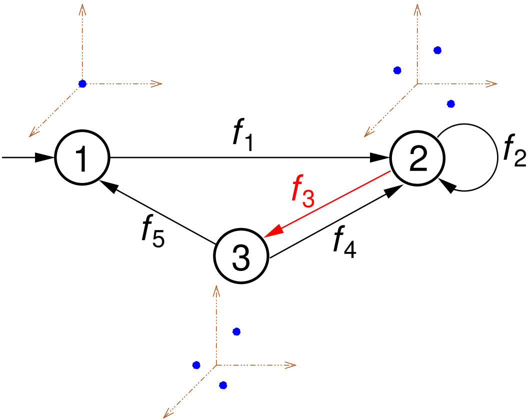
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



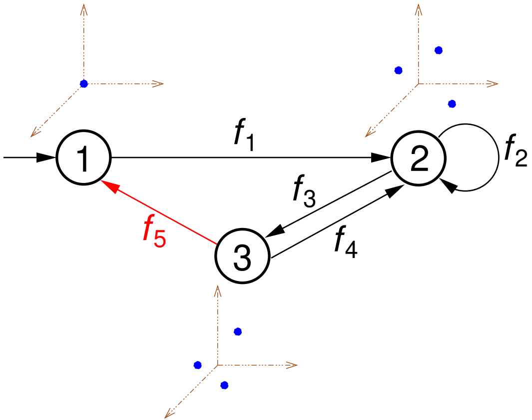
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



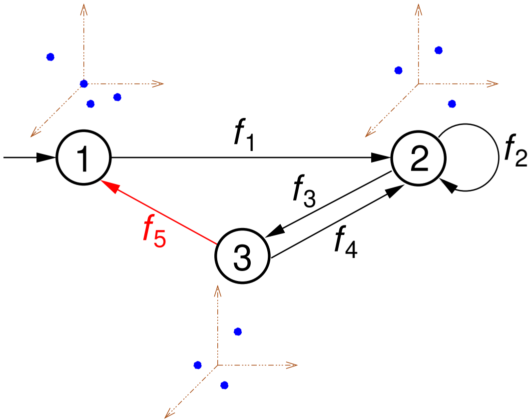
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



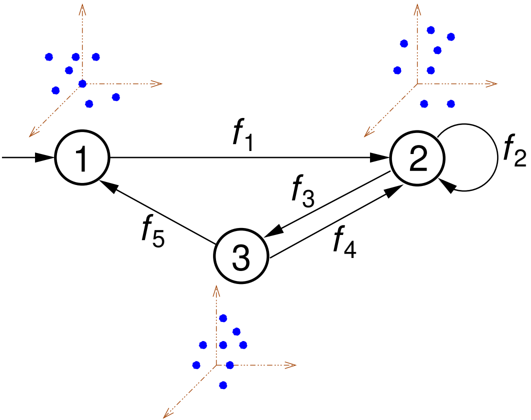
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



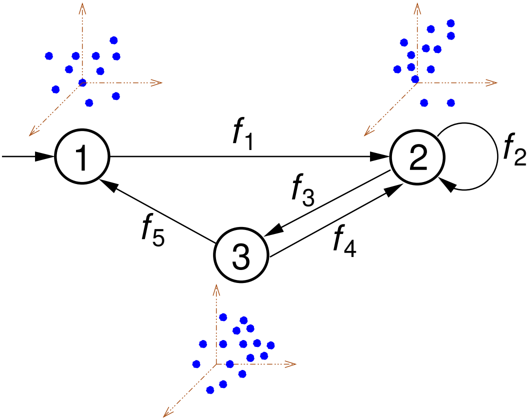
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



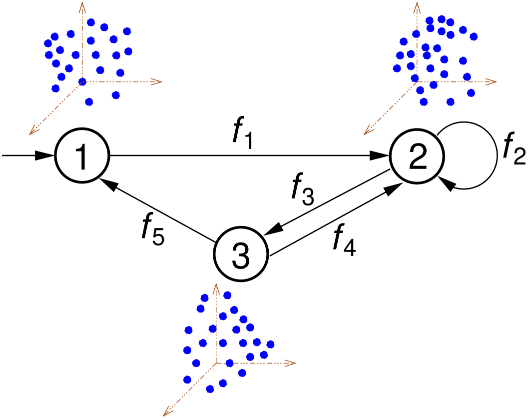
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



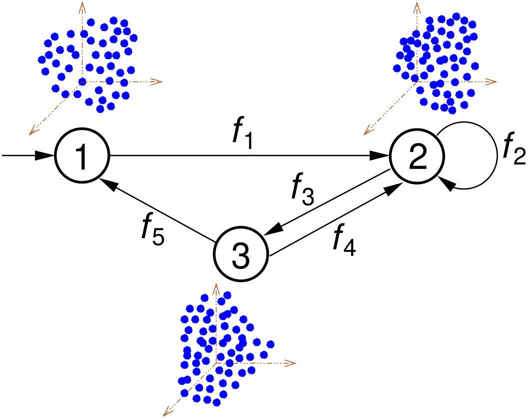
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



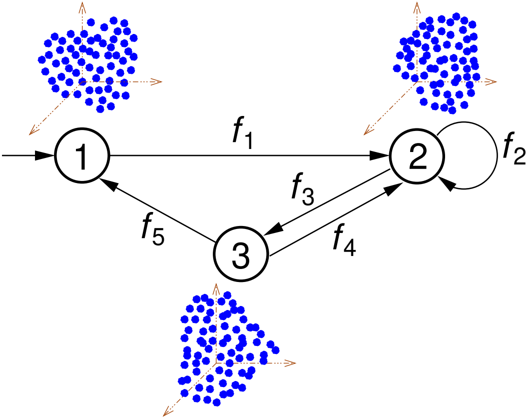
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



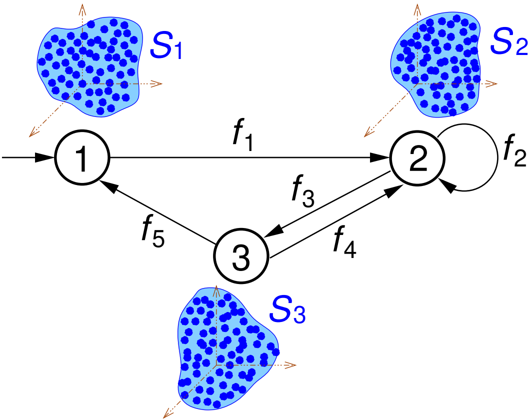
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



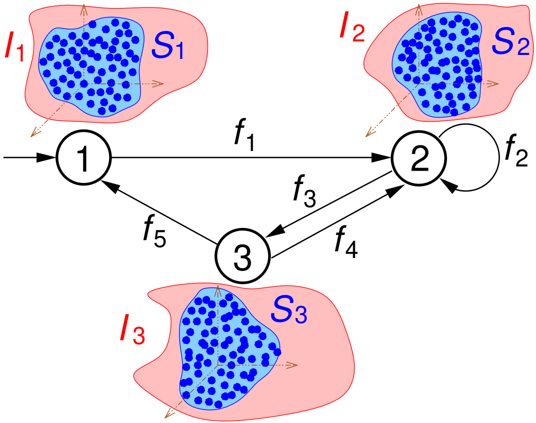
Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



Geometric Picture

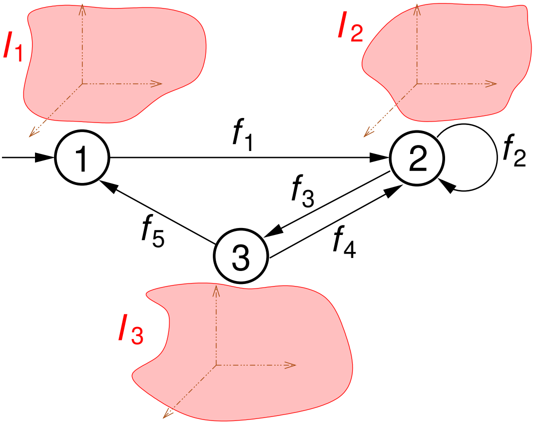
x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



$\langle I_1, I_2, I_3 \rangle$ is an **invariant**

Geometric Picture

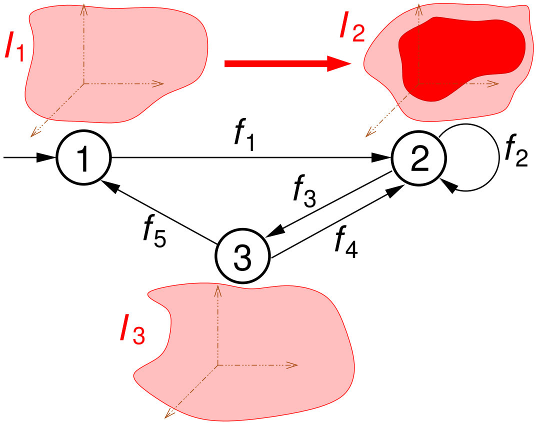
x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



$\langle I_1, I_2, I_3 \rangle$ is an **invariant**

Geometric Picture

x, y, z range over $\mathbb{Z}$ (or $\mathbb{Q}$)



$\langle I_1, I_2, I_3 \rangle$ is an **inductive invariant**

Undecidability

Theorem (Dufourd, Finkel, Schnoebelen 1998)

The boundedness problem for reset vector addition systems is undecidable.

Undecidability

Theorem (Dufourd, Finkel, Schnoebelen 1998)

The boundedness problem for reset vector addition systems is undecidable.

Theorem (Hrushovski, Ouaknine, Pouly, W. 20)

There is no algorithm that computes the Zariski closure of the reachable set of a polynomial program.

Undecidability

Theorem (Dufourd, Finkel, Schnoebelen 1998)

The boundedness problem for reset vector addition systems is undecidable.

Theorem (Hrushovski, Ouaknine, Pouly, W. 20)

There is no algorithm that computes the Zariski closure of the reachable set of a polynomial program.

- Simulate reset VAS by polynomial program:

Undecidability

Theorem (Dufourd, Finkel, Schnoebelen 1998)

The boundedness problem for reset vector addition systems is undecidable.

Theorem (Hrushovski, Ouaknine, Pouly, W. 20)

There is no algorithm that computes the Zariski closure of the reachable set of a polynomial program.

- Simulate reset VAS by polynomial program:
- Represent VAS configuration (a, b) "projectively" as (az, bz, z), $z \neq 0$:

$$f(x, y, z) = ((x - z)x, yx, zx)$$

Undecidability

Theorem (Dufourd, Finkel, Schnoebelen 1998)

The boundedness problem for reset vector addition systems is undecidable.

Theorem (Hrushovski, Ouaknine, Pouly, W. 20)

There is no algorithm that computes the Zariski closure of the reachable set of a polynomial program.

- Simulate reset VAS by polynomial program:
- Represent VAS configuration (a, b) "projectively" as (az, bz, z), $z \neq 0$:

$$f(x, y, z) = ((x - z)x, yx, zx)$$

- VAS is bounded iff the Zariski closure has dimension ≤ 1

Affine Invariants for Affine Programs

Affine Relationships Among Variables of a Program*

Michael Karr

Received May 8, 1974

Summary. Several optimizations of programs can be performed when in certain regions of a program equality relationships hold between a linear combination of the variables of the program and a constant. This paper presents a practical approach to detecting these relationships by considering the problem from the viewpoint of linear algebra. Key to the practicality of this approach is an algorithm for the calculation of the "sum" of linear subspaces.

Theorem (Karr 76)

There is an algorithm that computes, for any given affine program over $\mathbb{Q}$, its **strongest affine inductive invariant**.

Polynomial Invariants for Affine Programs

A Note on Karr's Algorithm

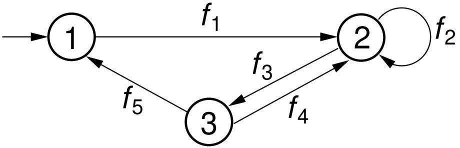
Markus Müller-Olm[1*] and Helmut Seidl[2]

Abstract. We give a simple formulation of Karr's algorithm for computing all affine relationships in affine programs. This simplified algorithm runs in time $\mathcal{O}(nk^3)$ where n is the program size and k is the number of program variables assuming unit cost for arithmetic operations. This improves upon the original formulation by a factor of k. Moreover, our re-formulation avoids exponential growth of the lengths of intermediately occurring numbers (in binary representation) and uses less complicated elementary operations. We also describe a generalization that determines all polynomial relations up to degree d in time $\mathcal{O}(nk^{3d})$.

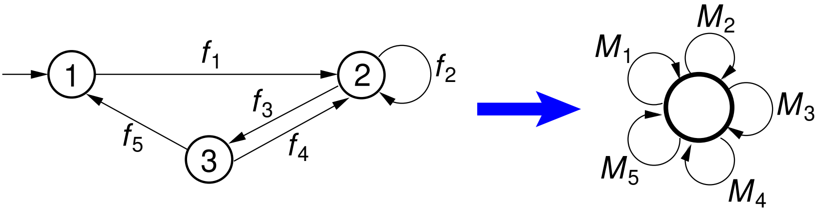
Theorem (ICALP 2004)

There is an algorithm that computes, for any given affine program over $\mathbb{Q}$, all its **polynomial invariants** *up to any* **fixed degree** *d.*

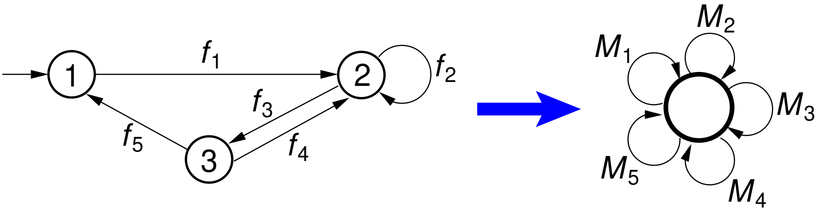
From Affine Programs to Linear Semigroups



From Affine Programs to Linear Semigroups



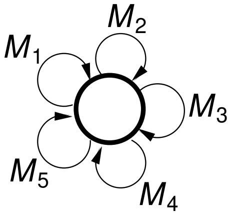
From Affine Programs to Linear Semigroups



each $M_i \in \mathbb{Q}^{d \times d}$

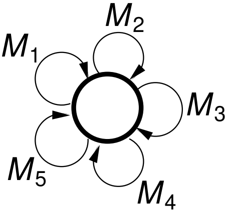
Zariski Closure of Linear Semigroups

- $M_1, \ldots, M_k \in \mathbb{Q}^{d \times d}$



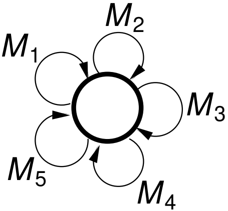
Zariski Closure of Linear Semigroups

- $M_1, \ldots, M_k \in \mathbb{Q}^{d \times d}$
- Linear semigroup $\langle M_1, \ldots, M_k \rangle \subseteq \mathbb{Q}^{d \times d}$



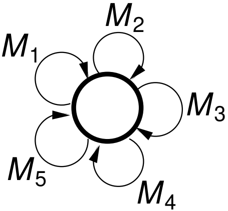
Zariski Closure of Linear Semigroups

- $M_1, \ldots, M_k \in \mathbb{Q}^{d \times d}$
- Linear semigroup $\langle M_1, \ldots, M_k \rangle \subseteq \mathbb{Q}^{d \times d}$
- Zariski closure $\overline{\langle M_1, \ldots, M_k \rangle} \subseteq \mathbb{R}^{d \times d}$



Zariski Closure of Linear Semigroups

- $M_1, \ldots, M_k \in \mathbb{Q}^{d \times d}$
- Linear semigroup $\langle M_1, \ldots, M_k \rangle \subseteq \mathbb{Q}^{d \times d}$
- Zariski closure $\overline{\langle M_1, \ldots, M_k \rangle} \subseteq \mathbb{R}^{d \times d}$

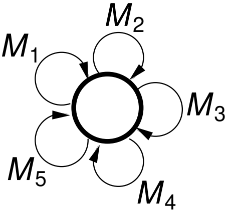


Theorem (Hrushovski, Ouaknine, Pouly, W. 18)

There is an algorithm that computes $\overline{\langle M_1, \ldots, M_k \rangle}$ (represented as the zero set of a list of polynomials $p_1, \ldots, p_m \in \mathbb{Z}[x_{1,1}, \ldots, x_{d,d}]$).

Zariski Closure of Linear Semigroups

- $M_1, \ldots, M_k \in \mathbb{Q}^{d \times d}$
- Linear semigroup $\langle M_1, \ldots, M_k \rangle \subseteq \mathbb{Q}^{d \times d}$
- Zariski closure $\overline{\langle M_1, \ldots, M_k \rangle} \subseteq \mathbb{R}^{d \times d}$



Theorem (Hrushovski, Ouaknine, Pouly, W. 18)

There is an algorithm that computes $\overline{\langle M_1, \ldots, M_k \rangle}$ (represented as the zero set of a list of polynomials $p_1, \ldots, p_m \in \mathbb{Z}[x_{1,1}, \ldots, x_{d,d}]$).

Corollary

There is an algorithm that computes the set of all polynomial invariants of an affine program.

Main Ingredients for the Group Case

Theorem (Masser 1988)

Given algebraic numbers $\lambda_1, \ldots, \lambda_k$, there is a procedure to compute the set of **multiplicative relations**

$$\left\{(n_1, \ldots, n_k) \in \mathbb{Z}^k : \lambda_1^{n_1} \cdots \lambda_k^{n_k} = 1\right\}.$$

Main Ingredients for the Group Case

Theorem (Masser 1988)

Given algebraic numbers $\lambda_1, \ldots, \lambda_k$, there is a procedure to compute the set of **multiplicative relations**

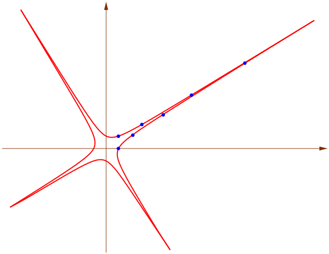
$$\left\{(n_1, \ldots, n_k) \in \mathbb{Z}^k : \lambda_1^{n_1} \cdots \lambda_k^{n_k} = 1\right\}.$$

Theorem (Schur 1911)

Every finitely generated periodic subgroup of $\mathrm{GL}_n(\mathbb{C})$ *is finite.*

Polynomial Invariants: One-Generator Case

$x := 1;\ ;\ y := 0;$
while **true** do
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};$$



Polynomial invariant: $x^4 + y^4 - 2x^3y - x^2y^2 + 2xy^3 - 1 = 0$

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$:

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: eigenvalues $\phi_1 := \frac{1+\sqrt{5}}{2}$, $\phi_2 := \frac{1-\sqrt{5}}{2}$

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: eigenvalues $\phi_1 := \frac{1+\sqrt{5}}{2}$, $\phi_2 := \frac{1-\sqrt{5}}{2}$

$$\overline{\{A^n : n \in \mathbb{Z}\}} \quad =$$

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: eigenvalues $\phi_1 := \frac{1+\sqrt{5}}{2}$, $\phi_2 := \frac{1-\sqrt{5}}{2}$

$$\overline{\{A^n : n \in \mathbb{Z}\}} = \overline{\left\{ P^{-1} \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} P : n \in \mathbb{Z} \right\}}$$

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: eigenvalues $\phi_1 := \frac{1+\sqrt{5}}{2}$, $\phi_2 := \frac{1-\sqrt{5}}{2}$

$$\begin{aligned} \overline{\{A^n : n \in \mathbb{Z}\}} &= \overline{\left\{P^{-1} \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} P : n \in \mathbb{Z}\right\}} \\ &= P^{-1} \overline{\left\{\begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} : n \in \mathbb{Z}\right\}} P \end{aligned}$$

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: eigenvalues $\phi_1 := \frac{1+\sqrt{5}}{2}$, $\phi_2 := \frac{1-\sqrt{5}}{2}$

$$\begin{aligned}
\overline{\{A^n : n \in \mathbb{Z}\}} &= \overline{\left\{ P^{-1} \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} P : n \in \mathbb{Z} \right\}} \\
&= P^{-1} \overline{\left\{ \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} : n \in \mathbb{Z} \right\}} P \\
&= P^{-1} \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : \begin{array}{l} x, y \in \mathbb{R}, \\ (xy-1)(xy+1) = 0 \end{array} \right\} P
\end{aligned}$$

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: eigenvalues $\phi_1 := \frac{1+\sqrt{5}}{2}$, $\phi_2 := \frac{1-\sqrt{5}}{2}$

$$\begin{aligned}
\overline{\{A^n : n \in \mathbb{Z}\}} &= \overline{\left\{ P^{-1} \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} P : n \in \mathbb{Z} \right\}} \\
&= P^{-1} \overline{\left\{ \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} : n \in \mathbb{Z} \right\}} P \\
&= P^{-1} \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : \begin{array}{l} x, y \in \mathbb{R}, \\ (xy-1)(xy+1) = 0 \end{array} \right\} P
\end{aligned}$$

- Closure determined by **multiplicative relation** $\phi_1^2 \phi_2^2 = 1$.

The One-Generator Case

Consider $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: eigenvalues $\phi_1 := \frac{1+\sqrt{5}}{2}$, $\phi_2 := \frac{1-\sqrt{5}}{2}$

$$\begin{aligned}
\overline{\{A^n : n \in \mathbb{Z}\}} &= \overline{\left\{ P^{-1} \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} P : n \in \mathbb{Z} \right\}} \\
&= P^{-1} \overline{\left\{ \begin{pmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{pmatrix} : n \in \mathbb{Z} \right\}} P \\
&= P^{-1} \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : \begin{array}{l} x, y \in \mathbb{R}, \\ (xy-1)(xy+1) = 0 \end{array} \right\} P
\end{aligned}$$

- Closure determined by **multiplicative relation** $\phi_1^2 \phi_2^2 = 1$.
- Two **irreducible components**, which are **cosets**.

The General Algorithm

Input: $A_1, \ldots, A_k \in \mathsf{GL}_n(\mathbb{C})$
Output: $\overline{\langle A_1, \ldots, A_k \rangle}$

The General Algorithm

Input: $A_1, \ldots, A_k \in \mathsf{GL}_n(\mathbb{C})$
Output: $\overline{\langle A_1, \ldots, A_k \rangle}$

$\boldsymbol{S} := \emptyset$
$\boldsymbol{H} := \{I\}$

The General Algorithm

Input: $A_1, \dots, A_k \in \mathrm{GL}_n(\mathbb{C})$
Output: $\overline{\langle A_1, \dots, A_k \rangle}$

$\boldsymbol{S} := \emptyset$
$\boldsymbol{H} := \{I\}$

for $A \in \langle A_1, \dots, A_k \rangle$ do

The General Algorithm

Input: $A_1, \ldots, A_k \in \mathsf{GL}_n(\mathbb{C})$
Output: $\overline{\langle A_1, \ldots, A_k \rangle}$

$\boldsymbol{S} := \emptyset$
$\boldsymbol{H} := \{I\}$

for $A \in \langle A_1, \ldots, A_k \rangle$ do

$\quad \boldsymbol{S} := \boldsymbol{S} \cup \{A\}$

The General Algorithm

Input: $A_1, \ldots, A_k \in \mathrm{GL}_n(\mathbb{C})$
Output: $\overline{\langle A_1, \ldots, A_k \rangle}$

$\boldsymbol{S} := \emptyset$
$\boldsymbol{H} := \{I\}$
for $A \in \langle A_1, \ldots, A_k \rangle$ do
  $\boldsymbol{S} := \boldsymbol{S} \cup \{A\}$
  $\boldsymbol{H} := \overline{\boldsymbol{H} \cdot \overline{\langle A \rangle}_{Id}}$

The General Algorithm

Input: $A_1, \ldots, A_k \in \mathrm{GL}_n(\mathbb{C})$
Output: $\overline{\langle A_1, \ldots, A_k \rangle}$

$\boldsymbol{S} := \emptyset$
$\boldsymbol{H} := \{I\}$
for $A \in \langle A_1, \ldots, A_k \rangle$ do
$\quad \boldsymbol{S} := \boldsymbol{S} \cup \{A\}$
$\quad \boldsymbol{H} := \overline{\boldsymbol{H} \cdot \overline{\langle A \rangle}_{Id}}$
$\quad$ repeat

$$\boldsymbol{H} := \overline{\boldsymbol{H} \cdot \boldsymbol{H} \cdot A_1 \boldsymbol{H} A_1^{-1} \cdots A_k \boldsymbol{H} A_k^{-1}}$$

$\quad$ until $\boldsymbol{H}$ stabilizes
end

The General Algorithm

Input: $A_1, \ldots, A_k \in \mathrm{GL}_n(\mathbb{C})$
Output: $\overline{\langle A_1, \ldots, A_k \rangle}$

$\boldsymbol{S} := \emptyset$
$\boldsymbol{H} := \{I\}$
for $A \in \langle A_1, \ldots, A_k \rangle$ do
  $\boldsymbol{S} := \boldsymbol{S} \cup \{A\}$
  $\boldsymbol{H} := \overline{\boldsymbol{H} \cdot \overline{\langle A \rangle}_{Id}}$
  repeat

$$\boldsymbol{H} := \overline{\boldsymbol{H} \cdot \boldsymbol{H} \cdot A_1 \boldsymbol{H} A_1^{-1} \cdots A_k \boldsymbol{H} A_k^{-1}}$$

  until $\boldsymbol{H}$ stabilizes
end

- $\boldsymbol{H}$ irreducible & $\boldsymbol{H} \triangleleft \langle A_1, \ldots, A_k \rangle \boldsymbol{H}$
- Eventually $\langle A_1, \ldots, A_k \rangle \boldsymbol{H} / \boldsymbol{H}$ is periodic.

Motivating Example for the Semigroup Case

Define $\boldsymbol{G} := \overline{\langle S, T, E \rangle}$, where

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad E := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Motivating Example for the Semigroup Case

Define $\boldsymbol{G} := \overline{\langle S, T, E \rangle}$, where

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad E := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then $\boldsymbol{G} = \{M \in \mathrm{M}_2(\mathbb{R}) : \det(M) \in \{0, 1\}\}$.

Motivating Example for the Semigroup Case

Define $\boldsymbol{G} := \overline{\langle S, T, E \rangle}$, where

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad E := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then $\boldsymbol{G} = \{M \in \mathrm{M}_2(\mathbb{R}) : \det(M) \in \{0, 1\}\}$.

Indeed, since

$$\{M \in \boldsymbol{G} : \mathrm{rank}(M) = 2\} = \overline{\langle S, T \rangle} = \overline{\mathrm{SL}_2(\mathbb{Z})} = \mathrm{SL}_2(\mathbb{R}),$$

Motivating Example for the Semigroup Case

Define $\boldsymbol{G} := \overline{\langle S, T, E \rangle}$, where

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad E := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then $\boldsymbol{G} = \{M \in \mathrm{M}_2(\mathbb{R}) : \det(M) \in \{0, 1\}\}$.

Indeed, since

$$\{M \in \boldsymbol{G} : \mathrm{rank}(M) = 2\} = \overline{\langle S, T \rangle} = \overline{\mathrm{SL}_2(\mathbb{Z})} = \mathrm{SL}_2(\mathbb{R}),$$

we have that $\{M \in \boldsymbol{G} : \mathrm{rank}(M) < 2\}$ is generated by

$$\{MEM', ME, EM : M, M' \in \mathrm{SL}_2(\mathbb{R})\}.$$

From Groups to Groupoids

Algebraic semigroup $\mathcal{S} \subseteq M_n(\mathbb{R})$:

$$\mathcal{S}_r := \{A \in \mathcal{S} : \mathrm{rank}(A) = r\} \ .$$

From Groups to Groupoids

Algebraic semigroup $\mathcal{S} \subseteq M_n(\mathbb{R})$:

$$\mathcal{S}_r := \{A \in \mathcal{S} : \mathrm{rank}(A) = r\} \ .$$

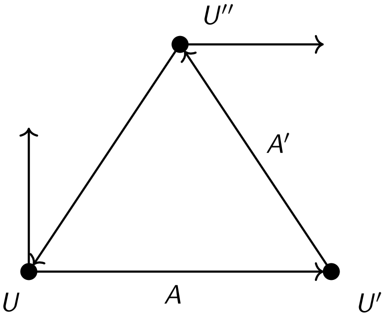
Consider $\mathcal{S}_r$ as a **category**:

From Groups to Groupoids

Algebraic semigroup $\mathcal{S} \subseteq M_n(\mathbb{R})$:

$$\mathcal{S}_r := \{A \in \mathcal{S} : \mathrm{rank}(A) = r\} \ .$$

Consider $\mathcal{S}_r$ as a **category**:

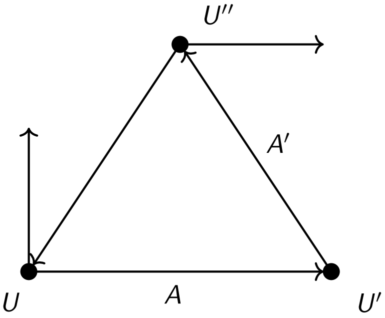


From Groups to Groupoids

Algebraic semigroup $\mathcal{S} \subseteq M_n(\mathbb{R})$:

$$\mathcal{S}_r := \{A \in \mathcal{S} : \mathrm{rank}(A) = r\} \ .$$

Consider $\mathcal{S}_r$ as a **category**:



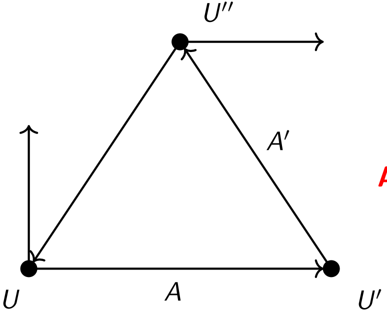
Object $U \subseteq \mathbb{C}^n$, $\dim(U) = r$

From Groups to Groupoids

Algebraic semigroup $\mathcal{S} \subseteq M_n(\mathbb{R})$:

$$\mathcal{S}_r := \{A \in \mathcal{S} : \mathrm{rank}(A) = r\} \ .$$

Consider $\mathcal{S}_r$ as a **category**:



Object $U \subseteq \mathbb{C}^n$, $\dim(U) = r$

Arrow $U \to V \ : \ A \in \mathcal{S}_r$ s.t. $A(U) = V$

Properties of $\mathcal{S}_r$

- Each non-trivial SCC is a groupoid.

Properties of $\mathcal{S}_r$

- Each non-trivial SCC is a groupoid.
- The number of non-trivial SCCs is at most $\binom{n}{r}$.

Properties of $\mathcal{S}_r$

- Each non-trivial SCC is a groupoid.
- The number of non-trivial SCCs is at most $\binom{n}{r}$.

Roughly Speaking . . .

Construct Zariski closure by induction on the rank. Generalise the algorithm of Derksen *et al.* from groups to groupoids.

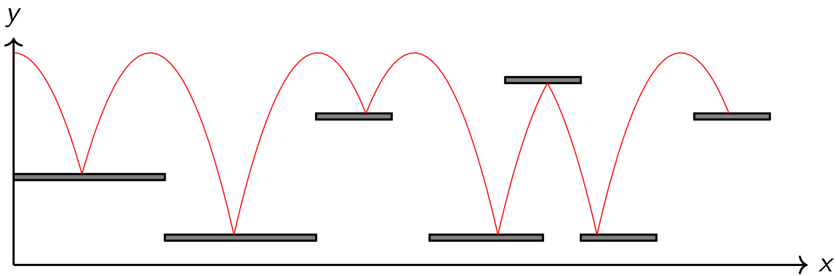
Theorem (Hrushovksi, Ouaknine, Pouly, W. 18)

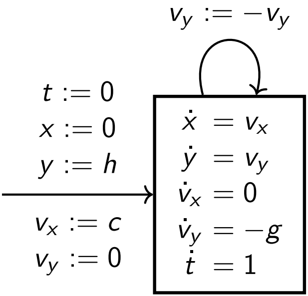
Given a finite set of rational square matrices of the same dimension, we can compute the Zariski closure of the semigroup that they generate.

Corollary

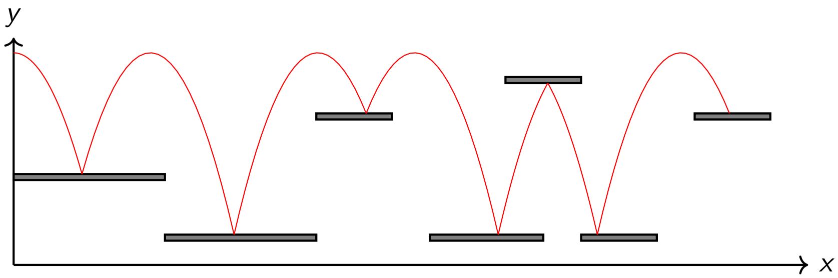
Given an affine program, we can compute for each location the ideal of all polynomial relations that hold at that location.

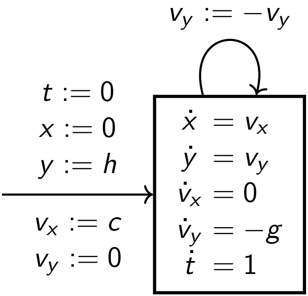
From Affine Programs to Hybrid Automata





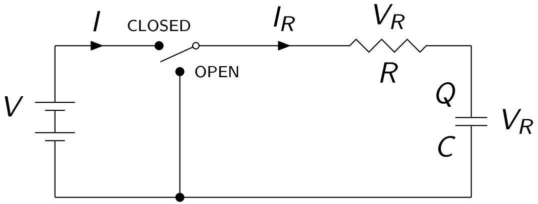
From Affine Programs to Hybrid Automata





$$\begin{aligned} v_x &= c \\ x &= tc \\ v_y^2 + 2g(y-h) &= 0 \end{aligned}$$

Hybrid Automata



OPEN

$$\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}$$

OPEN → CLOSED:

$$\begin{aligned} I &:= \frac{1}{R}(V - V_C) \\ I_R &:= \frac{1}{R}(V - V_C) \\ V_R &:= V - V_C \end{aligned}$$

CLOSED → OPEN:

$$\begin{aligned} I &:= 0 \\ I_R &:= -\frac{1}{R} V_C \\ V_R &:= -V_C \end{aligned}$$

CLOSED

$$\begin{aligned} \dot{I} &= -\frac{1}{RC} I_R \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}$$

A Challenge in Program Analysis

AUTOMATIC DISCOVERY OF LINEAR RESTRAINTS AMONG VARIABLES OF A PROGRAM

Patrick Cousot* and Nicolas Halbwachs**

Laboratoire d'Informatique, U.S.M.G., BP. 53
38041 Grenoble cédex, France

[...] use **inequality relationships** *to determine at compile time whether the value of an expression is within a specified range. This includes compile-time overflow, integer subrange, and array bound checking.*

A Challenge in Program Analysis

AUTOMATIC DISCOVERY OF LINEAR RESTRAINTS AMONG VARIABLES OF A PROGRAM

Patrick Cousot* and Nicolas Halbwachs**

Laboratoire d'Informatique, U.S.M.G., BP. 53
38041 Grenoble cédex, France

> *[...] use* **inequality relationships** *to determine at compile time whether the value of an expression is within a specified range. This includes compile-time overflow, integer subrange, and array bound checking.*

Compute inductive invariants determined by linear and polynomial inequalities?

Semi-Algebraic Invariant Synthesis

Computing Semi-Algebraic Invariants

Given $\mathcal{S} = \langle A_1, \ldots, A_k \rangle$, $x \in \mathbb{Q}^n$, and semi-algebraic $T \subseteq \mathbb{R}^n$, decide whether there exists semi-algebraic $I \subseteq \mathbb{R}^d$ such that:

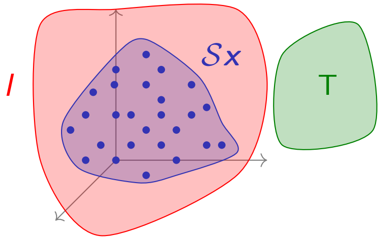
- $\boldsymbol{x} \in I$
- $\mathcal{S}I \subseteq I$
- $I \cap T = \emptyset$

Semi-Algebraic Invariant Synthesis

Computing Semi-Algebraic Invariants

Given $\mathcal{S} = \langle A_1, \ldots, A_k \rangle$, $x \in \mathbb{Q}^n$, and semi-algebraic $T \subseteq \mathbb{R}^n$, decide whether there exists semi-algebraic $I \subseteq \mathbb{R}^d$ such that:

- $\boldsymbol{x} \in I$
- $\mathcal{S}I \subseteq I$
- $I \cap T = \emptyset$

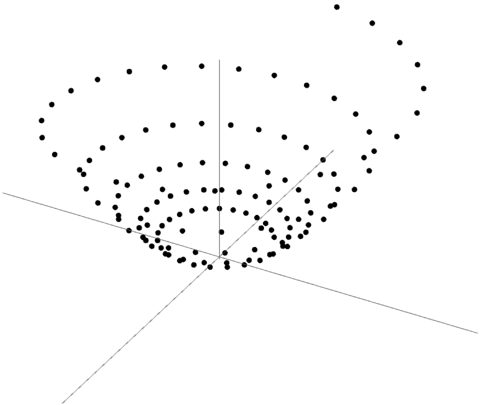


A Single Generator

$$A = \begin{pmatrix} 2\cos\theta & -2\sin\theta & 0 \\ 2\sin\theta & 2\cos\theta & 0 \\ 0 & 0 & 5 \end{pmatrix} \qquad \boldsymbol{x} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

A Single Generator

$$A = \begin{pmatrix} 2\cos\theta & -2\sin\theta & 0 \\ 2\sin\theta & 2\cos\theta & 0 \\ 0 & 0 & 5 \end{pmatrix} \qquad \boldsymbol{x} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$



Example

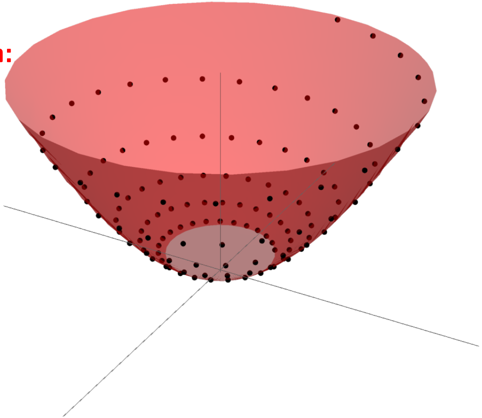
$$A^n \boldsymbol{x} = \begin{pmatrix} 2^n \cos n\theta \\ 2^n \sin n\theta \\ 5^n \end{pmatrix}$$

Example

$$A^n \boldsymbol{x} = \begin{pmatrix} 2^n \cos n\theta \\ 2^n \sin n\theta \\ 5^n \end{pmatrix}$$

Definable over-approximation:

$$\left\{ \begin{pmatrix} t^{\log 2} x \\ t^{\log 2} y \\ t^{\log 5} \end{pmatrix} : \begin{array}{l} t \geq 0, \\ x^2 + y^2 = 1 \end{array} \right\}$$

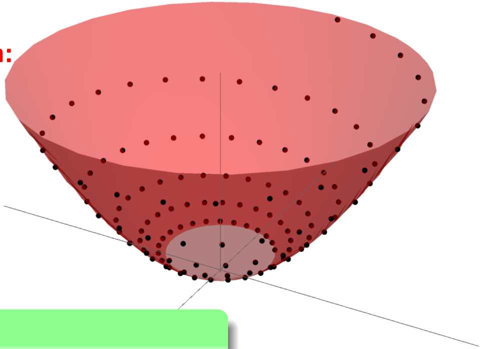


Example

$$A^n \boldsymbol{x} = \begin{pmatrix} 2^n \cos n\theta \\ 2^n \sin n\theta \\ 5^n \end{pmatrix}$$

Definable over-approximation:

$$\left\{ \begin{pmatrix} t^{\log 2} x \\ t^{\log 2} y \\ t^{\log 5} \end{pmatrix} : \begin{array}{l} t \geq 0, \\ x^2 + y^2 = 1 \end{array} \right\}$$



Key Observation:

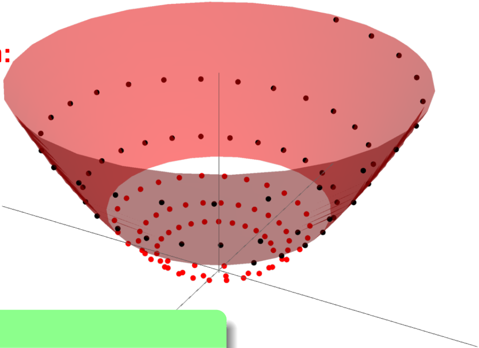
Every semi-algebraic invariant I must contain the entire cone from some height onwards.

Example

$$A^n \boldsymbol{x} = \begin{pmatrix} 2^n \cos n\theta \\ 2^n \sin n\theta \\ 5^n \end{pmatrix}$$

Definable over-approximation:

$$\left\{ \begin{pmatrix} t^{\log 2} x \\ t^{\log 2} y \\ t^{\log 5} \end{pmatrix} : \begin{array}{l} t \geq 0, \\ x^2 + y^2 = 1 \end{array} \right\}$$



Key Observation:

Every semi-algebraic invariant I must contain the entire cone from some height onwards.

Definable Invariants

Every invertible matrix $A \in \mathbb{Q}^{d \times d}$ admits a decomposition

$$A = \underbrace{A_r}_{\exp(L)} \cdot A_u$$

such that

- all eigenvalues of A_r are positive real
- all eigenvalues of A_u have absolute value one
- A_r and A_u commute

Definable Invariants

Every invertible matrix $A \in \mathbb{Q}^{d \times d}$ admits a decomposition

$$A = \underbrace{A_r}_{\exp(L)} \cdot A_u$$

such that

- all eigenvalues of A_r are positive real
- all eigenvalues of A_u have absolute value one
- A_r and A_u commute

Given $t_0 \in \mathbb{R}$,

$$\mathcal{C}_{t_0} := \{\exp(Lt)B\boldsymbol{x} : t \geq t_0, B \in \overline{\langle A_u \rangle}\}$$

is an inductive invariant, definable in $\mathfrak{R}_{\exp} = \langle \mathbb{R}, +, \times, \exp \rangle$.

Minimal Families of Invariants

Proposition

Given A and $\boldsymbol{x}$, there is a family of sets $C_t \subseteq \mathbb{R}^n$, $t \geq 0$, uniformly definable in $\mathfrak{R}_{\mathrm{exp}}$ s.t.

Minimal Families of Invariants

Proposition

Given A and $\boldsymbol{x}$, there is a family of sets $C_t \subseteq \mathbb{R}^n$, $t \geq 0$, uniformly definable in $\mathfrak{R}_{\exp}$ s.t.

1. *C_t is an inductive invariant, containing $\{A^n \boldsymbol{x} : n \geq t\}$.*

Minimal Families of Invariants

Proposition

Given A and $\boldsymbol{x}$, there is a family of sets $C_t \subseteq \mathbb{R}^n$, $t \geq 0$, uniformly definable in $\mathfrak{R}_{\exp}$ s.t.

1. *C_t is an inductive invariant, containing $\{A^n \boldsymbol{x} : n \geq t\}$.*
2. *Every semialgebraic invariant I contains some C_t.*

Minimal Families of Invariants

Proposition

Given A and $\boldsymbol{x}$, there is a family of sets $C_t \subseteq \mathbb{R}^n$, $t \geq 0$, uniformly definable in $\mathfrak{R}_{\exp}$ s.t.

1. *C_t is an inductive invariant, containing $\{A^n \boldsymbol{x} : n \geq t\}$.*
2. *Every semialgebraic invariant I contains some C_t.*
3. *For semialgebraic T, the truth of $\exists t \cdot C_t \cap T = \emptyset$ can be decided* **unconditionally**.

Minimal Families of Invariants

Proposition

Given A and $\boldsymbol{x}$, there is a family of sets $C_t \subseteq \mathbb{R}^n$, $t \geq 0$, uniformly definable in $\mathfrak{R}_{\exp}$ s.t.

1. *C_t is an inductive invariant, containing $\{A^n \boldsymbol{x} : n \geq t\}$.*
2. *Every semialgebraic invariant I contains some C_t.*
3. *For semialgebraic T, the truth of $\exists t \cdot C_t \cap T = \emptyset$ can be decided* **unconditionally**.

Theorem (Almagor, Chistikov, Ouaknine, W. 18)

The semi-algebraic synthesis problem is decidable for a single matrix.

The Monniaux Problem

P. Cousot

N. Halbwachs

D. Monniaux

"Forty years of research on convex polyhedral invariants have focused, on the one hand, on identifying "easier" subclasses, on the other hand on heuristics for finding general convex polyhedra. These heuristics are however not guaranteed to find polyhedral inductive invariants when they exist. To our best knowledge, the existence of polyhedral inductive invariants has never been proved to be undecidable."

– David Monniaux, Acta Inf. 2019

Part II: Loop Termination

Termination of Linear Loops

Single-path linear loop:

$\mathbf{x} := \mathbf{a}$
while $\mathbf{A}\mathbf{x} \geq \boldsymbol{b}$ do
$\quad \mathbf{x} := \mathbf{B} \cdot \mathbf{x} + \boldsymbol{c}$

Termination of Linear Loops

Single-path linear loop:

$\mathbf{x} := \mathbf{a}$
while $\mathbf{A}\mathbf{x} \geq \boldsymbol{b}$ do
$\quad \mathbf{x} := \mathbf{B} \cdot \mathbf{x} + \boldsymbol{c}$

Termination Problem (R)

Instance: $\langle\ \mathbf{A},\ \mathbf{B},\ \mathbf{b},\ \mathbf{c},\ \rangle$
Question: Does the loop terminate for all $\boldsymbol{a} \in R$?

Termination of Linear Loops

Single-path linear loop:

$\mathbf{x} := \mathbf{a}$
while $\mathbf{A}\mathbf{x} \geq \boldsymbol{b}$ do
    $\mathbf{x} := \mathbf{B} \cdot \mathbf{x} + \boldsymbol{c}$

Termination Problem (R)

Instance: $\langle\ \mathbf{A},\ \mathbf{B},\ \mathbf{b},\ \mathbf{c},\ \rangle$
Question: Does the loop terminate for all $\boldsymbol{a} \in R$?

Consider $R = \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \ldots$

History of the Problem

- Termination of linear constraint loops [Sohn and Gelder'91]

History of the Problem

- Termination of linear constraint loops [Sohn and Gelder'91]
  - $R = \{(x, y) \in \mathbb{R}^n \times \mathbb{R}^n : Ax + By \leq c\}$.

History of the Problem

- Termination of linear constraint loops [Sohn and Gelder'91]
  - $R = \{(x, y) \in \mathbb{R}^n \times \mathbb{R}^n : Ax + By \leq c\}$.
- Termination of linear loops over $\mathbb{R}$ [Tiwari'04]

History of the Problem

- Termination of linear constraint loops [Sohn and Gelder'91]
  - $R = \{(x, y) \in \mathbb{R}^n \times \mathbb{R}^n : Ax + By \leq c\}$.
- Termination of linear loops over $\mathbb{R}$ [Tiwari'04]
- Termination of linear loops over $\mathbb{Q}$ [Braverman'06]

History of the Problem

- Termination of linear constraint loops [Sohn and Gelder'91]
  - $R = \{(x, y) \in \mathbb{R}^n \times \mathbb{R}^n : Ax + By \leq c\}$.
- Termination of linear loops over $\mathbb{R}$ [Tiwari'04]
- Termination of linear loops over $\mathbb{Q}$ [Braverman'06]
- Termination over $\mathbb{Z}$ conjectured decidable [Tiwari'04, Braverman'06]

Termination Depends on the Numerical Domain

Loop that is terminating over $\mathbb{Q}$ but not $\mathbb{R}$:

Termination Depends on the Numerical Domain

Loop that is terminating over $\mathbb{Q}$ but not $\mathbb{R}$:

$$\begin{array}{rl} \textbf{while} & 4x + y > 0 \\ \textbf{do} & \begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} -2 & 4 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{array}$$

Termination Depends on the Numerical Domain

Loop that is terminating over $\mathbb{Q}$ but not $\mathbb{R}$:

$$\begin{array}{rl} \textbf{while} & 4x + y > 0 \\ \textbf{do} & \begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} -2 & 4 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{array}$$

- Eigenvalues $-1 - \sqrt{17}$ and $-1 + \sqrt{17}$.

Termination Depends on the Numerical Domain

Loop that is terminating over $\mathbb{Q}$ but not $\mathbb{R}$:

$$\begin{array}{rl} \textbf{while} & 4x + y > 0 \\ \textbf{do} & \begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} -2 & 4 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{array}$$

- Eigenvalues $-1 - \sqrt{17}$ and $-1 + \sqrt{17}$.
- Eigenvectors $\begin{pmatrix} -1 - \sqrt{17} \\ 4 \end{pmatrix}$ and $\begin{pmatrix} -1 + \sqrt{17} \\ 4 \end{pmatrix}$.

Termination vs Positivity

while $x_5 - x_6 \geq 0$

do $$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \leftarrow \begin{pmatrix} -\frac{19}{25} & -\frac{114}{125} & \frac{114}{125} & \frac{19}{25} & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}$$

Termination vs Positivity

$$\textbf{while} \quad x_5 - x_6 \geq 0$$

$$\textbf{do} \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \leftarrow \begin{pmatrix} -\frac{19}{25} & -\frac{114}{125} & \frac{114}{125} & \frac{19}{25} & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}$$

Termination vs Positivity

$$\textbf{while} \quad x_5 - x_6 \geq 0$$

$$\textbf{do} \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \leftarrow \begin{pmatrix} -\frac{19}{25} & -\frac{114}{125} & \frac{114}{125} & \frac{19}{25} & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}$$

Classify $\boldsymbol{a} \in \mathbb{R}^6$ as terminating, non-terminating, eventually non-terminating

Termination vs Positivity

$$\textbf{while} \quad x_5 - x_6 \geq 0$$

$$\textbf{do} \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \leftarrow \begin{pmatrix} -\frac{19}{25} & -\frac{114}{125} & \frac{114}{125} & \frac{19}{25} & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}$$

Classify $\boldsymbol{a} \in \mathbb{R}^6$ as terminating, non-terminating, eventually non-terminating

E.g., if $\boldsymbol{a} = (\ldots)$, then

$$\boldsymbol{e}_5^\top A^n \boldsymbol{a} := \frac{33}{8} + \lambda_1^n + \overline{\lambda_1^n} + 2\lambda_2^n + \overline{2\lambda_2^n},$$

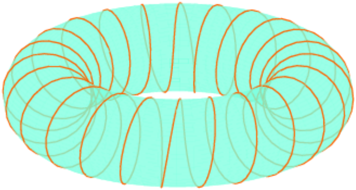
where $\lambda_1 = \frac{-3+4i}{5}$ and $\lambda_2 = \frac{-7+24i}{25}$.

Taking the Closure

Define $f_{\boldsymbol{a}} : \mathbb{T}^2 \to \mathbb{R}$ by

$$f_{\boldsymbol{a}}(z_1, z_2) = \frac{33}{8} + z_1 + \overline{z_1} + 2z_2 + 2\overline{z_2}\,.$$

Then $\boldsymbol{e}_5^\top A^n \boldsymbol{a} = f_{\boldsymbol{a}}(\lambda_1^n, \lambda_2^n)$.

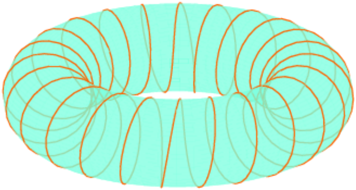


Taking the Closure

Define $f_{\boldsymbol{a}} : \mathbb{T}^2 \to \mathbb{R}$ by

$$f_{\boldsymbol{a}}(z_1, z_2) = \tfrac{33}{8} + z_1 + \overline{z_1} + 2z_2 + 2\overline{z_2}\,.$$

Then $\boldsymbol{e}_5^\top A^n \boldsymbol{a} = f_{\boldsymbol{a}}(\lambda_1^n, \lambda_2^n)$.



By **Kronecker's Theorem** on simultaneous Diophantine approximation:

$$\mathrm{Cl}\{(\lambda_1^n, \lambda_2^n) : n \in \mathbb{N}\} = \underbrace{\{(z_1, z_2) \in \mathbb{T}^2 : z_1^2 z_2 = 1\}}_{S}$$

Critical Points

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) < 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is terminating}$$

Critical Points

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) < 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is terminating}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) > 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is eventually non-terminating.}$$

Critical Points

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) < 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is terminating}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) > 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is eventually non-terminating.}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) = 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is ? ? ?}$$

Critical Points

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1,z_2) < 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is terminating}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1,z_2) > 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is eventually non-terminating.}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1,z_2) = 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is } \textbf{critical}$$

Critical Points

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) < 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is terminating}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) > 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is eventually non-terminating.}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) = 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is } \textbf{critical}$$

Theorem (Ouaknine, Sousa-Pinto, W. 15)

If the update matrix is diagonalisable or has dimension at most 5 then every rational critical point is eventually non-terminating.

Critical Points

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) < 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is terminating}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) > 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is eventually non-terminating.}$$

$$\inf_{(z_1,z_2)\in S} f_{\boldsymbol{a}}(z_1, z_2) = 0 \quad \Rightarrow \quad \boldsymbol{a} \text{ is } \textbf{critical}$$

Theorem (Ouaknine, Sousa-Pinto, W. 15)

If the update matrix is diagonalisable or has dimension at most 5 then every rational critical point is eventually non-terminating.

Proposition

The set of points that are either critical or eventually non-terminating is effectively semi-algebraic.

Flatness Theorem

Given convex $C \subseteq \mathbb{R}^d$, define

$$\mathrm{width}(C) := \inf_{\boldsymbol{v} \in \mathbb{Z}^d \setminus \{0\}} \sup_{\boldsymbol{x}, \boldsymbol{y} \in C} \boldsymbol{v}^\top (\boldsymbol{x} - \boldsymbol{y}) \,.$$

Flatness Theorem

Given convex $C \subseteq \mathbb{R}^d$, define

$$\mathrm{width}(C) := \inf_{\boldsymbol{v} \in \mathbb{Z}^d \setminus \{0\}} \sup_{\boldsymbol{x}, \boldsymbol{y} \in C} \boldsymbol{v}^\top (\boldsymbol{x} - \boldsymbol{y}) .$$

Lemma (Flatness Theorem)

If C is semi-algebraic and full dimensional then there exists $W > 0$ (depending on description of C) such that if $\mathrm{width}(C) > W$ then C contains an integer point.

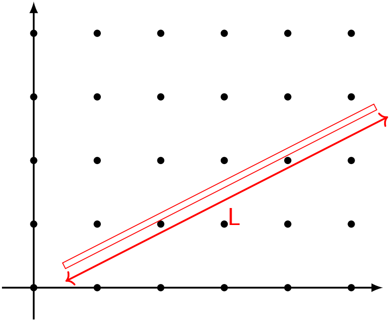
Flatness Theorem

Given convex $C \subseteq \mathbb{R}^d$, define

$$\operatorname{width}(C) := \inf_{\boldsymbol{v} \in \mathbb{Z}^d \setminus \{0\}} \sup_{\boldsymbol{x},\boldsymbol{y} \in C} \boldsymbol{v}^\top (\boldsymbol{x} - \boldsymbol{y}) .$$

Lemma (Flatness Theorem)

If C is semi-algebraic and full dimensional then there exists $W > 0$ (depending on description of C) such that if $\operatorname{width}(C) > W$ then C contains an integer point.



How does the lattice width vary as a function of L?

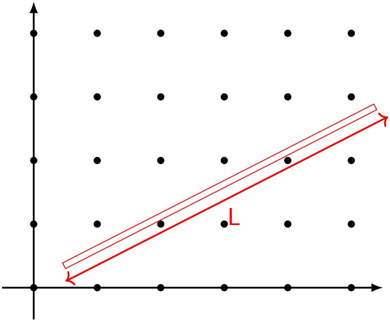
Flatness Theorem

Given convex $C \subseteq \mathbb{R}^d$, define

$$\mathrm{width}(C) := \inf_{\boldsymbol{v} \in \mathbb{Z}^d \setminus \{0\}} \sup_{\boldsymbol{x}, \boldsymbol{y} \in C} \boldsymbol{v}^\top (\boldsymbol{x} - \boldsymbol{y}) \,.$$

Lemma (Flatness Theorem)

If C is semi-algebraic and full dimensional then there exists $W > 0$ (depending on description of C) such that if $\mathrm{width}(C) > W$ then C contains an integer point.



How does the lattice width vary as a function of L?

Kronecker's Theorem is instrumental again!

Hilbert's Tenth Problem for Convex Sets

Theorem (Khachiyan, Porkolab'97)

It is decidable whether a given semi-algebraic set $C \subseteq \mathbb{R}^n$ *contains an integer point.*

Hilbert's Tenth Problem for Convex Sets

Theorem (Khachiyan, Porkolab'97)

It is decidable whether a given semi-algebraic set $C \subseteq \mathbb{R}^n$ contains an integer point.

- Assume C does not have an integer point:

Hilbert's Tenth Problem for Convex Sets

Theorem (Khachiyan, Porkolab'97)

It is decidable whether a given semi-algebraic set $C \subseteq \mathbb{R}^n$ contains an integer point.

- Assume C does not have an integer point:
- If C is not full dimensional, eliminiate a variable

Hilbert's Tenth Problem for Convex Sets

Theorem (Khachiyan, Porkolab'97)

It is decidable whether a given semi-algebraic set $C \subseteq \mathbb{R}^n$ contains an integer point.

- Assume C does not have an integer point:
- If C is not full dimensional, eliminiate a variable
- If C is not "fat", eliminate a variable

Handling Critical Points

Proposition

Suppose $\boldsymbol{a} \in \mathbb{R}^n$ *is critical. Then:*

Handling Critical Points

Proposition

Suppose $\boldsymbol{a} \in \mathbb{R}^n$ is critical. Then:

1. $A\boldsymbol{a}, A^2\boldsymbol{a}, A^3\boldsymbol{a}, \ldots$ *are all critical.*

Handling Critical Points

Proposition

Suppose $\boldsymbol{a} \in \mathbb{R}^n$ *is critical. Then:*

1. $A\boldsymbol{a}, A^2\boldsymbol{a}, A^3\boldsymbol{a}, \ldots$ *are all critical.*
2. *Every point in the relative interior of* $\mathrm{Conv}(\{\boldsymbol{a}, A\boldsymbol{a}, A^2\boldsymbol{a}, \ldots\})$ *is eventually non-terminating.*

Handling Critical Points

Proposition

Suppose $\boldsymbol{a} \in \mathbb{R}^n$ *is critical. Then:*

1. $A\boldsymbol{a}, A^2\boldsymbol{a}, A^3\boldsymbol{a}, \ldots$ *are all critical.*
2. *Every point in the relative interior of* $\mathrm{Conv}(\{\boldsymbol{a}, A\boldsymbol{a}, A^2\boldsymbol{a}, \ldots\})$ *is eventually non-terminating.*

Proposition

For all $\boldsymbol{a} \in \mathbb{Z}^n$, $\mathrm{Conv}(\{\boldsymbol{a}, A\boldsymbol{a}, A^2\boldsymbol{a}, \ldots\})$ *contains an integer point.*

Handling Critical Points

Proposition

Suppose $\boldsymbol{a} \in \mathbb{R}^n$ *is critical. Then:*

1. $A\boldsymbol{a}, A^2\boldsymbol{a}, A^3\boldsymbol{a}, \ldots$ *are all critical.*
2. *Every point in the relative interior of* $\mathrm{Conv}(\{\boldsymbol{a}, A\boldsymbol{a}, A^2\boldsymbol{a}, \ldots\})$ *is eventually non-terminating.*

Proposition

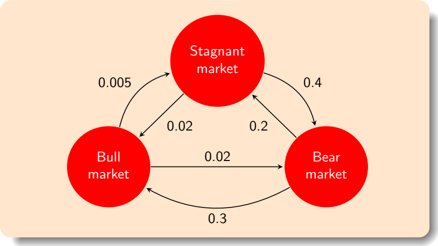
For all $\boldsymbol{a} \in \mathbb{Z}^n$, $\mathrm{Conv}(\{\boldsymbol{a}, A\boldsymbol{a}, A^2\boldsymbol{a}, \ldots\})$ *contains an integer point.*

Theorem (Hosseini, Ouaknine, W. 19)

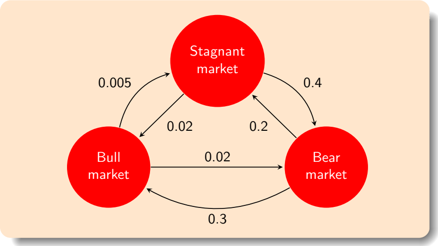
Termination of linear while loops over the integers is decidable.

Part III: Orbits in Continuous-Time

Reachability for Continuous-Time Markov Chains



Reachability for Continuous-Time Markov Chains

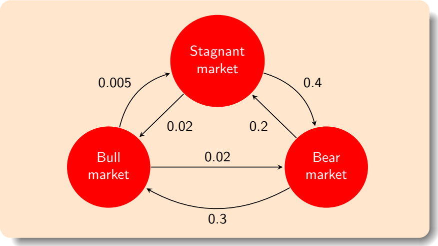


Distribution $P(t)$ at time t satisfies $P'(t) = P(t)Q$, where

$$Q = \begin{pmatrix} -0.025 & 0.02 & 0.005 \\ 0.3 & -0.5 & 0.2 \\ 0.02 & 0.4 & -0.42 \end{pmatrix}$$

is the **rate matrix**.

Reachability for Continuous-Time Markov Chains



Distribution $P(t)$ at time t satisfies $P'(t) = P(t)Q$, where

$$Q = \begin{pmatrix} -0.025 & 0.02 & 0.005 \\ 0.3 & -0.5 & 0.2 \\ 0.02 & 0.4 & -0.42 \end{pmatrix}$$

is the **rate matrix**.

"Is it ever more likely to be a Bear market than a Bull market?"

$$\exists t \, (P(t)_{\mathrm{Bear}} \geq P(t)_{\mathrm{Bull}})$$

Hitting a Hyperplane

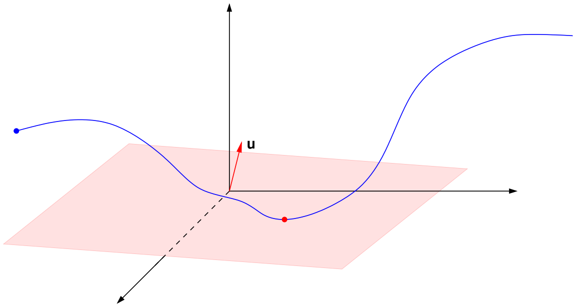
$\mathbf{x} : \mathbb{R}_{\geq 0} \to \mathbb{R}^k$
$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x}$

Hitting a Hyperplane

$\mathbf{x} : \mathbb{R}_{\geq 0} \to \mathbb{R}^k$
$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x}$
$\Rightarrow \quad \mathbf{x}(t) = \exp(\mathbf{A}t)\mathbf{x}(0)$

Hitting a Hyperplane

$$\mathbf{x} : \mathbb{R}_{\geq 0} \to \mathbb{R}^k$$
$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x}$$
$$\Rightarrow \quad \mathbf{x}(t) = \exp(\mathbf{A}t)\mathbf{x}(0)$$



$$f(t) \stackrel{\text{def}}{=} \mathbf{u}^{\mathsf{T}} \exp(\mathbf{A}t)\mathbf{x}(0)$$

Exponential Polynomials

Function f is an **exponential polynomial**:

$$f(t) \stackrel{\text{def}}{=} \mathbf{u}^{\mathsf{T}} \exp(\mathbf{A}t)\mathbf{x}(0)$$

Exponential Polynomials

Function f is an **exponential polynomial**:

$$f(t) \stackrel{\text{def}}{=} \mathbf{u}^{\mathsf{T}} \exp(\mathbf{A}t)\mathbf{x}(0) = \sum_{j=1}^{m} P_j(t) e^{\lambda_j t}$$

Exponential Polynomials

Function f is an **exponential polynomial**:

$$f(t) \stackrel{\text{def}}{=} \mathbf{u}^\mathsf{T} \exp(\mathbf{A}t)\mathbf{x}(0) = \sum_{j=1}^{m} P_j(t)e^{\lambda_j t}$$

Equivalently, f satisfies a **linear differential equation**:

$$f^{(k)}(t) + a_{k-1}f^{(k-1)}(t) + \ldots + a_1 f'(t) + a_0 f(t) = 0$$

Exponential Polynomials

Function f is an **exponential polynomial**:

$$f(t) \stackrel{\text{def}}{=} \mathbf{u}^{\mathsf{T}} \exp(\mathbf{A}t)\mathbf{x}(0) = \sum_{j=1}^{m} P_j(t) e^{\lambda_j t}$$

Equivalently, f satisfies a **linear differential equation**:

$$f^{(k)}(t) + a_{k-1} f^{(k-1)}(t) + \ldots + a_1 f'(t) + a_0 f(t) = 0$$

$$\text{Dimension} = \text{Order} = k$$

Zero Problems for Exponential Polynomials

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be given as above, with all coefficients algebraic.

Zero Problems for Exponential Polynomials

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be given as above, with all coefficients algebraic.

Bounded Zero Problem

Instance: f and bounded interval $[a, b]$
Question: Is there $t \in [a, b]$ such that $f(t) = 0$?

Zero Problems for Exponential Polynomials

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be given as above, with all coefficients algebraic.

Bounded Zero Problem

Instance: f and bounded interval $[a, b]$

Question: Is there $t \in [a, b]$ such that $f(t) = 0$?

Zero Problem

Instance: f

Question: Is there $t \in \mathbb{R}_{\geq 0}$ such that $f(t) = 0$?

Zero Problems for Exponential Polynomials

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be given as above, with all coefficients algebraic.

Bounded Zero Problem

Instance: f and bounded interval $[a, b]$

Question: Is there $t \in [a, b]$ such that $f(t) = 0$?

Zero Problem

Instance: f

Question: Is there $t \in \mathbb{R}_{\geq 0}$ such that $f(t) = 0$?

Infinite Zeros Problem

Instance: f

Question: Does f have infinitely many zeros in $\mathbb{R}_{\geq 0}$?

Zero Problems for Exponential Polynomials

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be given as above, with all coefficients algebraic.

Bounded Zero Problem

Instance: f and bounded interval $[a, b]$
Question: Is there $t \in [a, b]$ such that $f(t) = 0$?

Zero Problem

Instance: f
Question: Is there $t \in \mathbb{R}_{\geq 0}$ such that $f(t) = 0$?

Infinite Zeros Problem

Instance: f
Question: Does f have infinitely many zeros in $\mathbb{R}_{\geq 0}$?

- **Decidability open!** [Bell, Delvenne, Jungers, Blondel 2010]

Our Results

Theorem (Chonev, Ouaknine, W. 2015)

1. *Assuming Schanuel's Conjecture, Bounded Zero is decidable at all orders.*

Our Results

Theorem (Chonev, Ouaknine, W. 2015)

1. *Assuming Schanuel's Conjecture, Bounded Zero is decidable at all orders.*
2. *At order at most 8, Zero reduces to Bounded Zero.*

Our Results

Theorem (Chonev, Ouaknine, W. 2015)

1. *Assuming Schanuel's Conjecture, Bounded Zero is decidable at all orders.*
2. *At order at most 8, Zero reduces to Bounded Zero.*
3. *At order at most 8, Infinite Zeros is decidable.*

Our Results

Theorem (Chonev, Ouaknine, W. 2015)

1. *Assuming Schanuel's Conjecture, Bounded Zero is decidable at all orders.*
2. *At order at most 8, Zero reduces to Bounded Zero.*
3. *At order at most 8, Infinite Zeros is decidable.*
4. *At order 9, if Infinite Zeros is decidable then the Lagrange constant of any real algebraic number is computable.*

Our Results

Theorem (Chonev, Ouaknine, W. 2015)

1. *Assuming Schanuel's Conjecture, Bounded Zero is decidable at all orders.*
2. *At order at most 8, Zero reduces to Bounded Zero.*
3. *At order at most 8, Infinite Zeros is decidable.*
4. *At order 9, if Infinite Zeros is decidable then the Lagrange constant of any real algebraic number is computable.*

Schanuel's Conjecture

If $z_1, \ldots, z_n \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then the field $\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})$ has transcendence degree at least n over $\mathbb{Q}$.

The Bounded Zero Problem

Example

Let $f(t) := e^{(2+i)t} + e^{(2-i)t} - te^{-t}$. Then $f(t) = P(t, e^t, e^{it})$, where

$$P(x, y, z) = y^2 z + y^2 z^{-1} - xy^{-1}$$

The Bounded Zero Problem

Example

Let $f(t) := e^{(2+i)t} + e^{(2-i)t} - te^{-t}$. Then $f(t) = P(t, e^t, e^{it})$, where

$$P(x, y, z) = y^2 z + y^2 z^{-1} - xy^{-1}$$

Laurent-Polynomial Representation

Any exponential polynomial $f(t)$ can be written

$$f(t) = P(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t})$$

with

$$P \in \mathbb{C}[x, y_1^{\pm 1}, \ldots, y_m^{\pm 1}, z_1^{\pm 1}, \ldots, z_n^{\pm 1}]$$

and $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_n\}$ sets of real algebraic numbers linearly independent over $\mathbb{Q}$.

The Bounded Zero Problem

Example

Let $f(t) := e^{(2+i)t} + e^{(2-i)t} - te^{-t}$. Then $f(t) = P(t, e^t, e^{it})$, where

$$P(x, y, z) = y^2 z + y^2 z^{-1} - xy^{-1}$$

Laurent-Polynomial Representation

Any exponential polynomial $f(t)$ can be written

$$f(t) = P(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t})$$

with

$$P \in \mathbb{C}[x, y_1^{\pm 1}, \ldots, y_m^{\pm 1}, z_1^{\pm 1}, \ldots, z_n^{\pm 1}]$$

and $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_n\}$ sets of real algebraic numbers linearly independent over $\mathbb{Q}$. WLOG P is irreducible.

Applying Schanuel

Write

$$f(t) \quad = \quad P(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t}), \;\; P \text{ irreducible}$$

Applying Schanuel

Write

$$\begin{aligned} f(t) &= P(t, e^{a_1 t}, \dots, e^{a_m t}, e^{ib_1 t}, \dots, e^{ib_n t}), \text{ } P \text{ irreducible} \\ \overline{f(\overline{t})} &= Q(t, e^{a_1 t}, \dots, e^{a_m t}, e^{ib_1 t}, \dots, e^{ib_n t}), \text{ } Q \text{ irreducible} \end{aligned}$$

Applying Schanuel

Write

$$\begin{aligned} f(t) &= P(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t}), \ P \text{ irreducible} \\ \overline{f(\overline{t})} &= Q(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t}), \ Q \text{ irreducible} \end{aligned}$$

Two cases:

Applying Schanuel

Write

$$\begin{aligned} f(t) &= P(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t}),\ P \text{ irreducible} \\ \overline{f(\overline{t})} &= Q(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t}),\ Q \text{ irreducible} \end{aligned}$$

Two cases:

1. If P and Q are not associates then f has no real zeros by Schanuel's Conjecture.

Applying Schanuel

Write

$$\begin{aligned} f(t) &= P(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t}),\ P \text{ irreducible} \\ \overline{f(\bar{t})} &= Q(t, e^{a_1 t}, \ldots, e^{a_m t}, e^{ib_1 t}, \ldots, e^{ib_n t}),\ Q \text{ irreducible} \end{aligned}$$

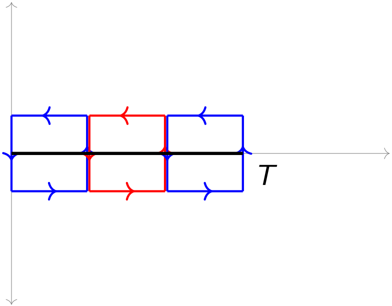
Two cases:

1. If P and Q are not associates then f has no real zeros by Schanuel's Conjecture.
2. If P and Q are associates, then complex zeros of f come in conjugate pairs. Real zeros are simple by Schanuel.

Bounded Zero Problem - An Argument Argument

Let $N =$ number of zeros of f inside closed contour C. Then

$$\int_C \frac{f'(z)}{f(z)} dz = 2\pi i N$$



Refine until N is odd or 0 for each square.

Diophantine Approximation

The **Lagrange constant** of $x \in \mathbb{R}$ is

$$L_\infty(x) = \liminf_{n \to \infty} n \|nx\|$$

Diophantine Approximation

The **Lagrange constant** of $x \in \mathbb{R}$ is

$$L_\infty(x) = \liminf_{n\to\infty} n \|nx\|$$

We have $0 \leq L_\infty(x) \leq \frac{1}{\sqrt{5}}$ for all $x \in \mathbb{R}$.

The **Lagrange constant** of $x \in \mathbb{R}$ is

$$L_\infty(x) = \liminf_{n \to \infty} n \|nx\|$$

We have $0 \leq L_\infty(x) \leq \frac{1}{\sqrt{5}}$ for all $x \in \mathbb{R}$.

"Is there a real algebraic number α of degree greater than two with $L(\alpha) = 0$? Do all such numbers have $L(\alpha) = 0$?"

R. K. Guy 2004 (paraphrased)

A Hard Case at Order 9

For α irrational, algebraic and c rational, define

$$\begin{aligned} f_1(t) &= e^t(1-\cos(t)) + t(1-\cos(\alpha t)) - c\sin(\alpha t) \\ f_2(t) &= e^t(1-\cos(t)) + t(1-\cos(\alpha t)) + c\sin(\alpha t) \\ f(t) &= \min\{f_1(t), f_2(t)\} \end{aligned}$$

A Hard Case at Order 9

For α irrational, algebraic and c rational, define

$$\begin{aligned} f_1(t) &= e^t(1-\cos(t)) + t(1-\cos(\alpha t)) - c\sin(\alpha t) \\ f_2(t) &= e^t(1-\cos(t)) + t(1-\cos(\alpha t)) + c\sin(\alpha t) \\ f(t) &= \min\{f_1(t), f_2(t)\} \end{aligned}$$

Proposition

1. $L_\infty(\alpha) < \frac{c}{2\pi^2}$ *implies* f *has infinitely many zeros*
2. $L_\infty(\alpha) > \frac{c}{2\pi^2}$ *implies* f *has finitely many zeros*

A Hard Case at Order 9

For α irrational, algebraic and c rational, define

$$\begin{aligned}
f_1(t) &= e^t(1-\cos(t)) + t(1-\cos(\alpha t)) - c\sin(\alpha t)\\
f_2(t) &= e^t(1-\cos(t)) + t(1-\cos(\alpha t)) + c\sin(\alpha t)\\
f(t) &= \min\{f_1(t), f_2(t)\}
\end{aligned}$$

Proposition

1. $L_\infty(\alpha) < \frac{c}{2\pi^2}$ *implies f has infinitely many zeros*
2. $L_\infty(\alpha) > \frac{c}{2\pi^2}$ *implies f has finitely many zeros*

Theorem

If the Zero Problem is decidable at order 9 then for any real algebraic number α, $L_\infty(\alpha)$ is computable.

Decidability Results at Low Order

Theorem

At order at most 8, Zero reduces to Bounded Zero, and Infinite Zeros is decidable.

Proof in a single picture:

Decidability Results at Low Order

Theorem

At order at most 8, Zero reduces to Bounded Zero, and Infinite Zeros is decidable.

Proof in a single picture:

Decidability Results at Low Order

Theorem

At order at most 8, Zero reduces to Bounded Zero, and Infinite Zeros is decidable.

Proof in a single picture:

Give procedure to decide whether f has infinitely many zeros and, if not, output T such that $f(t) \neq 0$ for all $t > T$.

Shrinking-Target Problem (I)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$f(t) \quad := \quad \cos^2(at - \psi_1) + \cos^2(bt - \psi_2) - e^{-t}$$

Shrinking-Target Problem (I)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$\begin{aligned} f(t) &:= \cos^2(at-\psi_1)+\cos^2(bt-\psi_2)-e^{-t} \\ \Gamma_t &:= \left\{(\theta_1,\theta_2)\in[0,2\pi]^2 : \cos^2(\theta_1-\psi_1)+\cos^2(\theta_2-\psi_2)\le e^{-t}\right\} \end{aligned}$$

Shrinking-Target Problem (I)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$\begin{aligned} f(t) &:= \cos^2(at - \psi_1) + \cos^2(bt - \psi_2) - e^{-t} \\ \Gamma_t &:= \left\{(\theta_1, \theta_2) \in [0, 2\pi]^2 : \cos^2(\theta_1 - \psi_1) + \cos^2(\theta_2 - \psi_2) \leq e^{-t}\right\} \end{aligned}$$

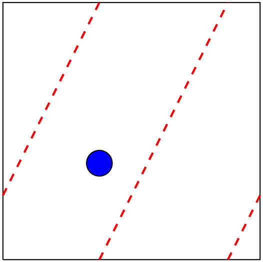
$$\exists^\infty t \, (at, bt) \in \Gamma_t \ ?$$

Shrinking-Target Problem (I)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$\begin{aligned} f(t) &:= \cos^2(at - \psi_1) + \cos^2(bt - \psi_2) - e^{-t} \\ \Gamma_t &:= \left\{(\theta_1, \theta_2) \in [0, 2\pi]^2 : \cos^2(\theta_1 - \psi_1) + \cos^2(\theta_2 - \psi_2) \le e^{-t}\right\} \end{aligned}$$

$$\exists^\infty t \, (at, bt) \in \Gamma_t \ ?$$



Shrinking-Target Problem (II)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$f(t) \quad := \quad (\cos(at) + 2\cos(bt))^2 - e^{-t}$$

Shrinking-Target Problem (II)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$\begin{aligned} f(t) &:= (\cos(at) + 2\cos(bt))^2 - e^{-t} \\ \Gamma_t &:= \left\{(\theta_1, \theta_2) \in [0, 2\pi]^2 : (\cos(\theta_1) + 2\cos(\theta_2))^2 \leq e^{-t}\right\} \end{aligned}$$

Shrinking-Target Problem (II)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$\begin{aligned} f(t) &:= (\cos(at) + 2\cos(bt))^2 - e^{-t} \\ \Gamma_t &:= \left\{(\theta_1, \theta_2) \in [0, 2\pi]^2 : (\cos(\theta_1) + 2\cos(\theta_2))^2 \leq e^{-t}\right\} \end{aligned}$$

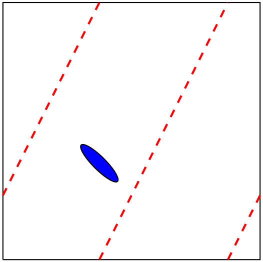
$$\exists^\infty t \, (at, bt) \in \Gamma_t \ ?$$

Shrinking-Target Problem (II)

Let $a, b \in \mathbb{R}$ be algebraic and linearly independent over $\mathbb{Q}$:

$$\begin{aligned} f(t) &:= (\cos(at) + 2\cos(bt))^2 - e^{-t} \\ \Gamma_t &:= \left\{(\theta_1, \theta_2) \in [0, 2\pi]^2 : (\cos(\theta_1) + 2\cos(\theta_2))^2 \leq e^{-t}\right\} \end{aligned}$$

$$\exists^\infty t \, (at, bt) \in \Gamma_t \; ?$$



A Landscape of Orbit Problems: Summary

Part I: **Invariants**. Compute all polynomial invariants of the orbit of a point under a finitely generated matrix semigroup.

Part II: **Termination**. Do all (integer) orbits under a single matrix escape a polyhedron?

Part III: **Reachability**. Does the orbit of a point under a one-parameter matrix semigroup reach a halfspace?

Tools: Kronecker, Masser, Baker, . . .