Specification and Verification of Linear Dynamical Systems: Advances and Challenges

Joël Ouaknine

Department of Computer Science, Oxford University

(Joint work with James Worrell)

FroCoS 2013
Nancy, France

Specification and Verification

$$M \vDash \varphi$$

Specification and Verification

$$M \models \varphi$$

M: linear dynamical systems

Specification and Verification

$$M \models \varphi$$

M: linear dynamical systems (discrete / continuous)

Specification and Verification

$$M \models \varphi$$

M: linear dynamical systems (discrete / continuous)

φ: ???

Termination of Simple Linear Programs

$\mathbf{x} := \mathbf{a};$
while $\mathbf{u} \cdot \mathbf{x} \neq 0$ do
$\quad \mathbf{x} := \mathbf{M} \cdot \mathbf{x};$

Termination of Simple Linear Programs

$\mathbf{x} := \mathbf{a};$
while $\mathbf{u} \cdot \mathbf{x} \neq 0$ do
    $\mathbf{x} := \mathbf{M} \cdot \mathbf{x};$

Termination Problem

Instance: $\langle\ \mathbf{a};\ \mathbf{u};\ \mathbf{M}\ \rangle$
Question: Does this program terminate?

Termination of Simple Linear Programs

Much work on this and related problems in the literature over the last three decades:

- Manna, Pnueli, Kannan, Lipton, Sagiv, Podelski, Rybalchenko, Cook, Dershowitz, Tiwari, Braverman, Kovács, Ben-Amram, Genaim, . . .
- Approaches include:
  - linear ranking functions
  - size-change termination methods
  - spectral techniques
  - . . .
- Tools include:

TERMINATOR
proof tools for termination and liveness

ACL2

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$(1, \quad 0, \quad 0, \quad 0)$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least 1/2 ?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob('being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$(1, \;\; 0, \;\; 0, \;\; 0) \cdot \mathbf{M} =$$
$$(0, \;\; 0.5, \;\; 0.2, \;\; 0.3)$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$\begin{aligned} (1, \;\; 0, \;\; 0, \;\; 0) \cdot \mathbf{M} &= \\ (0, \;\; 0.5, \;\; 0.2, \;\; 0.3) \cdot \mathbf{M} &= \\ (0.16, \;\; 0, \;\; 0.5, \;\; 0.34) & \end{aligned}$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$\begin{aligned} (1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\ (0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\ (0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\ (0.318, \quad 0.08, \quad 0.032, \quad 0.57) & \end{aligned}$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$\begin{aligned}
(1,\ \ 0,\ \ 0,\ \ 0) \cdot \mathbf{M} &= \\
(0,\ \ 0.5,\ \ 0.2,\ \ 0.3) \cdot \mathbf{M} &= \\
(0.16,\ \ 0,\ \ 0.5,\ \ 0.34) \cdot \mathbf{M} &= \\
(0.318,\ \ 0.08,\ \ 0.032,\ \ 0.57) \cdot \mathbf{M} &= \\
(0.13,\ \ 0.159,\ \ 0.1436,\ \ 0.5374) &
\end{aligned}$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob}(\text{`being in } s_k \text{ after } n \text{ steps'}) \geq 1/2 \text{ ?}$$

$$\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5374) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.51472) &
\end{aligned}$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \dots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least 1/2 ?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob('being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$
\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5374) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.51472) \cdot \mathbf{M} &= \\
(0.205444, \quad 0.09264, \quad 0.102056, \quad 0.50386) &
\end{aligned}
$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least 1/2 ?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5374) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.51472) \cdot \mathbf{M} &= \\
(0.205444, \quad 0.09264, \quad 0.102056, \quad 0.50386) \cdot \mathbf{M} &= \\
(0.171, \quad 0.102722, \quad 0.133729, \quad 0.500149)
\end{aligned}$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \text{ ?}$$

$$
\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5374) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.51472) \cdot \mathbf{M} &= \\
(0.205444, \quad 0.09264, \quad 0.102056, \quad 0.50386) \cdot \mathbf{M} &= \\
(0.171, \quad 0.102722, \quad 0.133729, \quad 0.500149) \cdot \mathbf{M} &= \\
(0.185374, \quad 0.0855, \quad 0.136922, \quad 0.500004) &
\end{aligned}
$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least 1/2 ?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob}(\text{`being in } s_k \text{ after } n \text{ steps'}) \geq 1/2 \text{ ?}$$

$$
\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad \color{red}{0.57}) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad \color{red}{0.5374}) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad \color{red}{0.51472}) \cdot \mathbf{M} &= \\
(0.205444, \quad 0.09264, \quad 0.102056, \quad \color{red}{0.50386}) \cdot \mathbf{M} &= \\
(0.171, \quad 0.102722, \quad 0.133729, \quad \color{red}{0.500149}) \cdot \mathbf{M} &= \\
(0.185374, \quad 0.0855, \quad 0.136922, \quad \color{red}{0.500004})
\end{aligned}
$$

Reachability/Invariance/Approximation in Markov Chains

M: Markov chain over states $s_1, \ldots, s_k$

- Is it the case, say, that starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?
- Does there exist T such that, for all $n \geq T$

$$\text{Prob(`being in } s_k \text{ after } n \text{ steps')} \geq 1/2 \ ?$$

Markov Chain Problem

Instance: $\langle$ stochastic matrix **M**; $r \in (0,1]$ $\rangle$

Question: Does $\exists T$ s.t. $\forall n \geq T$, $(1,0,\ldots,0) \cdot \mathbf{M}^n \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \geq r$?

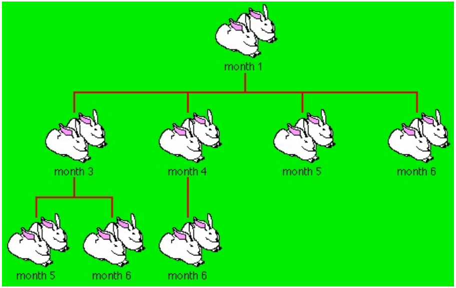
Positivity of Linear Recurrence Sequences

$u_0 = 1,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

Positivity of Linear Recurrence Sequences

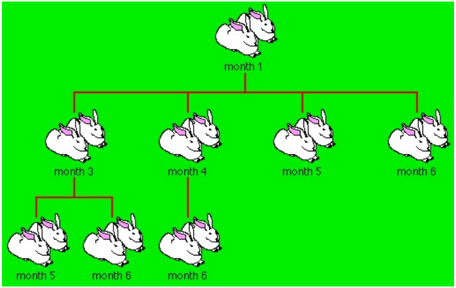
$u_0 = 1,\ u_1 = 1$

$u_{n+2} = u_{n+1} + u_n$



Positivity of Linear Recurrence Sequences

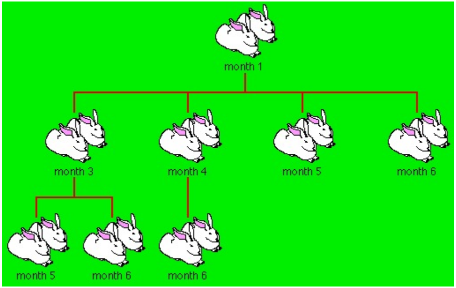
$u_0 = 1,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$



- 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, . . .

Positivity of Linear Recurrence Sequences

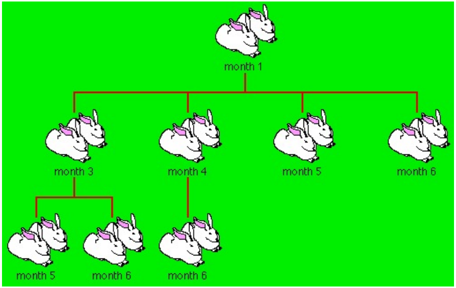
$u_0 = 1,\ u_1 = 1$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n$



- 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, . . .

Positivity of Linear Recurrence Sequences

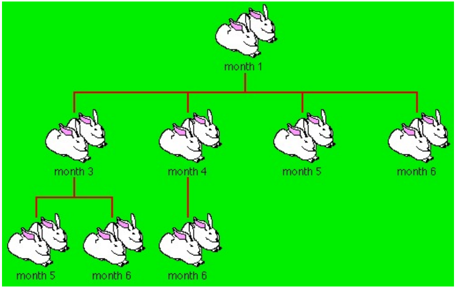
$$u_0 = 1,\ u_1 = 1,\ u_2 = 2,\ u_3 = 3,\ u_4 = 5$$
$$u_{n+5} = u_{n+4} + u_{n+3} - \tfrac{1}{3} u_n$$



- 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, . . .

Positivity of Linear Recurrence Sequences

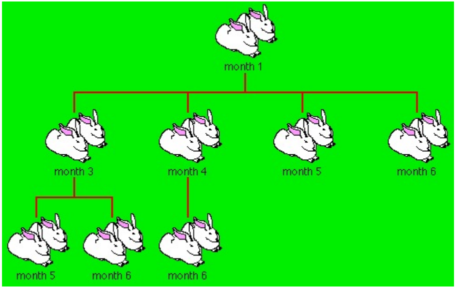
$$u_0 = 1,\ u_1 = 1,\ u_2 = 2,\ u_3 = 3,\ u_4 = 5$$
$$u_{n+5} = u_{n+4} + u_{n+3} - \tfrac{1}{3}u_n - 10w_{n+5}$$



- 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, . . .

Positivity of Linear Recurrence Sequences

$u_0 = 1,\ u_1 = 1,\ u_2 = 2,\ u_3 = 3,\ u_4 = 5$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3}u_n - 10w_{n+5}$



- 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, . . .

Positivity Problem

Instance: A linear recurrence sequence $\langle u_n \rangle$
Question: Is it the case that $\forall n,\ u_n \geq 0$?

Sample Decision Problems

Termination Problem for Simple Linear Programs

Instance: $\langle\ \mathbf{a};\ \mathbf{u};\ \mathbf{M}\ \rangle$ over $\mathbb{Z}$

Question: Does this program terminate?

```
x := a;
while  u · x ≠ 0  do
    x := M · x;
```

Markov Chain Problem

Instance: A stochastic matrix $\mathbf{M}$ over $\mathbb{Q}$

Question: Does $\exists T$ s.t. $\forall n \geq T$, $(1, 0, \ldots, 0) \cdot \mathbf{M}^n \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \geq \frac{1}{2}$?

Positivity Problem for Linear Recurrence Sequences

Instance: A linear recurrence sequence $\langle u_n \rangle$ over $\mathbb{Z}$ or $\mathbb{Q}$

Question: Is it the case that $\forall n$, $u_n \geq 0$?

Linear Recurrence Sequences

Definition

A **linear recurrence sequence** is a sequence $\langle u_0, u_1, u_2, \ldots \rangle$ of real numbers such that there exist k and constants $a_1, \ldots, a_k$, such that

$$\forall n \geq 0, \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n \, .$$

- k is the **order** of the sequence

Decision Problems for Linear Recurrence Sequences

- Let $\langle u_n \rangle$ be a linear recurrence sequence

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Decision Problems for Linear Recurrence Sequences

- Let $\langle u_n \rangle$ be a linear recurrence sequence

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Positivity Problem

Is it the case that $\forall n,\ u_n \geq 0$?

Decision Problems for Linear Recurrence Sequences

- Let $\langle u_n \rangle$ be a linear recurrence sequence

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Positivity Problem

Is it the case that $\forall n,\ u_n \geq 0$?

(Effective) Ultimate Positivity Problem

Does $\exists T$ such that, $\forall n \geq T,\ u_n \geq 0$?

Decision Problems for Linear Recurrence Sequences

- Let $\langle u_n \rangle$ be a linear recurrence sequence

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Positivity Problem

Is it the case that $\forall n,\ u_n \geq 0$?

(Effective) Ultimate Positivity Problem

Does $\exists T$ such that, $\forall n \geq T,\ u_n \geq 0$?

- *Effective* means T must also be provided.

Related Work and Applications

- Theoretical biology
  - Analysis of L-systems
  - Population dynamics
- Software verification
  - Termination of linear programs
- Probabilistic model checking
  - Reachability, invariance, and approximation in Markov chains
  - Stochastic logics
- Quantum computing
  - Threshold problems for quantum automata
- Economics
- Combinatorics
- Discrete linear dynamical systems
- Statistical physics
- ...

The Skolem Problem

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

- Open for about 80 years!

The Skolem Problem

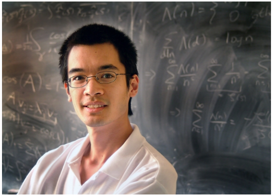
Skolem Problem

Does $\exists n$ such that $u_n = 0$?

- Open for about 80 years!

"It is faintly outrageous that this problem is still open; it is saying that we do not know how to decide the Halting Problem even for 'linear' automata!"

Terence Tao



The Skolem Problem

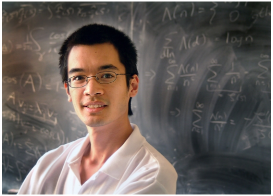
Skolem Problem

Does $\exists n$ such that $u_n = 0$?

- Open for about 80 years!

"It is faintly outrageous that this problem is still open; it is saying that we do not know how to decide the Halting Problem even for 'linear' automata!"

Terence Tao



". . . a mathematical embarrassment . . ."

Richard Lipton

The Skolem-Mahler-Lech Theorem

Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)

The set of zeros of a linear recurrence sequence is semi-linear:

$$\{n : u_n = 0\} = F \cup A_1 \cup \ldots \cup A_\ell$$

where F is finite and each A_i is a full arithmetic progression.

The Skolem-Mahler-Lech Theorem

Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)

The set of zeros of a linear recurrence sequence is semi-linear:

$$\{n : u_n = 0\} = F \cup A_1 \cup \ldots \cup A_\ell$$

where F is finite and each A_i is a full arithmetic progression.

- All known proofs make essential use of p-adic techniques

The Skolem-Mahler-Lech Theorem

Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)

The set of zeros of a linear recurrence sequence is semi-linear:

$$\{n : u_n = 0\} = F \cup A_1 \cup \ldots \cup A_\ell$$

where F is finite and each A_i is a full arithmetic progression.

- All known proofs make essential use of p-adic techniques

Theorem (Berstel and Mignotte 1976)

In Skolem-Mahler-Lech, the infinite part (arithmetic progressions $A_1, \ldots, A_\ell$) is fully effective.

The Skolem Problem at Low Orders

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Let u_n be a linear recurrence sequence of fixed order

The Skolem Problem at Low Orders

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Let u_n be a linear recurrence sequence of fixed order

Theorem (folklore)

For orders 1 and 2, Skolem is decidable.

The Skolem Problem at Low Orders

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Let u_n be a linear recurrence sequence of fixed order

Theorem (folklore)

For orders 1 and 2, Skolem is decidable.

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

For orders 3 and 4, Skolem is decidable.

The Skolem Problem at Low Orders

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Let u_n be a linear recurrence sequence of fixed order

Theorem (folklore)

For orders 1 and 2, Skolem is decidable.

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

For orders 3 and 4, Skolem is decidable.

Critical ingredient is Baker's theorem for linear forms in logarithms, which earned Baker the Fields Medal in 1970.

The Skolem Problem at Low Orders

Skolem Problem

Does $\exists n$ such that $u_n = 0$?

Let u_n be a linear recurrence sequence of fixed order

Theorem (folklore)

For orders 1 and 2, Skolem is decidable.

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

For orders 3 and 4, Skolem is decidable.

Decidability for order 5 was announced in 2005 by four Finnish mathematicians in a technical report (as yet unpublished). Their proof appears to have a serious gap.

The Positivity and Ultimate Positivity Problems

- Positivity and Ultimate Positivity open since at least 1970s

"In our estimation, these will be very difficult problems."

Matti Soittola

The Positivity and Ultimate Positivity Problems

- Positivity and Ultimate Positivity open since at least 1970s

"In our estimation, these will be very difficult problems."

Matti Soittola

Theorem (folklore)

Decidability of Positivity $\Rightarrow$ decidability of Skolem.

The Positivity and Ultimate Positivity Problems

Theorem (Burke, Webb 1981)

For order 2, Ultimate Positivity is decidable.

The Positivity and Ultimate Positivity Problems

Theorem (Burke, Webb 1981)

For order 2, Ultimate Positivity is decidable.

Theorem (Nagasaka, Shiue 1990)

For order 3 with repeated roots, Ultimate Positivity is decidable.

The Positivity and Ultimate Positivity Problems

Theorem (Burke, Webb 1981)

For order 2, Ultimate Positivity is decidable.

Theorem (Nagasaka, Shiue 1990)

For order 3 with repeated roots, Ultimate Positivity is decidable.

Theorem (Halava, Harju, Hirvensalo 2006)

For order 2, Positivity is decidable.

The Positivity and Ultimate Positivity Problems

Theorem (Burke, Webb 1981)

For order 2, Ultimate Positivity is decidable.

Theorem (Nagasaka, Shiue 1990)

For order 3 with repeated roots, Ultimate Positivity is decidable.

Theorem (Halava, Harju, Hirvensalo 2006)

For order 2, Positivity is decidable.

Theorem (Laohakosol and Tangsupphathawat 2009)

For order 3, Positivity and Ultimate Positivity are decidable.

The Positivity and Ultimate Positivity Problems

Theorem (Burke, Webb 1981)

For order 2, Ultimate Positivity is decidable.

Theorem (Nagasaka, Shiue 1990)

For order 3 with repeated roots, Ultimate Positivity is decidable.

Theorem (Halava, Harju, Hirvensalo 2006)

For order 2, Positivity is decidable.

Theorem (Laohakosol and Tangsupphathawat 2009)

For order 3, Positivity and Ultimate Positivity are decidable.

In *Colloquium Mathematicum* 128:1 (2012), Tangsupphathawat, Punnim, and Laohakosol claimed decidability of Positivity and Ultimate Positivity for order 4 (and noted being stuck for order 5). Unfortunately, their proof contains a major error.

Our Main Results (I)

Theorem

- *Positivity is decidable for order 5 or less.*

Our Main Results (I)

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.

Our Main Results (I)

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *Effective Ultimate Positivity is decidable for order 5 or less. The complexity is in P.*

Our Main Results (I)

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *Effective Ultimate Positivity is decidable for order 5 or less. The complexity is in* P.
- *At order 6, for both Positivity and Ultimate Positivity, proof of decidability would entail major breakthroughs in analytic number theory (Diophantine approximation of transcendental numbers).*

Our Main Results (I)

Theorem

- *Positivity is decidable for order 5 or less.*

  The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *Effective Ultimate Positivity is decidable for order 5 or less. The complexity is in P.*
- *At order 6, for both Positivity and Ultimate Positivity, proof of decidability would entail major breakthroughs in analytic number theory (Diophantine approximation of transcendental numbers).*
- *In the simple case, Positivity and Effective Ultimate Positivity are decidable for order 9 or less.*

Our Main Results (I)

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *Effective Ultimate Positivity is decidable for order 5 or less.*
  The complexity is in P.
- *At order 6, for both Positivity and Ultimate Positivity, proof of decidability would entail major breakthroughs in analytic number theory (Diophantine approximation of transcendental numbers).*
- *In the simple case, Positivity and Effective Ultimate Positivity are decidable for order 9 or less.*
  Complexity in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ *and P resp.*

Our Main Results (II)

Theorem

In the simple case, Positivity and Effective Ultimate Positivity are decidable for order 9 or less.

Our Main Results (II)

Theorem

In the simple case, Positivity and Effective Ultimate Positivity are decidable for order 9 or less.

Theorem (ineffective version)

In the simple case, Ultimate Positivity is decidable for ALL orders.

Our Main Results (II)

Theorem

In the simple case, Positivity and Effective Ultimate Positivity are decidable for order 9 or less.

Theorem (ineffective version)

In the simple case, Ultimate Positivity is decidable for ALL orders.

- *For each fixed order k, complexity is in P (depends on k).*

Our Main Results (II)

Theorem

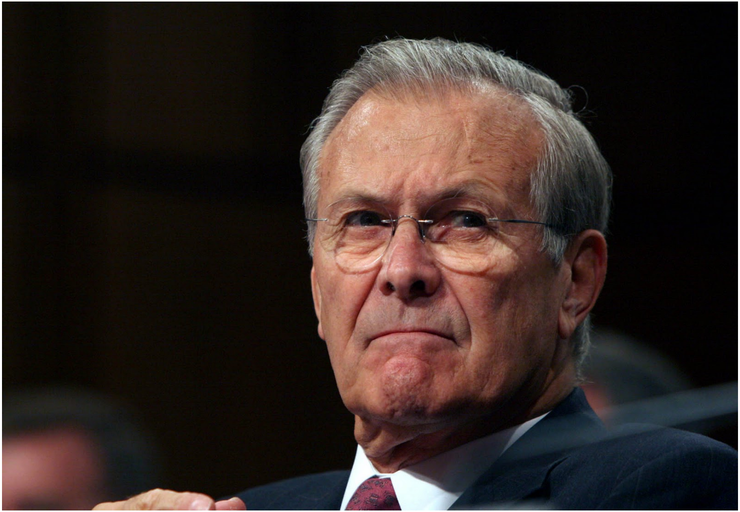
In the simple case, Positivity and Effective Ultimate Positivity are decidable for order 9 or less.

Theorem (ineffective version)

In the simple case, Ultimate Positivity is decidable for ALL orders.

- *For each fixed order k, complexity is in P (depends on k).*
- *In the general case, complexity is in PSPACE and co$\exists\mathbb{R}$-hard.*

Known Unknowns



"There are things that we know we don't know..."

Donald Rumsfeld

Diophantine Approximation

How well can one approximate a real number x with rationals?

$$\left| x - \frac{p}{q} \right|$$

Diophantine Approximation

How well can one approximate a real number x with rationals?

$$\left| x - \frac{p}{q} \right|$$

Theorem (Dirichlet 1842)

There are infinitely many integers p, q such that $\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$.

Diophantine Approximation

How well can one approximate a real number x with rationals?

$$\left| x - \frac{p}{q} \right|$$

Theorem (Dirichlet 1842)

There are infinitely many integers p, q such that $\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$.

Theorem (Hurwitz 1891)

There are infinitely many integers p, q such that $\left| x - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}$.

Diophantine Approximation

How well can one approximate a real number x with rationals?

$$\left| x - \frac{p}{q} \right|$$

Theorem (Dirichlet 1842)

There are infinitely many integers p, q such that $\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$.

Theorem (Hurwitz 1891)

There are infinitely many integers p, q such that $\left| x - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}$.

Moreover, $\frac{1}{\sqrt{5}}$ is the best possible constant that will work for all real numbers x.

Diophantine Approximation

Definition

Let $x \in \mathbb{R}$. The **Lagrange constant** $L_\infty(x)$ is:

$$L_\infty(x) = \inf\left\{c : \left|x - \frac{p}{q}\right| < \frac{c}{q^2} \text{ has infinitely many solutions}\right\}.$$

Diophantine Approximation

Definition

Let $x \in \mathbb{R}$. The **Lagrange constant** $L_\infty(x)$ is:

$$L_\infty(x) = \inf \left\{ c : \left| x - \frac{p}{q} \right| < \frac{c}{q^2} \text{ has infinitely many solutions} \right\}.$$

- $L_\infty(x)$ is closely related to the continued fraction expansion of x

Diophantine Approximation

Definition

Let $x \in \mathbb{R}$. The **Lagrange constant** $L_\infty(x)$ is:

$$L_\infty(x) = \inf \left\{ c : \left| x - \frac{p}{q} \right| < \frac{c}{q^2} \text{ has infinitely many solutions} \right\}.$$

- $L_\infty(x)$ is closely related to the continued fraction expansion of x
- Almost all reals x have $L_\infty(x) = 0$ [Khinchin 1926]

Diophantine Approximation

Definition

Let $x \in \mathbb{R}$. The **Lagrange constant** $L_\infty(x)$ is:

$$L_\infty(x) = \inf \left\{ c : \left| x - \frac{p}{q} \right| < \frac{c}{q^2} \text{ has infinitely many solutions} \right\} .$$

- $L_\infty(x)$ is closely related to the continued fraction expansion of x
- Almost all reals x have $L_\infty(x) = 0$ [Khinchin 1926]
- However if x is a real algebraic number of degree 2, $L_\infty(x) \neq 0$ [Euler, Lagrange]

Diophantine Approximation

Definition

Let $x \in \mathbb{R}$. The **Lagrange constant** $L_\infty(x)$ is:

$$L_\infty(x) = \inf \left\{ c : \left| x - \frac{p}{q} \right| < \frac{c}{q^2} \text{ has infinitely many solutions} \right\}.$$

- $L_\infty(x)$ is closely related to the continued fraction expansion of x
- Almost all reals x have $L_\infty(x) = 0$ [Khinchin 1926]
- However if x is a real algebraic number of degree 2, $L_\infty(x) \neq 0$ [Euler, Lagrange]
- All transcendental numbers x have $0 \leq L_\infty(x) \leq 1/3$ [Markov 1879]

Diophantine Approximation

Definition

Let $x \in \mathbb{R}$. The **Lagrange constant** $L_\infty(x)$ is:

$$L_\infty(x) = \inf \left\{ c : \left| x - \frac{p}{q} \right| < \frac{c}{q^2} \text{ has infinitely many solutions} \right\}.$$

- $L_\infty(x)$ is closely related to the continued fraction expansion of x
- Almost all reals x have $L_\infty(x) = 0$ [Khinchin 1926]
- However if x is a real algebraic number of degree 2, $L_\infty(x) \neq 0$ [Euler, Lagrange]
- All transcendental numbers x have $0 \leq L_\infty(x) \leq 1/3$ [Markov 1879]

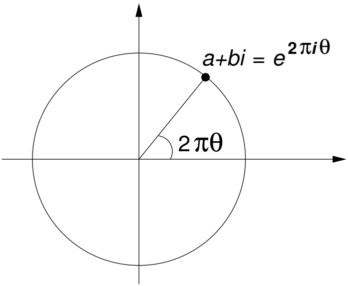
Almost nothing else is known about any specific irrational number!

Hardness

Let $\mathcal{T} = \{\theta \in (0,1) \ : \ e^{2\pi i\theta} \in \mathbb{Q}(i)\} \ \setminus \ \{\frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$

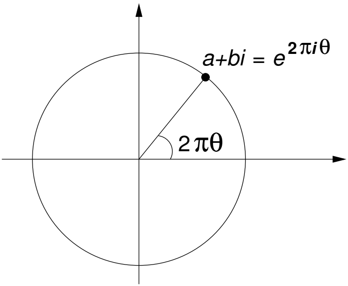
Hardness

Let $\mathcal{T} = \{\theta \in (0,1) \ : \ e^{2\pi i\theta} \in \mathbb{Q}(i)\} \ \setminus \ \{\frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$



Hardness

Let $\mathcal{T} = \{\theta \in (0,1) \ : \ e^{2\pi i\theta} \in \mathbb{Q}(i)\} \ \setminus \ \{\frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$



- $\mathcal{T}$ is a countable set of transcendental numbers

Hardness

- Recall that a real number θ is computable if there is an algorithm which, given any rational $\varepsilon > 0$, returns some $r \in \mathbb{Q}$ with $|\theta - r| < \varepsilon$.

Hardness

- Recall that a real number θ is computable if there is an algorithm which, given any rational $\varepsilon > 0$, returns some $r \in \mathbb{Q}$ with $|\theta - r| < \varepsilon$.

Theorem

Suppose that Ultimate Positivity is decidable for integer linear recurrence sequences of order 6. Then for any $\theta \in \mathcal{T}$, $L_\infty(\theta)$ is computable.

Hardness

- Recall that a real number θ is computable if there is an algorithm which, given any rational $\varepsilon > 0$, returns some $r \in \mathbb{Q}$ with $|\theta - r| < \varepsilon$.

Theorem

Suppose that Ultimate Positivity is decidable for integer linear recurrence sequences of order 6. Then for any $\theta \in \mathcal{T}$, $L_\infty(\theta)$ is computable.

- Several additional results hold (notably relating to the computability of *inhomogeneous* Diophantine approximation constants), and likewise for Positivity . . .

Main Tools and Techniques

- Algebraic and analytic number theory, Diophantine geometry
  - p-adic techniques
  - Baker's theorem on linear forms in logarithms
  - Kronecker's theorem on simultaneous Diophantine approximation
  - Masser's results on multiplicative relationships among algebraic numbers
  - Schmidt's Subspace theorem and Schlickewei's p-adic extension
  - Sums of S-units techniques
  - Gelfond-Schneider theorem
  - Other Diophantine geometry and approximation techniques
- Real algebraic geometry
- Decidability and fined-grained complexity of first-order theory of the reals (Renegar)

Termination of Linear Programs Again

$\mathbf{x} \in A$;
while $\mathbf{x} \in B$ do
  $\mathbf{x} := \mathbf{M} \cdot \mathbf{x}$;

Termination of Linear Programs Again

$\mathbf{x} \in A$;
while $\mathbf{x} \in B$ do
$\quad \mathbf{x} := \mathbf{M} \cdot \mathbf{x}$;

Question: Does this program terminate for all $\mathbf{x} \in A$?

Termination of Linear Programs Again

$\mathbf{x} \in A$;
while $\mathbf{x} \in B$ do
    $\mathbf{x} := \mathbf{M} \cdot \mathbf{x}$;

Question: Does this program terminate for all $\mathbf{x} \in A$?

- Ambient space: $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, $\ldots$
- A, B: semi-linear (or even algebraic for $\mathbb{Q}$ and $\mathbb{R}$?)

Termination of Linear Programs Again

$\mathbf{x} \in A$;
while $\mathbf{x} \in B$ do
    $\mathbf{x} := \mathbf{M} \cdot \mathbf{x}$;

Question: Does this program terminate for all $\mathbf{x} \in A$?

- Ambient space: $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, ...
- A, B: semi-linear (or even algebraic for $\mathbb{Q}$ and $\mathbb{R}$?)

- Decidability?
- Complexity?
- Synthesis problems: e.g., can we *compute* largest A such that program terminates for all $\mathbf{x} \in A$?

Discrete Linear Dynamical Systems

Definition

A **discrete linear dynamical systems** consists of a linear transformation $\mathbf{M}$ on a finite-dimensional vector space V.

- Typically $V = \mathbb{R}^n$ or $\mathbb{Q}^n$

Decision Problems for Linear Dynamical Systems

Definition

Given a vector $\mathbf{v} \in V$, the **orbit** of $\mathbf{v}$ under $\mathbf{M}$ is

$$\mathcal{O}_{\mathbf{M}}(\mathbf{v}) = \langle \mathbf{v}, \mathbf{M}\mathbf{v}, \mathbf{M}^2\mathbf{v}, \mathbf{M}^3\mathbf{v}, \ldots \rangle .$$

Decision Problems for Linear Dynamical Systems

Definition

Given a vector $\mathbf{v} \in V$, the **orbit** of $\mathbf{v}$ under $\mathbf{M}$ is

$$\mathcal{O}_{\mathbf{M}}(\mathbf{v}) = \langle \mathbf{v}, \mathbf{M}\mathbf{v}, \mathbf{M}^2\mathbf{v}, \mathbf{M}^3\mathbf{v}, \ldots \rangle \,.$$

- Is $\mathcal{O}_{\mathbf{M}}(\mathbf{v})$ periodic? Bounded? Divergent to ∞?
- Is $\mathcal{O}_{\mathbf{M}}(\mathbf{v}) \subseteq B$ for all/some $\mathbf{v} \in A$? What about *ultimately*?
- Does $\mathcal{O}_{\mathbf{M}}(\mathbf{v})$ hit B infinitely often for all/some $\mathbf{v} \in A$?
- ...
- *Synthesis*: Can we compute the largest/least/some $A/B/\mathbf{M}$ such that ...?

Decision Problems for Linear Dynamical Systems

Definition

Given a vector $\mathbf{v} \in V$, the **orbit** of $\mathbf{v}$ under $\mathbf{M}$ is

$$\mathcal{O}_{\mathbf{M}}(\mathbf{v}) = \langle \mathbf{v}, \mathbf{M}\mathbf{v}, \mathbf{M}^2\mathbf{v}, \mathbf{M}^3\mathbf{v}, \ldots \rangle \,.$$

- Is $\mathcal{O}_{\mathbf{M}}(\mathbf{v})$ periodic? Bounded? Divergent to ∞?
- Is $\mathcal{O}_{\mathbf{M}}(\mathbf{v}) \subseteq B$ for all/some $\mathbf{v} \in A$? What about *ultimately*?
- Does $\mathcal{O}_{\mathbf{M}}(\mathbf{v})$ hit B infinitely often for all/some $\mathbf{v} \in A$?
- ...
- *Synthesis*: Can we compute the largest/least/some $A/B/\mathbf{M}$ such that ...?

- A, B: semi-linear/algebraic/ ...
- Decidability?
- Complexity?
- ...

From LRS to Linear Dynamical Systems

$$\mathbf{v} = \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}$$

From LRS to Linear Dynamical Systems

$$\mathbf{v} = \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}$$

$$\mathcal{O}_{\mathbf{M}}(\mathbf{v}) = \langle \mathbf{v}, \mathbf{M}\mathbf{v}, \mathbf{M}^2\mathbf{v}, \ldots, \mathbf{M}^j\mathbf{v}, \ldots \rangle$$

From LRS to Linear Dynamical Systems

$$\mathbf{v} = \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}$$

$$\mathcal{O}_{\mathbf{M}}(\mathbf{v}) = \langle \mathbf{v}, \mathbf{M}\mathbf{v}, \mathbf{M}^2\mathbf{v}, \ldots, \mathbf{M}^j\mathbf{v}, \ldots \rangle$$

$$= \langle \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}, \begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix}, \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_j \\ b_j \\ c_j \\ d_j \end{pmatrix}, \ldots \rangle$$

From LRS to Linear Dynamical Systems

$$\mathbf{v} = \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}$$

$$\mathcal{O}_{\mathbf{M}}(\mathbf{v}) = \langle \mathbf{v}, \mathbf{Mv}, \mathbf{M}^2\mathbf{v}, \ldots, \mathbf{M}^j\mathbf{v}, \ldots \rangle$$

$$= \langle \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}, \begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix}, \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_j \\ b_j \\ c_j \\ d_j \end{pmatrix}, \ldots \rangle$$

From LRS to Linear Dynamical Systems

$$\mathbf{v} = \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}$$

$$\mathcal{O}_{\mathbf{M}}(\mathbf{v}) = \langle \mathbf{v}, \mathbf{M}\mathbf{v}, \mathbf{M}^2\mathbf{v}, \ldots, \mathbf{M}^j\mathbf{v}, \ldots \rangle$$

$$= \langle \begin{pmatrix} a_0 \\ b_0 \\ c_0 \\ d_0 \end{pmatrix}, \begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix}, \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_j \\ b_j \\ c_j \\ d_j \end{pmatrix}, \ldots \rangle$$

- $\langle b_0, b_1, b_2, \ldots, b_j, \ldots \rangle$ is an LRS of order n (here $n = 4$)

Linear Dynamical Systems: Specification and Verification

- A fresh look at an old area
- Lots of challenging problems
- Lots of interesting maths
- Many connections to variety of other fields