Decision Problems for Linear Recurrence Sequences

Joël Ouaknine

Department of Computer Science, Oxford University

(Joint work with James Worrell and Matt Daws)

Algorithms Workshop
Oxford, October 2012

Termination of Simple Linear Programs

$\mathbf{x} := \mathbf{a};$
while $\mathit{cond}(\mathbf{x})$ do
    $\mathbf{x} := \mathbf{M} \cdot \mathbf{x} + \mathbf{b};$

Termination of Simple Linear Programs

$\mathbf{x} := \mathbf{a}$;
while $\mathit{cond}(\mathbf{x})$ do
    $\mathbf{x} := \mathbf{M} \cdot \mathbf{x} + \mathbf{b}$;

where $\mathit{cond}(\mathbf{x})$ is linear, e.g. '$\mathbf{u} \cdot \mathbf{x} \neq 0$' or '$\mathbf{u} \cdot \mathbf{x} \geq 5$'.

Termination of Simple Linear Programs

$\mathbf{x} := \mathbf{a}$;
while $cond(\mathbf{x})$ do
  $\mathbf{x} := \mathbf{M} \cdot \mathbf{x} + \mathbf{b}$;

where $cond(\mathbf{x})$ is linear, e.g. '$\mathbf{u} \cdot \mathbf{x} \neq 0$' or '$\mathbf{u} \cdot \mathbf{x} \geq 5$'.

Termination Problem

Instance: $\langle\ \mathbf{a};\ cond;\ \mathbf{M};\ \mathbf{b}\ \rangle$
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, 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 and Invariance in Markov Chains

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

Reachability and Invariance 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 and Invariance 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 $n \geq T$

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

Reachability and Invariance 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 and Invariance 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 $n \geq T$

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

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

Reachability and Invariance 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 $n \geq T$

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

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

Reachability and Invariance 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 $n \geq T$

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

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

Reachability and Invariance 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 $n \geq T$

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

$$\begin{aligned}
(1,\quad 0,\quad 0,\quad 0) \cdot \mathbf{M} &= \\
(0,\quad 0.5,\quad 0.2,\quad 0.3) \cdot \mathbf{M} &= \\
(0.16,\quad 0,\quad 0.5,\quad 0.34) \cdot \mathbf{M} &= \\
(0.318,\quad 0.08,\quad 0.032,\quad 0.57) \cdot \mathbf{M} &= \\
(0.13,\quad 0.159,\quad 0.1436,\quad 0.5674)
\end{aligned}$$

Reachability and Invariance 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 $n \geq T$

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

$$\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5674) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.56472)
\end{aligned}$$

Reachability and Invariance 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 $n \geq T$

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

$$\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5674) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.56472) \cdot \mathbf{M} &= \\
(0.205444, \quad 0.09264, \quad 0.102056, \quad 0.59986) &
\end{aligned}$$

Reachability and Invariance 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 $n \geq T$

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

$$\begin{array}{r}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} = \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} = \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} = \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} = \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5674) \cdot \mathbf{M} = \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.56472) \cdot \mathbf{M} = \\
(0.205444, \quad 0.09264, \quad 0.102056, \quad 0.59986) \cdot \mathbf{M} = \\
(0.171, \quad 0.102722, \quad 0.133729, \quad 0.592549) \phantom{\cdot \mathbf{M} =}
\end{array}$$

Reachability and Invariance 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 $n \geq T$

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

$$
\begin{aligned}
(1, \quad 0, \quad 0, \quad 0) \cdot \mathbf{M} &= \\
(0, \quad 0.5, \quad 0.2, \quad 0.3) \cdot \mathbf{M} &= \\
(0.16, \quad 0, \quad 0.5, \quad 0.34) \cdot \mathbf{M} &= \\
(0.318, \quad 0.08, \quad 0.032, \quad 0.57) \cdot \mathbf{M} &= \\
(0.13, \quad 0.159, \quad 0.1436, \quad 0.5674) \cdot \mathbf{M} &= \\
(0.18528, \quad 0.065, \quad 0.185, \quad 0.56472) \cdot \mathbf{M} &= \\
(0.205444, \quad 0.09264, \quad 0.102056, \quad 0.59986) \cdot \mathbf{M} &= \\
(0.171, \quad 0.102722, \quad 0.133729, \quad 0.592549) \cdot \mathbf{M} &= \\
(0.185374, \quad 0.0855, \quad 0.136922, \quad 0.592204)
\end{aligned}
$$

Reachability and Invariance 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 $n \geq T$

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

$$
\begin{array}{r}
(1,\quad 0,\quad 0,\quad 0) \cdot \mathbf{M} = \\
(0,\quad 0.5,\quad 0.2,\quad 0.3) \cdot \mathbf{M} = \\
(0.16,\quad 0,\quad 0.5,\quad 0.34) \cdot \mathbf{M} = \\
(0.318,\quad 0.08,\quad 0.032,\quad \color{red}{0.57}) \cdot \mathbf{M} = \\
(0.13,\quad 0.159,\quad 0.1436,\quad \color{red}{0.5674}) \cdot \mathbf{M} = \\
(0.18528,\quad 0.065,\quad 0.185,\quad \color{red}{0.56472}) \cdot \mathbf{M} = \\
(0.205444,\quad 0.09264,\quad 0.102056,\quad \color{red}{0.59986}) \cdot \mathbf{M} = \\
(0.171,\quad 0.102722,\quad 0.133729,\quad \color{red}{0.592549}) \cdot \mathbf{M} = \\
(0.185374,\quad 0.0855,\quad 0.136922,\quad \color{red}{0.592204})
\end{array}
$$

Reachability and Invariance 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 $n \geq T$

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

Ultimate Invariance Problem

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

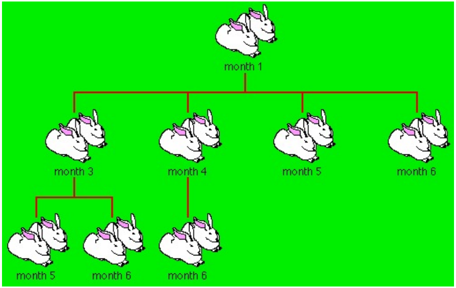
Question: Does $\exists T$ s.t. $\forall n \geq T$, $(1, 0, \ldots, 0) \cdot \mathbf{M}^n \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \geq r$?

Positivity of Linear Recurrence Sequences

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

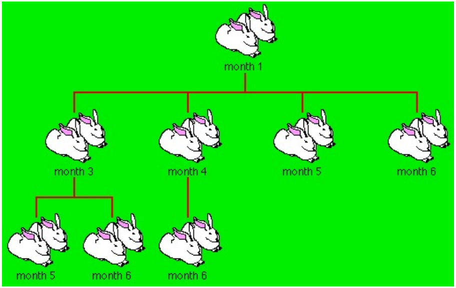
Positivity of Linear Recurrence Sequences

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



Positivity of Linear Recurrence Sequences

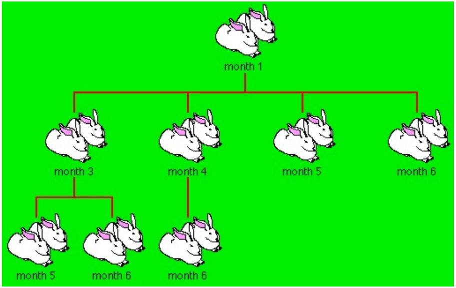
$u_0 = 1,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$



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

Positivity of Linear Recurrence Sequences

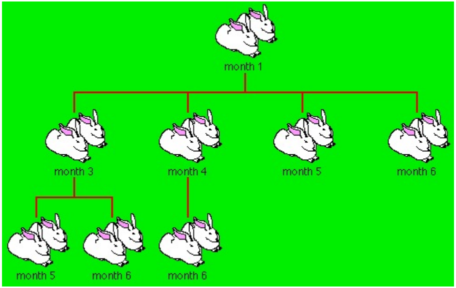
$u_0 = 1,\ u_1 = 1$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n$



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

Positivity of Linear Recurrence Sequences

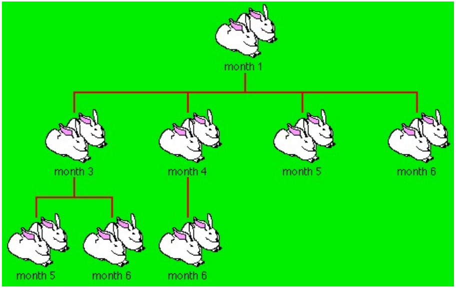
$u_0 = 1,\ u_1 = 1,\ u_2 = 2,\ u_3 = 3,\ u_4 = 5$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n$



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

Positivity of Linear Recurrence Sequences

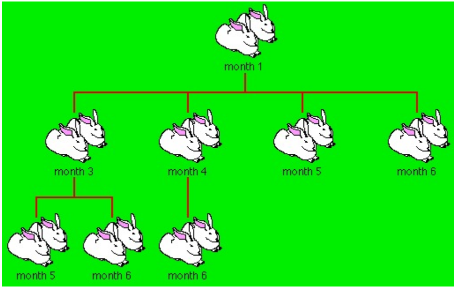
$u_0 = 1,\ u_1 = 1,\ u_2 = 2,\ u_3 = 3,\ u_4 = 5$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n - 10 w_{n+5}$



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

Question: Does this program terminate?

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

Ultimate Invariance Problem for Markov Chains

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

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
- For decision problems, will normally restrict to sequences over integers, rationals, or algebraic numbers

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 $\forall n,\ u_n \geq 0$?

Ultimate Positivity Problem

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

Related Work and Applications

- Theoretical biology
  - Analysis of L-systems
  - Population dynamics
- Software verification
  - Termination of linear programs
- Probabilistic model checking
  - Reachability and invariance in Markov chains
  - Stochatic logics
- Quantum computing
  - Threshold problems for quantum automata
- Economics
- Combinatorics
- Term rewriting
- Generating functions
- ...

The Skolem Problem

Skolem Problem

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

- Open for about 80 years!

The Skolem Problem

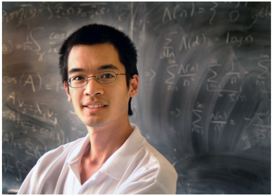
Skolem Problem

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

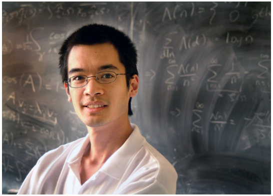
Skolem Problem

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

- 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.

Theorem (Halava, Harju, Hirvensalo 2006)

For order 2, Positivity is decidable.

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.

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.

Our Main Results

Theorem

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

Our Main Results

Theorem

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

Our Main Results

Theorem

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

Our Main Results

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{NP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *Ultimate Positivity is decidable for order 5 or less.*
  The complexity is in P.
- *At order 6, for both Positivity and Ultimate Positivity:*

Our Main Results

Theorem

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

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{NP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *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)*
  - *But proof of undecidability would also entail significant breakthroughs in analytic number theory!*

Our Main Results

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{NP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *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)*
  - *But proof of undecidability would also entail significant breakthroughs in analytic number theory!*
- *In the diagonalisable case, Positivity and Ultimate Positivity are decidable for order 9 or less.*

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 18??)

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 18??)

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 18??)

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 very 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 very 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 very 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 very 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 very 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!

Our Hardness Results

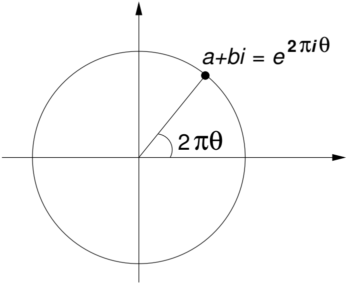
- Let $\mathcal{A} = \left\{ a + bi \ : \ a, b \in \mathbb{Q} \ \wedge \ a^2 + b^2 = 1 \ \wedge \ ab \neq 0 \right\}$

Our Hardness Results

- Let $\mathcal{A} = \left\{a + bi \ : \ a, b \in \mathbb{Q} \ \wedge \ a^2 + b^2 = 1 \ \wedge \ ab \neq 0\right\}$
- Let $\mathcal{T} = \left\{\dfrac{\arg(z)}{2\pi} \ : \ z \in \mathcal{A}\right\}$

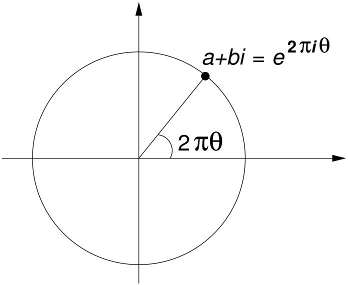
Our Hardness Results

- Let $\mathcal{A} = \left\{ a + bi \ : \ a, b \in \mathbb{Q} \ \wedge \ a^2 + b^2 = 1 \ \wedge \ ab \neq 0 \right\}$
- Let $\mathcal{T} = \left\{ \frac{\arg(z)}{2\pi} \ : \ z \in \mathcal{A} \right\}$



Our Hardness Results

- Let $\mathcal{A} = \left\{ a + bi \; : \; a, b \in \mathbb{Q} \;\wedge\; a^2 + b^2 = 1 \;\wedge\; ab \neq 0 \right\}$
- Let $\mathcal{T} = \left\{ \frac{\arg(z)}{2\pi} \; : \; z \in \mathcal{A} \right\}$



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

Our Hardness Results

- 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 $|\theta - r| < \varepsilon$.

Our Hardness Results

- 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.

Our Hardness Results

- 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 . . .

Our Hardness Results

- Let $\mathcal{C} = \left\{ \frac{\text{arg}(z)}{2\pi} \ : \ z \text{ is a complex algebraic number} \right\}$

Our Hardness Results

- Let $\mathcal{C} = \left\{ \frac{\arg(z)}{2\pi} \ : \ z \text{ is a complex algebraic number} \right\}$

Theorem

Suppose that, for all $\theta \in \mathcal{C} \setminus \mathbb{Q}$, and all $\varphi \in \mathcal{C}$, we have $L_\infty^+(\theta, \varphi) = 0$.
Then Ultimate Positivity is decidable for all algebraic linear recurrence sequences of order 6 (or less).

Our Hardness Results

- Let $\mathcal{C} = \left\{ \frac{\arg(z)}{2\pi} \ : \ z \text{ is a complex algebraic number} \right\}$

Theorem

Suppose that, for all $\theta \in \mathcal{C} \setminus \mathbb{Q}$, and all $\varphi \in \mathcal{C}$, we have $L_\infty^+(\theta, \varphi) = 0$.
Then Ultimate Positivity is decidable for all algebraic linear recurrence sequences of order 6 (or less).

Therefore:

Theorem

Suppose that Ultimate Positivity is undecidable for linear recurrence sequences of order 6. Then for at least some $\theta \in \mathcal{C} \setminus \mathbb{Q}$ and $\varphi \in \mathcal{C}$, we have $L_\infty^+(\theta, \varphi) \neq 0$.

Our Hardness Results

In summary:

Theorem

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

Theorem

Suppose that Ultimate Positivity is undecidable for linear recurrence sequences of order 6. Then for at least some $\theta \in \mathcal{C} \setminus \mathbb{Q}$ and $\varphi \in \mathcal{C}$, we have $L_\infty^+(\theta, \varphi) \neq 0$.

(And similarly for Positivity . . .)

Main Tools and Techniques

Theorem

- *Positivity is decidable for order 5 or less.*
  The complexity is in $\mathsf{NP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$.
- *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)*
  - *But proof of undecidability would also entail significant breakthroughs in analytic number theory!*
- *In the diagonalisable case, Positivity and Ultimate Positivity are decidable for order 9 or less.*

Main Tools and Techniques

- Algebraic and analytic number theory
  - p-adic techniques
  - Baker's theorem
  - Kronecker's theorem
  - Gelfond-Schneider theorem
  - Diophantine approximation techniques
- Real algebraic geometry
- Model theory of real closed fields

Ongoing Work and Research Programme

Decision problems for **linear dynamical systems**

- Ongoing work on higher-order generalisations of the Orbit Problem
- Both discrete and continuous dynamics
- Many other natural decision and ergodic problems . . .