A Survey of Program Termination: Practical and Theoretical Challenges

Joël Ouaknine

Department of Computer Science, Oxford University

VTSA 2014
Luxembourg, October 2014

Termination of Linear Programs

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

Termination of Linear Programs

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

Termination Problem

Instance: $\langle\ \mathbf{a};\ \mathbf{u};\ \mathbf{M}\ \rangle$ over $\mathbb{Z}$ or $\mathbb{Q}$
Question: Does this program terminate?

Termination of Linear Programs

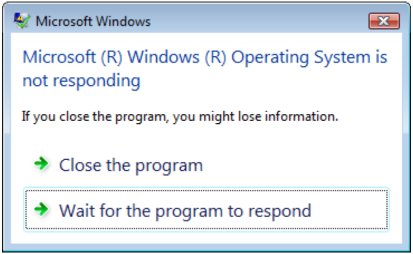
Much work on this and related problems in the literature over the last three decades:

- 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


Microsoft Windows
Microsoft (R) Windows (R) Operating System is not responding
If you close the program, you might lose information.
Close the program
Wait for the program to respond

Termination of 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:

Termination of Linear Programs

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

Termination Problem

Instance: $\langle\ \mathbf{a};\ \mathbf{u};\ \mathbf{M}\ \rangle$ over $\mathbb{Z}$ or $\mathbb{Q}$
Question: Does this program terminate?

Termination of Linear Programs

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

Termination Problem

Instance: $\langle\ \mathbf{a};\ \mathbf{u};\ \mathbf{M}\ \rangle$ over $\mathbb{Z}$ or $\mathbb{Q}$
Question: Does this program terminate?

Theorem

If $\mathbf{M}$ *has dimension* $5{\times}5$ *or less, Termination is decidable.*

Termination of Linear Programs

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

Termination Problem

Instance: $\langle\ \mathbf{a};\ \mathbf{u};\ \mathbf{M}\ \rangle$ over $\mathbb{Z}$ or $\mathbb{Q}$
Question: Does this program terminate?

Theorem

If $\mathbf{M}$ has dimension 5×5 or less, Termination is decidable.

Theorem

If $\mathbf{M}$ is diagonalisable and has dimension 9×9 or less, Termination is decidable.

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 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 that, starting in state s_1, ultimately I am in state s_k with probability at least $1/2$?

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

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

Reachability/Invariance/Approximation in Markov Chains

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

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

Markov Chain Problem

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

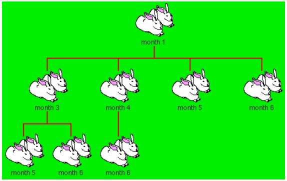
Question: Does $\exists T$ s.t. $\forall n \geq T$, $(1,0,\ldots,0) \cdot \mathbf{M}^n \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \geq r$?

Positivity and Zeros of Linear Recurrence Sequences

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

Positivity and Zeros of Linear Recurrence Sequences

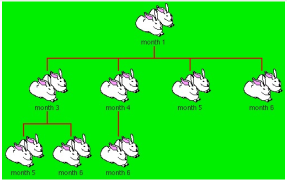
$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$



Positivity and Zeros of Linear Recurrence Sequences

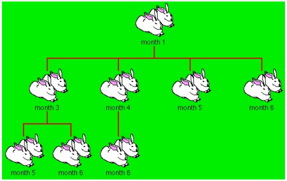
$u_0 = 0,\ u_1 = 1$

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



- 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, ...

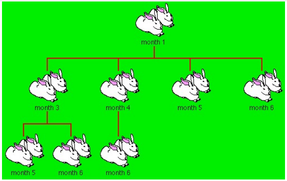
$u_0 = 0,\ u_1 = 1$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n$



- 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, ...

Positivity and Zeros of Linear Recurrence Sequences

$u_0 = 0,\ u_1 = 1,\ u_2 = 1,\ u_3 = 2,\ u_4 = 3$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n$

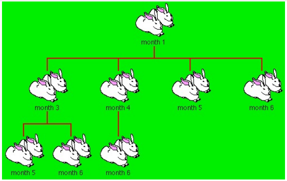


- 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, ...

Positivity and Zeros of Linear Recurrence Sequences

$u_0 = 0,\ u_1 = 1,\ u_2 = 1,\ u_3 = 2,\ u_4 = 3$

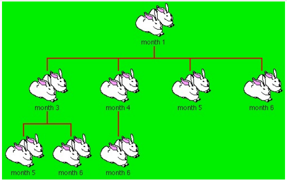
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n - 10 w_{n+5}$



- 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, . . .

Positivity and Zeros of Linear Recurrence Sequences

$u_0 = 0,\ u_1 = 1,\ u_2 = 1,\ u_3 = 2,\ u_4 = 3$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3} u_n - 10 w_{n+5}$



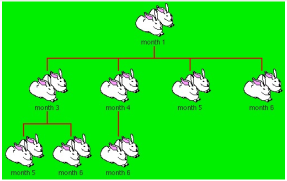
- 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, . . .

Positivity Problem

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

Positivity and Zeros of Linear Recurrence Sequences

$u_0 = 0,\ u_1 = 1,\ u_2 = 1,\ u_3 = 2,\ u_4 = 3$
$u_{n+5} = u_{n+4} + u_{n+3} - \frac{1}{3}u_n - 10w_{n+5}$



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

Skolem Problem

Instance: A linear recurrence sequence $\langle u_n \rangle$
Question: Does $\exists n$ such that $u_n = 0$?

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2
- Its **characteristic polynomial** is $p(x) = x^2 - x - 1$

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2
- Its **characteristic polynomial** is $p(x) = x^2 - x - 1$
- The **characteristic roots** are $\lambda_1 = \frac{1+\sqrt{5}}{2}$ and $\lambda_2 = \frac{1-\sqrt{5}}{2}$

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2
- Its **characteristic polynomial** is $p(x) = x^2 - x - 1$
- The **characteristic roots** are $\lambda_1 = \frac{1+\sqrt{5}}{2}$ and $\lambda_2 = \frac{1-\sqrt{5}}{2}$
- No repeated roots $\Rightarrow$ Fibonacci sequence is **simple**

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2
- Its **characteristic polynomial** is $p(x) = x^2 - x - 1$
- The **characteristic roots** are $\lambda_1 = \frac{1+\sqrt{5}}{2}$ and $\lambda_2 = \frac{1-\sqrt{5}}{2}$
- No repeated roots $\Rightarrow$ Fibonacci sequence is **simple**
- $u_n \ = \ \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \ = \ c_1\lambda_1^n + c_2\lambda_2^n$

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2
- Its **characteristic polynomial** is $p(x) = x^2 - x - 1$
- The **characteristic roots** are $\lambda_1 = \frac{1+\sqrt{5}}{2}$ and $\lambda_2 = \frac{1-\sqrt{5}}{2}$
- No repeated roots $\Rightarrow$ Fibonacci sequence is **simple**
- $u_n \ = \ \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \ = \ c_1\lambda_1^n + c_2\lambda_2^n$
- $u_n \ = \ \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ = \ \mathbf{v}^{\mathsf{T}}\mathbf{M}^n\mathbf{w}$

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2
- Its **characteristic polynomial** is $p(x) = x^2 - x - 1$
- The **characteristic roots** are $\lambda_1 = \frac{1+\sqrt{5}}{2}$ and $\lambda_2 = \frac{1-\sqrt{5}}{2}$
- No repeated roots $\Rightarrow$ Fibonacci sequence is **simple**
- $u_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n = c_1\lambda_1^n + c_2\lambda_2^n$
- $u_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathbf{v}^{\mathsf{T}}\mathbf{M}^n\mathbf{w}$
- Fibonacci has **order** 2 $\Longleftrightarrow$ matrix $\mathbf{M}$ has **dimension** 2×2

Fibonacci: A Closer Look

$u_0 = 0,\ u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$

- The Fibonacci sequence has **order** 2
- Its **characteristic polynomial** is $p(x) = x^2 - x - 1$
- The **characteristic roots** are $\lambda_1 = \frac{1+\sqrt{5}}{2}$ and $\lambda_2 = \frac{1-\sqrt{5}}{2}$
- No repeated roots $\Rightarrow$ Fibonacci sequence is **simple**
- $u_n \;=\; \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \;=\; c_1\lambda_1^n + c_2\lambda_2^n$
- $u_n \;=\; \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; \mathbf{v}^{\mathsf{T}}\mathbf{M}^n\mathbf{w}$
- Fibonacci has **order** 2 $\Longleftrightarrow$ matrix $\mathbf{M}$ has **dimension** 2×2
- Fibonacci sequence is **simple** $\Longleftrightarrow$ $\mathbf{M}$ is **diagonalisable**

Linear Recurrence Sequences

- Numbers $\langle u_0, u_1, u_2, \ldots \rangle$ form a **linear recurrence sequence** if there exist k and constants $a_1, \ldots, a_k$, such that

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

Linear Recurrence Sequences

- Numbers $\langle u_0, u_1, u_2, \ldots \rangle$ form a **linear recurrence sequence** if 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

- Numbers $\langle u_0, u_1, u_2, \ldots \rangle$ form a **linear recurrence sequence** if 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
- Its **characteristic polynomial** is

$$p(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_k$$

Linear Recurrence Sequences

- Numbers $\langle u_0, u_1, u_2, \ldots \rangle$ form a **linear recurrence sequence** if 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
- Its **characteristic polynomial** is

$$p(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_k$$

- The linear recurrence sequence is **simple** if its characteristic polynomial has no repeated roots

Linear Recurrence Sequences

- Numbers $\langle u_0, u_1, u_2, \ldots \rangle$ form a **linear recurrence sequence** if 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
- Its **characteristic polynomial** is

$$p(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_k$$

- The linear recurrence sequence is **simple** if its characteristic polynomial has no repeated roots
- Let $\lambda_1, \lambda_2, \ldots, \lambda_m \in \mathbb{C}$ be the characteristic roots. There exist polynomials $p_1(x), p_2(x), \ldots, p_m(x) \in \mathbb{C}[x]$ such that

$$u_n = p_1(n)\lambda_1^n + p_2(n)\lambda_2^n + \ldots + p_m(n)\lambda_m^n$$

  In general $\lambda_1, \ldots, \lambda_k$ and all coefficients of $p_1(x), \ldots, p_m(x)$ are algebraic numbers

Linear Recurrence Sequences

- Numbers $\langle u_0, u_1, u_2, \ldots \rangle$ form a **linear recurrence sequence** if 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
- Its **characteristic polynomial** is

$$p(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_k$$

- The linear recurrence sequence is **simple** if its characteristic polynomial has no repeated roots
- Let $\lambda_1, \lambda_2, \ldots, \lambda_m \in \mathbb{C}$ be the characteristic roots. There exist polynomials $p_1(x), p_2(x), \ldots, p_m(x) \in \mathbb{C}[x]$ such that

$$u_n = p_1(n)\lambda_1^n + p_2(n)\lambda_2^n + \ldots + p_m(n)\lambda_m^n$$

  In general $\lambda_1, \ldots, \lambda_k$ and all coefficients of $p_1(x), \ldots, p_m(x)$ are algebraic numbers
- If the linear recurrence sequence is **simple** then the polynomials $p_1(x), \ldots, p_m(x)$ are all **constant**

- 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, 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

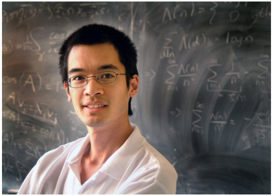
Skolem Problem

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

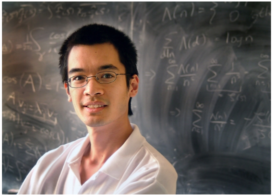
Skolem Problem

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 semilinear:

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

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 semilinear:

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

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 semilinear:

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

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 constructive.

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.

Some Recent Results (I)

Theorem

Positivity is decidable for order 5 or less.

Some Recent Results (I)

Theorem

Positivity is decidable for order 5 or less.

The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ $(\subseteq \mathsf{PSPACE})$.

Some Recent Results (I)

Theorem

Positivity is decidable for order 5 or less.
The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ $(\subseteq \mathsf{PSPACE})$.

Theorem

Ultimate Positivity is decidable for order 5 or less.
The complexity is in P.

Some Recent Results (I)

Theorem

Positivity is decidable for order 5 or less.
The complexity is in $\mathrm{coNP}^{\mathrm{PP}^{\mathrm{PP}^{\mathrm{PP}}}}$ $(\subseteq \mathrm{PSPACE})$.

Theorem

Ultimate Positivity is decidable for order 5 or less.
The complexity is in P.

Theorem

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).

Some Recent Results (II)

Theorem

For **simple** *linear recurrence sequences of order 9 or less, Positivity is decidable.*

The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ $(\subseteq \mathsf{PSPACE})$.

Some Recent Results (II)

Theorem

For **simple** *linear recurrence sequences of order 9 or less, Positivity is decidable.*

The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ ($\subseteq$ PSPACE).

We don't know what happens at order 10. But:

Some Recent Results (II)

Theorem

For **simple** *linear recurrence sequences of order 9 or less, Positivity is decidable.*

The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ $(\subseteq \mathsf{PSPACE})$.

We don't know what happens at order 10. But:

Proposition

Decidability of Positivity for simple linear recurrence sequences of order 14 $\Rightarrow$ *decidability of general Skolem Problem at order 5.*

Some Recent Results (II)

Theorem

For **simple** *linear recurrence sequences of order 9 or less, Positivity is decidable.*

The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ $(\subseteq \mathsf{PSPACE})$.

We don't know what happens at order 10. But:

Proposition

Decidability of Positivity for simple linear recurrence sequences of order 14 $\Rightarrow$ *decidability of general Skolem Problem at order 5.*

Theorem

For **simple** *linear recurrence sequences,*
Ultimate Positivity is decidable for **all** *orders.*

Some Recent Results (II)

Theorem

For **simple** *linear recurrence sequences of order 9 or less, Positivity is decidable.*

The complexity is in $\mathsf{coNP}^{\mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}}$ $(\subseteq \mathsf{PSPACE})$.

We don't know what happens at order 10. But:

Proposition

Decidability of Positivity for simple linear recurrence sequences of order 14 $\Rightarrow$ *decidability of general Skolem Problem at order 5.*

Theorem

For **simple** *linear recurrence sequences,*
Ultimate Positivity is decidable for **all** *orders.*

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

Some Recent Results (II)

Theorem

*For **simple** linear recurrence sequences of order 9 or less, Positivity is decidable.*

The complexity is in $\mathrm{coNP}^{\mathrm{PP}^{\mathrm{PP}^{\mathrm{PP}}}}$ ($\subseteq$ PSPACE)*.*

We don't know what happens at order 10. But:

Proposition

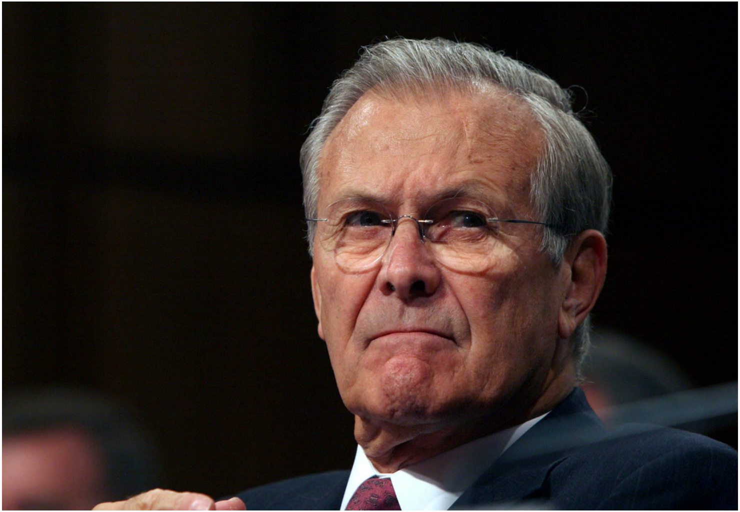
Decidability of Positivity for simple linear recurrence sequences of order 14 $\Rightarrow$ decidability of general Skolem Problem at order 5.

Theorem

*For **simple** linear recurrence sequences, Ultimate Positivity is decidable for **all** orders.*

- *For each fixed order k, complexity is in P (but 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]

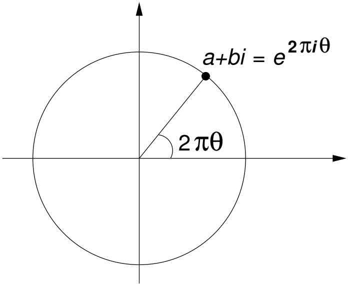
Almost nothing else is known about any specific irrational number!

Hardness

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

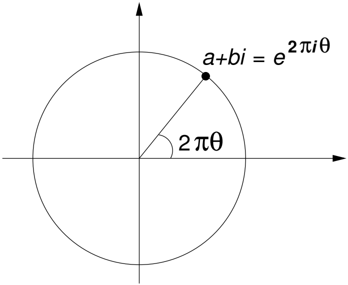
Hardness

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

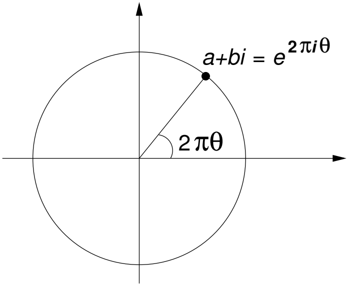
Let $\mathcal{T} = \{\theta \in (0,1) \ : \ e^{2\pi i\theta} \in \mathbb{Q}(i)\} \ \setminus \ \{\frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$



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

Hardness

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

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.

Positivity of Simple LRS: Algorithm Sketch

Theorem

For simple linear recurrence sequences:

- *Ultimate Positivity is decidable for all orders.*
- *Positivity is decidable for orders 9 or less.*

Positivity of Simple LRS: Algorithm Sketch

Theorem

For simple linear recurrence sequences:

- *Ultimate Positivity is decidable for all orders.*
- *Positivity is decidable for orders 9 or less.*

Input: a simple linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order ≤ 9

Positivity of Simple LRS: Algorithm Sketch

Theorem

For simple linear recurrence sequences:

- *Ultimate Positivity is decidable for all orders.*
- *Positivity is decidable for orders 9 or less.*

Input: a simple linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order ≤ 9

1. Decide if $\langle u_n \rangle_{n=0}^{\infty}$ is ultimately positive.
   If it isn't, $\langle u_n \rangle_{n=0}^{\infty}$ is **not** positive. Otherwise:

Positivity of Simple LRS: Algorithm Sketch

Theorem

For simple linear recurrence sequences:

- *Ultimate Positivity is decidable for all orders.*
- *Positivity is decidable for orders 9 or less.*

Input: a simple linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order ≤ 9

1. Decide if $\langle u_n \rangle_{n=0}^{\infty}$ is ultimately positive.
   If it isn't, $\langle u_n \rangle_{n=0}^{\infty}$ is **not** positive. Otherwise:
2. Compute a threshold T such that $\langle u_n \rangle_{n=T}^{\infty}$ is positive.

Positivity of Simple LRS: Algorithm Sketch

Theorem

For simple linear recurrence sequences:

- *Ultimate Positivity is decidable for all orders.*
- *Positivity is decidable for orders 9 or less.*

Input: a simple linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order ≤ 9

1. Decide if $\langle u_n \rangle_{n=0}^{\infty}$ is ultimately positive.
   If it isn't, $\langle u_n \rangle_{n=0}^{\infty}$ is **not** positive. Otherwise:
2. Compute a threshold T such that $\langle u_n \rangle_{n=T}^{\infty}$ is positive.
3. Check individually whether $u_0 \geq 0,\ u_1 \geq 0,\ \ldots,\ u_{T-1} \geq 0$.

Lower Bounds in Diophantine Approximation

Theorem (Dirichlet 1842)

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

Lower Bounds in Diophantine Approximation

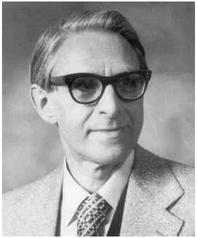
Theorem (Dirichlet 1842)

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

Theorem (Roth 1955)

Let $x \in \mathbb{R}$ *be algebraic. Then for any* $\varepsilon > 0$ *there are finitely many integers p, q such that*

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}} .$$



Lower Bounds in Diophantine Approximation

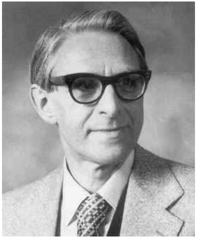
Theorem (Dirichlet 1842)

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

Theorem (Roth 1955)

Let $x \in \mathbb{R}$ be algebraic. Then for any $\varepsilon > 0$ there are finitely many integers p, q such that

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}} .$$



- Non-effective!

Lower Bounds in Diophantine Approximation

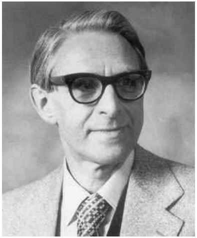
Theorem (Dirichlet 1842)

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

Theorem (Roth 1955)

Let $x \in \mathbb{R}$ be algebraic. Then for any $\varepsilon > 0$ there are finitely many integers p, q such that

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}} .$$



- Non-effective!
- Subsequent vast higher-dimensional generalisations:
  - Schmidt's **Subspace Theorem** (1965–1972)

Lower Bounds in Diophantine Approximation

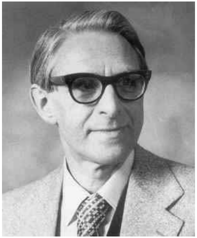
Theorem (Dirichlet 1842)

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

Theorem (Roth 1955)

Let $x \in \mathbb{R}$ be algebraic. Then for any $\varepsilon > 0$ there are finitely many integers p, q such that

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}}.$$



- Non-effective!
- Subsequent vast higher-dimensional generalisations:
    - Schmidt's **Subspace Theorem** (1965–1972)
    - Schlickewei's p-**adic Subspace Theorem** (1977)

Lower Bounds in Diophantine Approximation

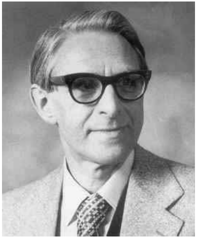
Theorem (Dirichlet 1842)

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

Theorem (Roth 1955)

Let $x \in \mathbb{R}$ be algebraic. Then for any $\varepsilon > 0$ there are finitely many integers p, q such that

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}} .$$



- Non-effective!
- Subsequent vast higher-dimensional generalisations:
  - Schmidt's **Subspace Theorem** (1965–1972)
  - Schlickewei's p-**adic Subspace Theorem** (1977)
- $\Rightarrow$ Evertse, van der Poorten, and Schlickewei's **lower bounds on sums of S-units** (1984–1985)

Lower Bounds on Sums of S-Units: A Simple Example

- How small can the following expression get?

$$|3^x - 7^y|$$

where $x, y \in \mathbb{N}$

Lower Bounds on Sums of S-Units: A Simple Example

- How small can the following expression get?

$$|3^x - 7^y|$$

where $x, y \in \mathbb{N}$

- For all $\varepsilon > 0$, if x and y are 'large enough', then

$$|3^x - 7^y| > M^{1-\varepsilon}$$

where $M = \max\{3^x, 7^y\}$

Lower Bounds on Sums of S-Units: A Simple Example

- How small can the following expression get?

$$|3^x - 7^y|$$

where $x, y \in \mathbb{N}$

- For all $\varepsilon > 0$, if x and y are 'large enough', then

$$|3^x - 7^y| > M^{1-\varepsilon}$$

where $M = \max\{3^x, 7^y\}$

- Constructive proof requires Baker's Theorem (!)

Lower Bounds on Sums of S-Units: A Simple Example

- How about

$$|\, 3^x \pm 7^y \pm 13^z \,|$$

where $x, y, z \in \mathbb{N}$

Lower Bounds on Sums of S-Units: A Simple Example

- How about

$$|\,3^x \pm 7^y \pm 13^z\,|$$

  where $x, y, z \in \mathbb{N}$

- For all $\varepsilon > 0$, if x, y, and z are 'large enough', then

$$|\,3^x \pm 7^y \pm 13^z\,| > M^{1-\varepsilon}$$

  where $M = \max\{3^x, 7^y, 13^z\}$

Lower Bounds on Sums of S-Units: A Simple Example

- How about

$$|\, 3^x \pm 7^y \pm 13^z \,|$$

where $x, y, z \in \mathbb{N}$

- For all $\varepsilon > 0$, if x, y, and z are 'large enough', then

$$|\, 3^x \pm 7^y \pm 13^z \,| > M^{1-\varepsilon}$$

where $M = \max\{3^x, 7^y, 13^z\}$

- **No constructive proof is known !**

Lower Bounds on Sums of S-Units and Simple Linear Recurrence Sequences

We use complex algebraic-integer extensions of such results to study expressions of the form:

$$u_n = c_1\lambda_1^n + c_2\lambda_2^n + \ldots + c_k\lambda_k^n + r(n)$$

Lower Bounds on Sums of S-Units and Simple Linear Recurrence Sequences

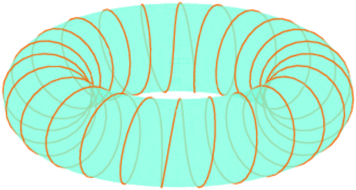
We use complex algebraic-integer extensions of such results to study expressions of the form:

$$u_n = c_1\lambda_1^n + c_2\lambda_2^n + \ldots + c_k\lambda_k^n$$

Lower Bounds on Sums of S-Units and Simple Linear Recurrence Sequences

We use complex algebraic-integer extensions of such results to study expressions of the form:

$$u_n = c_1\lambda_1^n + c_2\lambda_2^n + \ldots + c_k\lambda_k^n$$

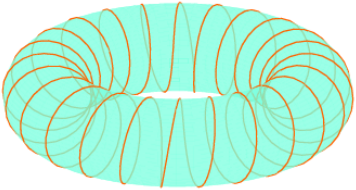


Lower Bounds on Sums of S-Units and Simple Linear Recurrence Sequences

We use complex algebraic-integer extensions of such results to study expressions of the form:

$$u_n = c_1\lambda_1^n + c_2\lambda_2^n + \ldots + c_k\lambda_k^n$$

$$f(z_1, z_2, \ldots, z_k) = c_1 z_1 + c_2 z_2 + \ldots + c_k z_k$$



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

Decision and Synthesis Problems for Linear Dynamical Systems

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