On the Skolem problem

Florian Luca

Wits, MPI-SWS

Banff, August 29, 2022

My main co-authors

J. Ouaknine

J. W. Worrell

Program Termination

- *Question:* so what is the simplest class of programs for which deciding termination/halting is **not** "obvious"?

Program Termination

- *Question:* so what is the simplest class of programs for which deciding termination/halting is **not** "obvious"?
- *Answer:* **simple linear loops!**

Program Termination

- *Question:* so what is the simplest class of programs for which deciding termination/halting is **not** "obvious"?
- *Answer:* **simple linear loops!**

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
  $x := 2x + y;$
  $y := y + 3 - z;$
  $z := -4z + 6;$

Program Termination

- *Question:* so what is the simplest class of programs for which deciding termination/halting is **not** "obvious"?
- *Answer:* **simple linear loops!**

$$
\begin{aligned}
&x := 1;\\
&y := 0;\\
&z := 0;\\
&\text{while} \quad x \neq 0 \quad \text{do}\\
&\qquad x := 2x + y;\\
&\qquad y := y + 3 - z;\\
&\qquad z := -4z + 6;
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{x} := \mathbf{a};\\
&\text{while} \quad x_1 \neq 0 \quad \text{do}\\
&\qquad \mathbf{x} := \mathbf{M}\mathbf{x};
\end{aligned}
$$

Program Termination

- *Question:* so what is the simplest class of programs for which deciding termination/halting is **not** "obvious"?
- *Answer:* **simple linear loops!**

$$
\begin{aligned}
&x := 1;\\
&y := 0;\\
&z := 0;\\
&\text{while} \quad x \neq 0 \quad \text{do}\\
&\qquad x := 2x + y;\\
&\qquad y := y + 3 - z;\\
&\qquad z := -4z + 6;
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{x} := \mathbf{a};\\
&\text{while} \quad x_1 \neq 0 \quad \text{do}\\
&\qquad \mathbf{x} := \mathbf{Mx};
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{x} := \mathbf{a};\\
&\text{while} \quad x_1 \geq 0 \quad \text{do}\\
&\qquad \mathbf{x} := \mathbf{Mx};
\end{aligned}
$$

Program Termination

- *Question:* so what is the simplest class of programs for which deciding termination/halting is **not** "obvious"?
- *Answer:* **simple linear loops!**

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
    $x := 2x + y;$
    $y := y + 3 - z;$
    $z := -4z + 6;$

Skolem Problem:

$\mathbf{x} := \mathbf{a};$
while $x_1 \neq 0$ do
    $\mathbf{x} := \mathbf{M}\mathbf{x};$

$\mathbf{x} := \mathbf{a};$
while $x_1 \geq 0$ do
    $\mathbf{x} := \mathbf{M}\mathbf{x};$

Program Termination

- *Question:* so what is the simplest class of programs for which deciding termination/halting is **not** "obvious"?
- *Answer:* **simple linear loops!**

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
  $x := 2x + y;$
  $y := y + 3 - z;$
  $z := -4z + 6;$

Skolem Problem:

$\mathbf{x} := \mathbf{a};$
while $x_1 \neq 0$ do
  $\mathbf{x} := \mathbf{M}\mathbf{x};$

Positivity Problem:

$\mathbf{x} := \mathbf{a};$
while $x_1 \geq 0$ do
  $\mathbf{x} := \mathbf{M}\mathbf{x};$

What Exactly Are the Skolem and Positivity Problems?

What Exactly Are the Skolem and Positivity Problems?

Problem SKOLEM

Instance: A square $k \times k$ integer matrix $\mathbf{M}$
Question: Is there a positive integer n such that the top-right entry of $\mathbf{M}^n$ is zero?

What Exactly Are the Skolem and Positivity Problems?

Problem SKOLEM

Instance: A square $k \times k$ integer matrix $\mathbf{M}$
Question: Is there a positive integer n such that the top-right entry of $\mathbf{M}^n$ is zero?

Problem POSITIVITY

Instance: A square $k \times k$ integer matrix $\mathbf{M}$
Question: Is it the case that, for all positive integers n, the top-right entry of $\mathbf{M}^n$ is ≥ 0?

Skolem and Positivity Problems: Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and,
$\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

Skolem and Positivity Problems: Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n$.

- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$

Skolem and Positivity Problems: Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and,
$\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- k is the **order** of the sequence
  - Fibonacci has order 2 $(u_{n+2} = u_{n+1} + u_n)$

Skolem and Positivity Problems: Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0: \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- k is the **order** of the sequence
  - Fibonacci has order 2 $(u_{n+2} = u_{n+1} + u_n)$

Problem SKOLEM

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Does $\exists n \geq 0$ such that $u_n = 0$?

Skolem and Positivity Problems: Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0: \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- k is the **order** of the sequence
  - Fibonacci has order 2 $(u_{n+2} = u_{n+1} + u_n)$

Problem SKOLEM

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Does $\exists n \geq 0$ such that $u_n = 0$?

Problem POSITIVITY

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Is it the case that, $\forall n \geq 0,\ u_n \geq 0$?

The Skolem Problem: Open for About 90 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: Open for About 90 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 . . . "

"Arguably, by some distance, the most prominent problem whose decidability status is currently unknown."

Richard Lipton

The Skolem-Mahler-Lech Theorem

Fact: any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

The Skolem-Mahler-Lech Theorem

Fact: any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

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

The set of zeros $\{n \in \mathbb{N} : u_n = 0\}$ *of a non-degenerate LRS* $\langle u_0, u_1, u_2, \ldots \rangle$ *is finite.*

The Skolem-Mahler-Lech Theorem

Fact: any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

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

The set of zeros $\{n \in \mathbb{N} : u_n = 0\}$ *of a non-degenerate LRS* $\langle u_0, u_1, u_2, \ldots \rangle$ *is finite.*

- Decidability of the Skolem Problem is equivalent to being able to compute the finite set of zeros of any given non-degenerate LRS

The Skolem-Mahler-Lech Theorem

Fact: any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

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

The set of zeros $\{n \in \mathbb{N} : u_n = 0\}$ *of a non-degenerate LRS* $\langle u_0, u_1, u_2, \ldots \rangle$ *is finite.*

- Decidability of the Skolem Problem is equivalent to being able to compute the finite set of zeros of any given non-degenerate LRS
- Unfortunately, all known proofs of the Skolem-Mahler-Lech Theorem make use of *non-constructive* p-adic techniques

Some Other Application Areas

SKOLEM and POSITIVITY arise in many other areas (often in hardness results), e.g.:

Some Other Application Areas

SKOLEM and POSITIVITY arise in many other areas (often in hardness results), e.g.:

- Theoretical biology
  - analysis of L-systems
  - population dynamics
- Software verification / program analysis
- Dynamical systems
- Differential privacy
- (Weighted) automata and games
- Analysis of stochastic systems
- Control theory
- Quantum computing
- Statistical physics
- Formal power series
- Combinatorics
- ...

Example: Does This Program Halt?

$$
\begin{aligned}
&x := 1;\\
&y := 0;\\
&z := 0;\\
&\text{while} \quad x \neq 0 \quad \text{do}\\
&\qquad x := 2x + y;\\
&\qquad y := y + 3 - z;\\
&\qquad z := -4z + 6;
\end{aligned}
$$

Example: Does This Program Halt?

$$
\begin{aligned}
&x := 1;\\
&y := 0;\\
&z := 0;\\
&\text{while} \;\; x \neq 0 \;\; \text{do}\\
&\qquad x := 2x + y;\\
&\qquad y := y + 3 - z;\\
&\qquad z := -4z + 6;
\end{aligned}
$$

No! Look at it modulo 3

Example: Does This Program Halt?

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
    $x := 2x + y;$
    $y := y + 3 - z;$
    $z := -4z + 6;$

No! Look at it modulo 3

$$x \equiv \langle 1, 2, 1, 2, 1, 2, \ldots \rangle \pmod{3}$$
$$y \equiv \langle 0, 0, 0, 0, 0, 0, \ldots \rangle \pmod{3}$$
$$z \equiv \langle 0, 0, 0, 0, 0, 0, \ldots \rangle \pmod{3}$$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

Consider this Fibonacci variant, starting with $\langle 2, 1 \rangle$:

$\langle 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, \ldots \rangle$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

Consider this Fibonacci variant, starting with $\langle 2, 1 \rangle$:

$\langle 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, \ldots \rangle$

$\langle 2, 1, 3, 4, 2, 1, 3, 4, 2, 1, 3, 4, \ldots \rangle \pmod 5$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

Consider this Fibonacci variant, starting with $\langle 2, 1 \rangle$:

$\langle 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, \ldots \rangle$

$\langle \underline{2, 1}, 3, 4, \underline{2, 1}, 3, 4, 2, 1, 3, 4, \ldots \rangle \pmod 5$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

Consider this Fibonacci variant, starting with $\langle 2, 1 \rangle$:

$\langle 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, \ldots \rangle$

$\langle \underline{2, 1}, 3, 4, \underline{2, 1}, 3, 4, 2, 1, 3, 4, \ldots \rangle \pmod{5}$

$\Rightarrow$ **Never zero!**

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod 2$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod 2$

$\langle 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \ldots \rangle \pmod 3$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod 2$

$\langle 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \ldots \rangle \pmod 3$

$\langle 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, \ldots \rangle \pmod 4$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod 2$

$\langle 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \ldots \rangle \pmod 3$

$\langle 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, \ldots \rangle \pmod 4$

$\langle 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, 2, \ldots \rangle \pmod 5$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

$\langle \underline{1, 1}, \mathbf{0}, \underline{1, 1}, \mathbf{0}, 1, 1, \mathbf{0}, 1, 1, \mathbf{0}, \ldots \rangle \pmod 2$

$\langle \underline{1, 1}, 2, \mathbf{0}, 2, 2, 1, \mathbf{0}, \underline{1, 1}, 2, \mathbf{0}, \ldots \rangle \pmod 3$

$\langle \underline{1, 1}, 2, 3, 1, \mathbf{0}, \underline{1, 1}, 2, 3, 1, \mathbf{0}, \ldots \rangle \pmod 4$

$\langle \underline{1, 1}, 2, 3, \mathbf{0}, 3, 3, 1, 4, \mathbf{0}, 4, 4, 3, 2, \mathbf{0}, 2, 2, 4, 1, \mathbf{0}, \underline{1, 1}, 2, \ldots \rangle \pmod 5$

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the “shifted” Fibonacci sequence, starting with $\langle 1, 1 \rangle$:
$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

- A modular argument can *never* work here!

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

- A modular argument can *never* work here!
- Because modulo m, the sequence is always periodic. But the same pattern (just shifted by 1) would also appear in the true Fibonacci sequence, starting $\langle 0, 1 \rangle$, and therefore will have to contain infinitely many occurrences of 0!

The Fibonacci Recurrence: $u_{n+2} = u_{n+1} + u_n$

How about the "shifted" Fibonacci sequence, starting with $\langle 1, 1 \rangle$:

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

- A modular argument can *never* work here!
- Because modulo m, the sequence is always periodic. But the same pattern (just shifted by 1) would also appear in the true Fibonacci sequence, starting $\langle 0, 1 \rangle$, and therefore will have to contain infinitely many occurrences of 0!
- The shifted Fibonacci sequence doesn't contain a zero, but is haunted by the ghost of a zero *in its past!*

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$\langle \ldots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots \rangle$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$\langle \ldots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots \rangle$

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

$$0, 1, 2, 3, 4, 5, \ldots$$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$\langle \ldots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots \rangle$

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

$\langle \ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots \rangle$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$\langle \ldots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots \rangle$

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

$\langle \ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots \rangle$

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

$$1, 2, 4, 8, 16, 32, \ldots$$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$$\langle \dots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \dots \rangle$$

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

$$\langle \dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots \rangle$$

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

$$\langle \dots, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, \dots \rangle$$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$\langle \ldots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots \rangle$

$\mathbb{Z}$-reversible

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

$\langle \ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots \rangle$

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

$$\langle \ldots, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, \ldots \rangle$$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$\langle \ldots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots \rangle$

$\mathbb{Z}$-reversible

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

$\langle \ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots \rangle$

$\mathbb{Z}$-reversible

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

$$\langle \ldots, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, \ldots \rangle$$

Reversing Linear Recurence Sequences

- Classical Fibonacci, $u_{n+2} = u_{n+1} + u_n$:

$\langle \dots, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, \dots \rangle$

$\mathbb{Z}$-reversible

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

$\langle \dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots \rangle$

$\mathbb{Z}$-reversible

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

$\langle \dots, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, \dots \rangle$

not $\mathbb{Z}$-reversible

The Bi-Skolem Problem

Problem BI-SKOLEM

Instance: A bi-LRS $\langle \ldots, u_{-2}, u_{-1}, u_0, u_1, u_2, \ldots \rangle$ over $\mathbb{Q}$

Question: Does $\exists n \in \mathbb{Z}$ such that $u_n = 0$?

Simple Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

Simple Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

- e.g., the Fibonacci sequence:

$$u_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Simple Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

- e.g., the Fibonacci sequence:

$$u_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

- The "vast majority" of LRS are simple...

Simple Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

- e.g., the Fibonacci sequence:

$$u_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

- The "vast majority" of LRS are simple...

Simple LRS correspond precisely to **diagonalisable** matrices

SKOLEM and POSITIVITY: State of the Art in One Slide

SKOLEM and POSITIVITY: State of the Art in One Slide

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

For LRS of order ≤ 4, SKOLEM is decidable.

SKOLEM and POSITIVITY: State of the Art in One Slide

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

For LRS of order ≤ 4, SKOLEM is decidable.

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

SKOLEM and POSITIVITY: State of the Art in One Slide

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

For LRS of order ≤ 4, *SKOLEM is decidable.*

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

Corollary

For bi-LRS of order ≤ 4, *BI-SKOLEM is decidable.*

SKOLEM and POSITIVITY: State of the Art in One Slide

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

For LRS of order ≤ 4, SKOLEM is decidable.

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

Corollary

For bi-LRS of order ≤ 4, BI-SKOLEM is decidable.

Theorem (Lipton, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

For $\mathbb{Z}$-reversible LRS of order ≤ 7, SKOLEM is decidable.

SKOLEM and POSITIVITY: State of the Art in One Slide

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

For LRS of order ≤ 4, SKOLEM is decidable.

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

Corollary

For bi-LRS of order ≤ 4, BI-SKOLEM is decidable.

Theorem (Lipton, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

For $\mathbb{Z}$-reversible LRS of order ≤ 7, SKOLEM is decidable.

Theorem (Ouaknine & Worrell 2014)

- *For LRS of order ≤ 5, POSITIVITY is decidable.*
- *For simple LRS of order ≤ 9, POSITIVITY is decidable.*
- *For LRS of order ≥ 6, POSITIVITY is hard with respect to longstanding Diophantine-approximation problems.*

Enter the Classical Conjectures!

Many problems in mathematics and computer science are solvable subject to various standard conjectures, e.g.:

Enter the Classical Conjectures!

Many problems in mathematics and computer science are solvable subject to various standard conjectures, e.g.:

- Miller's polynomial-time test for primality testing, whose correctness relies on the Riemann Hypothesis (Miller 1976)

Enter the Classical Conjectures!

Many problems in mathematics and computer science are solvable subject to various standard conjectures, e.g.:

- Miller's polynomial-time test for primality testing, whose correctness relies on the Riemann Hypothesis (Miller 1976)
- Security of RSA (and pretty much all of modern electronic commerce!), based on the conjecture that factoring is not polynomial time (Rivest, Shamir, Adleman 1977)

Enter the Classical Conjectures!

Many problems in mathematics and computer science are solvable subject to various standard conjectures, e.g.:

- Miller's polynomial-time test for primality testing, whose correctness relies on the Riemann Hypothesis (Miller 1976)
- Security of RSA (and pretty much all of modern electronic commerce!), based on the conjecture that factoring is not polynomial time (Rivest, Shamir, Adleman 1977)
- Decidability of the first-order theory of real arithmetic with exponentiation, subject to Schanuel's Conjecture (Macintyre & Wilkie 1996)

Enter the Classical Conjectures!

Many problems in mathematics and computer science are solvable subject to various standard conjectures, e.g.:

- Miller's polynomial-time test for primality testing, whose correctness relies on the Riemann Hypothesis (Miller 1976)
- Security of RSA (and pretty much all of modern electronic commerce!), based on the conjecture that factoring is not polynomial time (Rivest, Shamir, Adleman 1977)
- Decidability of the first-order theory of real arithmetic with exponentiation, subject to Schanuel's Conjecture (Macintyre & Wilkie 1996)
- Many, many results subject to P$\neq$NP, etc...

Schanuel's Conjecture

Schanuel's Conjecture (early 1960s)

Let $\alpha_1, \ldots, \alpha_n$ be n complex numbers linearly independent over $\mathbb{Q}$. Then the extension field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$ has transcendence degree at least n over $\mathbb{Q}$.

Schanuel's Conjecture

Schanuel's Conjecture (early 1960s)

Let $\alpha_1, \ldots, \alpha_n$ be n complex numbers linearly independent over $\mathbb{Q}$. Then the extension field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$ has transcendence degree at least n over $\mathbb{Q}$.

Equivalently:

Let $\alpha_1, \ldots, \alpha_n$ be n complex numbers linearly independent over $\mathbb{Q}$. Then within the set $\{\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}\}$, one can find (at least) n numbers $\beta_1, \ldots, \beta_n$ that are algebraically independent over $\mathbb{Q}$.

Schanuel's Conjecture

Schanuel's Conjecture (early 1960s)

Let $\alpha_1, \ldots, \alpha_n$ be n complex numbers linearly independent over $\mathbb{Q}$. Then the extension field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$ has transcendence degree at least n over $\mathbb{Q}$.

Equivalently:

Let $\alpha_1, \ldots, \alpha_n$ be n complex numbers linearly independent over $\mathbb{Q}$. Then within the set $\{\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}\}$, one can find (at least) n numbers $\beta_1, \ldots, \beta_n$ that are algebraically independent over $\mathbb{Q}$.

In other words: for any polynomial $P(x_1, \ldots, x_n)$ with rational (or algebraic) coefficients, if $P(\beta_1, \ldots, \beta_n) = 0$, then P must be the zero polynomial.

Schanuel's Conjecture — Example

- e is transcendental (Charles Hermite, 1873)
- π is transcendental (Ferdinand von Lindemann, 1882)

Schanuel's Conjecture — Example

- e is transcendental (Charles Hermite, 1873)
- π is transcendental (Ferdinand von Lindemann, 1882)
- What about $e + \pi$ and $e\pi$?

Schanuel's Conjecture — Example

- e is transcendental (Charles Hermite, 1873)
- π is transcendental (Ferdinand von Lindemann, 1882)
- What about $e + \pi$ and $e\pi$?

Consider

$$\begin{aligned} p(x) &= (x - e)(x - \pi) \\ &= x^2 - (e + \pi)x + e\pi \end{aligned}$$

Schanuel's Conjecture — Example

- e is transcendental (Charles Hermite, 1873)
- π is transcendental (Ferdinand von Lindemann, 1882)
- What about $e + \pi$ and $e\pi$?

Consider

$$\begin{aligned} p(x) &= (x - e)(x - \pi) \\ &= x^2 - (e + \pi)x + e\pi \end{aligned}$$

If *both* $e + \pi$ and $e\pi$ were rational, then e and π would be algebraic, contradiction.

Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

So (assuming Schanuel's Conjecture), $\beta_1 = i\pi$ and $\beta_2 = e$ must be algebraically independent, and therefore π and e must be algebraically independent.

Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

So (assuming Schanuel's Conjecture), $\beta_1 = i\pi$ and $\beta_2 = e$ must be algebraically independent, and therefore π and e must be algebraically independent.

Thus for *any* non-zero polynomial $P(x, y)$ with rational (or algebraic) coefficients, we have that $P(e, \pi)$ cannot be zero.

Schanuel's Conjecture — Example

- So what about $e+\pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

So (assuming Schanuel's Conjecture), $\beta_1 = i\pi$ and $\beta_2 = e$ must be algebraically independent, and therefore π and e must be algebraically independent.

Thus for *any* non-zero polynomial $P(x, y)$ with rational (or algebraic) coefficients, we have that $P(e, \pi)$ cannot be zero.

Therefore $e+\pi$, $e\pi$, and $e^5\pi^3 - e^2\pi^7 + e$ must all be irrational (in fact, transcendental).

Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

So (assuming Schanuel's Conjecture), $\beta_1 = i\pi$ and $\beta_2 = e$ must be algebraically independent, and therefore π and e must be algebraically independent.

Thus for *any* non-zero polynomial $P(x, y)$ with rational (or algebraic) coefficients, we have that $P(e, \pi)$ cannot be zero.

Therefore $e + \pi$, $e\pi$, and $e^5\pi^3 - e^2\pi^7 + e$ must all be irrational (in fact, transcendental).

Schanuel's Conjecture implies that the *only* algebraic relationships that can hold between e and π are the trivial ones (like $(e + \pi)^2 = e^2 + 2e\pi + \pi^2$).

Reversing Linear Recurence Sequences (mod m)

Let

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$$

Reversing Linear Recurence Sequences (mod m)

Let

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$$

Then

$$u_n = \frac{-1}{a_k}\left(a_{k-1}u_{n+1} + a_{k-2}u_{n+2} + \ldots + a_1 u_{n+k-1} - u_{n+k}\right)$$

Reversing Linear Recurence Sequences (mod m)

Let

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$$

Then

$$u_n = \frac{-1}{a_k}\left(a_{k-1}u_{n+1} + a_{k-2}u_{n+2} + \ldots + a_1 u_{n+k-1} - u_{n+k}\right)$$

So if a_k is invertible (mod m), the entire bi-infinite sequence is well-defined in $\mathbb{Z}/m\mathbb{Z}$.

Reversing Linear Recurence Sequences (mod m)

Let

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$$

Then

$$u_n = \frac{-1}{a_k} \left(a_{k-1} u_{n+1} + a_{k-2} u_{n+2} + \ldots + a_1 u_{n+k-1} - u_{n+k} \right)$$

So if a_k is invertible (mod m), the entire bi-infinite sequence is well-defined in $\mathbb{Z}/m\mathbb{Z}$. Therefore we require that $\gcd(m, a_k) = 1$.

Reversing Linear Recurence Sequences (mod m)

Let

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$$

Then

$$u_n = \frac{-1}{a_k}\left(a_{k-1}u_{n+1} + a_{k-2}u_{n+2} + \ldots + a_1 u_{n+k-1} - u_{n+k}\right)$$

So if a_k is invertible (mod m), the entire bi-infinite sequence is well-defined in $\mathbb{Z}/m\mathbb{Z}$. Therefore we require that $\gcd(m, a_k) = 1$.

- Example: $u_{n+1} = 2u_n$:

$$\langle \ldots, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, \ldots \rangle$$

Reversing Linear Recurence Sequences (mod m)

Let

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$$

Then

$$u_n = \frac{-1}{a_k}\left(a_{k-1}u_{n+1} + a_{k-2}u_{n+2} + \ldots + a_1 u_{n+k-1} - u_{n+k}\right)$$

So if a_k is invertible (mod m), the entire bi-infinite sequence is well-defined in $\mathbb{Z}/m\mathbb{Z}$. Therefore we require that $\gcd(m, a_k) = 1$.

- Example: $u_{n+1} = 2u_n$:

$$\langle \ldots, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, \ldots \rangle$$

$$\langle \ldots, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \ldots \rangle \pmod 3$$

Reversing Linear Recurence Sequences (mod m)

Let

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$$

Then

$$u_n = \frac{-1}{a_k}\left(a_{k-1}u_{n+1} + a_{k-2}u_{n+2} + \ldots + a_1 u_{n+k-1} - u_{n+k}\right)$$

So if a_k is invertible (mod m), the entire bi-infinite sequence is well-defined in $\mathbb{Z}/m\mathbb{Z}$. Therefore we require that $\gcd(m, a_k) = 1$.

- Example: $u_{n+1} = 2u_n$:

$$\langle \ldots, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, \ldots \rangle$$

$$\langle \ldots, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \ldots \rangle \pmod 3$$

$$\langle \ldots, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1, 2, \ldots \rangle \pmod 5$$

The Skolem Conjecture

- A fairly wide-ranging conjecture, formulated in 1937, also known as the **Exponential Local-Global Principle**
- Like Schanuel's Conjecture, widely believed by number theorists, but only proven in special cases

The Skolem Conjecture

The Skolem Conjecture for simple bi-LRS (1937)

Consider the recurrence equation $u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$, with $u_0, \ldots, u_{k-1}, a_1, \ldots, a_k \in \mathbb{Z}$. Suppose the bi-LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ is simple. Then $\langle u_n \rangle_{n=-\infty}^{\infty}$ has no zeros iff, for some integer $m \geq 2$ with $\gcd(m, a_k) = 1$, we have that for all $n \in \mathbb{Z}$, $u_n \not\equiv 0 \pmod{m}$.

The Skolem Conjecture

The Skolem Conjecture for simple bi-LRS (1937)

Consider the recurrence equation $u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$, with $u_0, \ldots, u_{k-1}, a_1, \ldots, a_k \in \mathbb{Z}$. Suppose the bi-LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ is simple. Then $\langle u_n \rangle_{n=-\infty}^{\infty}$ has no zeros iff, for some integer $m \geq 2$ with $\gcd(m, a_k) = 1$, we have that for all $n \in \mathbb{Z}$, $u_n \not\equiv 0 \pmod{m}$.

Equivalently:

If a simple bi-infinite LRS over the rationals has no zeros, then this will necessarily be witnessed modulo *some* integer m.

The Skolem Conjecture

The Skolem Conjecture for simple bi-LRS (1937)

Consider the recurrence equation $u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$, with $u_0, \ldots, u_{k-1}, a_1, \ldots, a_k \in \mathbb{Z}$. Suppose the bi-LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ is simple. Then $\langle u_n \rangle_{n=-\infty}^{\infty}$ has no zeros iff, for some integer $m \geq 2$ with $\gcd(m, a_k) = 1$, we have that for all $n \in \mathbb{Z}$, $u_n \not\equiv 0 \pmod{m}$.

Equivalently:

If a simple bi-infinite LRS over the rationals has no zeros, then this will necessarily be witnessed modulo *some* integer m.

Theorem (Lipton, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

The Skolem Problem for LRS of order 5 *is decidable, assuming the Skolem Conjecture.*

The Skolem Conjecture

The Skolem Conjecture for simple bi-LRS (1937)

Consider the recurrence equation $u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$, with $u_0, \ldots, u_{k-1}, a_1, \ldots, a_k \in \mathbb{Z}$. Suppose the bi-LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ is simple. Then $\langle u_n \rangle_{n=-\infty}^{\infty}$ has no zeros iff, for some integer $m \geq 2$ with $\gcd(m, a_k) = 1$, we have that for all $n \in \mathbb{Z}$, $u_n \not\equiv 0 \pmod{m}$.

Equivalently:

If a simple bi-infinite LRS over the rationals has no zeros, then this will necessarily be witnessed modulo *some* integer m.

Theorem (Lipton, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

The Skolem Problem for LRS of order 5 *is decidable, assuming the Skolem Conjecture.*

- Note the above applies to *all* order-5 LRS (simple/non-simple)

The Skolem Problem for Simple LRS

The Skolem Problem for Simple LRS

Theorem (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

There is an algorithm which takes as input a simple, non-degenerate LRS and produces its (finite) set of zeros.

The Skolem Problem for Simple LRS

Theorem (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

There is an algorithm which takes as input a simple, non-degenerate LRS and produces its (finite) set of zeros. Termination is guaranteed assuming the Skolem Conjecture and the p-adic Schanuel Conjecture.

The Skolem Problem for Simple LRS

Theorem (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

There is an algorithm which takes as input a simple, non-degenerate LRS and produces its (finite) set of zeros. Termination is guaranteed assuming the Skolem Conjecture and the p-adic Schanuel Conjecture.

- The two conjectures are *only* needed to prove termination, *not* correctness

The Skolem Problem for Simple LRS

Theorem (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

There is an algorithm which takes as input a simple, non-degenerate LRS and produces its (finite) set of zeros. Termination is guaranteed assuming the Skolem Conjecture and the p-adic Schanuel Conjecture.

- The two conjectures are *only* needed to prove termination, *not* correctness
- In other words, the algorithm also produces an independent (conjecture-free) **correctness certificate**

The Skolem Problem for Simple LRS

Theorem (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

There is an algorithm which takes as input a simple, non-degenerate LRS and produces its (finite) set of zeros. Termination is guaranteed assuming the Skolem Conjecture and the p-adic Schanuel Conjecture.

- The two conjectures are *only* needed to prove termination, *not* correctness
- In other words, the algorithm also produces an independent (conjecture-free) **correctness certificate**
- Implemented in our online tool SKOLEM !
  `https://skolem.mpi-sws.org/`

skolem.mpi-sws.org

Accounts Teams

SKOLEM: Solves the Skolem Problem for simple integer LRS

System Explanation Show/Hide

- On the first line write the coefficients of the recurrence relation, separated by spaces.
- On the second line write an equal number of space-separated initial values.
- The LRS must be simple, non-degenerate, and not the zero LRS.
- The tool will output all zeros (at both positive and negative indices), along with a completeness certificate.

Input Format

$a_1\ a_2\ \dots\ a_k$
$u_0\ u_1\ \dots\ u_{k-1}$

where:
$u_{n+k} = a_1 \cdot u_{n+k-1} + a_2 \cdot u_{n+k-2} + \dots + a_k \cdot u_n$

Input area

Auto-fill examples: Show/Hide

Zero LRS | Degenerate LRS | Non-simple LRS | Trivial | Fibonacci | Tribonacci | Berstel sequence [1] | Order 5 [3] | Order 6 [3] | Reversible order 8 [3]

Manual input:

```
6 -25 66 -120 150 -89 18 -1
0 0 -48 -120 0 520 624 -2016
```

- Always render full LRS (otherwise restricted to 400 characters)
- I solemnly swear the LRS is non-degenerate (skips degeneracy check, it will timeout or break if the LRS is degenerate!)
- Factor subcases (merges subcases into single linear set, sometimes requires higher modulo classes)
- Use GCD reduction (reduces initial values by GCD)
- Use fast identification of mod-m (requires GCD reduction) (may result in non-minimal mod-m argument)

Go | Clear | Stop

Output area

Zeros: 0, 1, 4

Zero at 0 in $(0 + 1\mathbb{Z})$ hide/show

- p-adic non-zero in $(0 + 136\mathbb{Z}_{\neq 0})$
- Zero at 1 in $(1 + 136\mathbb{Z})$ hide/show
  - p-adic non-zero in $(1 + 680\mathbb{Z}_{\neq 0})$ $((0 + 5\mathbb{Z}_{\neq 0})$ of parent)
  - Non-zero mod 3 in $(137 + 680\mathbb{Z})$ $((1 + 5\mathbb{Z})$ of parent)
  - Non-zero mod 3 in $(273 + 680\mathbb{Z})$ $((2 + 5\mathbb{Z})$ of parent)
  - Non-zero mod 9 in $(409 + 680\mathbb{Z})$ $((3 + 5\mathbb{Z})$ of parent)
  - Non-zero mod 3 in $(545 + 680\mathbb{Z})$ $((4 + 5\mathbb{Z})$ of parent)
- Non-zero mod 7 in $(2 + 136\mathbb{Z})$

```
================
LRS: u_{n} =
-271613116171209744858663520558946347040150955089064191363633545467540976915
1} +
-508757179425530608464927613320696582397187501636529439512475357072393244955
2} +
-102066400158641189915199426519447202492215998409667435547930568677820080526
3} +
-141209566240600031036449671518126066729890157506482293126851759080465437598
4} +
190695589477320710360984265894091422375694233909158701965446106943727346702
5} +
```

Computing the Zero Set of Simple, Non-Degenerate LRS

Key technical tool: *"p-adic leapfrogging"*

Computing the Zero Set of Simple, Non-Degenerate LRS

Key technical tool: *"p-adic leapfrogging"*

Lemma (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ *be a non-degenerate LRS with* $u_0 = 0$.
Assuming the p-adic Schanuel Conjecture, one can compute an integer $M \geq 1$ *such that, for all* $n \geq 1$, $u_{nM} \neq 0$.
In other words, the subsequence $\langle u_M, u_{2M}, u_{3M}, \ldots \rangle$ *has no zeros.*

Computing the Zero Set of Simple, Non-Degenerate LRS

Key technical tool: *"p-adic leapfrogging"*

Lemma (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ be a non-degenerate LRS with $u_0 = 0$. Assuming the p-adic Schanuel Conjecture, one can compute an integer $M \geq 1$ such that, for all $n \geq 1$, $u_{nM} \neq 0$. In other words, the subsequence $\langle u_M, u_{2M}, u_{3M}, \ldots \rangle$ has no zeros.

- The resulting subsequence is guaranteed not to contain any zeros, and an independent correctness certificate can be produced; the p-adic Schanuel Conjecture is needed only to ensure termination (of the calculation of M)

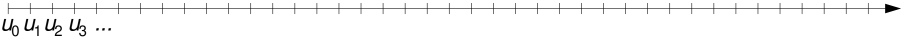
Computing the Zero Set of Simple, Non-Degenerate LRS

Key technical tool: *"p-adic leapfrogging"*

Lemma (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ *be a non-degenerate LRS with* $u_0 = 0$*.*
Assuming the p-adic Schanuel Conjecture, one can compute an integer $M \geq 1$ *such that, for all* $n \geq 1$, $u_{nM} \neq 0$*.*
In other words, the subsequence $\langle u_M, u_{2M}, u_{3M}, \ldots \rangle$ *has no zeros.*

- The resulting subsequence is guaranteed not to contain any zeros, and an independent correctness certificate can be produced; the p-adic Schanuel Conjecture is needed only to ensure termination (of the calculation of M)



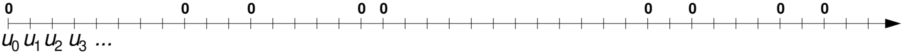
Computing the Zero Set of Simple, Non-Degenerate LRS

Key technical tool: *"p-adic leapfrogging"*

Lemma (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ be a non-degenerate LRS with $u_0 = 0$.
Assuming the p-adic Schanuel Conjecture, one can compute an integer $M \geq 1$ such that, for all $n \geq 1$, $u_{nM} \neq 0$.
In other words, the subsequence $\langle u_M, u_{2M}, u_{3M}, \ldots \rangle$ has no zeros.

- The resulting subsequence is guaranteed not to contain any zeros, and an independent correctness certificate can be produced; the p-adic Schanuel Conjecture is needed only to ensure termination (of the calculation of M)



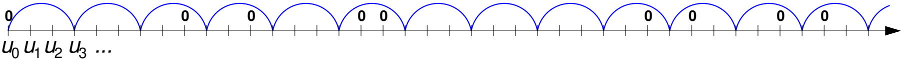
Computing the Zero Set of Simple, Non-Degenerate LRS

Key technical tool: *"p-adic leapfrogging"*

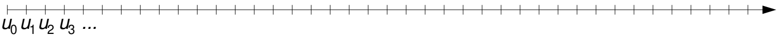
Lemma (Bilu, L., Nieuwveld, Ouaknine, Purser, Worrell 2022)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ be a non-degenerate LRS with $u_0 = 0$. Assuming the p-adic Schanuel Conjecture, one can compute an integer $M \geq 1$ such that, for all $n \geq 1$, $u_{nM} \neq 0$. In other words, the subsequence $\langle u_M, u_{2M}, u_{3M}, \ldots \rangle$ has no zeros.

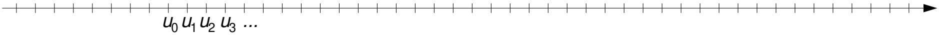
- The resulting subsequence is guaranteed not to contain any zeros, and an independent correctness certificate can be produced; the p-adic Schanuel Conjecture is needed only to ensure termination (of the calculation of M)



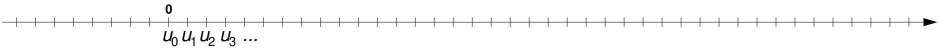
Computing the Zero Set of Simple, Non-Degenerate LRS



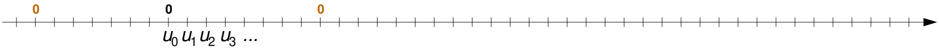
Computing the Zero Set of Simple, Non-Degenerate LRS



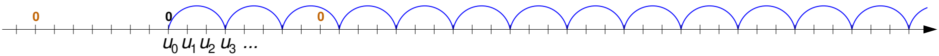
Computing the Zero Set of Simple, Non-Degenerate LRS



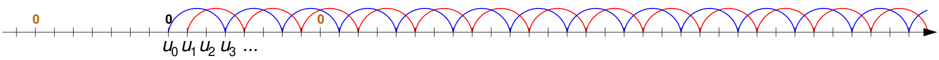
Computing the Zero Set of Simple, Non-Degenerate LRS



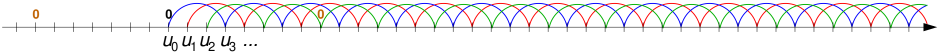
Computing the Zero Set of Simple, Non-Degenerate LRS



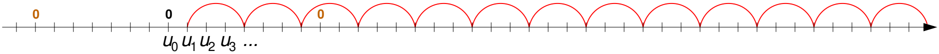
Computing the Zero Set of Simple, Non-Degenerate LRS



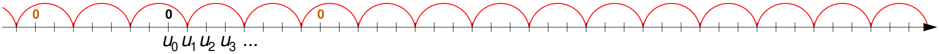
Computing the Zero Set of Simple, Non-Degenerate LRS



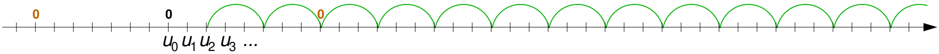
Computing the Zero Set of Simple, Non-Degenerate LRS



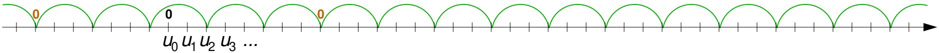
Computing the Zero Set of Simple, Non-Degenerate LRS



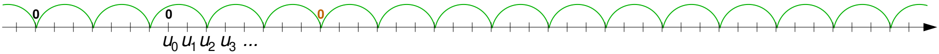
Computing the Zero Set of Simple, Non-Degenerate LRS



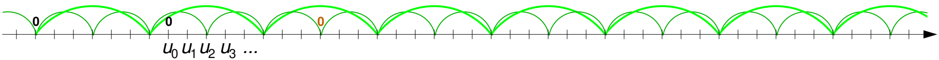
Computing the Zero Set of Simple, Non-Degenerate LRS



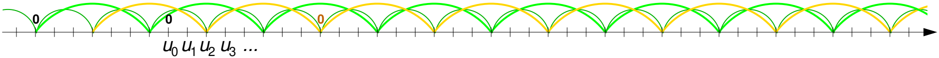
Computing the Zero Set of Simple, Non-Degenerate LRS



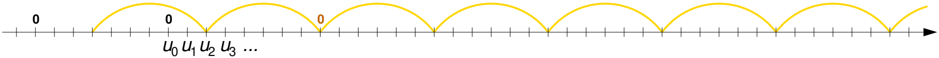
Computing the Zero Set of Simple, Non-Degenerate LRS



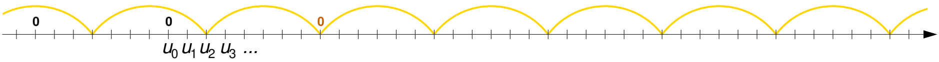
Computing the Zero Set of Simple, Non-Degenerate LRS



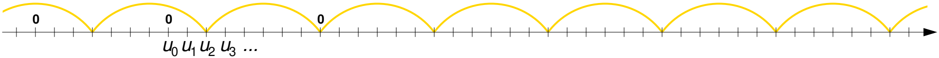
Computing the Zero Set of Simple, Non-Degenerate LRS



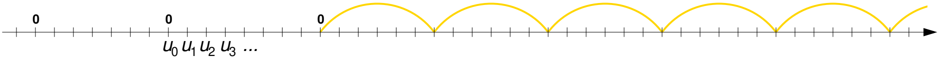
Computing the Zero Set of Simple, Non-Degenerate LRS



Computing the Zero Set of Simple, Non-Degenerate LRS

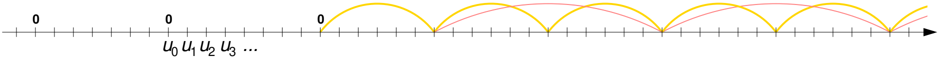


Computing the Zero Set of Simple, Non-Degenerate LRS

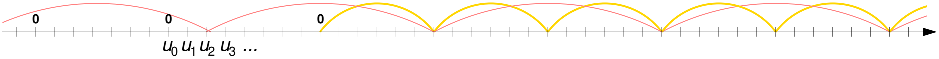


Computing the Zero Set of Simple, Non-Degenerate LRS

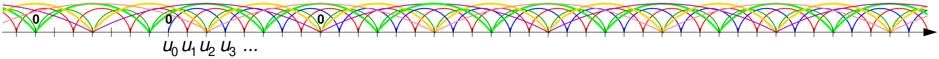
Computing the Zero Set of Simple, Non-Degenerate LRS



Computing the Zero Set of Simple, Non-Degenerate LRS



Computing the Zero Set of Simple, Non-Degenerate LRS



skolem.mpi-sws.org

Accounts Teams

SKOLEM: Solves the Skolem Problem for simple integer LRS

System Explanation Show/Hide

- On the first line write the coefficients of the recurrence relation, separated by spaces.
- On the second line write an equal number of space-separated initial values.
- The LRS must be simple, non-degenerate, and not the zero LRS.
- The tool will output all zeros (at both positive and negative indices), along with a completeness certificate.

Input Format

$a_1 \; a_2 \; \ldots \; a_k$

$u_0 \; u_1 \; \ldots \; u_{k-1}$

where:

$u_{n+k} = a_1 \cdot u_{n+k-1} + a_2 \cdot u_{n+k-2} + \ldots + a_k \cdot u_n$

Input area

Auto-fill examples: Show/Hide

Zero LRS | Degenerate LRS | Non-simple LRS | Trivial | Fibonacci | Tribonacci | Berstel sequence [1] | Order 5 [3] | Order 6 [3] | Reversible order 8 [3]

Manual input:

```
6 -25 66 -120 150 -89 18 -1
0 0 -48 -120 0 520 624 -2016
```

- Always render full LRS (otherwise restricted to 400 characters)
- I solemnly swear the LRS is non-degenerate (skips degeneracy check, it will timeout or break if the LRS is degenerate!)
- Factor subcases (merges subcases into single linear set, sometimes requires higher modulo classes)
- Use GCD reduction (reduces initial values by GCD)
- Use fast identification of mod-m (requires GCD reduction) (may result in non-minimal mod-m argument)

Go | Clear | Stop

Output area

Zeros: 0, 1, 4

Zero at 0 in (0+ 1ℤ) hide/show

- p-adic non-zero in (0+ 136$\mathbb{Z}_{\neq 0}$)
- Zero at 1 in (1+ 136ℤ) hide/show
  - p-adic non-zero in (1+ 680$\mathbb{Z}_{\neq 0}$) ((0+ 5$\mathbb{Z}_{\neq 0}$) of parent)
  - Non-zero mod 3 in (137+ 680ℤ) ((1+ 5ℤ) of parent)
  - Non-zero mod 3 in (273+ 680ℤ) ((2+ 5ℤ) of parent)
  - Non-zero mod 9 in (409+ 680ℤ) ((3+ 5ℤ) of parent)
  - Non-zero mod 3 in (545+ 680ℤ) ((4+ 5ℤ) of parent)
- Non-zero mod 7 in (2+ 136ℤ)

```
=================
LRS: u_{n} =
-27161311617120974485866352055894634704015095508906419136363354546754097691
1} +
-50875717942553060846492761332069658239718750163652943951247535707239324495
2} +
-10206640015864118991519942651944720249221599840966743554793056867782008052
3} +
-14120956624060003103644967151812606672989015750648229312685175908046543759
4} +
19069558947732071036098426589409142237569423390915870196544610694372734670
5} +
```

Universal Skolem sets

We initiated an alternative approach to the decidability of Skolem's Problem. Rather than place restrictions on sequences (e.g., on the order of the recurrence or dominance pattern of the characteristic roots), the idea is to restrict the domain in which to search for zeros.

Definition

We say that $\mathcal{S} \subseteq \mathbb{N}$ is a *Universal Skolem Set* if there is an effective procedure that, given an integer linear recurrence sequence $\boldsymbol{u}$, outputs whether or not there exists $n \in \mathcal{S}$ with $u(n) = 0$.

Universal Hilbert sets

• Definition 9 is inspired by the notion of a *Universal Hilbert set*.

• Let $P(X, Y) \in \mathbb{Q}[X, Y]$ be an irreducible polynomial in two variables in which X has degree at least two.

• Hilbert's Irreducibility Theorem asserts that the set

$$S_P = \{n \in \mathbb{Z} : P(X, n) \text{ is reducible in } \mathbb{Q}[X]\}$$

has density zero, i.e.,

$$\lim_{T \to \infty} \frac{1}{T} \#(S_P \cap [-T, T]) = 0\,.$$

• S. D. Cohen (**1981**) proved that

$$\#(S_P \cap [-T, T]) = O(T^{1/2} \log T)$$

On the other hand, there are polynomials P for which

$$\#(S_P \cap [-T, T]) \asymp (T^{1/2}) \quad \text{for example} \quad (X, Y) = X^2 - Y$$

for which

$$S_P = \{m^2 : m \in \mathbb{Z}\}.$$

• Motivated by such a result, a Universal Hilbert set is an infinite set S of integers such that $S \cap S_P$ is finite for all irreducible polynomials $P(X, Y) \in \mathbb{Q}[X, Y]$.

• Bilu (**1996**) proved that

$$\{m^3 + \lfloor \log\log |m| \rfloor : m \in \mathbb{Z},\ |m| \geq 3\}$$

is a Universal Hilbert set.

• Filaseta and Wilcox (**2019**) constructed a dense Universal Hilbert set.

The first Universal Skolem set known to mankind

Theorem

*(L., Ouaknine, Worrell, **2021**). Define* $f : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ *by*

$$f(n) := \lfloor \sqrt{\log n} \rfloor,$$

and define the sequence $(s_n)_{n \geq 0}$*, inductively by*

$$s_0 = 1 \qquad \text{and} \qquad s_n = n! + s_{f(n)} \quad \text{for} \quad n > 0.$$

Then $\mathcal{S} := \{s_n : n \in \mathbb{N}\}$ *is a Universal Skolem Set.*

The first few elements of $\mathcal{S}$ are

$$\{1, 1! + 1, 2! + 1, 3! + 1, 4! + 1, 5! + 1, 6! + 1, 7! + 1, 8! + 2! + 1, \ldots\}$$

or

$$\{1, 2, 37, 25, 121, 721, 5041, 40323, \ldots\}.$$

Assume $(u(n))_{n\geq 0}$ is given by the minimal recurrence

$$u(n+k) = a_1 u(n+k-1) + \cdots + a_k u(n) \qquad n \geq 0.$$

Let Δ be the discriminant of the characteristic polynomial

$$f(X) = X^k - a_1 X^{k-1} - \cdots - a_k$$

and d be the degree of its splitting field over $\mathbb{Q}$. The proof is based on the following result.

Proposition

For all $m, n, p \in \mathbb{N}$ such that p is a prime that does not divide $a_k\Delta$ and $p^d \leq m$, we have

$$u(n+m!) \equiv u(n) \bmod p\,.$$

In particular, if $u(s_n) = 0$, then

$$u(n! + s_{f(n)}) = 0.$$

Thus,

$$u(s_{f(n)}) \equiv 0 \pmod{P} \quad \text{where} \quad P = \prod_{\substack{p \le n^{1/d} \\ p \nmid \Delta a_k}} p.$$

Since $P > \exp(Kf(n)!) > |u(s_{f(n)})|$ for $n > n_u$, we get that

$$u(s_{f(n)}) = 0.$$

Thus, if n is large and $u(s_n) = 0$, then

$$u(s_{f(n)}) = u(s_{f^2(n)}) = \cdots = u(s_{f^k(n)}) = 0$$

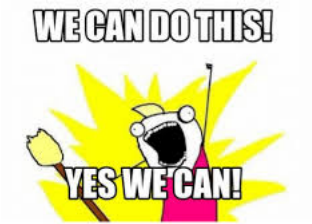
for $n > N_k$. Since k is explicitely bounded by results of Schlickewei, Schmidt, we get that n is explicitly bounded.

How thick is our set?

Our set is not too thick. In fact if $s_n \leq x$, then $n! \leq x$, so that

$$\#(\mathcal{S} \cap [1, x]) = (1 + o(1)) \frac{\log x}{\log \log x} \quad \text{as} \quad x \to \infty.$$

Can we do better?



Meme Maker - we-can-do-this-yes-we-can

An Universal Skolem Set of positive lower density

- For a $k \geq 1$ and real $x \geq 3$, we define inductively $\log_k x$ as

$$\log_1 x = \log x, \quad \log_k x = \max\{1, \log_{k-1} \log x\} \quad \text{for} \quad k \geq 2.$$

- For $X \geq 10$, we let

$$A(X) := [(\log_2 X)^{10}, \sqrt{\log X}], \quad B(X) := \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2 \log X}{\sqrt{\log_3 X}} \right].$$

- For $n \in [X, 2X]$, we write $r(n)$ for the number

$$\#\{(q, P, a) : n = qP + a,\ q \in A(X),\ P \text{ primes},\ a \in B(X)\}.$$

We let

$$N(X) := \{n \in [X, 2X] : r(n) > \log_4 X \text{ and all representations } n = qP + a \text{ have distinct } q,\ a,\ a \pm q\}.$$

Then our set is

$$\mathcal{S} := \bigcup_{k \geq 10} N(2^k).$$

The set $\mathcal{S}$ is a Universal Skolem set

Using a result of H.-P. Schlikewei, W. Schmidt (**2000**) on the number of solutions of multivariate exponential polynomial equations, we proved:

Theorem

Let $\mathbf{u}$ *be a non-degenerate linearly recurrent sequence of order* $k \geq 2$ *of integers given by*

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n$$

for $n \geq 1$*, with given initial terms* $u_1, \ldots, u_k$ *not all zero. Let*

$$A = \max\{10, |u_i|, |a_i| : 1 \leq i \leq k\}.$$

If $u_n = 0$ *and* $n \in \mathcal{S}$*, then*

$$n < \max\{\exp_3(A^2), \exp_5(10^{10} k^6)\}.$$

The fact that $\mathcal{S}$ is of positive lower density follows from a Cauchy-Schwartz argument.

The Skolem Landscape

The Skolem Landscape