Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

Large zeros of Linearly Recurrent Sequences

Florian Luca
Stellenbosch, MPI-SWS, Oxford

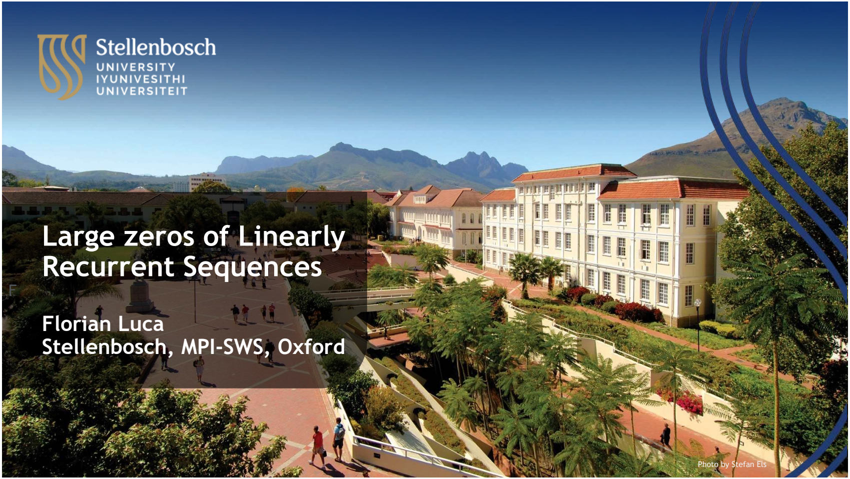


Photo by Stefan Els

Linearly recurrent sequences

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

Linearly recurrent sequences

A **linear recurrent 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 $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$

Linearly recurrent sequences

A **linear recurrent 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

Linearly recurrent sequences

A **linear recurrent 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
- The Fibonacci sequence has order 2 $\;(F_{n+2} = F_{n+1} + F_n)$

A **linear recurrent 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
- The Fibonacci sequence has order 2 $\;(F_{n+2} = F_{n+1} + F_n)$

One can write

$$u_n = \sum_{j=1}^{k} P_j(n) \lambda_j^n \qquad \forall n \geq 0,$$

with $P_j(x) \in \mathbb{C}[x]$, where the above data can be read from the recurrence and initial values.

The Skolem Problem

Problem SKOLEM

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$

Question: Does $\exists n \geq 0$ such that $u_n = 0$?

The Skolem Problem

Problem SKOLEM

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

This problem has been open for about 90 years.

The Skolem-Mahler-Lech Theorem

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

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

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

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

The Skolem-Mahler-Lech Theorem

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

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

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

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

Various proofs are known:

The Skolem-Mahler-Lech Theorem

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

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

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

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

Various proofs are known:

- Using p-adic analysis
- Using the Subspace theorem

The Skolem-Mahler-Lech Theorem

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

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

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

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

Various proofs are known:

- Using p-adic analysis
- Using the Subspace theorem

Neither is effective

Bounds on the number of zeros

Theorem (Schmidt 2000; Amoroso and Viada 2011)

A **non-degenerate** *linear recurrence sequence of order k that is not identically zero has at most* $\exp\exp 70k$ *zeros.*

Bounds on the number of zeros

Theorem (Schmidt 2000; Amoroso and Viada 2011)

A **non-degenerate** *linear recurrence sequence of order k that is not identically zero has at most* $\exp\exp 70k$ *zeros.*

An LRS is degenerate if λ_i/λ_j is a root of unity for some $i \neq j$.

Bounds on the number of zeros

Theorem (Schmidt 2000; Amoroso and Viada 2011)

A **non-degenerate** *linear recurrence sequence of order k that is not identically zero has at most* $\exp\exp 70k$ *zeros.*

An LRS is degenerate if λ_i/λ_j is a root of unity for some $i \neq j$.

Such sequences can be written as merge of lower-order LRS's (e.g., $\langle 1, 2, 1, 2, 1, 2, \ldots \rangle$).

Classical State of the Art in One Slide

Classical State of the Art in One Slide

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

For LRS of order ≤ 4, SKOLEM is decidable.

Classical 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.

Classical 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.

MSTV property: at most 3 dominant roots w.r.t. usual absolute value on $\mathbb{C}$ and at most 2 dominant roots w.r.t. p-adic absolute value.

An example

An example

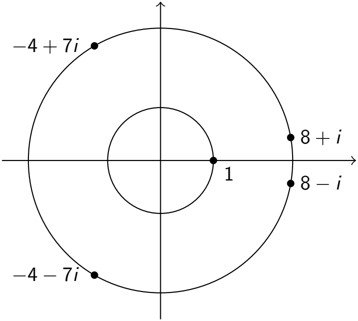
Consider the recurrence

$$u_{n+5} = 9u_{n+4} - 10u_{n+3} + 522u_{n+2} - 4745u_{n+1} + 4225u_n$$

An example

Consider the recurrence

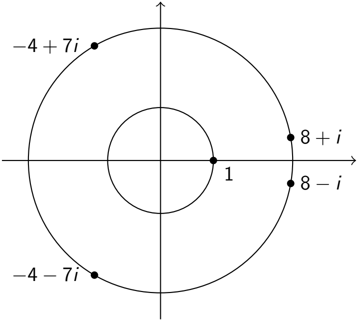
$$u_{n+5} = 9u_{n+4} - 10u_{n+3} + 522u_{n+2} - 4745u_{n+1} + 4225u_n$$



An example

Consider the recurrence

$$u_{n+5} = 9u_{n+4} - 10u_{n+3} + 522u_{n+2} - 4745u_{n+1} + 4225u_n$$

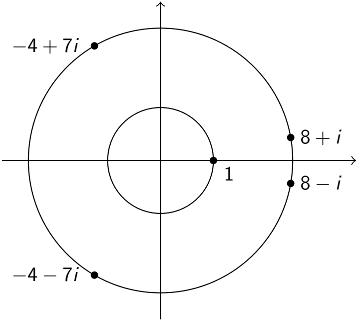


- Dominant roots $(1 \pm 2i)(2 \pm 3i)$

An example

Consider the recurrence

$$u_{n+5} = 9u_{n+4} - 10u_{n+3} + 522u_{n+2} - 4745u_{n+1} + 4225u_n$$

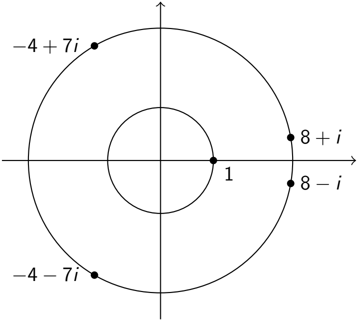


- Dominant roots $(1 \pm 2i)(2 \pm 3i)$
- Each prime above divides exactly two roots

An example

Consider the recurrence

$$u_{n+5} = 9u_{n+4} - 10u_{n+3} + 522u_{n+2} - 4745u_{n+1} + 4225u_n$$

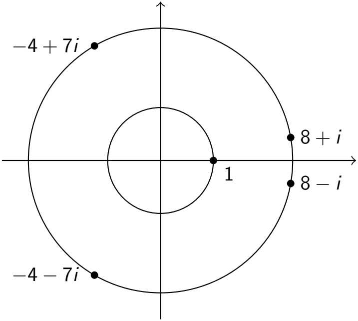


- Dominant roots $(1 \pm 2i)(2 \pm 3i)$
- Each prime above divides exactly two roots
- **Empirically**: for all $u_0, \ldots, u_4$ there exists k s.t. $u_n = 0 \pmod{5^k}$ for only finitely many n.

An example

Consider the recurrence

$$u_{n+5} = 9u_{n+4} - 10u_{n+3} + 522u_{n+2} - 4745u_{n+1} + 4225u_n$$



- Dominant roots $(1 \pm 2i)(2 \pm 3i)$
- Each prime above divides exactly two roots
- **Empirically**: for all $u_0, \ldots, u_4$ there exists k s.t. $u_n = 0 \pmod{5^k}$ for only finitely many n. **Why??**

A **universal Skolem set (USS)** is a subset $\mathcal{S}$ of $\mathbb{N}$ such that for all linearly recurrent sequences $\langle u_n \rangle$ the set

$$\{n \in \mathcal{S} : u_n = 0\}$$

is computable.

Universal Skolem Sets

A **universal Skolem set (USS)** is a subset $\mathcal{S}$ of $\mathbb{N}$ such that for all linearly recurrent sequences $\langle u_n \rangle$ the set

$$\{n \in \mathcal{S} : u_n = 0\}$$

is computable.
Finite sets are universal Skolem sets.

Universal Skolem Sets

A **universal Skolem set (USS)** is a subset $\mathcal{S}$ of $\mathbb{N}$ such that for all linearly recurrent sequences $\langle u_n \rangle$ the set

$$\{n \in \mathcal{S} : u_n = 0\}$$

is computable.
Finite sets are universal Skolem sets.

"Can one solve the Skolem Problem on the set of primes? "

The first universal Skolem set

The first universal Skolem set

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 universal Skolem set

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

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

LICS 2021 Distinguished Papers

Fusible numbers and Peano Arithmetic – Jeff Erickson, Gabriel Nivasch and Junyan Xu.

Positive first-order logic on words – Denis Kuperberg.

Inapproximability of Unique Games in Fixed-Point Logic with Counting – Jamie Tucker-Foltz. (co-winner of Kleene Award for Best Student Paper)

Separating Rank Logic from Polynomial Time – Moritz Lichter. (co-winner of Kleene Award for Best Student Paper)

Lacon- and Shrub-Decompositions: A New Characterization of First-Order Transductions of Bounded Expansion Classes – Jan Dreier.

A Logic for Locally Complete Abstract Interpretations – Roberto Bruni, Roberto Giacobazzi, Roberta Gori and Francesco Ranzato.

Orbit-Finite-Dimensional Vector Spaces and Weighted Register Automata – Mikołaj Bojańczyk, Bartek Klin and Joshua Moerman.

Universal Skolem Sets – Florian Luca, Joel Ouaknine and James Worrell.

Compositional Semantics for Probabilistic Programs with Exact Conditioning – Dario Stein and Sam Staton.

Minimal Taylor Algebras as a Common Framework for the Three Algebraic Approaches to the CSP – Libor Barto, Zarathustra Brady, Andrei Bulatov, Marcin Kozik and Dmitriy Zhuk.

How thick is our set?

How thick is our set?

- Our set is not too thick.

How thick is our set?

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

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

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?

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?

Highly representable integers

Definition

A **representation** of $n \in \mathbb{N}$ is a triple (P, q, a) such that

$$n = Pq + a,$$

where

- P is prime;
- $q \in Q := [\log\log n, \sqrt{\log n}]$;
- $a \in A := \left[\dfrac{\log n}{2\sqrt{\log\log\log n}}, \dfrac{\log n}{\sqrt{\log\log\log n}}\right]$.

Let $r(n)$ denote the number of representations of n. We say that $n > 10^{10}$ is **highly representable** if

$$r(n) > \log\log\log\log n.$$

Highly representable integers: Examples

Highly representable integers: Examples

Example

For example, $n = 10^{1000} + k$ is **highly representable** for $k \in [0, 1000]$ exactly for

$$k \in \{161, \ldots, 248\} \cup \{325, \ldots, 553\} \cup \{606, \ldots, 730\}.$$

Hint: For all the above n we have

$$Q = [6, 15], \qquad A = [89, 176], \qquad \log\log\log\log n \approx 0.52.$$

A thicker universal Skolem set

A thicker universal Skolem set

Theorem (L., Maynard, Noubissie, Ouaknine, Worrell 2023)

Let $\mathcal{S}$ be the set of highly representable n's. Then

- *$\mathcal{S}$ is a universal Skolem set*
- *$\mathcal{S}$ has positive lower density*
- *$\mathcal{S}$ has density one subject to the Bateman-Horn conjecture*

A thicker universal Skolem set

Theorem (L., Maynard, Noubissie, Ouaknine, Worrell 2023)

Let $\mathcal{S}$ be the set of highly representable n's. Then

- *$\mathcal{S}$ is a universal Skolem set*
- *$\mathcal{S}$ has positive lower density*
- *$\mathcal{S}$ has density one subject to the Bateman-Horn conjecture*

We believe that there are infinitely many n's which are not highly representable.

A thicker universal Skolem set

Theorem (L., Maynard, Noubissie, Ouaknine, Worrell 2023)

Let $\mathcal{S}$ be the set of highly representable n's. Then

- *$\mathcal{S}$ is a universal Skolem set*
- *$\mathcal{S}$ has positive lower density*
- *$\mathcal{S}$ has density one subject to the Bateman-Horn conjecture*

We believe that there are infinitely many n's which are not highly representable.

So, this does not yet solve the Skolem problem.

Large zeros of LRS's

Definition

For a nondegenerate LRS $\mathbf{u} = \langle u_n \rangle_{n \geq 0} \subset \mathbb{Z}$ given by

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n \qquad \forall n \geq 0,$$

let its size be

$$C_{\mathbf{u}} := \max\{k, |a_1|, \ldots, |a_k|, |u_0|, \ldots, |u_{k-1}|, 12\}.$$

Definition

For a nondegenerate LRS $\mathbf{u} = \langle u_n \rangle_{n \geq 0} \subset \mathbb{Z}$ given by

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n \qquad \forall n \geq 0,$$

let its size be

$$C_{\mathbf{u}} := \max\{k, |a_1|, \ldots, |a_k|, |u_0|, \ldots, |u_{k-1}|, 12\}.$$

Given a function $f : \mathbb{R}_+ \mapsto \mathbb{R}_+$ and an integer $k \geq 1$, we write

$$\underbrace{f \circ f \circ \cdots \circ f}_{k \ \ times}(x) = f_k(x).$$

Large zeros of LRS's

Definition

For a nondegenerate LRS $\mathbf{u} = \langle u_n \rangle_{n \geq 0} \subset \mathbb{Z}$ given by

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n \qquad \forall n \geq 0,$$

let its size be

$$C_{\mathbf{u}} := \max\{k, |a_1|, \ldots, |a_k|, |u_0|, \ldots, |u_{k-1}|, 12\}.$$

Given a function $f : \mathbb{R}_+ \mapsto \mathbb{R}_+$ and an integer $k \geq 1$, we write

$$\underbrace{f \circ f \circ \cdots \circ f}_{k \ \ times}(x) = f_k(x).$$

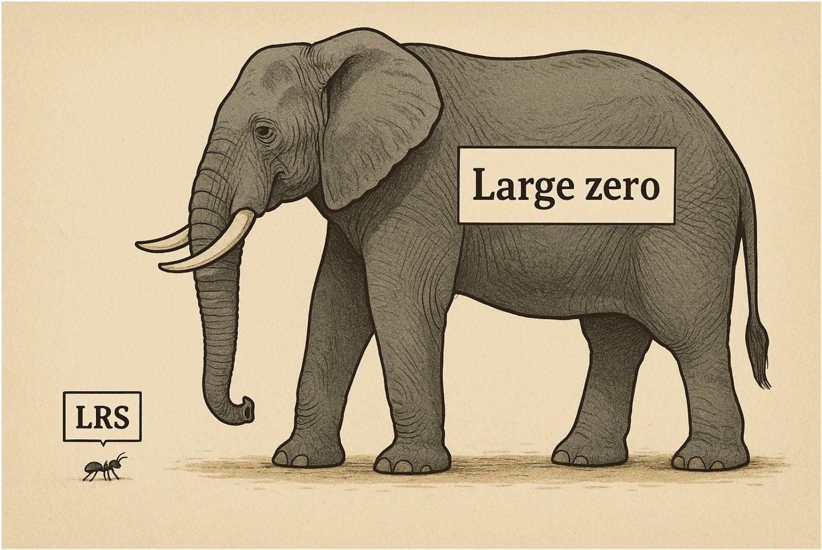
Definition

Given a nondegenerate LRS $\mathbf{u} \subset \mathbb{Z}$, we say that n is a **large zero** of $\mathbf{u}$ if

$$u_n = 0 \qquad \text{and} \qquad n > 2\exp_6(C_{\mathbf{u}}).$$

Example

Example



The set of large zeros of some LRS

The set of large zeros of some LRS

Definition

Let $\mathcal{L}$ be the set of large zeros of some LRS.

The set of large zeros of some LRS

Definition

Let $\mathcal{L}$ be the set of large zeros of some LRS.

Theorem (L., Ouaknine, Worrell, 2025)

The set $\mathcal{L}$ has zero density. In fact, writing $\mathcal{L}(X) = \mathcal{L} \cap [0, X]$, the inequality

$$\#\mathcal{L}(X) = O\left(\frac{X}{(\log X)^B}\right)$$

holds with any $B > 0$ for all $X \geq 2$.

The proof

The proof

- Let X be large and count $n \in \mathcal{L} \cap [X, 2X]$.

The proof

- Let X be large and count $n \in \mathcal{L} \cap [X, 2X]$.
- So, there exists an LRS $\mathbf{u}$ which is nondegenerate with

$$n > 2\exp_6(C_{\mathbf{u}}).$$

Thus,

$$u_n = 0 \qquad \text{and} \qquad C_{\mathbf{u}} < \log_6(X).$$

The proof

- Let X be large and count $n \in \mathcal{L} \cap [X, 2X]$.
- So, there exists an LRS $\mathbf{u}$ which is nondegenerate with

$$n > 2\exp_6(C_{\mathbf{u}}).$$

Thus,

$$u_n = 0 \qquad \text{and} \qquad C_{\mathbf{u}} < \log_6(X).$$

- There are very few such $\mathbf{u}$.

The proof

- Let X be large and count $n \in \mathcal{L} \cap [X, 2X]$.
- So, there exists an LRS $\mathbf{u}$ which is nondegenerate with

$$n > 2\exp_6(C_{\mathbf{u}}).$$

Thus,

$$u_n = 0 \qquad \text{and} \qquad C_{\mathbf{u}} < \log_6(X).$$

- There are very few such $\mathbf{u}$.
- They all have $k \leq C_{\mathbf{u}} < \log_6(X)$.
- By the results of Amoroso and Viada each such LRS has very few zeros. Namely, at most

$$\exp\exp(70k).$$

The proof

- Let X be large and count $n \in \mathcal{L} \cap [X, 2X]$.
- So, there exists an LRS $\mathbf{u}$ which is nondegenerate with

$$n > 2\exp_6(C_{\mathbf{u}}).$$

Thus,

$$u_n = 0 \qquad \text{and} \qquad C_{\mathbf{u}} < \log_6(X).$$

- There are very few such $\mathbf{u}$.
- They all have $k \leq C_{\mathbf{u}} < \log_6(X)$.
- By the results of Amoroso and Viada each such LRS has very few zeros. Namely, at most

$$\exp\exp(70k).$$

- Now conclude.

A new universal Skolem set

A new universal Skolem set

Corollary

The set $\mathcal{S} = \mathbb{N} \backslash \mathcal{L}$ is a universal Skolem set of density 1.

A new universal Skolem set

Corollary

The set $\mathcal{S} = \mathbb{N} \backslash \mathcal{L}$ is a universal Skolem set of density 1.

- We conjecture that $\mathcal{S}$ contains all the positive integers.

A new universal Skolem set

Corollary

The set $\mathcal{S} = \mathbb{N} \backslash \mathcal{L}$ is a universal Skolem set of density 1.

- We conjecture that $\mathcal{S}$ contains all the positive integers.
- That is, we conjecture that there is no large zero of any nondegenerate LRS.

A new universal Skolem set

Corollary

The set $\mathcal{S} = \mathbb{N} \setminus \mathcal{L}$ is a universal Skolem set of density 1.

- We conjecture that $\mathcal{S}$ contains all the positive integers.
- That is, we conjecture that there is no large zero of any nondegenerate LRS.
- In the rest of the talk, I would like to bring some heuristic arguments to support the above conjecture.

A new universal Skolem set

Corollary

The set $\mathcal{S} = \mathbb{N} \backslash \mathcal{L}$ is a universal Skolem set of density 1.

- We conjecture that $\mathcal{S}$ contains all the positive integers.
- That is, we conjecture that there is no large zero of any nondegenerate LRS.
- In the rest of the talk, I would like to bring some heuristic arguments to support the above conjecture.
- More surprisingly, a classical conjecture concerning the distribution of primes seems to have something to do with the above conjecture.

Some notations

Some notations

Let $\mathbf{u} = \langle u_n \rangle_{n \geq 0}$ be a nondegenerate linearly recurrent sequence. Assume

$$u_n := \sum_{j=1}^{s} P_j(n)\lambda_j^n \qquad \forall n \in \mathbb{N} \tag{1}$$

Some notations

Let $\mathbf{u} = \langle u_n \rangle_{n \geq 0}$ be a nondegenerate linearly recurrent sequence. Assume

$$u_n := \sum_{j=1}^{s} P_j(n)\lambda_j^n \qquad \forall n \in \mathbb{N} \tag{1}$$

Let $\mathbb{K} := \mathbb{Q}(\lambda_1, \ldots, \lambda_s)$.

Some notations

Let $\mathbf{u} = \langle u_n \rangle_{n \geq 0}$ be a nondegenerate linearly recurrent sequence. Assume

$$u_n := \sum_{j=1}^{s} P_j(n)\lambda_j^n \qquad \forall n \in \mathbb{N} \tag{1}$$

Let $\mathbb{K} := \mathbb{Q}(\lambda_1, \ldots, \lambda_s)$.

For a permutation σ of $\{1, \ldots, s\}$ let $\gamma_j := \lambda_{\sigma(j)}$.

Some notations

Let $\mathbf{u} = \langle u_n \rangle_{n \geq 0}$ be a nondegenerate linearly recurrent sequence. Assume

$$u_n := \sum_{j=1}^{s} P_j(n)\lambda_j^n \qquad \forall n \in \mathbb{N} \tag{1}$$

Let $\mathbb{K} := \mathbb{Q}(\lambda_1, \ldots, \lambda_s)$.

For a permutation σ of $\{1, \ldots, s\}$ let $\gamma_j := \lambda_{\sigma(j)}$.

For a positive integer m let

$$v_{\sigma,m} := \sum_{j=1}^{s} P_j(m)\gamma_j\lambda_j^m. \tag{2}$$

Good and bad primes

Good and bad primes

Definition

We say that $P \in [X, 2X]$ is **bad** if there exists:

(i) a nondegenerate LRS $\mathbf{u}$ given by which is small at level X; i.e.,

$$C_{\mathbf{u}} < \log_6 X,$$

(ii) a permutation σ of $\{1, \ldots, s\}$,

(iii) a positive integer $m \in [1, X^{1/4}]$,

such that

(1) The number $v_{\sigma,m}$ shown at (2) is nonzero and

(2) P divides the numerator of

$$N_{\mathbb{K}/\mathbb{Q}}(v_{\sigma,m}).$$

Counting bad primes

Let $\mathcal{P}_{\mathrm{bad}}(X)$ be the set of bad primes in $[X, 2X]$.

Counting bad primes

Let $\mathcal{P}_{\mathrm{bad}}(X)$ be the set of bad primes in $[X, 2X]$.

Theorem (L., Ouaknine, Worrell 2025)

We have

$$\#\mathcal{P}_{\mathrm{bad}}(X) < X^{2/3}$$

for all $X > X_0$.

Proof

Proof

In order to estimate $\#\mathcal{P}_{\mathrm{bad}}(X)$ we need to find out:

(1) How many numbers of the form (2) are there?

(2) How large are they?

Proof

In order to estimate $\#\mathcal{P}_{\rm bad}(X)$ we need to find out:

(1) How many numbers of the form (2) are there?

(2) How large are they?

(1) is easy. Since $C_{\mathbf{u}}$ is tiny, there are $X^{o(1)}$ ways of choosing $\mathbf{u}$.

Proof

In order to estimate $\#\mathcal{P}_{\mathrm{bad}}(X)$ we need to find out:

(1) How many numbers of the form (2) are there?

(2) How large are they?

(1) is easy. Since $C_{\mathbf{u}}$ is tiny, there are $X^{o(1)}$ ways of choosing $\mathbf{u}$.

Given $\mathbf{u}$, there are $k! = X^{o(1)}$ ways of choosing σ.

Proof

In order to estimate $\#\mathcal{P}_{\mathrm{bad}}(X)$ we need to find out:

(1) How many numbers of the form (2) are there?

(2) How large are they?

(1) is easy. Since $C_{\mathbf{u}}$ is tiny, there are $X^{o(1)}$ ways of choosing $\mathbf{u}$.

Given $\mathbf{u}$, there are $k! = X^{o(1)}$ ways of choosing σ.

There are $X^{1/4}$ ways of choosing m.

Proof

In order to estimate $\#\mathcal{P}_{\mathrm{bad}}(X)$ we need to find out:

(1) How many numbers of the form (2) are there?

(2) How large are they?

(1) is easy. Since $C_{\mathbf{u}}$ is tiny, there are $X^{o(1)}$ ways of choosing $\mathbf{u}$.

Given $\mathbf{u}$, there are $k! = X^{o(1)}$ ways of choosing σ.

There are $X^{1/4}$ ways of choosing m.

The norm of each of $v_{\sigma,m}$ is a nonzero rational number of denominator $X^{o(1)}$ and numerator

$$\exp(mX^{o(1)}) = \exp(X^{1/4+o(1)}).$$

Proof

In order to estimate $\#\mathcal{P}_{\mathrm{bad}}(X)$ we need to find out:

(1) How many numbers of the form (2) are there?

(2) How large are they?

(1) is easy. Since $C_{\mathbf{u}}$ is tiny, there are $X^{o(1)}$ ways of choosing $\mathbf{u}$.

Given $\mathbf{u}$, there are $k! = X^{o(1)}$ ways of choosing σ.

There are $X^{1/4}$ ways of choosing m.

The norm of each of $v_{\sigma,m}$ is a nonzero rational number of denominator $X^{o(1)}$ and numerator

$$\exp(mX^{o(1)}) = \exp(X^{1/4+o(1)}).$$

Thus, there are $\log N_{\mathbb{K}/\mathbb{Q}}(v_{\sigma,m}) \leq X^{1/4+o(1)}$ possibilities for the prime P.

Proof

In order to estimate $\#\mathcal{P}_{\mathrm{bad}}(X)$ we need to find out:

(1) How many numbers of the form (2) are there?

(2) How large are they?

(1) is easy. Since $C_{\mathbf{u}}$ is tiny, there are $X^{o(1)}$ ways of choosing $\mathbf{u}$.

Given $\mathbf{u}$, there are $k! = X^{o(1)}$ ways of choosing σ.

There are $X^{1/4}$ ways of choosing m.

The norm of each of $v_{\sigma,m}$ is a nonzero rational number of denominator $X^{o(1)}$ and numerator

$$\exp(mX^{o(1)}) = \exp(X^{1/4+o(1)}).$$

Thus, there are $\log N_{\mathbb{K}/\mathbb{Q}}(v_{\sigma,m}) \leq X^{1/4+o(1)}$ possibilities for the prime P.

Now we sum up over all the $X^{1/4+o(1)}$ possibilities for $(\mathbf{u}, \sigma, m)$ getting a bound of $X^{1/2+o(1)}$ on $\#\mathcal{P}_{\mathrm{bad}}(X)$.

Primes in short intervals

Primes in short intervals

Let p_n be the nth prime.

Primes in short intervals

Let p_n be the nth prime.

Conjecture (Cramér, Granville)

There exists κ *such that*

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = \kappa.$$

Primes in short intervals

Let p_n be the nth prime.

Conjecture (Cramér, Granville)

There exists κ such that

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = \kappa.$$

- Cramér believed that $\kappa = 1$. This was refuted by Maier.

Primes in short intervals

Let p_n be the nth prime.

Conjecture (Cramér, Granville)

There exists κ such that

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = \kappa.$$

- Cramér believed that $\kappa = 1$. This was refuted by Maier.
- Granville produced some evidence that $\kappa \geq 2e^{-\gamma} = 1.229\ldots$

Primes in short intervals

Let p_n be the nth prime.

Conjecture (Cramér, Granville)

There exists κ such that

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = \kappa.$$

- Cramér believed that $\kappa = 1$. This was refuted by Maier.
- Granville produced some evidence that $\kappa \geq 2e^{-\gamma} = 1.229\ldots$.
- The Riemann Hypothesis gives $p_{n+1} - p_n = O(\sqrt{p_n} \log p_n)$.

Primes in short intervals

Let p_n be the nth prime.

Conjecture (Cramér, Granville)

There exists κ such that

$$\limsup_{n\to\infty} \frac{p_{n+1}-p_n}{(\log p_n)^2} = \kappa.$$

- Cramér believed that $\kappa = 1$. This was refuted by Maier.
- Granville produced some evidence that $\kappa \geq 2e^{-\gamma} = 1.229\ldots$.
- The Riemann Hypothesis gives $p_{n+1} - p_n = O(\sqrt{p_n}\log p_n)$.
- Baker, Harman and Pinz showed that $p_{n+1} - p_n = O(p_n^{0.525})$.

Primes in short intervals

Let p_n be the nth prime.

Conjecture (Cramér, Granville)

There exists κ such that

$$\limsup_{n\to\infty} \frac{p_{n+1}-p_n}{(\log p_n)^2} = \kappa.$$

- Cramér believed that $\kappa = 1$. This was refuted by Maier.
- Granville produced some evidence that $\kappa \geq 2e^{-\gamma} = 1.229\ldots$.
- The Riemann Hypothesis gives $p_{n+1}-p_n = O(\sqrt{p_n}\log p_n)$.
- Baker, Harman and Pinz showed that $p_{n+1}-p_n = O(p_n^{0.525})$.
- Ford, Green, Konyagin, Tao and Maynard showed that

$$p_{n+1}-p_n \gg \frac{\log p_n \log\log p_n \log\log\log\log p_n}{\log\log\log p_n} \qquad \text{i. o.}$$

How did Cramér arrive at his conjecture?

How did Cramér arrive at his conjecture?

- Well the probability that n is prime is $1/\log n$. So, the probability that it is composite is

$$1 - \frac{1}{\log n}.$$

How did Cramér arrive at his conjecture?

- Well the probability that n is prime is $1/\log n$. So, the probability that it is composite is

$$1 - \frac{1}{\log n}.$$

- So, the probability that $n, \; n+1, \ldots, n+k-1$ are all composites is, assuming these events are independent,

$$\prod_{j=0}^{k-1}\left(1 - \frac{1}{\log(n+j)}\right) \sim \left(1 - \frac{1}{\log n}\right)^k,$$

provided k is small with respect to n.

How did Cramér arrive at his conjecture?

- Well the probability that n is prime is $1/\log n$. So, the probability that it is composite is

$$1 - \frac{1}{\log n}.$$

- So, the probability that $n,\ n+1, \ldots, n+k-1$ are all composites is, assuming these events are independent,

$$\prod_{j=0}^{k-1}\left(1 - \frac{1}{\log(n+j)}\right) \sim \left(1 - \frac{1}{\log n}\right)^{k},$$

provided k is small with respect to n.

- So, taking $k = \lfloor \kappa(\log n)^2 \rfloor$ with some $\kappa > 1$, this is

$$\left(1 - \frac{1}{\log n}\right)^{\kappa(\log n)^2} = \frac{1}{n^{\kappa}} = o\left(\frac{1}{n}\right)$$

Continuation

Continuation

- So, taking $n \in [X, 2X]$, the probability of all the above happening is
$$o\left(\frac{1}{X}\right),$$
but the above interval has length X, so maybe there is no such n in $[X, 2X]$ for large X.

Continuation

- So, taking $n \in [X, 2X]$, the probability of all the above happening is
$$o\left(\frac{1}{X}\right),$$
but the above interval has length X, so maybe there is no such n in $[X, 2X]$ for large X.

- The model is wrong since the events "n is composite" and "$n+1$ is composite" are not independent (one of them is always even).

A modified Cramér conjecture

A modified Cramér conjecture

Since $\#\mathcal{P}_{\rm bad}(X) < X^{2/3}$ for $X > X_0$ it follows that asymptotically $\mathcal{P}\backslash\mathcal{P}_{\rm bad}$ has the same counting function as the primes.

A modified Cramér conjecture

Since $\#\mathcal{P}_{\mathrm{bad}}(X) < X^{2/3}$ for $X > X_0$ it follows that asymptotically $\mathcal{P} \backslash \mathcal{P}_{\mathrm{bad}}$ has the same counting function as the primes.

Let q_n be the $n$the element of $\mathcal{P} \backslash \mathcal{P}_{\mathrm{bad}}$.

Conjecture (Modified Cramér conjecture)

Assume that there exists $\kappa > 0$ such that

$$\limsup_{n \to \infty} \frac{q_{n+1} - q_n}{(\log q_n)^2} = \kappa.$$

Solving the Skolem problem conditionally

Theorem (L., Ouaknine, Worrell 2025)

The modifed Cramér conjecture implies that there exists an absolute constant n_0 such that a nondegenerate LRS $\mathbf{u}$ has no large zeros $n > n_0$. That is, if $u_n = 0$, then

$$n < \max\{n_0, C_{\mathbf{u}}\}.$$

Proof

Proof

- Assume the modified Cramér conjecture.

Proof

- Assume the modified Cramér conjecture.
- Let $\mathbf{u}$ be a nondegenerate LRS and n be a large zero of it.

Proof

- Assume the modified Cramér conjecture.
- Let $\mathbf{u}$ be a nondegenerate LRS and n be a large zero of it.
- If n is large, then $[n - \kappa(\log n)^3, n]$ contains at least $\log n$ primes $P \in \mathcal{P} \backslash \mathcal{P}_{\mathrm{bad}}$. Write $n = P + m$ with such P.

Proof

- Assume the modified Cramér conjecture.
- Let $\mathbf{u}$ be a nondegenerate LRS and n be a large zero of it.
- If n is large, then $[n - \kappa(\log n)^3, n]$ contains at least $\log n$ primes $P \in \mathcal{P} \backslash \mathcal{P}_{\mathrm{bad}}$. Write $n = P + m$ with such P.
- Note that $m = O((\log n)^3)$ and such m's are distinct.

Proof

- Assume the modified Cramér conjecture.
- Let $\mathbf{u}$ be a nondegenerate LRS and n be a large zero of it.
- If n is large, then $[n - \kappa(\log n)^3, n]$ contains at least $\log n$ primes $P \in \mathcal{P} \backslash \mathcal{P}_{\mathrm{bad}}$. Write $n = P + m$ with such P.
- Note that $m = O((\log n)^3)$ and such m's are distinct.
- Reduce the equation $u_n = 0$ modulo P to get

$$u_n = \sum_{j=1}^{s} P_j(m+P)\lambda_j^{P+m} \equiv 0 \pmod{P}.$$

Proof

- Assume the modified Cramér conjecture.
- Let $\mathbf{u}$ be a nondegenerate LRS and n be a large zero of it.
- If n is large, then $[n-\kappa(\log n)^3, n]$ contains at least $\log n$ primes $P \in \mathcal{P} \backslash \mathcal{P}_{\mathrm{bad}}$. Write $n = P + m$ with such P.
- Note that $m = O((\log n)^3)$ and such m's are distinct.
- Reduce the equation $u_n = 0$ modulo P to get

$$u_n = \sum_{j=1}^{s} P_j(m+P)\lambda_j^{P+m} \equiv 0 \pmod{P}.$$

- This implies

$$v_{\sigma,m} \equiv 0 \pmod{P},$$

where σ is the Frobenius with respect to P (so $\gamma_j \equiv \lambda_j^P \pmod{P}$).

Proof (continued)

Proof (continued)

- Since P is good, $v_{\sigma,m} = 0$. Thus,

$$\sum_{j=1}^{s} P_j(m)\gamma_j\lambda_j^m = 0.$$

Proof (continued)

- Since P is good, $v_{\sigma,m} = 0$. Thus,

$$\sum_{j=1}^{s} P_j(m)\gamma_j\lambda_j^m = 0.$$

- Fixing σ, we get that the nondegenerate LRS $\mathbf{v}_\sigma = (v_{\sigma,m})$ has

$$(\log n)^{1-o(1)}$$

zeros m.

Proof (continued)

- Since P is good, $v_{\sigma,m} = 0$. Thus,

$$\sum_{j=1}^{s} P_j(m)\gamma_j\lambda_j^m = 0.$$

- Fixing σ, we get that the nondegenerate LRS $\mathbf{v}_\sigma = (v_{\sigma,m})$ has

$$(\log n)^{1-o(1)}$$

  zeros m.

- However, this can have at most $\exp_2(O(k)) = (\log n)^{o(1)}$ zeros.

Proof (continued)

- Since P is good, $v_{\sigma,m} = 0$. Thus,

$$\sum_{j=1}^{s} P_j(m)\gamma_j\lambda_j^m = 0.$$

- Fixing σ, we get that the nondegenerate LRS $\mathbf{v}_\sigma = (v_{\sigma,m})$ has

$$(\log n)^{1-o(1)}$$

  zeros m.

- However, this can have at most $\exp_2(O(k)) = (\log n)^{o(1)}$ zeros.

- Putting it together we get $n = O(1)$.


Thank you very much
Hartelijk dank
Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT
Photo by Stefan Els