Universal Skolem Sets

Joël Ouaknine

Max Planck Institute for Software Systems

(joint work with Florian Luca, James Maynard, Armand Noubissie, James Worrell)

WORReLL'23
Paderborn, 10 July 2023


HOT MALE
STRIPPERS

Joël Ouaknine is with James Worrell and Amaury Pouly at Mathematical Institute, University of Oxford.

October 25, 2017 · Oxford ·

a mathematical storm is brewing

45

2 Comments 1 Share


PISSOIR

Seek collaborations with people smarter than yourself

Seek collaborations with people smarter than yourself

The Skolem Problem

What do these sequences have in common?

- The Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- $\langle p(1), p(2), p(3), p(4), \ldots \rangle$
- $\langle \cos\theta, \cos 2\theta, \cos 3\theta, \cos 4\theta, \ldots \rangle$

The Skolem Problem

What do these sequences have in common?

- The Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- $\langle p(1), p(2), p(3), p(4), \ldots \rangle$
- $\langle \cos\theta, \cos 2\theta, \cos 3\theta, \cos 4\theta, \ldots \rangle$

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

The Skolem Problem

What do these sequences have in common?

- The Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- $\langle p(1), p(2), p(3), p(4), \ldots \rangle$
- $\langle \cos\theta, \cos 2\theta, \cos 3\theta, \cos 4\theta, \ldots \rangle$

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

Problem SKOLEM (1934)

Instance: An LRS $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Does $\exists n \geq 0$ such that $u_n = 0$?

Quick Quiz: two ‘simple’ problems

- Given two automata A and B, is there some ‘word-length’ n such that A and B accept exactly *the same words* of length n?
- Given two automata A and B, is there some ‘word-length’ n such that A and B accept exactly *the same number of words* of length n?

Quick Quiz: two 'simple' problems

- Given two automata A and B, is there some 'word-length' n such that A and B accept exactly *the same words* of length n?
    - **DECIDABLE** (in fact NEXPTIME-COMPLETE)
- Given two automata A and B, is there some 'word-length' n such that A and B accept exactly *the same number of words* of length n?

Quick Quiz: two ‘simple’ problems

- Given two automata A and B, is there some ‘word-length’ n such that A and B accept exactly *the same words* of length n?
  - **DECIDABLE** (in fact NEXPTIME-COMPLETE)
- Given two automata A and B, is there some ‘word-length’ n such that A and B accept exactly *the same number of words* of length n?
  - **SKOLEM-COMPLETE**

Some other application areas

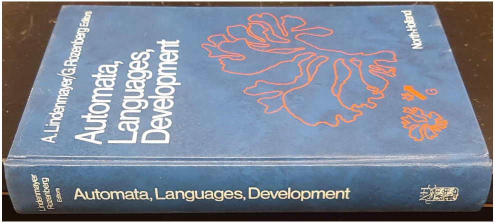
The Skolem Problem (and related questions) arise in many other areas (often in hardness results), e.g.:

Some other application areas

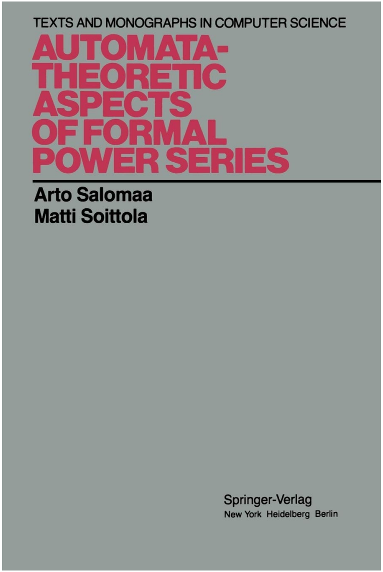
The Skolem Problem (and related questions) arise in many other areas (often in hardness results), e.g.:

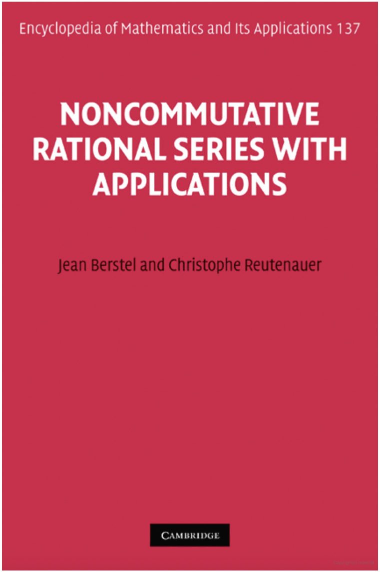
- theoretical biology (analysis of L-systems)
- software verification / program analysis
- dynamical systems
- differential privacy
- (weighted) automata and games
- analysis of stochastic systems
- control theory
- quantum computing
- statistical physics
- formal power series
- combinatorics
- ...

L-Systems (after Aristid Lindenmayer, late 1960s)



Automata and power series





The Skolem-Mahler-Lech Theorem

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

Exponential-polynomial closed forms for LRS

Let $\langle u_n \rangle_{n=0}^{\infty}$ satisfy the recurrence

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

Exponential-polynomial closed forms for LRS

Let $\langle u_n \rangle_{n=0}^{\infty}$ satisfy the recurrence

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

The **characteristic polynomial** of $\langle u_n \rangle$ is

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

Exponential-polynomial closed forms for LRS

Let $\langle u_n \rangle_{n=0}^{\infty}$ satisfy the recurrence

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

The **characteristic polynomial** of $\langle u_n \rangle$ is

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

Let the **characteristic roots** be $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$.

Exponential-polynomial closed forms for LRS

Let $\langle u_n \rangle_{n=0}^{\infty}$ satisfy the recurrence

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

The **characteristic polynomial** of $\langle u_n \rangle$ is

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

Let the **characteristic roots** be $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$.

Then one has the exponential-polynomial closed form

$$u_n = \sum_{j=1}^{m} Q_j(n) \lambda_j^n$$

where the Q_j are polynomials with (complex) algebraic-number coefficients.

Special case: *simple* linear recurrence sequences

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

Special case: *simple* linear recurrence sequences

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

- e.g., the Fibonacci sequence:

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

Special case: *simple* linear recurrence sequences

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

- e.g., the Fibonacci sequence:

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

- Equivalently, an LRS is simple if all Q_j are constant

$$\left(\text{ in } u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n \right)$$

Special case: *simple* linear recurrence sequences

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

- e.g., the Fibonacci sequence:

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

- Equivalently, an LRS is simple if all Q_j are constant

$$\left(\text{ in } u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n\right)$$

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

Special case: *simple* linear recurrence sequences

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

- e.g., the Fibonacci sequence:

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

- Equivalently, an LRS is simple if all Q_j are constant

$$\left(\text{ in } u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n\ \right)$$

- The "vast majority" of LRS are simple...
- Simple LRS correspond precisely to **diagonalisable** matrices

The Skolem Problem at low orders

The Skolem Problem at low orders

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

For LRS of order ≤ 4, SKOLEM is decidable.

The Skolem Problem at low orders

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.

The Skolem Problem at low orders

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.

- Note: even for *simple* LRS, decidability at order 5 is not known!

Conditional results

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

Conditional results

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

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

Conditional results

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

- Miller's polynomial-time algorithm 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)

Conditional results

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

- Miller's polynomial-time algorithm 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)

Conditional results

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

- Miller's polynomial-time algorithm 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, or ETH, etc...

The Skolem Problem for simple LRS (conditional on classical conjectures in number theory)

The Skolem Problem for simple LRS (conditional on classical conjectures in number theory)

Theorem (Bilu, Luca, Nieuwveld, O., Purser, Worrell, MFCS 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 (conditional on classical conjectures in number theory)

Theorem (Bilu, Luca, Nieuwveld, O., Purser, Worrell, MFCS 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 p-adic Schanuel Conjecture and the Exponential Local-Global Principle.

The Skolem Problem for simple LRS (conditional on classical conjectures in number theory)

Theorem (Bilu, Luca, Nieuwveld, O., Purser, Worrell, MFCS 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 p-adic Schanuel Conjecture and the Exponential Local-Global Principle.

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

The Skolem Problem for simple LRS (conditional on classical conjectures in number theory)

Theorem (Bilu, Luca, Nieuwveld, O., Purser, Worrell, MFCS 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 p-adic Schanuel Conjecture and the Exponential Local-Global Principle.

- 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 (conditional on classical conjectures in number theory)

Theorem (Bilu, Luca, Nieuwveld, O., Purser, Worrell, MFCS 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 p-adic Schanuel Conjecture and the Exponential Local-Global Principle.

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

Universal Skolem Sets

Definition

An infinite set $\mathcal{S} \subseteq \mathbb{N}$ is a **Universal Skolem Set** if there is an effective procedure that inputs a non-degenerate integer LRS $\langle u_n \rangle$ and outputs the set $\{n \in \mathcal{S} : u_n = 0\}$.

Universal Skolem Sets

Definition

An infinite set $\mathcal{S} \subseteq \mathbb{N}$ is a **Universal Skolem Set** if there is an effective procedure that inputs a non-degenerate integer LRS $\langle u_n \rangle$ and outputs the set $\{n \in \mathcal{S} : u_n = 0\}$.

Equivalently, $\mathcal{S} \subseteq \mathbb{N}$ is a Universal Skolem Set if, given any non-degenerate LRS, it is decidable whether that LRS has a zero in $\mathcal{S}$.

Universal Skolem Sets

Definition

An infinite set $\mathcal{S} \subseteq \mathbb{N}$ is a **Universal Skolem Set** if there is an effective procedure that inputs a non-degenerate integer LRS $\langle u_n \rangle$ and outputs the set $\{n \in \mathcal{S} : u_n = 0\}$.

Equivalently, $\mathcal{S} \subseteq \mathbb{N}$ is a Universal Skolem Set if, given any non-degenerate LRS, it is decidable whether that LRS has a zero in $\mathcal{S}$.

- Decidability of the Skolem Problem is equivalent to proving that $\mathbb{N}$ is a Universal Skolem Set

Universal Skolem Sets

Definition

An infinite set $\mathcal{S} \subseteq \mathbb{N}$ is a **Universal Skolem Set** if there is an effective procedure that inputs a non-degenerate integer LRS $\langle u_n \rangle$ and outputs the set $\{n \in \mathcal{S} : u_n = 0\}$.

Equivalently, $\mathcal{S} \subseteq \mathbb{N}$ is a Universal Skolem Set if, given any non-degenerate LRS, it is decidable whether that LRS has a zero in $\mathcal{S}$.

- Decidability of the Skolem Problem is equivalent to proving that $\mathbb{N}$ is a Universal Skolem Set
- In fact, it would suffice to show the existence of a Universal Skolem Set containing *some* infinite arithmetic progression!

Universal Skolem Sets exist!

Theorem (Luca, O., Worrell, LICS 2021)

Define $f : \mathbb{N}_+ \to \mathbb{N}$ *by* $f(t) = \lfloor \sqrt{\log t} \rfloor$. *Write* $s_0 = 1$ *and, inductively, set* $s_t := t! + s_{f(t)}$ *for* $t \geq 1$.
Then $\mathcal{S} := \{s_t : t \in \mathbb{N}\}$ *is a Universal Skolem Set.*

Universal Skolem Sets exist!

Theorem (Luca, O., Worrell, LICS 2021)

Define $f : \mathbb{N}_+ \to \mathbb{N}$ *by* $f(t) = \lfloor \sqrt{\log t} \rfloor$*. Write* $s_0 = 1$ *and, inductively, set* $s_t := t! + s_{f(t)}$ *for* $t \geq 1$*.*
Then $\mathcal{S} := \{s_t : t \in \mathbb{N}\}$ *is a Universal Skolem Set.*

We have

$$\mathcal{S} = \{1, 1! + 1, 2! + 1, 3! + 1! + 1, 4! + 1! + 1, 5! + 1! + 1, \ldots\}$$

Universal Skolem Sets exist!

Theorem (Luca, O., Worrell, LICS 2021)

Define $f : \mathbb{N}_+ \to \mathbb{N}$ *by* $f(t) = \lfloor \sqrt{\log t} \rfloor$. *Write* $s_0 = 1$ *and, inductively, set* $s_t := t! + s_{f(t)}$ *for* $t \geq 1$.
Then $\mathcal{S} := \{s_t : t \in \mathbb{N}\}$ *is a Universal Skolem Set.*

We have

$$\begin{aligned}\mathcal{S} &= \{1, 1! + 1, 2! + 1, 3! + 1! + 1, 4! + 1! + 1, 5! + 1! + 1, \ldots\} \\ &= \{1, 2, 3, 8, 26, 122, 722, 5042, 40322, 362882, 3628802, \ldots\}\end{aligned}$$

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

Proposition

Given $\langle u_n \rangle$, and any prime p such that $p \nmid \Delta$, then for all $t, \ell \in \mathbb{N}$ with $t \geq p^d$, $u_{t!+\ell} \equiv u_\ell \pmod{p}$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

Proposition

Given $\langle u_n \rangle$, and any prime p such that $p \nmid \Delta$, then for all $t, \ell \in \mathbb{N}$ with $t \geq p^d$, $u_{t!+\ell} \equiv u_\ell \pmod{p}$.
(Here Δ is the discriminant of the splitting field of the characteristic polynomial of $\langle u_n \rangle$, and d is its degree over $\mathbb{Q}$.)

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

Proposition

Given $\langle u_n \rangle$, and any prime p such that $p \nmid \Delta$, then for all $t, \ell \in \mathbb{N}$ with $t \geq p^d$, $u_{t!+\ell} \equiv u_\ell \pmod{p}$.
(Here Δ is the discriminant of the splitting field of the characteristic polynomial of $\langle u_n \rangle$, and d is its degree over $\mathbb{Q}$.)

(Proof sketch) To see this, write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

Proposition

Given $\langle u_n \rangle$, and any prime p such that $p \nmid \Delta$, then for all $t, \ell \in \mathbb{N}$ with $t \geq p^d$, $u_{t!+\ell} \equiv u_\ell \pmod{p}$.
(Here Δ is the discriminant of the splitting field of the characteristic polynomial of $\langle u_n \rangle$, and d is its degree over $\mathbb{Q}$.)

(Proof sketch) To see this, write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n$.
Recall Fermat's Little Theorem: if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

Proposition

Given $\langle u_n \rangle$, and any prime p such that $p \nmid \Delta$, then for all $t, \ell \in \mathbb{N}$ with $t \geq p^d$, $u_{t!+\ell} \equiv u_\ell \pmod{p}$.
(Here Δ is the discriminant of the splitting field of the characteristic polynomial of $\langle u_n \rangle$, and d is its degree over $\mathbb{Q}$.)

(Proof sketch) To see this, write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n$.
Recall Fermat's Little Theorem: if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.
By a corresponding version for algebraic integers,

$$\lambda_j^{t!} = (\lambda_j^{p^h-1})^R \equiv 1^R \equiv 1 \pmod{\mathfrak{p}}.$$

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

Proposition

Given $\langle u_n \rangle$, and any prime p such that $p \nmid \Delta$, then for all $t, \ell \in \mathbb{N}$ with $t \geq p^d$, $u_{t!+\ell} \equiv u_\ell \pmod{p}$.
(Here Δ is the discriminant of the splitting field of the characteristic polynomial of $\langle u_n \rangle$, and d is its degree over $\mathbb{Q}$.)

(Proof sketch) To see this, write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n$.
Recall Fermat's Little Theorem: if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.
By a corresponding version for algebraic integers,

$$\lambda_j^{t!} = (\lambda_j^{p^h-1})^R \equiv 1^R \equiv 1 \pmod{\mathfrak{p}}.$$

So $u_{t!+\ell} = \sum_{j=1}^{m} Q_j(t!+\ell)\lambda_j^{t!+\ell} \equiv \sum_{j=1}^{m} Q_j(\ell)\lambda_j^{\ell} = u_\ell \pmod{p}$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

In particular, if $u_{s_t} = u_{t!+s_{f(t)}} = 0$, then

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

In particular, if $u_{s_t} = u_{t!+s_{f(t)}} = 0$, then

$$u_{s_{f(t)}} \equiv 0 \pmod{P}, \quad \text{where} \quad P = \prod_{\substack{p \text{ prime} \\ p^d \leq t \\ p \nmid \Delta}} p\,.$$

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

In particular, if $u_{s_t} = u_{t!+s_{f(t)}} = 0$, then

$$u_{s_{f(t)}} \equiv 0 \pmod{P}, \quad \text{where} \quad P = \prod_{\substack{p \text{ prime} \\ p^d \leq t \\ p \nmid \Delta}} p \, .$$

One can show that, for t sufficiently large, $P > u_{s_{f(t)}}$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

In particular, if $u_{s_t} = u_{t!+s_{f(t)}} = 0$, then

$$u_{s_{f(t)}} \equiv 0 \pmod{P}, \quad \text{where} \quad P = \prod_{\substack{p \text{ prime} \\ p^d \leq t \\ p \nmid \Delta}} p\,.$$

One can show that, for t sufficiently large, $P > u_{s_{f(t)}}$. Combining:

For t large enough, if $u_{s_t} = 0$, then $u_{s_{f(t)}} = 0$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

In particular, if $u_{s_t} = u_{t!+s_{f(t)}} = 0$, then

$$u_{s_{f(t)}} \equiv 0 \pmod{P}, \quad \text{where} \quad P = \prod_{\substack{p \text{ prime} \\ p^d \leq t \\ p \nmid \Delta}} p\,.$$

One can show that, for t sufficiently large, $P > u_{s_{f(t)}}$. Combining:

For t large enough, if $u_{s_t} = 0$, then $u_{s_{f(t)}} = 0$.

Finally, find N sufficiently large and such that $\langle u_n \rangle$ has no zeros in the interval $[s_N, s_L]$, where L is the smallest integer such that $f(L) = N$.

Skolem-Universality of $\mathcal{S}$

Define $f : \mathbb{N}_+ \to \mathbb{N}$ by $f(t) = \lfloor \sqrt{\log t} \rfloor$. Write $s_0 = 1$ and, inductively, set $s_t := t! + s_{f(t)}$ for $t \geq 1$.

In particular, if $u_{s_t} = u_{t!+s_{f(t)}} = 0$, then

$$u_{s_{f(t)}} \equiv 0 \pmod{P}, \quad \text{where} \quad P = \prod_{\substack{p \text{ prime} \\ p^d \leq t \\ p \nmid \Delta}} p \,.$$

One can show that, for t sufficiently large, $P > u_{s_{f(t)}}$. Combining:

For t large enough, if $u_{s_t} = 0$, then $u_{s_{f(t)}} = 0$.

Finally, find N sufficiently large and such that $\langle u_n \rangle$ has no zeros in the interval $[s_N, s_L]$, where L is the smallest integer such that $f(L) = N$.

Then for any $t \geq N$, $u_{s_t} \neq 0$.

How dense is $\mathcal{S}$?

Recall $\mathcal{S} = \{1, 2, 3, 8, 26, 122, 722, 5042, 40322, 362882, \ldots\}$

How dense is $\mathcal{S}$?

Recall $\mathcal{S} = \{1, 2, 3, 8, 26, 122, 722, 5042, 40322, 362882, \ldots\}$

Unfortunately, $\mathcal{S}$ has density zero:

$$|\mathcal{S} \cap \{1, \ldots, n\}| \approx \frac{\log n}{\log \log n}$$

Exponential Diophantine equations in multiple variables

Theorem (after Schlickewei and Schmidt, 2000)

There is an explicit upper bound on the number of 'non-overlapping' solutions of the equation

$$\sum_{j=1}^{m} Q_j(y)\alpha_j^x\lambda_j^y = 0$$

in integers $x, y \in \mathbb{N}$.

Exponential Diophantine equations in multiple variables

Theorem (after Schlickewei and Schmidt, 2000)

There is an explicit upper bound on the number of 'non-overlapping' solutions of the equation

$$\sum_{j=1}^{m} Q_j(y)\alpha_j^x \lambda_j^y = 0$$

in integers $x, y \in \mathbb{N}$.

(Here α_j *and* λ_j *are complex algebraic numbers, and the* Q_j *are polynomials with complex algebraic-number coefficients.)*

Exponential Diophantine equations in multiple variables

Theorem (after Schlickewei and Schmidt, 2000)

There is an explicit upper bound on the number of 'non-overlapping' solutions of the equation

$$\sum_{j=1}^{m} Q_j(y)\alpha_j^x \lambda_j^y = 0$$

in integers $x, y \in \mathbb{N}$.

(Here α_j *and* λ_j *are complex algebraic numbers, and the* Q_j *are polynomials with complex algebraic-number coefficients.)*

This is in fact a deep generalisation of the Skolem-Mahler-Lech Theorem

A denser Universal Skolem Set

A denser Universal Skolem Set

- Given positive integer parameter X, define

$$A(X) := \left[\log_2 X, \sqrt{\log X}\right] \text{ and } B(X) := \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2\log X}{\sqrt{\log_3 X}}\right]$$

A denser Universal Skolem Set

- Given positive integer parameter X, define

$$A(X) := \left[\log_2 X, \sqrt{\log X}\right] \text{ and } B(X) := \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2\log X}{\sqrt{\log_3 X}}\right]$$

- A **representation** of $n \in [X, 2X]$ is a triple (P, q, b) such that $n = Pq + b$, P and q are prime, $q \in A(X)$, and $b \in B(X)$.

A denser Universal Skolem Set

- Given positive integer parameter X, define

$$A(X) := \left[\log_2 X, \sqrt{\log X}\right] \text{ and } B(X) := \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2\log X}{\sqrt{\log_3 X}}\right]$$

- A **representation** of $n \in [X, 2X]$ is a triple (P, q, b) such that $n = Pq + b$, P and q are prime, $q \in A(X)$, and $b \in B(X)$. Let $r(n)$ be number of representations of n.

A denser Universal Skolem Set

- Given positive integer parameter X, define

$$A(X) := \left[\log_2 X, \sqrt{\log X}\right] \text{ and } B(X) := \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2\log X}{\sqrt{\log_3 X}}\right]$$

- A **representation** of $n \in [X, 2X]$ is a triple (P, q, b) such that $n = Pq + b$, P and q are prime, $q \in A(X)$, and $b \in B(X)$. Let $r(n)$ be number of representations of n.
- Define $\mathcal{S}(X) := \{n \in [X, 2X] : r(n) > \log_4 X\}$ and

$$\mathcal{S} := \bigcup_{k \in \mathbb{N}} \mathcal{S}(2^k)$$

A denser Universal Skolem Set

- Given positive integer parameter X, define

$$A(X) := \left[\log_2 X, \sqrt{\log X}\right] \text{ and } B(X) := \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2\log X}{\sqrt{\log_3 X}}\right]$$

- A **representation** of $n \in [X, 2X]$ is a triple (P, q, b) such that $n = Pq + b$, P and q are prime, $q \in A(X)$, and $b \in B(X)$. Let $r(n)$ be number of representations of n.
- Define $\mathcal{S}(X) := \{n \in [X, 2X] : r(n) > \log_4 X\}$ and

$$\mathcal{S} := \bigcup_{k\in\mathbb{N}} \mathcal{S}(2^k)$$

Theorem (Luca, Maynard, Noubissie, O., Worrell, 2023)

$\mathcal{S}$ is a Universal Skolem Set of strictly positive lower density.

A denser Universal Skolem Set

- Given positive integer parameter X, define

$$A(X) := \left[\log_2 X, \sqrt{\log X}\right] \text{ and } B(X) := \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2\log X}{\sqrt{\log_3 X}}\right]$$

- A **representation** of $n \in [X, 2X]$ is a triple (P, q, b) such that $n = Pq + b$, P and q are prime, $q \in A(X)$, and $b \in B(X)$. Let $r(n)$ be number of representations of n.
- Define $\mathcal{S}(X) := \{n \in [X, 2X] : r(n) > \log_4 X\}$ and

$$\mathcal{S} := \bigcup_{k \in \mathbb{N}} \mathcal{S}(2^k)$$

Theorem (Luca, Maynard, Noubissie, O., Worrell, 2023)

$\mathcal{S}$ is a Universal Skolem Set of strictly positive lower density. Moreover, assuming the Bateman-Horn Conjecture, $\mathcal{S}$ has density exactly 1.

$\mathcal{S}$ has strictly positive lower density

Theorem (Luca, O., Worrell, MFCS 2022)

$\mathcal{S}$ has strictly positive lower density.

$\mathcal{S}$ has strictly positive lower density

Theorem (Luca, O., Worrell, MFCS 2022)

$\mathcal{S}$ has strictly positive lower density.

Technical combinatorial argument, involving two key ingredients:

- Sieve techniques, esp. the Selberg upper-bound sieve for linear forms

$\mathcal{S}$ has strictly positive lower density

Theorem (Luca, O., Worrell, MFCS 2022)

$\mathcal{S}$ has strictly positive lower density.

Technical combinatorial argument, involving two key ingredients:

- Sieve techniques, esp. the Selberg upper-bound sieve for linear forms
- the "moment method" together with a Cauchy-Schwarz argument

$\mathcal{S}$ has strictly positive lower density

Theorem (Luca, O., Worrell, MFCS 2022)

$\mathcal{S}$ has strictly positive lower density.

Technical combinatorial argument, involving two key ingredients:

- Sieve techniques, esp. the Selberg upper-bound sieve for linear forms
- the "moment method" together with a Cauchy-Schwarz argument

Calculations show we can obtain unconditional density at least $1/2$.

$\mathcal{S}$ has density 1 assuming Bateman-Horn

Theorem (Luca, Maynard, Noubissie, O., Worrell, 2023)

Assuming the Bateman-Horn Conjecture, $\mathcal{S}$ has density 1.

$\mathcal{S}$ has density 1 assuming Bateman-Horn

Theorem (Luca, Maynard, Noubissie, O., Worrell, 2023)

Assuming the Bateman-Horn Conjecture, $\mathcal{S}$ has density 1.

Bateman–Horn Conjecture. *Let $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$ be distinct irreducible polynomials with positive leading coefficients, and let*

$$Q(f_1, f_2, \ldots, f_k; x) = \#\{n \le x : f_1(n), f_2(n), \ldots, f_k(n) \text{ are prime}\}. \quad (3.6.1)$$

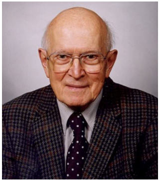
Suppose that $f = f_1 f_2 \cdots f_k$ does not vanish identically modulo any prime. Then

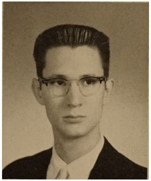
$$Q(f_1, f_2, \ldots, f_k; x) \sim \frac{C(f_1, f_2, \ldots, f_k)}{\prod_{i=1}^k \deg f_i} \int_2^x \frac{dt}{(\log t)^k}, \quad (3.6.2)$$

in which

$$C(f_1, f_2, \ldots, f_k) = \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\omega_f(p)}{p}\right) \quad (3.6.3)$$

and $\omega_f(p)$ is the number of solutions to $f(x) \equiv 0 \pmod p$.





The Bateman-Horn Conjecture

- It is a central, unifying, far-reaching statement about the distribution of prime numbers
- It implies many known results, such as the prime number theorem and the Green–Tao theorem, along with many famous conjectures, such the twin prime conjecture and Landau's conjecture
- It has been described as

  "ranking among the Riemann hypothesis and abc-conjecture as one of the most important and pivotal unproven conjectures in number theory"


BATEMAN-HORN
BATEMAN HOUSE
82-88 Hills Road
Vine FX
BenchSci
GTR
Intrasonics
University of Cambridge
Tucker Gardner
British Medical Group

$\mathcal{S}$ is a Universal Skolem Set

(Proof ingredient) Write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n = 0$, and let n have representation $n = Pq + b$.

$\mathcal{S}$ is a Universal Skolem Set

(Proof ingredient) Write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n = 0$, and let n have representation $n = Pq + b$. Then

$$0 = \sum_{j=1}^{m} Q_j(Pq+b)\lambda_j^{Pq+b} = \sum_{j=1}^{m} Q_j(Pq+b)\left(\lambda_j^P\right)^q \lambda_j^b$$

$$\equiv \sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q \lambda_j^b \pmod{\mathfrak{p}}$$

for $\mathfrak{p}$ a prime ideal above P and σ a Frobenius automorphism.

$\mathcal{S}$ is a Universal Skolem Set

(Proof ingredient) Write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n = 0$, and let n have representation $n = Pq + b$. Then

$$0 = \sum_{j=1}^{m} Q_j(Pq+b)\lambda_j^{Pq+b} = \sum_{j=1}^{m} Q_j(Pq+b)\left(\lambda_j^P\right)^q \lambda_j^b$$
$$\equiv \sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b \pmod{\mathfrak{p}}$$

for $\mathfrak{p}$ a prime ideal above P and σ a Frobenius automorphism. It follows that $P \mid \mathcal{N}\left(\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$.

$\mathcal{S}$ is a Universal Skolem Set

(Proof ingredient) Write $u_n = \sum_{j=1}^m Q_j(n)\lambda_j^n = 0$, and let n have representation $n = Pq + b$. Then

$$\begin{aligned} 0 = \sum_{j=1}^{m} Q_j(Pq+b)\lambda_j^{Pq+b} &= \sum_{j=1}^{m} Q_j(Pq+b)\left(\lambda_j^P\right)^q \lambda_j^b \\ &\equiv \sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b \pmod{\mathfrak{p}} \end{aligned}$$

for $\mathfrak{p}$ a prime ideal above P and σ a Frobenius automorphism.

It follows that $P \mid \mathcal{N}\left(\sum_{j=1}^m Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$.

But q and b are 'small', hence $\mathcal{N}\left(\sum_{j=1}^m Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$ is also 'small'.

$\mathcal{S}$ is a Universal Skolem Set

(Proof ingredient) Write $u_n = \sum_{j=1}^{m} Q_j(n)\lambda_j^n = 0$, and let n have representation $n = Pq + b$. Then

$$
\begin{aligned}
0 = \sum_{j=1}^{m} Q_j(Pq+b)\lambda_j^{Pq+b} &= \sum_{j=1}^{m} Q_j(Pq+b)\left(\lambda_j^P\right)^q \lambda_j^b \\
&\equiv \sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b \pmod{\mathfrak{p}}
\end{aligned}
$$

for $\mathfrak{p}$ a prime ideal above P and σ a Frobenius automorphism.

It follows that $P \mid \mathcal{N}\left(\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$.

But q and b are 'small', hence $\mathcal{N}\left(\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$ is also 'small'. Thus for n sufficiently large, P too will be large, and in particular $P > \mathcal{N}\left(\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$

$\mathcal{S}$ is a Universal Skolem Set

(Proof ingredient) Write $u_n = \sum_{j=1}^m Q_j(n)\lambda_j^n = 0$, and let n have representation $n = Pq + b$. Then

$$0 = \sum_{j=1}^{m} Q_j(Pq+b)\lambda_j^{Pq+b} = \sum_{j=1}^{m} Q_j(Pq+b)\left(\lambda_j^P\right)^q \lambda_j^b$$
$$\equiv \sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b \pmod{\mathfrak{p}}$$

for $\mathfrak{p}$ a prime ideal above P and σ a Frobenius automorphism.

It follows that $P \mid \mathcal{N}\left(\sum_{j=1}^m Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$.

But q and b are 'small', hence $\mathcal{N}\left(\sum_{j=1}^m Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$ is also 'small'. Thus for n sufficiently large, P too will be large, and in particular $P > \mathcal{N}\left(\sum_{j=1}^m Q_j(b)\sigma(\lambda_j)^q\lambda_j^b\right)$, whence

$$\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q\lambda_j^b = 0\,.$$

$\mathcal{S}$ is a Universal Skolem Set

We have that, for n large enough, if $u_n = 0$ and n has representation $n = Pq + b$, then

$$\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q \lambda_j^b = 0 \tag{1}$$

$\mathcal{S}$ is a Universal Skolem Set

We have that, for n large enough, if $u_n = 0$ and n has representation $n = Pq + b$, then

$$\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q \lambda_j^b = 0 \tag{1}$$

Now recall:

Theorem (after Schlickewei and Schmidt, 2000)

There is an explicit upper bound on the number of 'non-overlapping' solutions of the equation $\sum_{j=1}^{m} Q_j(y)\alpha_j^x \lambda_j^y = 0$ in integers $x, y \in \mathbb{N}$.

$\mathcal{S}$ is a Universal Skolem Set

We have that, for n large enough, if $u_n = 0$ and n has representation $n = Pq + b$, then

$$\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q \lambda_j^b = 0 \tag{1}$$

Now recall:

Theorem (after Schlickewei and Schmidt, 2000)

There is an explicit upper bound on the number of 'non-overlapping' solutions of the equation $\sum_{j=1}^{m} Q_j(y)\alpha_j^x \lambda_j^y = 0$ *in integers* $x, y \in \mathbb{N}$.

Each representation (P, q, b) of n gives rise to a solution (q, b) of the **companion equation** (1) above.

$\mathcal{S}$ is a Universal Skolem Set

We have that, for n large enough, if $u_n = 0$ and n has representation $n = Pq + b$, then

$$\sum_{j=1}^{m} Q_j(b)\sigma(\lambda_j)^q \lambda_j^b = 0 \qquad (1)$$

Now recall:

Theorem (after Schlickewei and Schmidt, 2000)

There is an explicit upper bound on the number of 'non-overlapping' solutions of the equation $\sum_{j=1}^{m} Q_j(y)\alpha_j^x \lambda_j^y = 0$ in integers $x, y \in \mathbb{N}$.

Each representation (P, q, b) of n gives rise to a solution (q, b) of the **companion equation** (1) above.

As the number of representations of n tends to infinity, but the number of solutions to the companion equation is explicitly bounded, this yields an effective upper bound on $n \in \mathcal{S}$ such that $u_n = 0$.

Outlook

Universal Skolem Sets are a radically new line of attack on the Skolem Problem

Outlook

Universal Skolem Sets are a radically new line of attack on the Skolem Problem

Three critical directions:

- Can one attain density one unconditionally?

Outlook

Universal Skolem Sets are a radically new line of attack on the Skolem Problem

Three critical directions:

- Can one attain density one unconditionally?
- Is there a construction yielding a Universal Skolem Set containing *some* infinite arithmetic progression?
  - $\Rightarrow$ this would solve the Skolem Problem!

Outlook

Universal Skolem Sets are a radically new line of attack on the Skolem Problem

Three critical directions:

- Can one attain density one unconditionally?
- Is there a construction yielding a Universal Skolem Set containing *some* infinite arithmetic progression?
  - $\Rightarrow$ this would solve the Skolem Problem!
- Can these ideas be applied to other problems, such as Positivity or Ultimate Positivity, etc.?

"...on something like equal terms..."
[with apologies to G. H. Hardy]