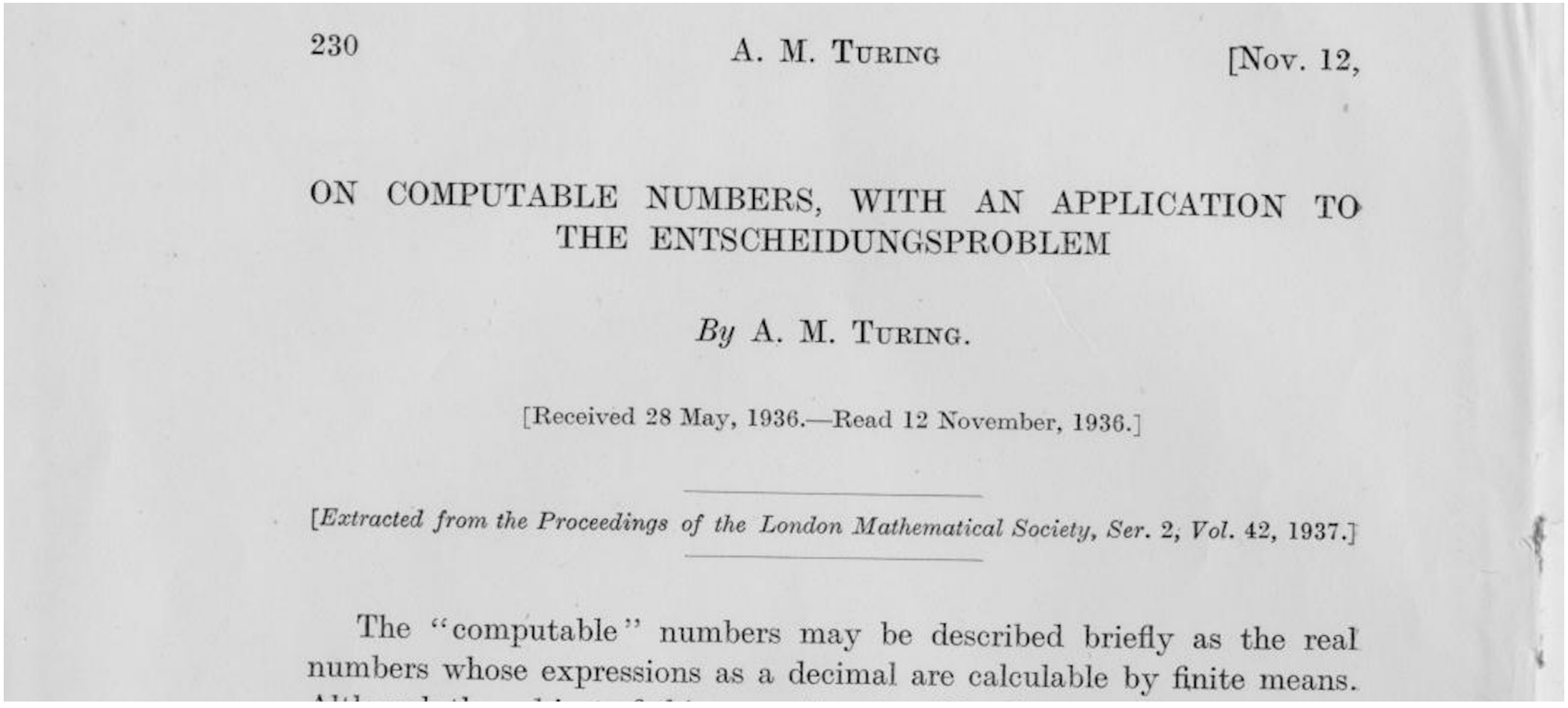
The Skolem Landscape

Joël Ouaknine

Max Planck Institute for Software Systems

One World Numeration Seminar
12 March 2024



230 A. M. TURING [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

[*Extracted from the Proceedings of the London Mathematical Society, Ser.* 2, *Vol.* 42, 1937.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means.

Among others, Turing . . .

- defines the notion of **universal Turing machine**; and with it, the formal notions of **algorithm** and **computability**
- introduces the **Halting Problem** and establishes its **undecidability**
- introduces the notion of **computable numbers** and solves Hilbert's **Entscheidungsproblem**

Proving Program Termination @ CACM'11

In contrast to popular belief, proving termination is not always impossible.

BY BYRON COOK, ANDREAS PODELSKI, AND ANDREY RYBALCHENKO

Proving Program Termination

"[. . .] termination tools can automatically prove or disprove termination of many famous complex examples such as Ackermann's function or McCarthy's 91 function as well as moderately sized industrial examples"

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
    $\mathbf{x} := \mathbf{M}\mathbf{x};$

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-COMPLETE:

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

POSITIVITY-COMPLETE:

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

What Exactly Are the Skolem and Positivity Problems?

Problem SKOLEM (1934)

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 (mid-1970s)

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,

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

- 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 (1934)

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

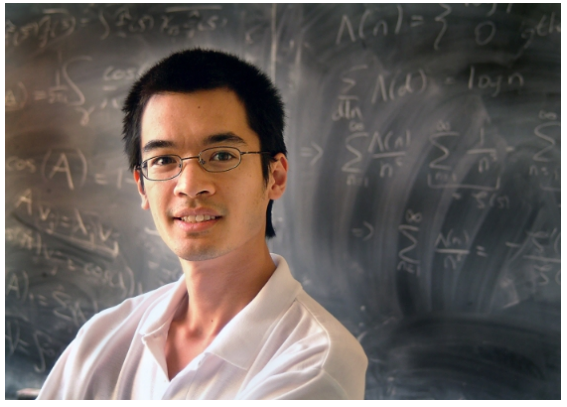
Problem POSITIVITY (mid-1970s)

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



"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.

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

Quick Quiz

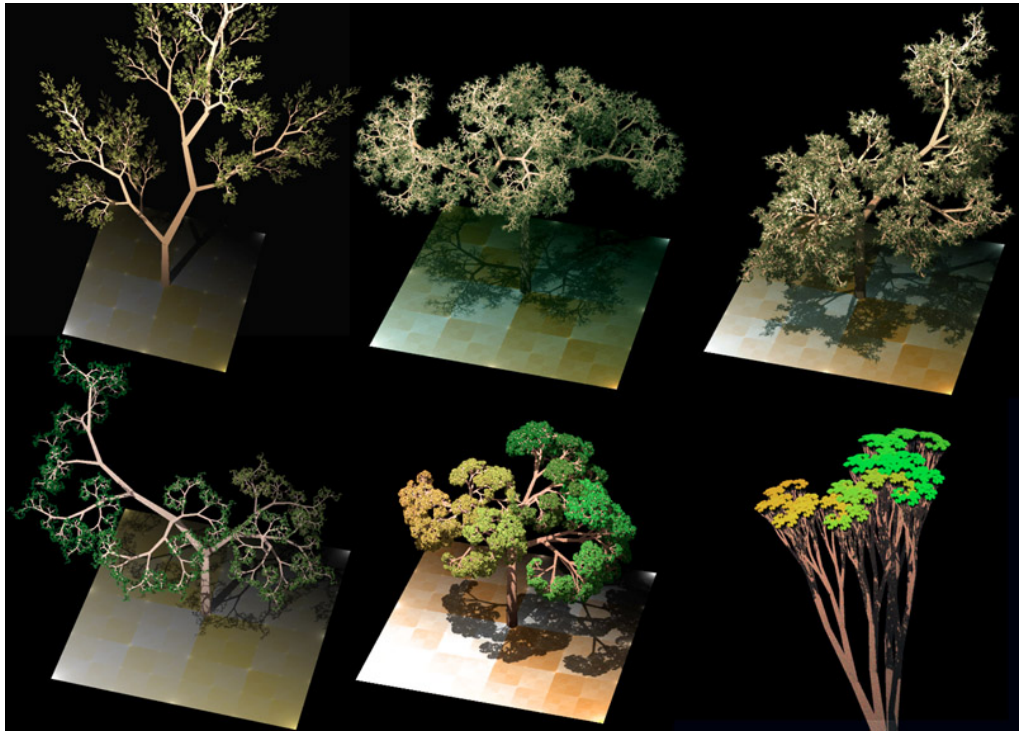
- Given two automata A and B, is every word accepted by A also accepted by B?
  - **PSPACE-COMPLETE**
- Given two automata A and B, for every n, does B always accept at least as many words of length n as A?
  - **POSITIVITY-COMPLETE**
- Consider a discrete Markov chain over states $s_1, \ldots, s_k$, with rational transition probabilities. Starting in state s_1 with probability 1, is there an integer n such that after n steps, the probability of being in state s_k is exactly $1/2$?
  - **SKOLEM-COMPLETE**

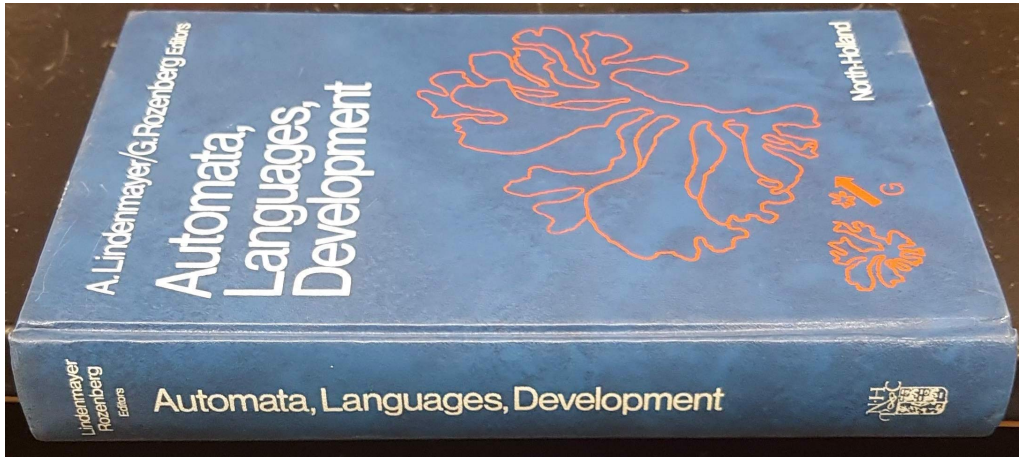
Some Other Application Areas

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

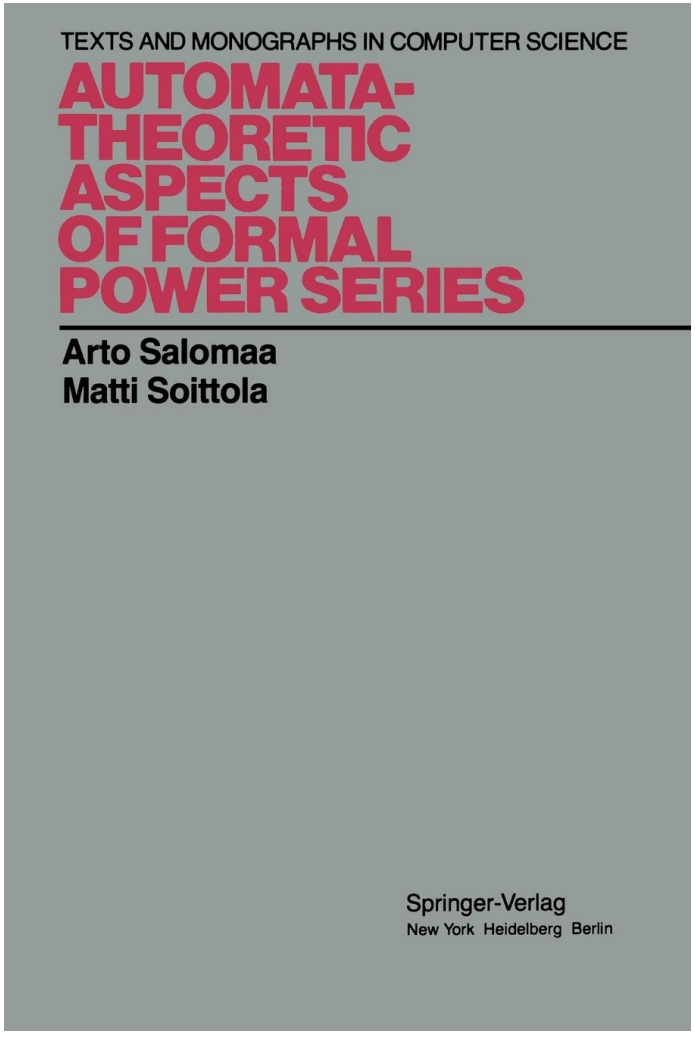
- theoretical biology (analysis of L-systems)
- software verification / program analysis
- dynamical systems
- differential privacy
- (weighted) automata and games
- analysis of stochastic systems
- control theory
- quantum computing
- statistical physics
- formal power series
- combinatorics
- ...

L-Systems (Aristid Lindenmayer, late 1960s)





Automata and Power Series (from 1960s, published 1978)



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 $\langle 2, 1 \rangle$:

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

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

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

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

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

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

$\Rightarrow$ **Never zero!**

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $u_n = 0$?

Turing Reductions

Theorem (Folklore)

BI-SKOLEM $\leq_T$ *SKOLEM* $\leq_T$ *POSITIVITY.*

- Note that these are Turing (i.e., oracle) reductions: in particular the order of LRS is not necessarily preserved (so, for example, to solve the Skolem Problem at order 5, it would suffice to solve the Positivity Problem at order 10)

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

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 (O. & 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.:

- 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...

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)
- 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) $e^5\pi^3 - e^2\pi^7 + e$?

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

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

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 $\gcd(m, a_k) = 1$.

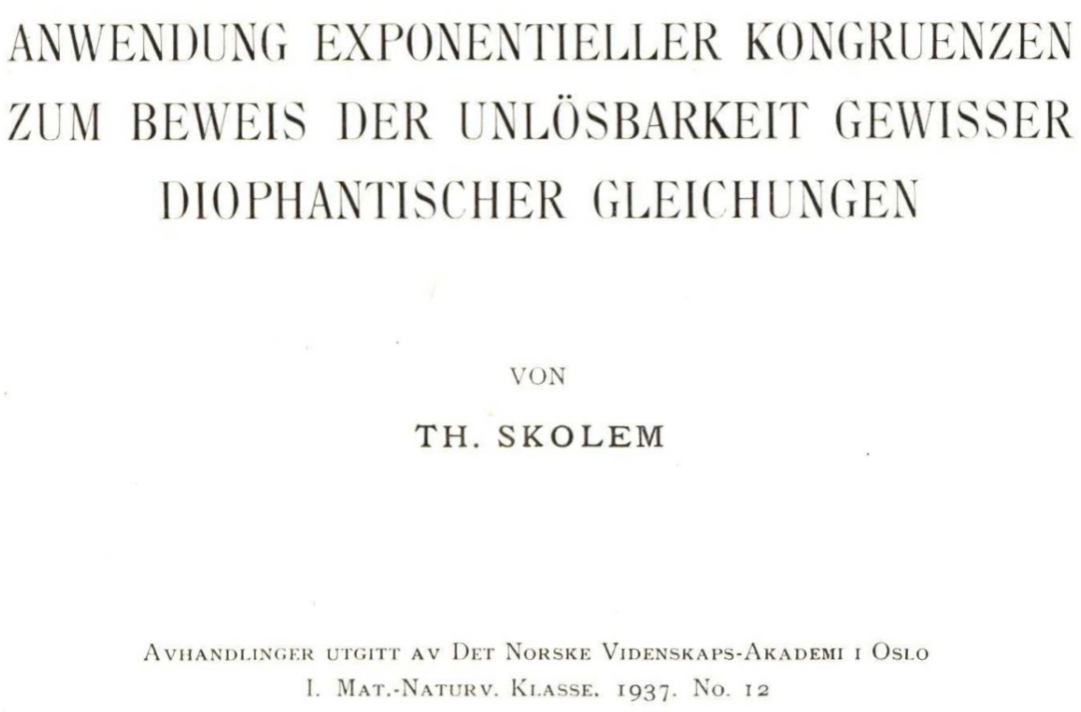
- Example: $u_{n+1} = 2u_n$:

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

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

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

The Exponential Local-Global Principle



ANWENDUNG EXPONENTIELLER KONGRUENZEN
ZUM BEWEIS DER UNLÖSBARKEIT GEWISSER
DIOPHANTISCHER GLEICHUNGEN

VON

TH. SKOLEM

AVHANDLINGER UTGITT AV DET NORSKE VIDENSKAPS-AKADEMI I OSLO
I. MAT.-NATURV. KLASSE. 1937. NO. 12

- The **Exponential Local-Global Principle (ELGP)** is a wide-ranging conjecture formulated in 1937
- Like Schanuel's Conjecture, widely believed by number theorists, but only proven in special cases

The Exponential Local-Global Principle

The ELGP 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 Problem for Simple LRS

Theorem (Bilu, Luca, Nieuwveld, O., 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 ELGP 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**
- 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

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

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
```

- [x] 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} =
-2716131161712097448586635205589463470401509550890641913636335454675409769151
1} +
-5087571794255306084649276133206965823971875016365294395124753570723932449955
2} +
-1020664001586411899151994265194472024922159984096674355479305686778200805260
3} +
-1412095662406000310364496715181260667298901575064822931268517590804654375986
4} +
1906955894773207103609842658940914223756942339091587019654461069437273467027
5} +
```

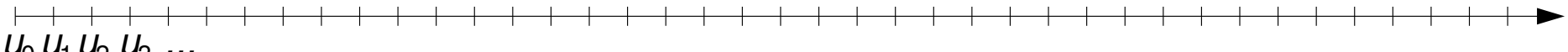
Computing the Zero Set of Simple, Non-Degenerate LRS

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

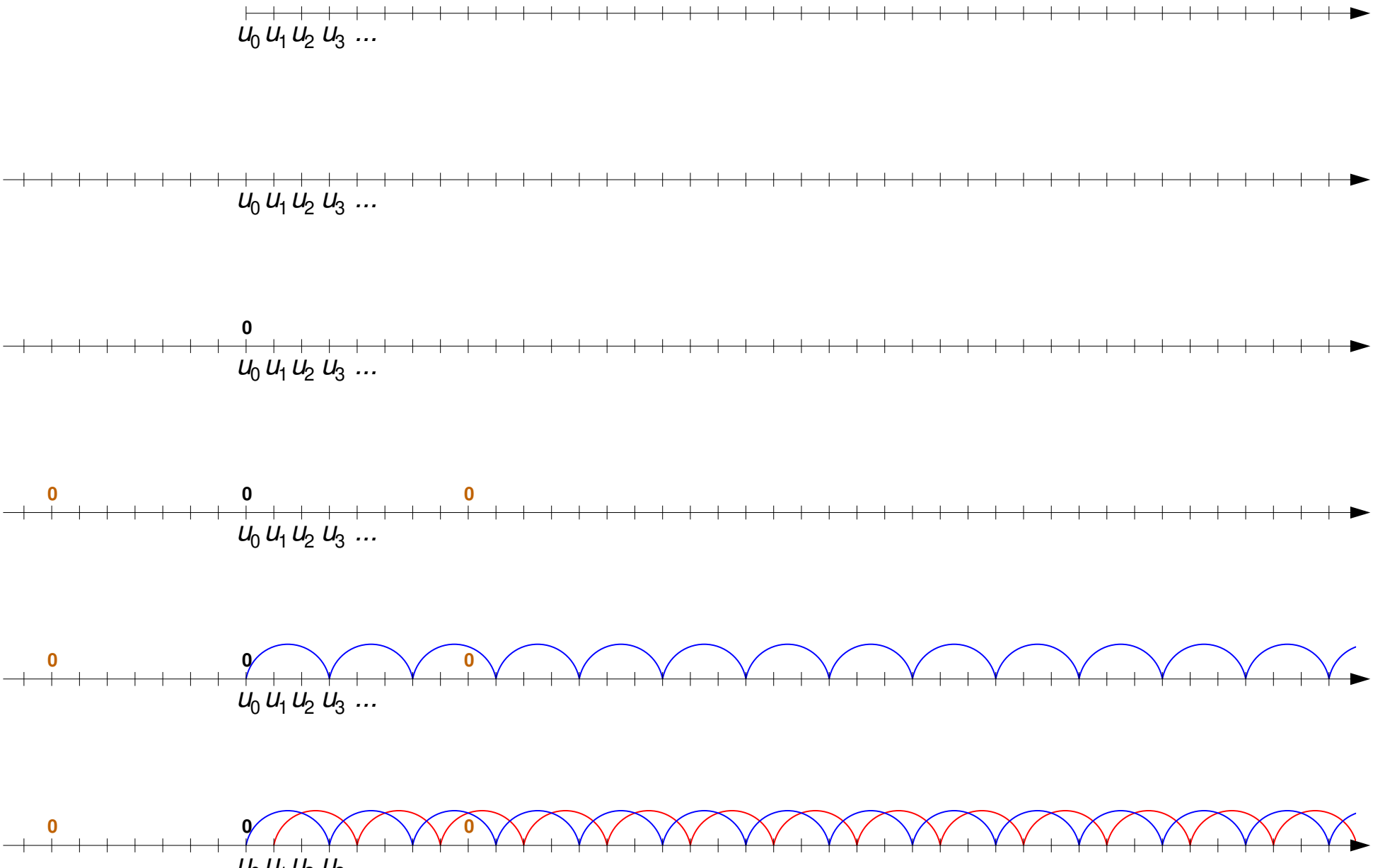
Lemma (Bilu, Luca, Nieuwveld, O., Purser, Worrell 2022)

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



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
```

- [x] 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} =
-2716131161712097448586635205589463470401509550890641913636335454675409769151
1} +
-5087571794255306084649276133206965823971875016365294395124753570723932449955
2} +
-1020664001586411899151994265194472024922159984096674355479305686778200805260
3} +
-1412095662406000310364496715181260667298901575064822931268517590804654375986
4} +
1906955894773207103609842658940914223756942339091587019654461069437273467027
5} +
```

Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 26 (2015) 113–136

indagationes mathematicae

www.elsevier.com/locate/indag

Linear equations over multiplicative groups, recurrences, and mixing II

H. Derksen[a,*], D. Masser[b]

[a] *Department of Mathematics, University of Michigan, East Hall 530 Church Street, Ann Arbor, MI 48109, USA*
[b] *Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland*

Received 16 December 2013; received in revised form 1 August 2014; accepted 10 August 2014

Communicated by F. Beukers

Abstract

Let $u_1, \ldots, u_m$ be linear recurrences with values in a field K of positive characteristic p. We show that the set of integer vectors $(k_1, \ldots, k_m)$ such that $u_1(k_1) + \cdots + u_m(k_m) = 0$ is p-normal in a natural sense generalizing that of the first author, who proved the result for $m = 1$. Furthermore the set is effectively computable if K is. We illustrate this with an example for $m = 4$. We also show that the corresponding set for zero characteristic is not decidable for $m = 557844$, thus verifying a conjecture of Cerlienco, Mignotte, and Piras.
© 2014 Royal Dutch Mathematical Society (KWG). Published by Elsevier B.V. All rights reserved.

Keywords: Recurrence sequences; Skolem–Mahler–Lech theorem; Algebraical dynamical systems; Mixing

We should say something about effectivity.

In zero characteristic Theorem A remains ineffective, even for rational recurrences of order 5 like

$$u(k) = (8+i)^k + (8-i)^k - (7+4i)^k - (7-4i)^k - 1, \tag{1.6}$$

(for which we thank Maurice Mignotte), where we still cannot in principle find all the k with $u(k) = 0$ (the trouble is $|8+i| = |8-i| = |7+4i| = |7-4i|$). But there are many estimates

for the number of solutions. For example, Beukers [4] showed that if a rational recurrence of order at most 3 has only finitely many zeros, then it has at most 6, as in the Berstel sequence. The more recent estimates from [12] imply the upper bound $\exp(2.18^9) = \exp(396718580736)$ for the number of k in (1.6). Very recently Amoroso and Viada [2] have improved the results of [12], giving $24^{1620} < \exp(5149)$. And more generally Schmidt [26] showed in Theorem A for order at most d that at most $\exp\exp\exp(20d)$ singletons and infinite arithmetic progressions are needed. The works [21,22] cited above, as well as [23] and [24], also contain explicit estimates for the number of solutions.

David Masser <david.masser@unibas.ch> 18 Jan 2024, 19:26
to Joël, ha.derksen@northeastern.edu

Dear Joël,

Thank you very much for the message. But I now see that something strange has happened. In the final version of our tex file we had a slightly different example (see (1.6) page 6 below). I seem to recall that the extra coefficients 2 were suggested by Mignotte, possibly because of the "fairly simple geometric argument" that you have in mind (something vaguely "trigonometrical" as I remember). I have no idea why the extra coefficients did not appear in the printed version. But in the tex file |c_1| is no longer |c_2|.

What happens if you "Skolem Tool" the original recurrence?

Best wishes,
David Masser.

Joël Ouaknine <joel@mpi-sws.org> 18 Jan 2024, 19:56
to David, ha.derksen@northeastern.edu

Dear David,

Ah, very interesting! But now I'm genuinely confused. Your original sequence (meaning the one in the draft you sent me, and for which you thank Mignotte) is a rational-valued sequence of order 4, for which Mignotte himself famously proved Theorem A (Skolem-Mahler-Lech) was effective! Maybe you meant to add a constant to it, to make it order 5?

At any rate, I entered it into our Skolem tool, which tells us it's always non-zero mod 4.
(The coefficients of the recurrence equation are 30 -354 1950 -4225, and the initial values are
2 18 186 1938.)

Happy to try with an extra constant, if you'd like to suggest one... :)

All the best,

-- Joël

David Masser <david.masser@unibas.ch> 18 Jan 2024, 23:14
to Joël

Thanks! I could easily suggest other modifications but I suspect that "Skolem Tool" will always win. It is a nice piece of work!

The Skolem Landscape