Linear recurrences: A short journey across number theory, dynamics, and decidability

Daniel Smertnig

Mathematics in Ljubljana

Summer School

June 30 – July 4, 2025

UNIVERSITY OF LJUBLJANA
Faculty of Mathematics and Physics

The Basic Problem

Linear Recurrence Sequences

Fibonacci numbers: $0, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots$

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad \text{for } n \geq 2.$$

Definition

Let K be a field. A sequence $(a_n)_{n\geq 0}$ is a linear recurrence sequence (LRS) if there exist $c_1, \ldots, c_d \in K$ such that

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d} \qquad \text{for } n \geq d. \tag{$\bigstar$}$$

($\bigstar$) together with $a_0, \ldots, a_{d-1}$ completely determines the sequence.

Examples

- Fibonacci numbers: $\mathbf{0}, \mathbf{1}, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots$
- $\mathbf{1}, \mathbf{0}, -2, 0, 4, 0, -8, \ldots \qquad (a_n = -2a_{n-2})$
- $\mathbf{1}, \mathbf{3}, 7, 17, 41, 99, 239, 577, \ldots \qquad (P_n = 2P_{n-1} + P_{n-2})$

  Number of n-step non-self-intersecting paths in $\mathbb{Z}^2$ with possible steps North $(0, 1)$, East $(1, 0)$, and West $(-1, 0)$.

Zeros of LRS

Definition

An (infinite) arithmetic progression is a set of the form

$$\{ ak + b \in \mathbb{N}_0 : k \geq 0 \} = a\mathbb{N}_0 + b$$

with $a \geq 1$, $b \geq 0$.

Theorem (Skolem–Mahler–Lech)

If K is a field of characteristic 0, and $(a_n)_{n\geq 0}$ is an LRS, then its set of zeros is a union of

- finitely many arithmetic progressions, and
- a finite set.

Decidability?

Berstel's sequence: $a_n = 2a_{n-1} - 4a_{n-2} + 4a_{n-3}$ starting with $0, 0, 1$.

$0,\ 0,\ 1,\ 2,\ 0,\ -4,\ 0,\ 16,\ 16,\ -32,\ -64,\ 64,\ 256,\ 0,\ -768,\ -512,\ 2048,\ 3072,$
$-4096,\ -12288,\ 4096,\ 40960,\ 16384,\ -114688,\ -131072,\ 262144,\ 589824,\ -393216,$
$-2097152,\ -262144,\ 6291456,\ 5242880,\ -15728640,\ -27262976,\ 29360128,$
$104857600,\ -16777216,\ -335544320,\ -184549376,\ 905969664,\ 1207959552,$
$-1946157056,\ -5100273664,\ 2415919104,\ 17448304640,\ 4831838208,\ -50465865728,$
$-50465865728,\ 120259084288,\ 240518168576,\ -201863462912,\ -884763262976,\ 0,$
$2731599200256,\ 1924145348608,\ -7078106103808,\ -10926396801024,\ 14156212207616,$
$43705587204096,\ -12919261626368,\ -144036023238656,\ -61572651155456,$
$401321744138240,\ 472789999943680,\ -905997581287424,\ -2097868185796608,$
$1319413953331200,\ 7406310324699136,\ 1143492092887040,\ -22060601299697664,$
$-19069929672146944,\ 54676514226044928,\ 97390341941886976,\ \ldots$

Zeros at indices 0, 1, 4, 6, 13, 52.

The Skolem Problem

Skolem Problem (open)

Is it **decidable** whether an arbitrary LRS (over $\mathbb{Q}$) has a zero?

Explicitly: Is there an algorithm that takes as input an arbitrary LRS over $\mathbb{Q}$, and outputs whether or not that LRS has a zero?

- **Known**: this is sufficient to find all zeros. (Berstel–Mignotte '76)

'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, 2006, "What's New — Open question: effective Skolem–Mahler–Lech Theorem)

The Skolem Problem

Skolem Problem (open)

Is it decidable whether an arbitrary LRS (over $\mathbb{Q}$) has a zero?

- Small order: $d = 1, 2$ is easy; $d = 3, 4$ by Mignotte–Shorey–Tijdeman '84, Vereshchagin '85; $d = 5$: only partial results.
- Bilu–Luca–Nieuwveld–Ouaknine–Purser–Worrell '22: *Skolem Meets Schanuel*.
  - The Skolem Problem for simple LRS is decidable **assuming** the Skolem Conjecture and the weak p-adic Schanuel Conjecture.
  - Conjectures only used for termination.


The Many Faces of LRS

Rational Functions

Proposition

$(a_n)_{n\geq 0}$ is an LRS if and only if the generating function $f = \sum_{n=0}^{\infty} a_n x^n \in K[\![x]\!]$ is rational.

Example

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2} \qquad \sum_{n=0}^{\infty} P_n x^n = \frac{1+x}{1-2x-x^2}$$

Skolem problem: Is it decidable if at least one of the coefficients of the Taylor expansion of a rational function is zero? Equivalently: some derivative vanishes at zero?

Linear Representations

Proposition

$(a_n)_{n \geq 0}$ is an LRS if and only if there exist $d \geq 0$, vectors u, $v \in K^d$ and a matrix $A \in K^{d \times d}$ such that

$$a_n = u^T A^n v.$$

Example

$$F_n = (1, 0) \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad P_n = (1, 0) \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^n \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Skolem problem: (A, v) is a discrete dynamical system, and u defines a hyperplane in K^d. Is it decidable if the orbit $\{ A^n v : n \geq 0 \}$ ever hits the hyperplane?

Exponential Polynomials

Proposition

Suppose K is of characteristic 0 and algebraically closed. Then $(a_n)_{n\geq 0}$ is an LRS if and only if there exist $\lambda_1, \ldots, \lambda_r \in K$ and polynomials $P_i \in K[x]$ such that

$$a_n = P_1(n)\lambda_1^n + \cdots + P_r(n)\lambda_r^n \qquad \text{for sufficiently large } n.$$

Example

$$F_n = \frac{1}{\sqrt{5}}\left(\phi^n - (1-\phi)^n\right) \text{ with } \phi = \frac{1+\sqrt{5}}{2}, \qquad P_n = \frac{1}{2}\left((1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1}\right)$$

Skolem problem: Is it decidable if an exponential polynomial has a zero (in $\mathbb{N}_0$)?

More Facets

Simple linear loops:

```
x=-4, y=0, z=16
while z != 0:
    ...
    t = x, x = y, y = z,
    z = 2y - 4x + 4t
```

Skolem Problem: Is it decidable whether a simple linear loop terminates? (One of the easiest open instances of the halting problem.)

Matrices: Given $A \in \mathbb{Z}^{d \times d}$, is it decidable whether there exists some $n \geq 0$ such that the top-right entry of A^n is zero?

The Ubiquity of LRS

- Arithmetic progressions $(an+b)_{n\geq 0}$, geometric progressions $(a^n b)_{n\geq 0}$, sequences generated by polynomials $(a_n = P(n))$ are LRS.
- LRS are closed under addition, Hadamard products $(a_n b_n)_{n\geq 0}$, Cauchy products $(\sum_{k=0}^{n} a_k b_{n-k})_{n\geq 0}$.
- Arise in many places in mathematics and computer science, e.g., zeta functions of varieties over finite fields and Hilbert-Poincaré series are rational in many interesting cases.

The Bigger Picture: Generalizations and Connections

Positive Characteristic and Diophantine Equations

Example

Let $K = \mathbb{F}_p(x)$. The sequence

$$a_n = (x+1)^n - x^n - 1$$

is an LRS with zeros at $\{ p^m : m \geq 0 \}$ (Frobenius endomorphism).

Theorem (Derksen '07)

Let $\operatorname{char} K = p > 0$. The zero set of an LRS $(a_n)_{n\geq 0}$ is p-automatic and can be effectively determined.

More general results in Diophantine number theory: Unit equations, Schmidt's subspace theorem.

Semigroups of Matrices and Weighted Automata

Linear representation of an LRS: $n \mapsto u^T A^n v$.

Definition

Let $X = \{x_1, \ldots, x_l\}$ be a non-empty set (alphabet). A linear representation consists of $d \geq 0$, vectors u, $v \in K^d$, and for each $x_i \in X$, a matrix $A_i \in \mathbb{Z}^{d \times d}$.

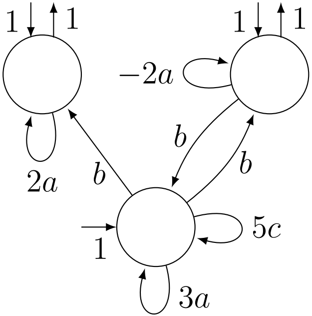
A linear representation induces a map $X^* \to \mathbb{Z}^{d \times d}$

$$w = x_{i_1} \cdots x_{i_l} \mapsto u^T A_{i_1} \cdots A_{i_l} v.$$

Gives a noncommutative multivariate generalization of LRS.

- The data of a linear representation defines a weighted automaton (WA), by viewing the A_i's as adjacency matrices (and conversely).
- Existence of a zero is **undecidable** (Hilbert-10 or Post correspondence problem).

A weighted automaton



$$u = \begin{pmatrix} 1,1,1 \end{pmatrix}$$

$$\mu(a) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\mu(b) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$\mu(c) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

$$v = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Non-linear Version

Conjecture (Dynamical Mordell–Lang Conjecture)

Let X be a quasi-projective variety defined over $\mathbb{C}$, let Φ be an endomorphism of X, let $V \subseteq X$ be a subvariety and let $\alpha \in X(\mathbb{C})$. Then the set

$$\{ n \in \mathbb{N}_0 : \Phi^n(\alpha) \in V(\mathbb{C}) \}$$

is a union of a finite set and finitely many arithmetic progressions.


The Course

Structure of Mini-Course

- Day 0: Introduction $\longleftarrow$ You are here
- Day 1: Characterizations of LRS
- Day 2: p-adic numbers
- Day 3: Proving the Skolem–Mahler–Lech Theorem (over $\mathbb{Q}$)
- Day 4: *Skolem meets Schanuel* [BLNOPW'22].

Notes and Exercises available on my website:
https://math.smertnig.at/teaching/s25/minicourse/

Resources

LRS (in particular Day 1, 3):

- [BR'11] Berstel, Reutenauer. *Noncommutative Rational Series and Their Applications*. Encyclopedia Math. Appl., 137, Cambridge University Press, 2011.
- [EvdPSW'03] Everest, van der Poorten, Shparlinski, Ward. *Recurrence sequences*. Math. Surveys Monogr., 104, American Mathematical Society, 2003.

p-adic numbers (in particular Day 2):

- [Gou'20] Gouvêa. *p-adic numbers. An introduction*. Third edition. Springer, 2020.
- [Rob'00] Robert. *A course in p-adic analysis*. GTM 198 Springer, 2000.

Skolem-Mahler-Lech Theorem and Decidability (in particular, Day 3, 4):

- [BLNOPW'22] Bilu, Luca, Nieuwveld, Ouaknine, Purser, Worrell. *Skolem Meets Schanuel*. 47th International Symposium on Mathematical Foundations of Computer Science, Art. No. 20, 15 pp. arXiv:2204.13417
- [Tao'07] *Effective Skolem-Mahler-Lech theorem*, What's New (Tao's Blog). https://terrytao.wordpress.com/2007/05/25/open-question-effective-skolem-mahler-lech-theorem/

My coordinates:

Daniel Smertnig,
daniel.smertnig@fmf.uni-lj.si,
4th floor, room 4.23.