Decidability of logical theories via rigidity and randomness in dynamical systems

Toghrul Karimov

Max Planck Institute for Software Systems, Saarbrücken, Germany

This talk

Let $\mathcal{M}$ be a mathematical structure, e.g. $\mathcal{M} = (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$

Does there exist an algorithm that takes a sentence φ and decides whether $\mathcal{M} \models \varphi$?

Ex.: $\varphi := \exists x.\, \forall y.\, \exists z_1.\, \exists z_2 :\ z_1 > y\ \land\ z_2 > y\ \land\ x = z_1 - z_2\ \land\ z_1 \in 2^{\mathbb{N}}\ \land\ z_2 \in 3^{\mathbb{N}}$

This talk

Let $\mathcal{M}$ be a mathematical structure, e.g. $\mathcal{M} = (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$

Does there exist an algorithm that takes a sentence φ and decides whether $\mathcal{M} \models \varphi$?

Ex.: $\varphi := \exists x. \forall y. \exists z_1. \exists z_2 : z_1 > y \ \land \ z_2 > y \ \land \ x = z_1 - z_2 \ \land \ z_1 \in 2^{\mathbb{N}} \ \land \ z_2 \in 3^{\mathbb{N}}$
$\equiv$ "There exist x such that $x = 2^n - 3^m$ for infinitely many $n, m \geq 0$"

This talk

Let $\mathcal{M}$ be a mathematical structure, e.g. $\mathcal{M} = (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$

Does there exist an algorithm that takes a sentence φ and decides whether $\mathcal{M} \models \varphi$?

Ex.: $\varphi := \exists x.\, \forall y.\, \exists z_1.\, \exists z_2 \colon z_1 > y \ \wedge\ z_2 > y \ \wedge\ x = z_1 - z_2 \ \wedge\ z_1 \in 2^{\mathbb{N}} \ \wedge\ z_2 \in 3^{\mathbb{N}}$
$\equiv$ "There exist x such that $x = 2^n - 3^m$ for infinitely many $n, m \geq 0$"

Step 1. Link the algebraic object to dynamical systems, e.g. $(\mathbb{R}/\mathbb{Z}, x \mapsto x + \log_2(3))$

Step 2. Study whether the relevant system(s) are rigid ($\approx$ zero-entropy, deterministic) or fully random ("everything that can happen will happen")

Step 3. Deduce decidability or undecidability

Problems can be undecidable

Decision problem: yes/no question about the input

Undecidable problem: there does not exist an algorithm that terminates on all inputs and correctly outputs yes/no

Problems can be undecidable

Decision problem: yes/no question about the input

Undecidable problem: there does not exist an algorithm that terminates on all inputs and correctly outputs yes/no

Gödel 1931

The theory of $\langle \mathbb{Z}; <, +, \cdot \rangle$ is undecidable

Matiyasevich, Robinson, Davis, Putnam 1949-1970

H10 (given $p \in \mathbb{Z}[x_1, \ldots, x_d]$, decide whether $\exists x_1, \ldots, x_d \in \mathbb{Z}\colon p(x_1, \ldots, x_d) = 0$) is undecidable

Canonical undecidable problem

Given a program $\mathcal{P}$, decide whether it terminates

What are our dynamical systems?

Discrete dynamical system: $(X, f : X \mapsto X)$. The *orbit* of $x \in X$ is $\langle x, f(x), f(f(x)), \ldots \rangle$

Polynomial dynamics: $X = \mathbb{R}^d$, $f(x) = (p_1(x), \ldots, p_d(x))$

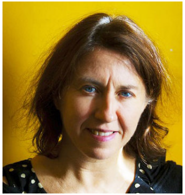
Translations on a torus: $X = (\mathbb{R}/\mathbb{Z})^d$, $f(x) = x + t$ for some $t \in X$

The Gauss map: $X = (0, 1)$, $f(x) = \frac{1}{x} - \lfloor \frac{1}{x} \rfloor$. Orbits compute continued fraction expansions

Expansions in base $\beta > 1$: $X = [0, 1)$, $f(x) = \beta x - \lfloor \beta x \rfloor$

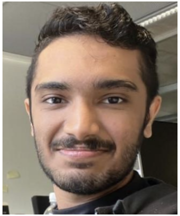
Shift spaces: $X = \Sigma^\omega$, $f((x_n)_n) = ((x_{n+1})_n)$

Valérie Berthé



Florian Luca

Mihir Vahanwala



Joël Ouaknine

James Worrell

Joris Nieuwveld

Integers with addition and powers

Semënov 1980

The theory of $(\mathbb{Z}; <, +, 2^{\mathbb{N}})$ is decidable

Proof 1: given $\varphi := Q_1 x_1 \cdots Q_m x_m \colon \psi(x_1, \ldots, x_m)$, where $Q_i \in \{\exists, \forall\}$ and ψ is quantifier-free, eliminate $Q_m x_m, \ldots, Q_1 x_1$

Integers with addition and powers

Semënov 1980

The theory of $(\mathbb{Z}; <, +, 2^{\mathbb{N}})$ is decidable

Proof 1: given $\varphi := Q_1 x_1 \ \cdots Q_m x_m \colon \psi(x_1, \ldots, x_m)$, where $Q_i \in \{\exists, \forall\}$ and ψ is quantifier-free, eliminate $Q_m x_m, \ldots, Q_1 x_1$

Proof 2: Represent integers by their binary expansions. Given φ, construct a finite-state machine (=automaton) that takes as input

$$(s_1, \ldots, s_m) \in \big(\pm \{0,1\}^* \big)^m$$

and computes the truth value of $\psi(\mathrm{eval}(s_1), \ldots, \mathrm{eval}(s_m))$.

Integers with addition and powers

Semënov 1980

The theory of $(\mathbb{Z}; <, +, 2^{\mathbb{N}})$ is decidable

Proof 1: given $\varphi := Q_1 x_1 \cdots Q_m x_m \colon \psi(x_1, \ldots, x_m)$, where $Q_i \in \{\exists, \forall\}$ and ψ is quantifier-free, eliminate $Q_m x_m, \ldots, Q_1 x_1$

Proof 2: Represent integers by their binary expansions. Given φ, construct a finite-state machine (=automaton) that takes as input

$$(s_1, \ldots, s_m) \in \big(\pm \{0,1\}^* \big)^m$$

and computes the truth value of $\psi(\mathrm{eval}(s_1), \ldots, \mathrm{eval}(s_m))$. Decide the truth of $Q_1 s_1 \cdots Q_m s_m \colon \psi(\mathrm{eval}(s_1), \ldots, \mathrm{eval}(s_m))$ using automata theory

Integers with addition and powers

Hieronymi, Schulz 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

Integers with addition and powers

Hieronymi, Schulz 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

Proof idea: there exists a function $g\colon \mathbb{Z}^k \to \mathbb{N}^*$ that

1. can be implemented in $\mathcal{M}$
2. is onto

Integers with addition and powers

Hieronymi, Schulz 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

Proof idea: there exists a function $g \colon \mathbb{Z}^k \to \mathbb{N}^*$ that

1. can be implemented in $\mathcal{M}$
2. is onto

For $x \in 3^{\mathbb{N}}$, $x \neq 1$ write $x = 2^{\alpha(x)} + 2^{\beta(x)} + R(x)$ where $2^{\alpha(x)} > 2^{\beta(x)} > R(x)$.
Hieronymi and Schulz have $k = 2$ and

$$g(3^a, 3^b) = \left(\beta(3^n) - \beta(3^a)\right)_{n=a+1}^{b-1} \cap [0, \beta(3^b))$$

The dynamical system: $x \mapsto x + \log_2(3) \bmod 1$

Integers with addition and powers

Hieronymi-Schulz, 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

Proof idea: reduce from the problem of deciding whether a given program $\mathcal{P}$ halts

Integers with addition and powers

Hieronymi-Schulz, 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

Proof idea: reduce from the problem of deciding whether a given program $\mathcal{P}$ halts

Program $\mathcal{P}$: two variables c_1, c_2 initialised to 1, lines $1, \ldots, L$, instructions of the form $c_i = c_i + 1$, JUMP TO ℓ, IF $c_i > 1$ THEN $c_i = c_i - 1$ ELSE JUMP TO ℓ, HALT

The run of $\mathcal{P}$ is $\langle 0, c_{1,0}, c_{2,0}, \ell_0, 0, c_{1,1}, c_{2,1}, \ell_1, 0 \ldots \rangle$

Integers with addition and powers

Hieronymi-Schulz, 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

Proof idea: reduce from the problem of deciding whether a given program $\mathcal{P}$ halts

Program $\mathcal{P}$: two variables c_1, c_2 initialised to 1, lines $1, \ldots, L$, instructions of the form $c_i = c_i + 1$, JUMP TO ℓ, IF $c_i > 1$ THEN $c_i = c_i - 1$ ELSE JUMP TO ℓ, HALT

The run of $\mathcal{P}$ is $\langle 0, c_{1,0}, c_{2,0}, \ell_0, 0, c_{1,1}, c_{2,1}, \ell_1, 0 \ldots \rangle$

$\mathcal{P}$ halts $\Leftrightarrow$ there exists a finite sequence $(x_n)_{n=0}^m$ such that $(x_0, \ldots, x_3) = (0, 1, 1, 1)$, $x_m = L$, and for all $n, n+1, \ldots, n+7 \leq m$,

$$x_n = 0 \Rightarrow x_{n+4} = 0 \text{ and } (x_{n+1}, x_{n+2}, x_{n+3}) \rightarrow_{\mathcal{P}} (x_{n+5}, x_{n+6}, x_{n+7})$$

Integers with addition and powers

Hieronymi, Schulz 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

Reduction from the halting problem: given a program $\mathcal{P}$, construct the formula

$$\varphi := \exists 3^a, 3^b : \text{ the sequence } g(3^a, 3^b) \text{ is a halting run of } \mathcal{P}.$$

Check whether $\mathcal{M} \models \varphi$

Integers with addition and powers: the bigger picture

Hieronymi, Schulz 2022

The theory of $\mathcal{M} := (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is undecidable

K., Luca, Nieuwveld, Ouaknine, Worrell 2025

1. The existential theory of $\mathcal{M}$ is decidable
2. The existential theory of $(\mathbb{Z}; <, +, n \mapsto 2^n, n \mapsto 3^n)$ is hard: decidability would yield algorithms for checking whether a given word occurs in $\mathrm{bin}(\log_2(3))$

Problem

Is the theory of $(\mathbb{Z}; <, n \mapsto 2^n, n \mapsto 3^n)$ is decidable?

The tau function

The function $\tau \colon \mathbb{N} \to \mathbb{Z}$ returns the nth Fourier coefficient of the cusp modular form

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

where $q = e^{i2\pi z}$. We have $\tau(0) = 0$, and $\tau(n) \neq 0$ for $n \geq 1$ by Lehmer's conjecture. The first few values of $\tau(n)$ are

$$0, 1, -24, 252, -1472, 4830, -6048, -16744, \ldots$$

K., Nieuwveld, Ouaknine 2025+

The theory of $(\mathbb{N}; <, n \mapsto |\tau(n)|)$ is undecidable assuming Lehmer's conjecture

The tau function

Bilu, Deshouillers, Gun, Luca 2018

Assume $\tau(n) \neq 0$ for all $n \geq 1$. Then for any permutation $\sigma \colon \{1, \ldots, m\} \to \{1, \ldots, m\}$ there exist infinitely many n such that

$$|\tau(n + \sigma(1))| < \cdots < |\tau(n + \sigma(m))|$$

To prove undecidability of the theory of $(\mathbb{N}; <, n \mapsto |\tau(n)|)$, we need $g \colon \mathbb{Z}^k \to \mathbb{N}^*$ that

1. can be implemented in $(\mathbb{N}; <, n \mapsto |\tau(n)|)$
2. is onto

We have $k = 3$ and

$$g(a, b, c) = (\ \#\{a \leq m < b \colon |\tau(m)| < |\tau(n)|\}\ )_{n=b}^{c}$$

More undecidability via randomness

Let $u_n = a\lambda^n + \overline{a}\,\overline{\lambda^n} + v_n$ be a non-degenerate integer linear recurrence sequence with exactly two dominant roots $\lambda, \overline{\lambda}$

Ex.: $u_n = (2+i)^n + (2-i)^n - 2^n$, satisfies $u_{n+3} = 6u_{n+2} - 13u_{n+1} + 10u_n$

Let $(p_n)_{n=-\infty}^{\infty}$ be an ordering of $\{u_n \colon n \geq 0\}$

More undecidability via randomness

Let $u_n = a\lambda^n + \overline{a}\,\overline{\lambda^n} + v_n$ be a non-degenerate integer linear recurrence sequence with exactly two dominant roots $\lambda, \overline{\lambda}$

Ex.: $u_n = (2+i)^n + (2-i)^n - 2^n$, satisfies $u_{n+3} = 6u_{n+2} - 13u_{n+1} + 10u_n$

Let $(p_n)_{n=-\infty}^{\infty}$ be an ordering of $\{u_n : n \geq 0\}$

K., Nieuwveld, Ouaknine 2025+

1. There exists $\varepsilon > 0$ with the following property. For any $0 = \varepsilon_1 < \cdots < \varepsilon_{m+1} < \varepsilon$, there exist bi-infinitely many n such that for all $1 \leq i \leq m$

$$1 + \varepsilon_i < \frac{p_{n+i}}{p_n} < 1 + \varepsilon_{i+1}$$

More undecidability via randomness

Let $u_n = a\lambda^n + \overline{a}\,\overline{\lambda^n} + v_n$ be a non-degenerate integer linear recurrence sequence with exactly two dominant roots $\lambda, \overline{\lambda}$

Ex.: $u_n = (2+i)^n + (2-i)^n - 2^n$, satisfies $u_{n+3} = 6u_{n+2} - 13u_{n+1} + 10u_n$

Let $(p_n)_{n=-\infty}^{\infty}$ be an ordering of $\{u_n \colon n \geq 0\}$

K., Nieuwveld, Ouaknine 2025+

1. There exists $\varepsilon > 0$ with the following property. For any $0 = \varepsilon_1 < \cdots < \varepsilon_{m+1} < \varepsilon$, there exist bi-infinitely many n such that for all $1 \leq i \leq m$

$$1 + \varepsilon_i < \frac{p_{n+i}}{p_n} < 1 + \varepsilon_{i+1}$$

2. The theories of $(\mathbb{Z}; <, +, \{u_n \colon n \geq 0\})$ and $(\mathbb{Z}; <, n \mapsto u_n)$ are undecidable

Decidability via randomness

Let $u_n = a\lambda^n + \overline{a}\,\overline{\lambda^n} + v_n$ be a non-degenerate integer linear recurrence sequence with exactly two dominant roots $\lambda, \overline{\lambda}$

Let $(p_n)_{n=-\infty}^{\infty}$ be an ordering of $\{u_n \colon n \geq 0\}$

Nieuwveld, Ouaknine 2025

1. The sequence $(p_n)_n$ is pro-disjunctive: For every $m \geq 1$, every

$$w \in \{0 \leq c < m \colon p_n \equiv c \pmod{m} \text{ for infinitely many } n\}^*$$

appears bi-infinitely often in $(p_n \bmod m)_n$

Decidability via randomness

Let $u_n = a\lambda^n + \overline{a}\,\overline{\lambda^n} + v_n$ be a non-degenerate integer linear recurrence sequence with exactly two dominant roots $\lambda, \overline{\lambda}$

Let $(p_n)_{n=-\infty}^{\infty}$ be an ordering of $\{u_n \colon n \geq 0\}$

Nieuwveld, Ouaknine 2025

1. The sequence $(p_n)_n$ is pro-disjunctive: For every $m \geq 1$, every

$$w \in \{0 \leq c < m \colon p_n \equiv c \pmod m \text{ for infinitely many } n\}^*$$

   appears bi-infinitely often in $(p_n \bmod m)_n$
2. The *monadic second-order* theory of $(\mathbb{Z}; <, \{u_n \colon n \geq 0\})$ is decidable

MSO generalises first-order logic by allowing quantifications over $X \subseteq \mathbb{Z}$

Undecidability via randomness: open problems

Problem

Classify all LRS $(u_n)_n$ for which the theory of $(\mathbb{Z}; <, +, \{u_n : n \geq 0\})$ is decidable

Problem

Is the theory of $(\mathbb{Z}; <, +, \text{PRIMES})$ decidable?

Problem

Does Sarnak's conjecture imply undecidability of the theory of $(\mathbb{Z}; <, +, n \mapsto \mu(n))$?
Here $\mu\colon \mathbb{Z} \to \{-1, 0, 1\}$ is the *Möbius function*

Decidability via rigidity

Berthé, K., Nieuwveld, Ouaknine, Vahanwala, Worrell 2024

The monadic second-order theory of $\mathcal{M} := (\mathbb{Z}; <, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is decidable

Define

$$\alpha = \varnothing\ \{2,3\}\ \{2\}\ \{3\}\ \{2\}\ \varnothing\ \varnothing\ \varnothing\ \{2\}\ \{3\}\ \varnothing\ \cdots$$
$$\beta = 2\ 3\ 2\ 2\ 3\ 2\ 3\ 2 \cdots$$

Then

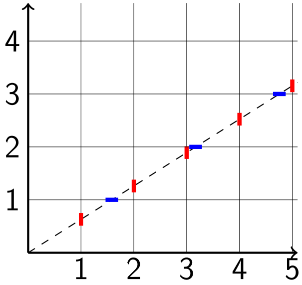
$$\begin{aligned} \text{Deciding } \mathcal{M} \models \varphi &\Leftrightarrow \text{Deciding } \mathcal{A} \models \alpha \text{ for a given automaton } \mathcal{A} \\ &\Leftrightarrow \text{Deciding } \mathcal{B} \models \beta \text{ for a given automaton } \mathcal{B} \end{aligned}$$

Decidability via rigidity

Need to decide whether a given automaton $\mathcal{B}$ accepts $\beta = 2\ 3\ 2\ 2\ 3\ 2\ 3\ 2 \cdots$

β is the *cutting sequence* generated by $y = \log_3(2)x$

β is Sturmian: it has exactly $n+1$ distinct subwords of length n, which is the lowest possible among non-periodic words

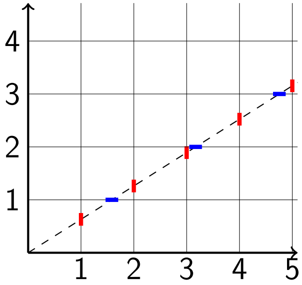


Decidability via rigidity

Need to decide whether a given automaton $\mathcal{B}$ accepts $\beta = 2\ 3\ 2\ 2\ 3\ 2\ 3\ 2 \cdots$

β is the *cutting sequence* generated by $y = \log_3(2)x$

β is Sturmian: it has exactly $n+1$ distinct subwords of length n, which is the lowest possible among non-periodic words



Berthé, K., Vahanwala 2025

Given an automaton $\mathcal{B}$, we can compute N such that for any cutting sequence β with the slope κ, whether $\mathcal{B} \models \beta$ only depends on the first N terms of the continued fraction expansion of κ

Decidability via rigidity, summary

Berthé, K., Nieuwveld, Ouaknine, Vahanwala, Worrell 2024

The monadic second-order theory of $\mathcal{M} := (\mathbb{Z}; <, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ is decidable

Need to decide whether a given automaton $\mathcal{B}$ accepts $\beta = 2\ 3\ 2\ 2\ 3\ 2\ 3\ 2 \cdots$

β is the cutting sequence generated by $y = \log_3(2)x$

Berthé, K., Vahanwala 2025

Given an automaton $\mathcal{B}$, we can compute N such that for any cutting sequence β with the slope κ, whether $\mathcal{B} \models \beta$ only depends on the first N terms of the continued fraction expansion of κ

The Ergodic Dream

Let $\mathcal{M}$ be a mathematical structure, e.g. $\mathcal{M} = (\mathbb{Z}; <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$

Does there exist an algorithm that takes a sentence φ and decides whether $\mathcal{M} \models \varphi$?

Step 1. Link the algebraic object to dynamical systems, e.g. $(\mathbb{R}/\mathbb{Z}, x \mapsto x + \log_2(3))$

Step 2. Study whether the relevant system(s) are rigid or fully random

Step 3. Deduce decidability or undecidability

Problem

Classify all LRS $(u_n)_n$ for which the theory of $(\mathbb{Z}; <, +, \{u_n : n \geq 0\})$ is decidable

Problem

Is the theory of $(\mathbb{Z}; <, +, \text{PRIMES})$ decidable?