Algorithmic Verification of Linear Dynamical Systems

Toghrul Karimov

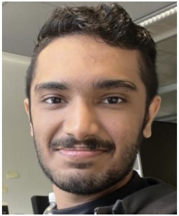
Saarland University & Max Planck Institute for Software Systems

My co-authors

Valérie Berthé

Florian Luca

Mihir Vahanwala



Joël Ouaknine

James Worrell

Joris Nieuwveld

Motivating example

initialise x_1, x_2

while $\neg\mathrm{P}(x_1, x_2)$**:**

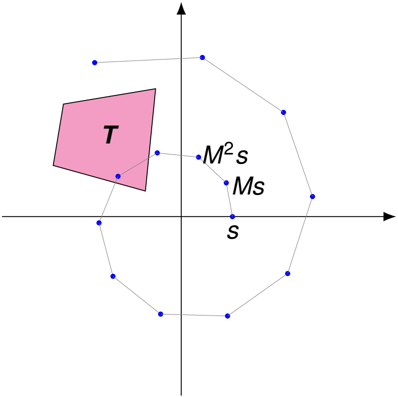
$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Motivating example

initialise x_1, x_2

while $\neg \mathrm{P}(x_1, x_2)$**:**

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$



$T = \{(x_1, x_2) \colon P(x_1, x_2)\}$, s is the initial value of (x_1, x_2)

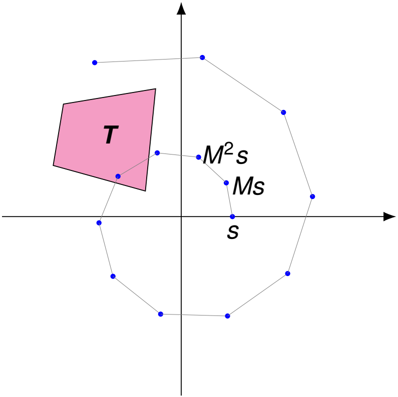
$(x_1, x_2) = M^n s$ after n iterations

Motivating example

initialise x_1, x_2

while $\neg \mathrm{P}(x_1, x_2)$**:**

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$



$$\boxed{\text{Loop terminates} \Leftrightarrow \langle s, Ms, M^2 s, \ldots \rangle \text{ reaches } \boldsymbol{T}}$$

Linear dynamical systems

A *linear dynamical system* is given by (M, s) where

- $M \in \mathbb{Q}^{d \times d}$ is the *update matrix*
- $s \in \mathbb{Q}^{d}$ is the *initial configuration*

Linear dynamical systems

A *linear dynamical system* is given by (M, s) where

- $M \in \mathbb{Q}^{d \times d}$ is the *update matrix*
- $s \in \mathbb{Q}^{d}$ is the *initial configuration*

The *trajectory* of (M, s) is the sequence $\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Linear dynamical systems

A *linear dynamical system* is given by (M, s) where

- $M \in \mathbb{Q}^{d \times d}$ is the *update matrix*
- $s \in \mathbb{Q}^{d}$ is the *initial configuration*

The *trajectory* of (M, s) is the sequence $\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Verification of LDS

Find algorithms that

1. take (M, s) and a property φ, and
2. decide whether $\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$ satisfies φ

Linear loops, cont'd

Termination problem for linear loops $\equiv$

Reachability Problem

Given $M \in \mathbb{Q}^{d \times d}$, $s \in \mathbb{Q}^d$ and a semialgebraic target T, decide whether $\langle s, Ms, M^2 s, \ldots, \rangle$ reaches T

Linear loops, cont'd

Termination problem for linear loops $\equiv$

Reachability Problem

Given $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$ and a semialgebraic target T, decide whether $\langle s, Ms, M^2s, \ldots, \rangle$ reaches T

Many sound but incomplete approaches exist: invariants, ranking functions etc.

Linear loops, cont'd

Termination problem for linear loops $\equiv$

Reachability Problem

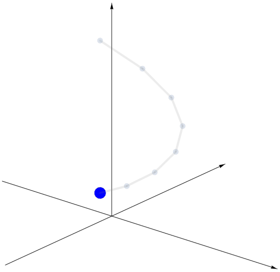
Given $M \in \mathbb{Q}^{d \times d}$, $s \in \mathbb{Q}^d$ and a semialgebraic target T, decide whether $\langle s, Ms, M^2 s, \ldots, \rangle$ reaches T

Many sound but incomplete approaches exist: invariants, ranking functions etc.

Branching in the loop update $\Rightarrow$ termination undecidable

Skolem Problem

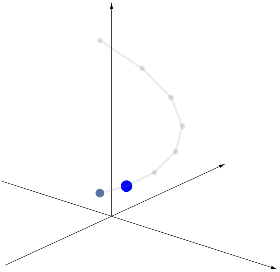
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

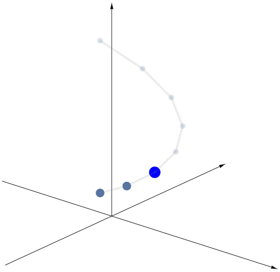
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

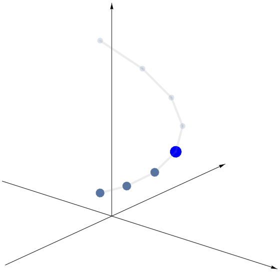
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



$$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$$

Skolem Problem

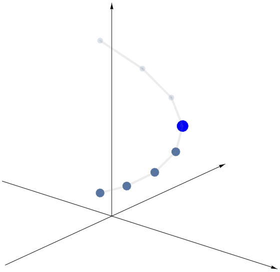
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



$$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$$

Skolem Problem

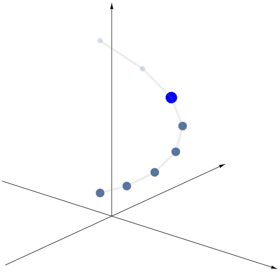
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

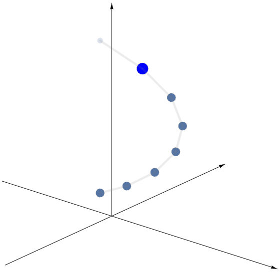
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

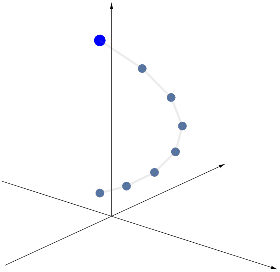
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

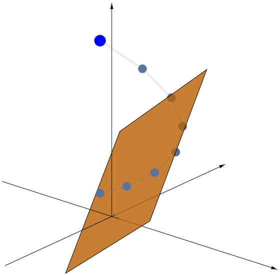
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$$

Skolem Problem

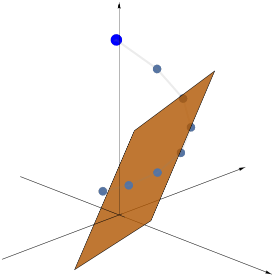
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

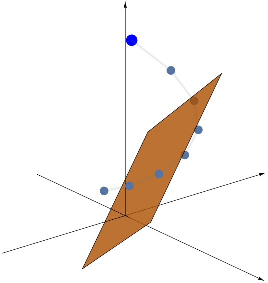
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

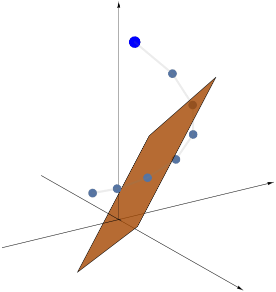
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



$$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$$

Skolem Problem

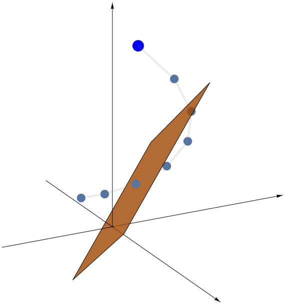
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$$

Skolem Problem

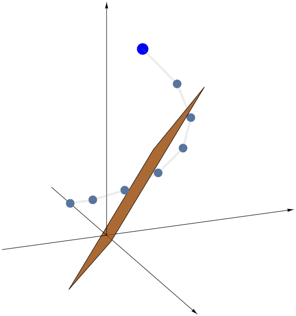
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

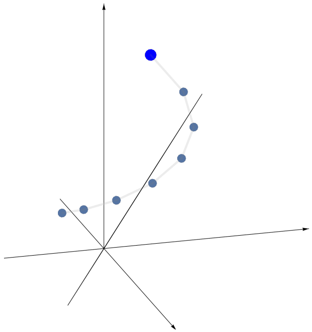
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n

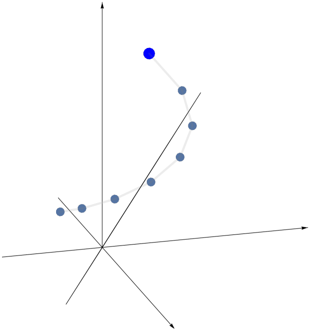


$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem

Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n

Decidable in dimension $d \leq 4$, famously open in dimension $d = 5$



$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

Skolem Problem, cont'd

We want to decide whether $\exists n \colon c^\top M^n s = 0$

The sequence $u_n := c^\top M^n s$ is a *linear recurrence sequence*

Skolem Problem, cont'd

We want to decide whether $\exists n\colon c^\top M^n s = 0$

The sequence $u_n := c^\top M^n s$ is a *linear recurrence sequence*

Examples: $u_n = 3u_{n-1} + u_{n-2} - 2u_{n-3}$ and

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

Skolem Problem, cont'd

We want to decide whether $\exists n\colon c^\top M^n s = 0$

The sequence $u_n := c^\top M^n s$ is a *linear recurrence sequence*

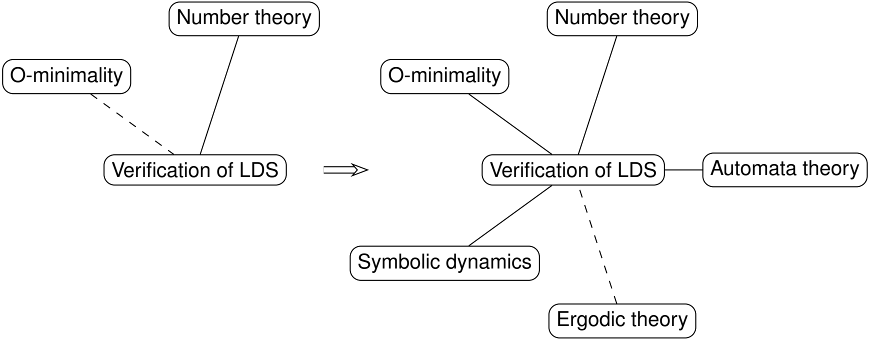
Examples: $u_n = 3u_{n-1} + u_{n-2} - 2u_{n-3}$ and

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

Skolem Problem, LRS version

Given an LRS $(u_n)_n$, decide whether $u_n = 0$ for some n

Contributions of the thesis



Contribution 1: reachability and model checking

Reachability Problem

Given $M \in \mathbb{Q}^{d \times d}$, $s \in \mathbb{Q}^d$ and semialgebraic T, decide whether $\langle s, Ms, M^2 s, \ldots, \rangle$ reaches T

Model-Checking Problem

Given M, s, a semialgebraic partition $\mathcal{T} = \{T_1, \ldots, T_m\}$, and an ω-regular property φ over $\mathcal{T}$, decide whether $\langle s, Ms, M^2 s, \ldots \rangle$ satisfies φ

E.g. does the orbit visit T_1 infinitely often? Eventually get trapped in T_2? Stay in T_1 until it visits T_2?

Contribution 1: reachability and model checking

Call a set T *tame* if it can be obtained through finitely many set operations from semialgebraic sets that either (i) have intrinsic dimension 1, or (ii) are contained in a 3-dimensional subspace

Contribution 1: reachability and model checking

Call a set T *tame* if it can be obtained through finitely many set operations from semialgebraic sets that either (i) have intrinsic dimension 1, or (ii) are contained in a 3-dimensional subspace

Theorem

The Model-Checking Problem is decidable for tame targets. For the classes of (i) sets of intrinsic dimension 1 and (ii) sets of linear dimension 4, deciding reachability is *Diophantine-hard*

That is, deciding model checking $\approx$ deciding reachability

Contribution 1: reachability and model checking

Call a set T *tame* if it can be obtained through finitely many set operations from semialgebraic sets that either (i) have intrinsic dimension 1, or (ii) are contained in a 3-dimensional subspace

Theorem

The Model-Checking Problem is decidable for tame targets. For the classes of (i) sets of intrinsic dimension 1 and (ii) sets of linear dimension 4, deciding reachability is *Diophantine-hard*

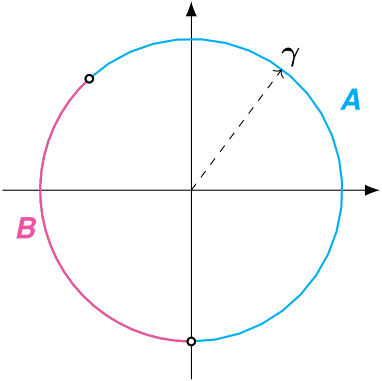
That is, deciding model checking $\approx$ deciding reachability

Theorem

The Model-Checking Problem is decidable up to a measure zero set of inputs

Contribution 2: toric words

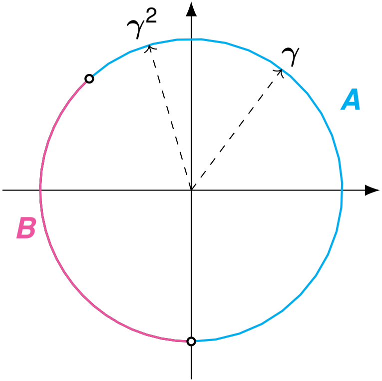
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A

Contribution 2: toric words

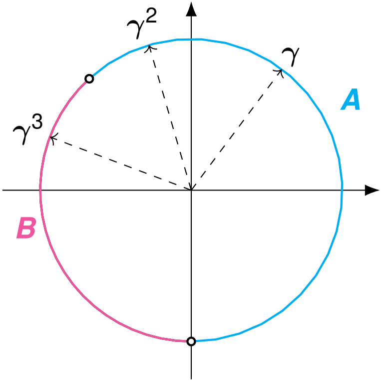
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A

Contribution 2: toric words

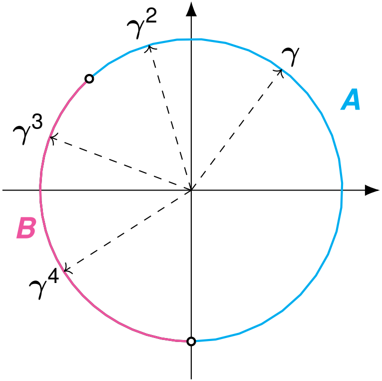
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A B

Contribution 2: toric words

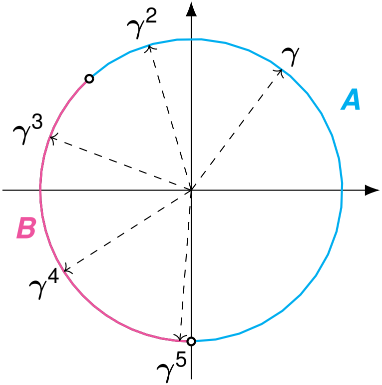
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A B B

Contribution 2: toric words

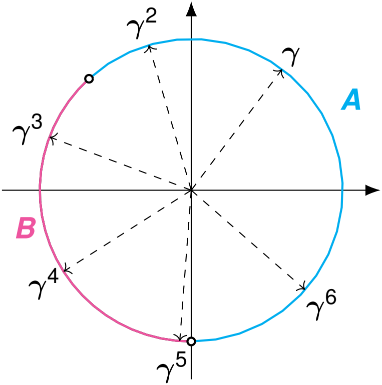
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A B B B

Contribution 2: toric words

A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A B B B A $\cdots$

Toric words

We develop the automata theory of toric words

The decidability/hardness boundary of the Model-Checking Problem matches the boundary of $(M, s, T_1, \ldots, T_m)$ for which the *characteristic word* α, $\alpha(n) = T_i \Leftrightarrow M^n s \in T_i$, is toric

Toric words

We develop the automata theory of toric words

The decidability/hardness boundary of the Model-Checking Problem matches the boundary of $(M, s, T_1, \ldots, T_m)$ for which the *characteristic word* α, $\alpha(n) = T_i \Leftrightarrow M^n s \in T_i$, is toric

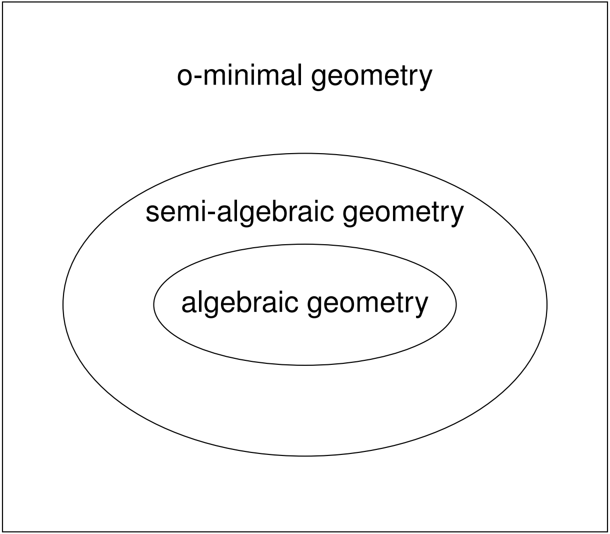
Theorem, LICS 2024

The MSO theory of $\langle \mathbb{N}; <, \{a^n \colon n \geq 0\}\rangle_{a \geq 2}$ is decidable

Theorem, SODA 2025

The elementary theory of $\langle \mathbb{N}; +, \{a^n \colon n \geq 0\}, \{b^n \colon n \geq 0\}\rangle$ is decidable

Contribution 3: o-minimality



Contribution 3: o-minimality

Everything about LDS that is not explained by number theory + toric words, is explained by o-minimality

Contribution 3: o-minimality

Everything about LDS that is not explained by number theory + toric words, is explained by o-minimality

O-minimality of $\langle \mathbb{R}; <, +, \cdot, \exp(\cdot) \rangle \quad \Rightarrow \quad$ every first-order definable subset of $\mathbb{R}^k$ has finitely many connected components

Contribution 3: o-minimality

Everything about LDS that is not explained by number theory + toric words, is explained by o-minimality

O-minimality of $\langle \mathbb{R}; <, +, \cdot, \exp(\cdot) \rangle \quad \Rightarrow \quad$ every first-order definable subset of $\mathbb{R}^k$ has finitely many connected components

Robust safety for LDS is decidable

Given (M, s) and T, it is decidable whether there exists $\varepsilon > 0$ such that $(M^n \cdot B(s, \varepsilon))_n$ avoids T

Contribution 3: o-minimality

Everything about LDS that is not explained by number theory + toric words, is explained by o-minimality

O-minimality of $\langle \mathbb{R}; <, +, \cdot, \exp(\cdot) \rangle \quad \Rightarrow \quad$ every first-order definable subset of $\mathbb{R}^k$ has finitely many connected components

Robust safety for LDS is decidable

Given (M, s) and T, it is decidable whether there exists $\varepsilon > 0$ such that $(M^n \cdot B(s, \varepsilon))_n$ avoids T

An ergodic theorem for LDS

Given M, s and o-minimal $f\colon \mathbb{R}^d \to \mathbb{R}$, we can express

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} f(M^i s) = \int_X g \, d\mu$$

where X is compact and g is o-minimal

What is happening now?

European Research Council
Established by the European Commission

Dynamical and Arithmetical Model Checking

Fact Sheet | Results

Project description

DE EN ES FR IT PL

An interdisciplinary approach to the study of discrete dynamical systems

Discrete dynamical systems are mathematical models used in many fields including computer science and biology, to study how systems change over time. While they seem simple to describe, they give rise to compelling open problems. One such example is the Skolem Problem, which asks if a dynamical system ever hits a given hyperplane. The EU-funded DynAMiCs project will combine tools from different areas of mathematics and computer science such as number theory and logic to study discrete dynamical systems. The project will combine expertise in number theory, symbolic dynamics and mathematical logic.