Algorithmic Verification of Linear Dynamical Systems

Toghrul Karimov

Saarland University & Max Planck Institute for Software Systems

What is a decision problem?

Decision problem: a yes/no question

A decision problem is decidable: there exists an algorithm that halts on all inputs and outputs the correct answer

What is a decision problem?

Decision problem: a yes/no question

A decision problem is decidable: there exists an algorithm that halts on all inputs and outputs the correct answer

Problem 1

Given $p \in \mathbb{Z}[X_1, \ldots, X_d]$, does there exist $x_1, \ldots, x_d \in \mathbb{R}$ such that $p(x_1, \ldots, x_d) = 0$?

What is a decision problem?

Decision problem: a yes/no question

A decision problem is decidable: there exists an algorithm that halts on all inputs and outputs the correct answer

Problem 1

Given $p \in \mathbb{Z}[X_1, \dots, X_d]$, does there exist $x_1, \dots, x_d \in \mathbb{R}$ such that $p(x_1, \dots, x_d) = 0$?

Problem 2

Given $p \in \mathbb{Z}[X_1, \dots, X_d]$, does there exist $x_1, \dots, x_d \in \mathbb{Z}$ such that $p(x_1, \dots, x_d) = 0$?

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

Example of LDS: linear loops

initialise x_1, x_2

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

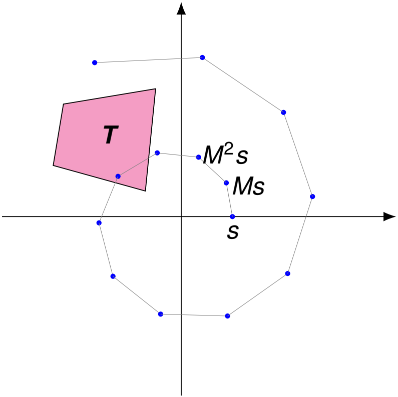
$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Example of LDS: linear loops

initialise x_1, x_2

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

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



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

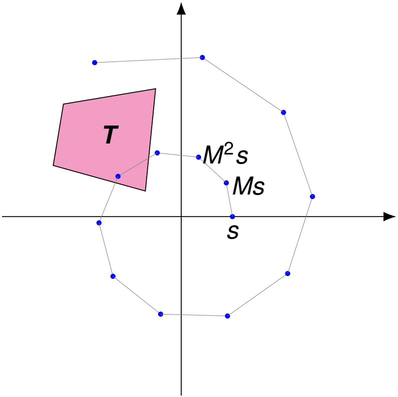
$(x_1, x_2) = M^n s$ after n iterations

Example of LDS: linear loops

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 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

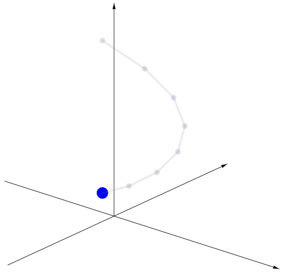
Given $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$ and a semialgebraic target T, decide whether $\langle s, Ms, M^2s, \ldots, \rangle$ reaches T

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

Branching in the loop update $\Rightarrow$ termination undecidable

Skolem Problem

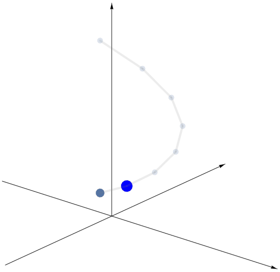
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

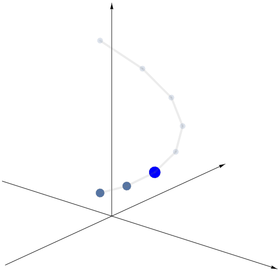
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



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

Skolem Problem

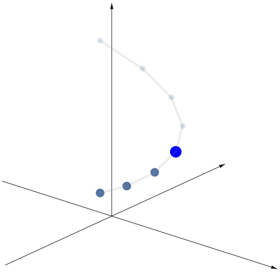
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

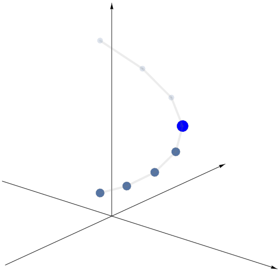
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



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

Skolem Problem

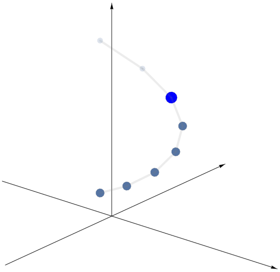
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



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

Skolem Problem

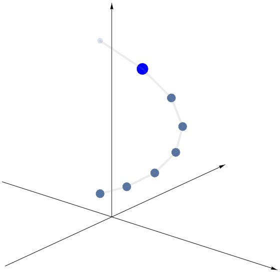
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

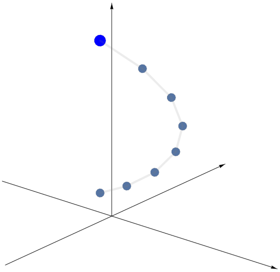
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

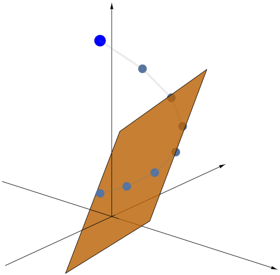
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

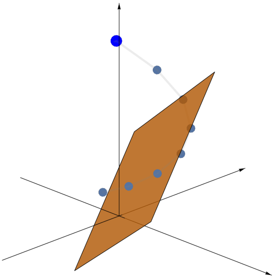
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

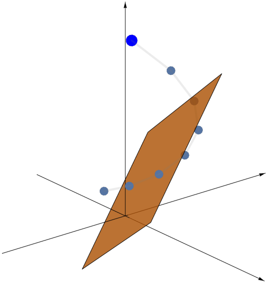
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



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

Skolem Problem

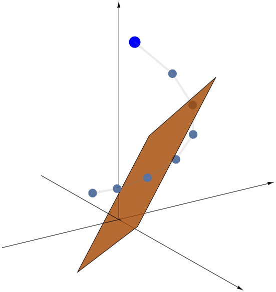
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

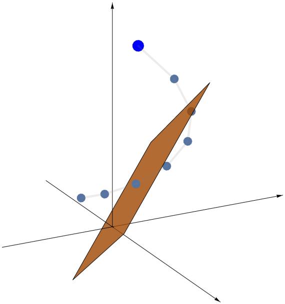
Given (M, s) and a hyperplane H,
decide whether $M^n s \in H$ for some n



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

Skolem Problem

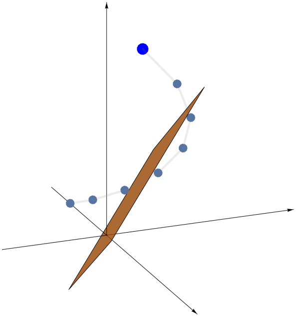
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



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

Skolem Problem

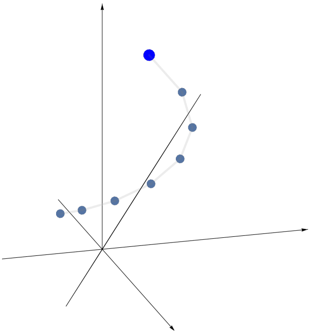
Given (M, s) and a hyperplane H, decide whether $M^n s \in H$ for some n



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

Skolem Problem

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

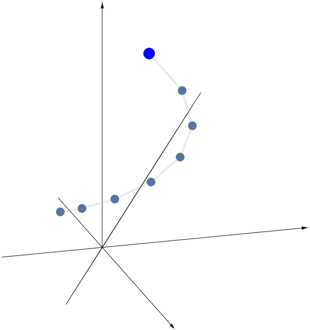


$\langle s, Ms, M^2 s, M^3 s, \ldots \rangle$

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 $(u_n)_{n\in\mathbb{N}}$, decide whether $u_n = 0$ for some n

Our contributions

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

Our contributions

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

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

Our contributions

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

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 Reachability Problem is decidable for tame T

Uses classical number-theoretic tools: Baker's theorem, its p-adic version, heights of algebraic numbers

Generalising reachability

Suppose we have (M, s) and semialgebraic $T_1, \ldots, T_m$

Generalising reachability

Suppose we have (M, s) and semialgebraic $T_1, \ldots, T_m$

We can ask whether the trajectory of (M, s)

- visits T_1 infinitely often

Generalising reachability

Suppose we have (M, s) and semialgebraic $T_1, \ldots, T_m$

We can ask whether the trajectory of (M, s)

- visits T_1 infinitely often
- eventually gets trapped in T_2

Generalising reachability

Suppose we have (M, s) and semialgebraic $T_1, \ldots, T_m$

We can ask whether the trajectory of (M, s)

- visits T_1 infinitely often
- eventually gets trapped in T_2
- stays in T_1 until it visits T_2

Generalising reachability

Suppose we have (M, s) and semialgebraic $T_1, \ldots, T_m$

We can ask whether the trajectory of (M, s)

- visits T_1 infinitely often
- eventually gets trapped in T_2
- stays in T_1 until it visits T_2

Model-Checking Problem

Given $M \in \mathbb{Q}^{d \times d}$, $s \in \mathbb{Q}^d$, semialgebraic $T_1, \ldots, T_m$ and an ω-regular property φ over $T_1, \ldots, T_m$, decide whether the orbit $\langle s, Ms, M^2 s, \ldots \rangle$ satisfies φ

Our contributions, cont'd

Model-Checking Problem

Given $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$, semialgebraic $T_1, \ldots, T_m$ and an ω-regular property φ over $T_1, \ldots, T_m$, decide whether the orbit $\langle s, Ms, M^2 s, \ldots \rangle$ satisfies φ

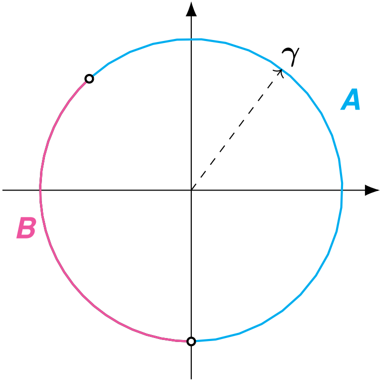
Theorem

The Model-Checking Problem is decidable for tame targets

Main idea: the sequence $(\mathbb{1}(M^n s \in T))_n$ is *toric*

Toric words

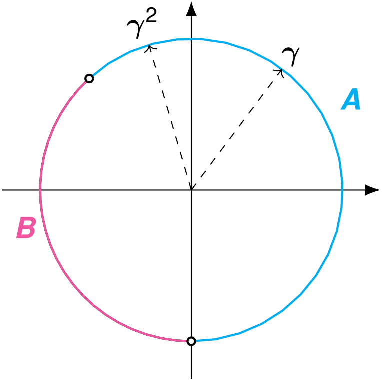
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A

Toric words

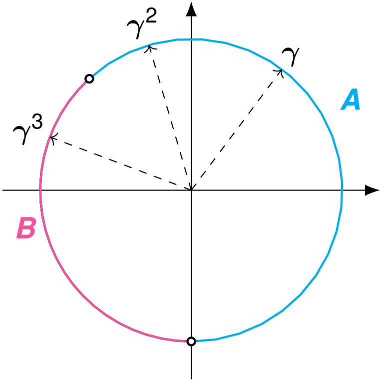
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A

Toric words

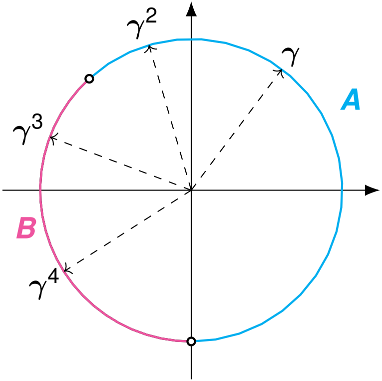
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A B

Toric words

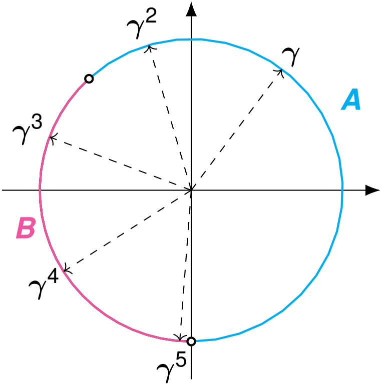
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A B B

Toric words

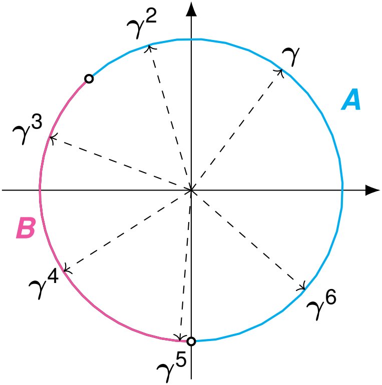
A toric word is the coding of an orbit of a rotation on a k-dimensional torus with respect to open sets



A A B B B

Toric words

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



$A\ A\ B\ B\ B\ A \cdots$

Automaton on toric words

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

Theorem

Given a toric word u and an automaton $\mathcal{A}$, it is decidable whether $\mathcal{A}$ accepts u

Boundaries of decidability

Theorem

For even the simplest non-tame targets, (un)decidability of the Reachability Problem would entail major breakthroughs either in Diophantine approximation, or regarding the Skolem Problem

Boundaries of decidability

Theorem

For even the simplest non-tame targets, (un)decidability of the Reachability Problem would entail major breakthroughs either in Diophantine approximation, or regarding the Skolem Problem

Hartmanis-Stearns Conjecture

Any number whose nth binary digit can be computed in time $O(n)$ must be either rational or transcendental

What is happening now?

Number theory + toric words + automata theory is now a well-known powerful combination

What is happening now?

Number theory + toric words + automata theory is now a well-known powerful combination

New results within the **DynAMiCs** project:

- An algorithm for solving integer linear programming problems with some variables restricted to $2^{\mathbb{N}}$ and some to $3^{\mathbb{N}}$ (SODA25)

What is happening now?

Number theory + toric words + automata theory is now a well-known powerful combination

New results within the **DynAMiCs** project:

- An algorithm for solving integer linear programming problems with some variables restricted to $2^{\mathbb{N}}$ and some to $3^{\mathbb{N}}$ (SODA25)
- An algorithm for deciding the monadic second-order theory of $\langle \mathbb{N}; <, a_1^{\mathbb{N}}, \ldots, a_m^{\mathbb{N}} \rangle$, where $a_i \in \mathbb{N}$ (LICS24)

What is happening now?

Number theory + toric words + automata theory is now a well-known powerful combination

New results within the **DynAMiCs** project:

- An algorithm for solving integer linear programming problems with some variables restricted to $2^{\mathbb{N}}$ and some to $3^{\mathbb{N}}$ (SODA25)
- An algorithm for deciding the monadic second-order theory of $\langle \mathbb{N}; <, a_1^{\mathbb{N}}, \dots, a_m^{\mathbb{N}} \rangle$, where $a_i \in \mathbb{N}$ (LICS24)

> "Wir müssen wissen, wir werden wissen."
>
> — David Hilbert, 1930

Verification of LDS via 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