On Robustness for Linear Recurrence Sequences

Based on joint work with Akshay, Bazille, and Genest

Mihir Vahanwala [1]

[1] Max Planck Institute for Software Systems

April 5, 2023

A very well known example

- $\langle 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots \rangle$
- **The Recurrence Relation:** $Y_2 = Y_1 + Y_0$
- **The Characteristic Polynomial:**
  $X^2 - X - 1 = (X - \phi)(X + 1/\phi)$, where

$$\phi = \frac{1 + \sqrt{5}}{2} = 1.61803398875...$$

Linear Recurrence Sequences

Definition (Linear Recurrence Relation, LRR)

An LRR $\mathbf{a}$ of order k is a $(k+1)$-ary relation, given by a tuple $(a_0, \ldots, a_{k-1})$ with $a_0 \neq 0$. $\mathbf{a}(Y_0, \ldots, Y_k)$ is interpreted as $Y_k = \sum_{i=0}^{k-1} a_i Y_i$

Definition (Characteristic Polynomial)

The characteristic polynomial of a Linear Recurrence $\mathbf{a}$ is $X^k - \sum_{i=0}^{k-1} a_i X^i$.

Definition (Linear Recurrence Sequences, LRS)

An LRS $\mathbf{u}$ of order k is an infinite sequence $\langle u_n \rangle_{n=0}^{\infty}$, given by a linear recurrence $\mathbf{a}$ of order k, and the initial k terms $\mathbf{c} = (u_0, \ldots, u_{k-1})$. For all n, $\mathbf{a}(u_n, \ldots, u_{n+k})$ holds.

Other Sequences satisfying $u_{n+2} = u_{n+1} + u_n$

- $2\mathbf{f} = \langle 0, 2, 2, 4, 6, 10, 16, 26, 42, 68, \ldots \rangle$
- $\mathbf{g} = \langle 7, 4, 11, 15, 26, 41, 67, \ldots \rangle$
- $2\mathbf{f} + \mathbf{g} = \langle 7, 6, 13, 19, 32, 51, 83, \ldots \rangle$
- What does

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

give?

For an LRR, one can easily check that

- The LRS satisfying the relation form a vector space
- If γ is a root of the characteristic polynomial with multiplicity m, then the sequences $\langle \gamma^n \rangle_{n=0}^{\infty}, \langle n\gamma^n \rangle_{n=0}^{\infty}, \ldots, \langle n^{m-1}\gamma^n \rangle_{n=0}^{\infty}$ satisfy the LRR (take the derivatives of the polynomial!)
- Thus, LRS have a general "exponential polynomial" closed form, $u_n = \sum_i f_i(n){\gamma_i}^n$, where f_i are polynomials.
- From this characterisation, it is clear that LRS are closed under pointwise addition and multiplication.

Open Decision problems about LRS

We consider rational LRS, i.e whose recurrence $\mathbf{a}$ and initialisation $\mathbf{c}$ lie in $\mathbb{Q}^k$.

Definition (Skolem Problem)

Given an LRS $\mathbf{u}$, does there exist $n \in \mathbb{N}$ such that $u_n = 0$?

Definition (Positivity Problem)

Given an LRS $\mathbf{u}$, is $u_n \geq 0$ for all $n \in \mathbb{N}$?

Definition (Ultimate Positivity Problem)

Given an LRS $\mathbf{u}$, does there exist an $n_0 \in \mathbb{N}$ such that $u_n \geq 0$ for all $n \geq n_0, n \in \mathbb{N}$?

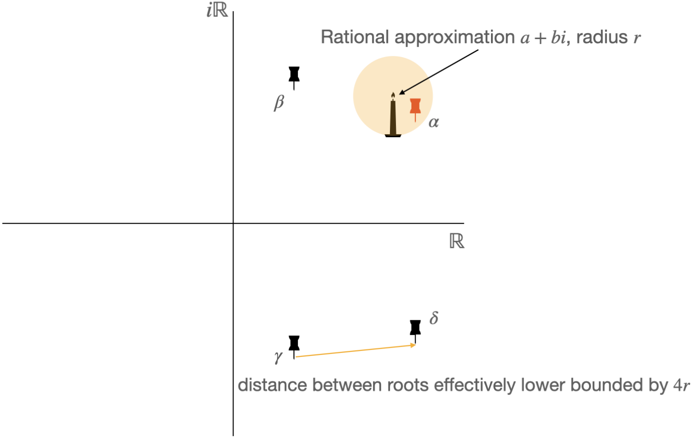
Remark

The Skolem Problem is known to reduce to the Positivity Problem.

Working with Algebraic Numbers

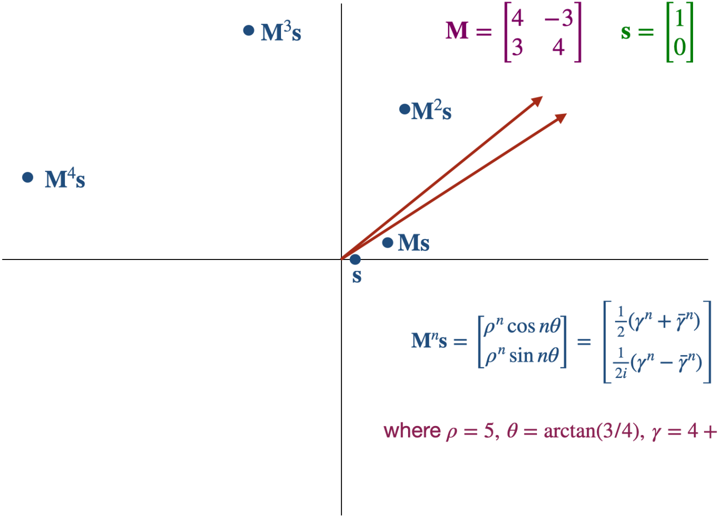
Since our problems are given over $\mathbb{Q}$, our computations involving the exponential polynomial closed form take us to $\bar{\mathbb{Q}}$, the "algebraic closure".

Roots of the minimum polynomial p of $\alpha \in \bar{\mathbb{Q}}$



LRS in Trajectories

$$\mathbf{M} = \begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix} \qquad \mathbf{s} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$



$$\mathbf{M}^n\mathbf{s} = \begin{bmatrix} \rho^n \cos n\theta \\ \rho^n \sin n\theta \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(\gamma^n + \bar{\gamma}^n) \\ \frac{1}{2i}(\gamma^n - \bar{\gamma}^n) \end{bmatrix}$$

where $\rho = 5,\ \theta = \arctan(3/4),\ \gamma = 4 + 3i$

LRS in Trajectories: Formally

Lemma

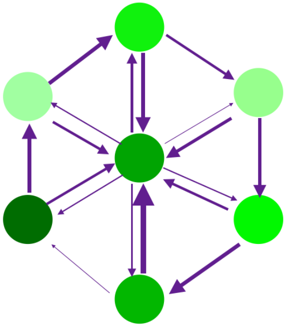
Let $\mathbf{M} \in \mathbb{Q}^{k \times k}$, $\mathbf{s} \in \mathbb{Q}^{k}$. *Then,* $\langle \mathbf{M}^n \mathbf{s}_1 \rangle_{n=0}^{\infty}$ *is a rational LRS.*

Proof.

Compute the characteristic polynomial of $\mathbf{M}$, and apply the Cayley-Hamilton Theorem. $\square$

Typical problem: Finite Markov Chains

Markov Chain, 7 states.
Transition Probabilities **M** marked by prominence of arrows,
Initial distribution **s** marked by darkness of colour



At every step, is the probability of being in the central state greater than the given threshold r? Formally, is

$$\forall n \,.\, (\mathbf{M}^n \mathbf{s})_1 \geq r$$

Embedding LRS into powers of useful matrices

Lemma

For any rational LRS $\mathbf{u}$ *of order* k*, one can efficiently compute an ergodic Markov Chain* $\mathbf{M} \in \mathbb{Q}^{(k+1)\times(k+1)}$*, along with rational* $\mathbf{S}, \mathbf{D}, \rho, \eta$ *such that*

- $\mathbf{M} = \mathbf{S} + \mathbf{D}$
- $\mathbf{MS} = \mathbf{S}$
- $\lim_{n\to\infty} \mathbf{D}^n = \mathbf{O}$
- $\mathbf{D}^n_{1,1} = \eta u_n / \rho^n$

Motivating Robustness

- Consider the Markov Chain reachability problem. The mathematical hardness shows up only when the threshold is equal to the limiting value!
- Real-world measurements are **inherently imprecise**, and practical guarantees need **safety margins**
- **Is the delicate corner case practically significant?**

Our notion of robustness

Given an LRR **a** and an initial point **c**, rather than considering only **c** as our initialisation, we ask,

Definition (Robustness)

Does initialising with an **arbitrary point in a neighbourhood** of **c** guaranteed to give an LRS that is

- Positive?
- Ultimately Positive?
- always non-zero?[1]

[1] For robustness, we complement the Skolem problem

Painting with broad strokes: the growth argument

- Recall the exponential polynomial closed form,

$$u_n = \sum_i \sum_{j=0}^{m_i-1} f_{ij}(\mathbf{c}) n^j {\gamma_i}^n$$

and that f_{ij} are linear.

- We can normalise this, and note we have a real sequence:

$$u_n / n^d \rho^n = \left(\sum_{j=1}^{\ell} 2 \cdot \mathrm{Re}(f_j(\mathbf{c}) \cdot (\cos n\theta_j + i \sin n\theta_j)) \right) + r(n)$$

where $r(n) \in o(1)$, eventually becoming negligible.

The Plan

1. **Abstraction.** Define a continuous multilinear function dominant : $\mathbb{R}^k \times \mathbb{R}^{2\ell} \to \mathbb{R}$ as follows:

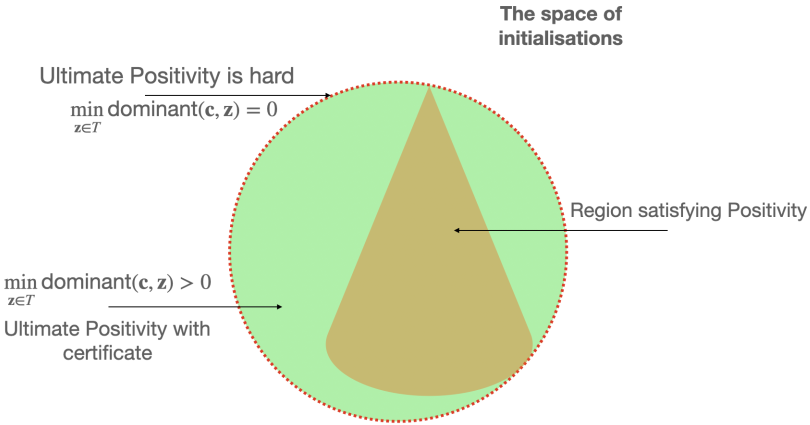
$$\begin{aligned}\mathrm{dominant}(\mathbf{c}, \mathbf{z}) &= \mathrm{dominant}(\mathbf{c}, x_1, y_1, \ldots x_\ell, y_\ell) \\ &= \sum_{j=1}^{\ell} 2 \cdot \mathrm{Re}(f_j(\mathbf{c}) \cdot (x_j + i y_j))\end{aligned}$$

2. **Number Theory.** Find T, the minimal closed over-approximation of the set

$$S = \{(\cos n\theta_1, \sin n\theta_1, \ldots, \cos n\theta_\ell, \sin n\theta_\ell) : n \in \mathbb{N}\}$$

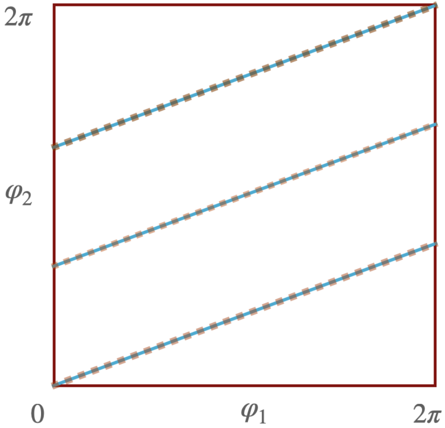
3. **Logic.** Query $\nu(\mathbf{c}) = \min_{\mathbf{z} \in T} \mathrm{dominant}(\mathbf{c}, \mathbf{z})$. For any $\mathbf{c}$,
   - $\nu(\mathbf{c}) > 0$ is sufficient for $\mathbf{c}$ to be Ultimately Positive
   - $\nu(\mathbf{c}) < 0$ is sufficient for $\mathbf{c}$ to not be Ultimately Positive

The Plan, Visualised



The Number Theory

$$\lambda_1 \lambda_2^{-3} = 1, \quad \lambda_j = e^{i\theta_j}$$



The Argument Space

S_{arg}

$\{(n\theta_1, n\theta_2)_{\mod 2\pi} : n \in \mathbb{N}\}$

T_{arg}

$\{(\varphi_1, \varphi_2) : \varphi_1 - 3\varphi_2 = 0 \mod 2\pi\}$

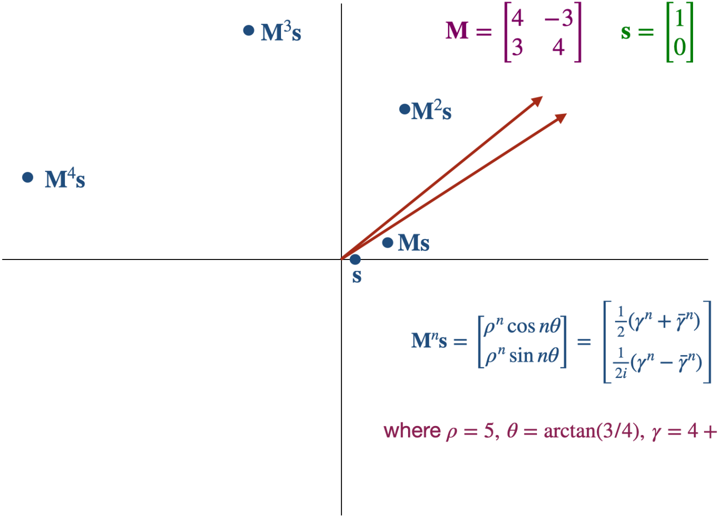
Theorem (Masser)
Integer multiplicative relationships between algebraic numbers of unit modulus correspond to additive relationships in the argument space. They can be computed in PSPACE.

Theorem (Kronecker)

S_{arg} is dense in T_{arg}

Recall: Is the region between the red rays avoided?

$$\mathbf{M} = \begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix} \qquad \mathbf{s} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$



$$\mathbf{M}^n\mathbf{s} = \begin{bmatrix} \rho^n \cos n\theta \\ \rho^n \sin n\theta \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(\gamma^n + \bar{\gamma}^n) \\ \frac{1}{2i}(\gamma^n - \bar{\gamma}^n) \end{bmatrix}$$

where $\rho = 5$, $\theta = \arctan(3/4)$, $\gamma = 4 + 3i$

The Logic: First Order Theory of the Reals

- **Grammar for terms.** $t := 0 \mid 1 \mid x \mid t + t \mid t \cdot t$
- **Grammar for formulae.** $\varphi := t \geq t \mid \neg\varphi \mid \varphi \vee \varphi \mid \exists x.\varphi$
- For simplicity, we assume access to the easily derivable all Boolean connectives, $=, >$ predicates, and universal quantifier.
- Intuitively, the propositional atoms are (in-)equalities involving multivariate polynomials with integer coefficients.

Quantifier Elimination

Variables can either be bound by a quantifier, or free. A formula without any free variables is called a sentence.

- Consider $\chi(a, b, c) := a \neq 0 \wedge \exists x.\ ax^2 + bx + c = 0$
- What does it mean?
- What about $\psi(a, b, c) := a \neq 0 \wedge b^2 - 4ac \geq 0$?

Decidability of the Theory

Theorem (Tarski)

The First Order Theory of the Reals admits quantifier elimination, i.e. for any formula $\chi(\mathbf{x})$, there is another formula $\psi(\mathbf{x})$ such that:

- *ψ does not contain any quantifiers*
- *For all assignments $\mathbf{x_0}$, $\chi(\mathbf{x_0})$ holds if and only if $\psi(\mathbf{x_0})$ holds.*

Theorem

Evaluating the truth of a sentence is decidable. Moreover, the truth of sentences in the existential and universal fragments is decidable in PSPACE.

Applying decidability

There exists a neighbourhood of $\mathbf{c}$ that is Ultimately Positive, if and only if $\nu(\mathbf{c}) = \min_{\mathbf{z} \in T} \mathrm{dominant}(\mathbf{c}, \mathbf{z}) > 0$

- Given $\mathbf{a}$, the description of T is fixed, and can be hardcoded as multivariate polynomial equalities

- Thus, given $\mathbf{c}$, one can encode $\forall \mathbf{z}.\ \mathbf{z} \in T \Rightarrow \mathrm{dominant}(\mathbf{c}, \mathbf{z}) > 0$ as a universal first order sentence in the theory of the reals.

- The minimum $\nu(\mathbf{c})$ itself is an algebraic number: it is the unique satisfying assignment to ν in the formula

$$(\forall \mathbf{z}.\ \mathbf{z} \in T \Rightarrow \mathrm{dominant}(\mathbf{c}, \mathbf{z}) \geq \nu) \wedge (\exists \mathbf{z} \in T.\ \mathrm{dominant}(\mathbf{c}, \mathbf{z}) = \nu)$$

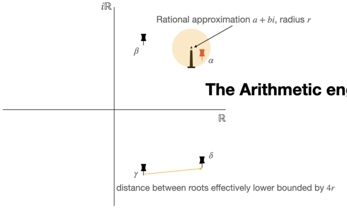
Robust Positivity Wrap-up: Accounting for the prefix

- In the case $\nu(\mathbf{c}) = \min_{\mathbf{z} \in T} \text{dominant}(\mathbf{c}, \mathbf{z}) > 0$, it is an effectively lower bounded algebraic number, and we can compute n_{thr} beyond which Positivity is robustly guaranteed.

- All we need to do is to explicitly check that terms of the sequence up to n_{thr} are greater than 0.

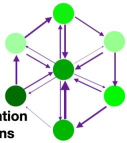
Summary: How (and why) to tame your LRS

Roots of the minimum polynomial p of $\alpha \in \bar{\mathbb{Q}}$



The Arithmetic engine

Markov Chain, 7 states.
Transition Probabilities **M** marked by prominence of arrows,
Initial distribution **s** marked by darkness of colour



The Logic

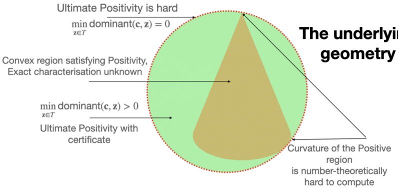
$$\langle \mathbb{R}; +, \cdot, \geq, 0, 1 \rangle$$

The practical motivation for Robust solutions

At every step, is the probability of being in the central state greater than the given threshold r? Formally, is

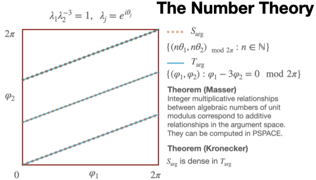
$$\forall n\,.\; (\mathbf{M}^n \mathbf{s})_1 \geq r$$

The space of initialisations



The underlying geometry

The Number Theory



The Argument Space