The Skolem problem: variants, applications and results — A survey talk

S Akshay

FM methods update meeting
IIT Delhi 27/28 July 2013

July 27, 2013
The Fibonacci Sequence

- Fibonacci sequence: $1, 1, 2, 3, 5, 8, 13, 21, \ldots$
The Fibonacci Sequence

- Fibonacci sequence: 1, 1, 2, 3, 5, 8, 13, 21, ...  
- Fibonacci sequence: $u_n = u_{n-1} + u_{n-2}$ where $u_1 = u_0 = 1$
The Fibonacci Sequence

- Fibonacci sequence: 1, 1, 2, 3, 5, 8, 13, 21, ...
- Fibonacci sequence: $u_n = u_{n-1} + u_{n-2}$ where $u_1 = u_0 = 1$
- But rabbits die!
The Fibonacci Sequence

- Fibonacci sequence: $1, 1, 2, 3, 5, 8, 13, 21, \ldots$
- Fibonacci sequence: $u_n = u_{n-1} + u_{n-2}$ where $u_1 = u_0 = 1$
- But rabbits die!
- Consider $u_n = u_{n-1} + u_{n-2} - u_{n-3}$ where $u_2 = 2, u_1 = u_0 = 1$
The Fibonacci Sequence

- Fibonacci sequence: $1, 1, 2, 3, 5, 8, 13, 21, \ldots$
- Fibonacci sequence: $u_n = u_{n-1} + u_{n-2}$ where $u_1 = u_0 = 1$
- But rabbits die!
- Consider $u_n = u_{n-1} + u_{n-2} - u_{n-3}$ where $u_2 = 2, u_1 = u_0 = 1$
- **The Question:** Can they ever die out?
Linear Recurrence Sequences (LRS)

Definition

A sequence \( \langle u_0, u_1, \ldots \rangle \) of numbers is called an LRS if there exists \( k \in \mathbb{N} \) and constants \( a_0, \ldots, a_{k-1} \) s.t., for all \( n \geq k \),

\[
u_n = a_{k-1}u_{n-1} + \ldots + a_1u_{n-k+1} + a_0u_{n-k}\]

- \( k \) is called the order/depth of the sequence.
- The first \( k \) elements \( u_0, \ldots, u_{k-1} \) are called initial conditions and they determine the whole sequence.
- We can define the sequences and constants to be over integers or rationals or reals.
The Skolem Problem

Figure: Thoralf Skolem

The Skolem Problem (also called the Skolem-Pisot Problem)
Given a linear recurrence sequence (with initial conditions) over integers, does it have a zero?
The Skolem Problem

The Skolem Problem (also called the Skolem-Pisot Problem)

Given a linear recurrence sequence (with initial conditions) over integers, does it have a zero?

i.e., does $\exists n$ such that $u_n = 0$?

i.e., do the rabbits ever die out?
The Skolem Problem

Skolem Problem: Does $\exists n$ such that $u_n = 0$?
Surprisingly, this problem has been open for 80 years!

Well, in 1934 decidability wasn’t as relevant...
The Skolem Problem

Skolem Problem: Does $\exists n$ such that $u_n = 0$?

Surprisingly, this problem has been open for 80 years!

“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, Famous blog entry 2007
The Skolem Problem

Skolem Problem: Does $\exists n$ such that $u_n = 0$?

Surprisingly, this problem has been open for 80 years!

“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, Famous blog entry 2007

Outline

- Alternative formulations and variants
- Applications
  1. Program Termination
  2. Probabilistic verification
- Results
  1. Classical results on Skolem
  2. Relation between the problems
  3. Results on Program termination
  4. Recent results
Equivalent formulations of the Skolem Problem

Linear recurrence sequence form
Given an LRS $\langle u_1, u_2, \ldots \rangle$ (with initial conditions), does $\exists n$ s.t., $u_n = 0$?

Matrix Form
Given a $k \times k$ matrix $M$, does $\exists n$ s.t., $M^n(1, k) = 0$?

Dot Product Form
Given a $k \times k$ matrix $M$, $k$-dim vectors $\vec{v}, \vec{w}$, does $\exists n$ s.t., $\vec{v} \cdot M^n \cdot \vec{w}^T = 0$?
Equivalent formulations

(1) $\implies$ (2) Let $u_n = a_{k-1}u_{n-1} + \ldots + a_0u_{n-k}$, $a' = (a_{k-1} \ldots a_1)$.

- Let

$$M_1 = \begin{pmatrix} \vec{a}' & \text{Id}_{k-1} \\ a_0 & 0 \end{pmatrix}$$

Then $\forall n \geq 0$, $u_n = \vec{v} \cdot M_1^n \cdot \vec{w}^T$, where $\vec{v} = \vec{u}$, $\vec{w} = (0 \ldots 0 1)$.

- Define

$$M = \begin{pmatrix} 0 & \vec{v} \cdot M_1 \\ \vec{0}^T & M_1 \end{pmatrix} \quad M^n = \begin{pmatrix} 0 & \vec{v} \cdot M_1^n \\ \vec{0}^T & M_1^n \end{pmatrix}$$

- Then, $M^n(1, k + 1) = (1 0) \cdot (M^n) \cdot (0 \vec{w})^T = u_n$.

(3) $\implies$ (1) follows from taking the characteristic polynomial and using Cayley Hamilton Theorem.
Variants

Skolem Problem

- Given an LRS $\langle u_1, u_2, \ldots \rangle$, does $\exists n$ s.t., $u_n = 0$?

Positivity Problem

- Given an LRS $\langle u_1, u_2, \ldots \rangle$, $\forall n$, is $u_n \geq 0$?
- Ultimate Positivity: $\forall n$, $n \geq T$, is $u_n \geq 0$?
Skolem Problem

- Given an LRS $\langle u_1, u_2, \ldots \rangle$, does $\exists n$ s.t., $u_n = 0$?
- Given $k \times k$ matrix $M$, $k$-dim vectors $\vec{v}, \vec{w}$, does $\exists n$ s.t., $\vec{v} \cdot M^n \cdot \vec{w}^T = 0$?

Positivity Problem

- Given an LRS $\langle u_1, u_2, \ldots \rangle$, $\forall n$, is $u_n \geq 0$?
- **Ultimate Positivity:** $\forall n$, $n \geq T$, is $u_n \geq 0$?

Orbit Problem

- Given a $k \times k$ matrix $M$, $k$-dim vectors $\vec{x}$ and $\vec{y}$, does $\exists n$ s.t., $\vec{x} \cdot M^n = \vec{y}$?
Variants

Skolem Problem

- Given an LRS \( \langle u_1, u_2, \ldots \rangle \), does \( \exists n \) s.t., \( u_n = 0 \)?
- Given \( k \times k \) matrix \( M \), \( k \)-dim vectors \( \vec{v}, \vec{w} \), does \( \exists n \) s.t., \( \vec{v} \cdot M^n \cdot \vec{w}^T = 0 \)?

Positivity Problem

- Given an LRS \( \langle u_1, u_2, \ldots \rangle \), \( \forall n \), is \( u_n \geq 0 \)?
- Ultimate Positivity: \( \forall n, n \geq T \), is \( u_n \geq 0 \)?

Orbit Problem

- Given a \( k \times k \) matrix \( M \), \( k \)-dim vectors \( \vec{x}, \vec{y} \), does \( \exists n \) s.t., \( \vec{x} \cdot M^n = \vec{y} \)?
- Higher Order Orbit Problem: Given \( k \times k \) matrix \( M \), \( k \)-dim vector \( \vec{x} \), a subspace \( V \) of dim \( \leq k \), does \( \exists n \) s.t., \( \vec{x} \cdot M^n \in V \)?
Applications of these and other variants!

- Software verification
  - Termination of linear programs
- Probabilistic model checking
  - Reachability in Markov chains
- Theoretical Biology
  - Analysis of L-systems, Population dynamics
- Economics
  - Stability of supply-demand equilibria in cyclical markets
- Quantum Computing
  - Threshold problems for quantum automata
- Dynamical systems
  - Reachability and invariance problems
- Combinatorics
- Term rewriting

...
Applications of these and other variants!

- **Software verification**
  - Termination of linear programs

- **Probabilistic model checking**
  - Reachability in Markov chains

- **Theoretical Biology**
  - Analysis of L-systems, Population dynamics

- **Economics**
  - Stability of supply-demand equilibria in cyclical markets

- **Quantum Computing**
  - Threshold problems for quantum automata

- **Dynamical systems**
  - Reachability and invariance problems

- **Combinatorics**

- **Term rewriting**

- ...
Program Termination

Basic undecidability result – Turing 1936
Termination of a generic program with a loop:

\[
\textbf{while } (\textit{conditions}) \quad \{\textit{commands}\}
\]

is undecidable.
Program Termination

Basic undecidability result – Turing 1936
Termination of a generic program with a loop:

while (conditions) {commands}

is undecidable.

But now, let us consider a much simpler case:

A simple linear program

\( \vec{x} := \vec{b}; \quad \text{while} \ ( \vec{c}^T \vec{x} > \vec{0} ) \quad \{ \vec{x} := A\vec{x} \} \)
Linear Programs

An initialized (homogenous) linear program

\[
\vec{x} := \vec{b}; \quad \textbf{while} \ (\vec{c}^T \vec{x} > 0) \ \{ \vec{x} := A\vec{x} \}
\]

Termination problem for simple linear programs

Does an instance of the above program i.e., \( \langle \vec{b}; \vec{c}; A \rangle \), terminate?
Linear Programs

An initialized (homogenous) linear program

\[ \vec{x} := \vec{b}; \quad \textbf{while} \ (\vec{c}^T \vec{x} > \vec{0}) \ \{ \vec{x} := A\vec{x}\} \]

Termination problem for simple linear programs

Does an instance of the above program i.e., \(\langle \vec{b}; \vec{c}; A\rangle\), terminate?

This problem is equivalent to the positivity problem!
Linear Programs

An initialized (homogenous) linear program
\[ \vec{x} := \vec{b}; \text{ while } (\vec{c}^T \vec{x} > \vec{0}) \{ \vec{x} := A\vec{x} \} \]

Termination problem for simple linear programs
Does an instance of the above program i.e., \( \langle \vec{b}; \vec{c}; A \rangle \), terminate?

This problem is equivalent to the positivity problem!

Theorem [Rohit Singh, Supratik Chakraborty]
Consider the following single input initialized linear loop program:
\[ \vec{x} := \vec{b}; \text{ while } (B\vec{x} > \vec{e}) \{ \vec{x} := A\vec{x} + \vec{d} \} \]

The termination problem for this program is equivalent to the positivity problem.
Reachability in Markov chains

Consider a Markov chain $M$ over states $s_1, \ldots, s_t$.

Question

Starting from a given initial probability distribution $\vec{v}$, is it the case that eventually the probability of staying in state $s_t$ will stay within $[0, 1/2]$?

For e.g., the nodes above could be protein concentrations, and the Markov chain a model of biochemical reactions and we want to check for high conc.
Reachability in Markov chains

Example: Consider $\vec{v} = (1/4, 1/4, 1/2)$ and

$$M = \begin{pmatrix} 0.6 & 0.1 & 0.3 \\ 0.3 & 0.6 & 0.1 \\ 0.1 & 0.3 & 0.6 \end{pmatrix}$$

- Then, does $\exists T$ s.t., for all $t > T$, $\vec{v} \cdot M^t \cdot (1 \ 0 \ 0) > 1/3$?
- Then, does $\exists t$ s.t., $\vec{v} \cdot M^t \cdot (1 \ 0 \ -1) = 0$?
Reachability in Markov chains

Example: Consider $\vec{v} = (1/4, 1/4, 1/2)$ and

$$M = \begin{pmatrix} 0.6 & 0.1 & 0.3 \\ 0.3 & 0.6 & 0.1 \\ 0.1 & 0.3 & 0.6 \end{pmatrix}$$

Then, does $\exists T$ s.t., for all $t > T$, $\vec{v} \cdot M^t \cdot (1 \ 0 \ 0) > 1/3$?

Then, does $\exists t$ s.t., $\vec{v} \cdot M^t \cdot (1 \ 0 \ -1) = 0$?

Theorem

The Skolem over rationals can be reduced to (two!) Stochastic version(s):

- Given stochastic vector $\vec{v}$, vector $w$, row-stochastic matrix $M$, does $\exists t$ s.t., $\vec{v} \cdot M^t \vec{w} = 1/2$

- Given stochastic vectors $\vec{v}$, $\vec{w}$, row-stochastic matrix $M$, rational $r$, does $\exists t$ s.t., $\vec{v} \cdot M^t \vec{w} = r$
Results

1. Classical results on Skolem
   - Skolem-Mahler-Lech Theorem
   - Decidability of Skolem/Positivity for 2,3,4...

2. Relation between the problems

3. Results on Program termination- Tiwari, Braverman, Supratik et al.

   - Orbit problem - extension of Kannan/Lipton
   - Positivity problem
   - Other/probabilistic results and reductions
The Skolem-Mahler-Lech Theorem (1934, 1935, 1953)

The set of zeros of any linear recurrence set is the union of a finite set and a finite number of arithmetic progressions (periodic sets).
Classical Results on Skolem

The Skolem-Mahler-Lech Theorem (1934, 1935, 1953)

The set of zeros of any linear recurrence set is the union of a finite set and a finite number of arithmetic progressions (periodic sets).

- The Skolem asks if the set of zeros is empty.
Classical Results on Skolem

The Skolem-Mahler-Lech Theorem (1934, 1935, 1953)

The set of zeros of any linear recurrence set is the union of a finite set and a finite number of arithmetic progressions (periodic sets).

- The Skolem asks if the set of zeros is empty.
- However, Skolem’s result also shows that it is decidable to check whether or not the set of zeros is infinite!
- In other words, the hardness of the result is in characterizing the finite set.
Classical Results on Skolem

The Skolem-Mahler-Lech Theorem (1934, 1935, 1953)

The set of zeros of any linear recurrence set is the union of a finite set and a finite number of arithmetic progressions (periodic sets).

- The Skolem asks if the set of zeros is empty.
- However, Skolem’s result also shows that it is decidable to check whether or not the set of zeros is infinite!
- In other words, the hardness of the result is in characterizing the finite set.
- All known proofs of the above result use $p$-adic integers.
Lower order results

Skolem’s problem

- Order 1: Trivial (why?).
- Order 2: Folklore!
- Order 3,4: Proved by Vereshchagin in 1985 using results on linear logarithms by Baker and van der Poorten.
  - This theory fetched Baker the Field’s medal in 1970!

In a TUCS Tech report (2005), Havala, Harju, Hirvensalo, Karhumäki prove 2,3,4 in detail. They also claim for order 5, but Ouaknine, Worrell (RP’12) pointed out a serious flaw in it.

(Ultimate) Positivity problem

Order 2: Burke and Webb (1981) – Ultimate
Order 3: Laohakosol and Tangsupphathawat (2009)
Skolem Problem Variants Applications Results

Lower order results

Skolem’s problem

- Order 1: Trivial (why?).
- Order 2: Folklore!
- Order 3,4: Proved by Vereshchagin in 1985 using results on linear logarithms by Baker and van der Poorten.
- In a TUCS Tech report (2005), Havala, Harju, Hirvensalo, Karhumäki prove 2,3,4 in detail.
- They also claim for order 5, but Ouaknine, Worrell (RP’12) pointed out a serious flaw in it.
Skolem Problem Variants Applications Results

Lower order results

Skolem’s problem

- Order 1: Trivial (why?).
- Order 2: Folklore!
- Order 3,4: Proved by Vereshchagin in 1985 using results on linear logarithms by Baker and van der Poorten.
- In a TUCS Tech report (2005), Havala, Harju, Hirvensalo, Karhumäki prove 2,3,4 in detail.
- They also claim for order 5, but Ouaknine, Worrell (RP’12) pointed out a serious flaw in it.

(Ultimate) Positivity problem

- Order 3: Laohakosol and Tangsupphathawat (2009)
Hardness results

- Skolem is NP hard - Blondel and Portier (2002)
Hardness results

- Skolem is NP hard - Blondel and Portier (2002)
- The (complement of) Skolem problem reduces to Positivity
Hardness results

- Skolem is NP hard - Blondel and Portier (2002)
- The (complement of) Skolem problem reduces to Positivity
  - LRS are closed under pointwise product and sum
  - given LRS $u_n$, $u_n \neq 0$ iff $u_n^2 - 1 \geq 0$. 
Hardness results

- Skolem is NP hard - Blondel and Portier (2002)
- The (complement of) Skolem problem reduces to Positivity
  - LRS are closed under pointwise product and sum
  - Given LRS $u_n$, $u_n \neq 0$ iff $u_n^2 - 1 \geq 0$.
- Thus, Positivity is coNP hard.
- Ultimate Positivity is also coNP hard.
The Orbit problem

Orbit Problem

- Given a $k \times k$ matrix $M$, $k$-dim vectors $\vec{x}$ and $\vec{y}$, does $\exists n$ s.t., $\vec{x} \cdot M^n = \vec{y}$?

- Higher Order Orbit Problem: Given $k \times k$ matrix $M$, $k$-dim vector $\vec{x}$, a subspace $V$ of dim $\leq k$, does $\exists n$ s.t., $\vec{x} \cdot M^n \in V$?

- Skolem problem (does $\exists n$ s.t., $\vec{v} \cdot M^n \cdot \vec{w}^T = 0$?) is special case of the higher order Orbit Problem

- Thus, Higher order Orbit Problem is also NP hard.
The Orbit problem

Orbit Problem

- Given a $k \times k$ matrix $M$, $k$-dim vectors $\vec{x}$ and $\vec{y}$, does $\exists n$ s.t., $\vec{x} \cdot M^n = \vec{y}$?

- Higher Order Orbit Problem: Given $k \times k$ matrix $M$, $k$-dim vector $\vec{x}$, a subspace $V$ of dim $\leq k$, does $\exists n$ s.t., $\vec{x} \cdot M^n \in V$?

Kannan, Lipton – STOC’80, JACM’86

The Orbit problem is decidable in $P$. Higher order was left open.
The Orbit problem

**Orbit Problem**
- Given a $k \times k$ matrix $M$, $k$-dim vectors $\vec{x}$ and $\vec{y}$, does $\exists n$ s.t., $\vec{x} \cdot M^n = \vec{y}$?

**Higher Order Orbit Problem**: Given $k \times k$ matrix $M$, $k$-dim vector $\vec{x}$, a subspace $V$ of dim $\leq k$, does $\exists n$ s.t., $\vec{x} \cdot M^n \in V$?

**Kannan, Lipton – STOC’80, JACM’86**
The Orbit problem is decidable in $P$. Higher order was left open.

**Chonev, Ouaknine, Worrell– STOC’12**
- High dim Orbit Problem for dim 1 is in $P$
- High dim Orbit Problem for dim 2 or 3 is in $NP^{RP}$
Termination of Linear Programs

Non-homogenous to Homogenous

\[ \vec{x} := \vec{b}; \quad \textbf{while} \ (B \vec{x} > \vec{e}) \ \{ \vec{x} := A \vec{x} + \vec{d} \} \]

By adding a new scalar variable \( z \),

\[ \vec{x} := \vec{b}, \ z = 1; \quad \textbf{while} \ (B \vec{x} - \vec{e}z > 0) \ \{ \vec{x} := A \vec{x} + \vec{d}z; \ z = z \} \]

Thus, we only have to consider:

\[ \vec{x} := \vec{b} \quad \textbf{while} \ (B \vec{x} > 0) \ \{ \vec{x} := A \vec{x} \} \]

- Tiwari CAV’04: \textbf{while} \ (B \vec{x} > 0) \ \{ \vec{x} := A \vec{x} \} \ termination is decidable over reals
- Braverman CAV’06: The above problem is decidable over integers
- Singh, Supratik: Reduction to Positivity, decidability for subclass
Recentmost Results

Ouaknine, Worrell – Announced on webpage

- positivity for LRS of order 5 or less is decidable with complexity $\text{coNP}^{PPPP}$. 
- ultimate positivity for LRS of order 5 or less is decidable in $P$. 
- decidability for order 6 would imply major breakthroughs in analytic number theory (Diophantine approx of transcendental numbers).
Recentmost Results

Ouaknine, Worrell – Announced on webpage

- positivity for LRS of order 5 or less is decidable with complexity \( coNP^{PP^{PP^{PP}}}/coNP^{PP^{PP^{PP}}} \).
- ultimate positivity for LRS of order 5 or less is decidable in \( P \).
- decidability for order 6 would imply major breakthroughs in analytic number theory (Diophantine approx of transcendental numbers).

“All prior work on Positivity problems that we are aware of has been confined to the use of linear algebra and elementary algebraic number theoretic techniques. By contrast, we are deploying an eclectic arsenal of deep and sophisticated tools from analytic and algebraic number theory, Diophantine geometry, . . .”
Recentmost Results

Ouaknine, Worrell – Announced on webpage

- positivity for LRS of order 5 or less is decidable with complexity $coNP^{PP^{PP^{PP}}}$.
- ultimate positivity for LRS of order 5 or less is decidable in $P$.
- decidability for order 6 would imply major breakthroughs in analytic number theory (Diophantine approx of transcendental numbers).

Some high-level intuition:

1. check if $u_n$ ultimately positive by looking at its “exponential polynomial soln” in $P$.
2. if $u_n$ is ult. pos. with $ord < 5$, we can compute $N$ (of at most exp magnitude) s.t., $u_n$ is positive after $N$. 
Acknowledgments

1. Supratik Chakraborty for sharing manuscript
2. Joel Ouaknine’s slides from RP’12
Acknowledgments

1. Supratik Chakraborty for sharing manuscript
2. Joel Ouaknine’s slides from RP’12

References

References, Contd

5 Tiwari, Termination of Linear Programs, CAV 2004.
6 Braverman, Termination of Integer Linear Programs, CAV 2006.
7 Kannan, Lipton, Polynomial time Algorithm for the Orbit Problem, JACM, 1986.
8 Chakraborty, Singh, Termination of Initialized Rational Linear Programs, Manuscript.
References, Contd

5 Tiwari, Termination of Linear Programs, CAV 2004.
6 Braverman, Termination of Integer Linear Programs, CAV 2006.
7 Kannan, Lipton, Polynomial time Algorithm for the Orbit Problem, JACM, 1986.
8 Chakraborty, Singh, Termination of Initialized Rational Linear Programs, Manuscript.
13 Vereshchagin, The problem of appearance of a zero in a linear