Algorithms, Complexity, Verification: From Cook and Karp to Vardi; or, a Brief Glimpse of the Skolem Landscape

Joël Ouaknine

Max Planck Institute for Software Systems

Vardifest, FLoC'22, Haifa
July 2022

"Tractable Problems $\equiv$ Polynomial Time"

In contrast to popular belief, proving termination is not always impossible.

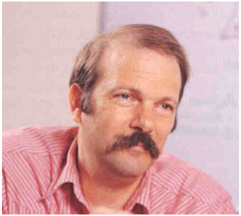
BY BYRON COOK, ANDREAS PODELSKI, AND ANDREY RYBALCHENKO

Proving Program Termination

The Verification Viewpoint

"Any verification problem worth its salt is at least PSPACE-hard!"

Moshe Y. Vardi



Termination of Linear Loops

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
$\quad x := 2x + y;$
$\quad y := y + 3 - z;$
$\quad z := -4z + 6;$

Termination of Linear Loops

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
$\quad x := 2x + y;$
$\quad y := y + 3 - z;$
$\quad z := -4z + 6;$

$\mathbf{x} := \mathbf{a};$
while $x_1 \neq 0$ do
$\quad \mathbf{x} := \mathbf{M}\mathbf{x};$

Termination of Linear Loops

$x := 1;$
$y := 0;$
$z := 0;$
while $\;x \neq 0\;$ do
$\quad x := 2x + y;$
$\quad y := y + 3 - z;$
$\quad z := -4z + 6;$

$\mathbf{x} := \mathbf{a};$
while $\;x_1 \neq 0\;$ do
$\quad \mathbf{x} := \mathbf{M}\mathbf{x};$

$\mathbf{x} := \mathbf{a};$
while $\;x_1 \geq 0\;$ do
$\quad \mathbf{x} := \mathbf{M}\mathbf{x};$

Termination of Linear Loops

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
    $x := 2x + y;$
    $y := y + 3 - z;$
    $z := -4z + 6;$

Skolem Problem:

$\mathbf{x} := \mathbf{a};$
while $x_1 \neq 0$ do
    $\mathbf{x} := \mathbf{M}\mathbf{x};$

$\mathbf{x} := \mathbf{a};$
while $x_1 \geq 0$ do
    $\mathbf{x} := \mathbf{M}\mathbf{x};$

Termination of Linear Loops

$x := 1;$
$y := 0;$
$z := 0;$
while $x \neq 0$ do
    $x := 2x + y;$
    $y := y + 3 - z;$
    $z := -4z + 6;$

Skolem Problem:

$\mathbf{x} := \mathbf{a};$
while $x_1 \neq 0$ do
    $\mathbf{x} := \mathbf{M}\mathbf{x};$

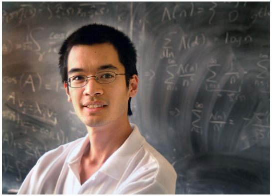
Positivity Problem:

$\mathbf{x} := \mathbf{a};$
while $x_1 \geq 0$ do
    $\mathbf{x} := \mathbf{M}\mathbf{x};$

Skolem and Positivity: Open for About 90 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!"

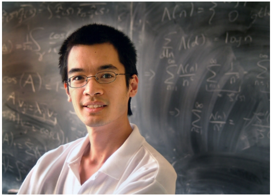
Terence Tao



Skolem and Positivity: Open for About 90 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!"

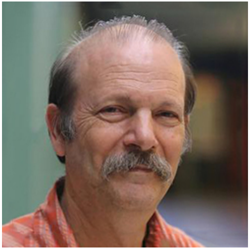
Terence Tao



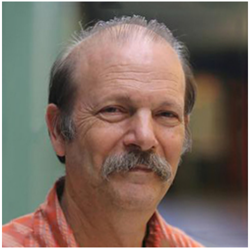
"A mathematical embarrassment . . ."

"Arguably, by some distance, the most prominent problem whose decidability status is currently unknown."

Richard Lipton

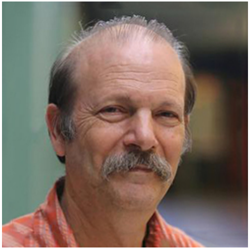


2008: “You’re barking up the wrong tree”



2008: “You’re barking up the wrong tree”

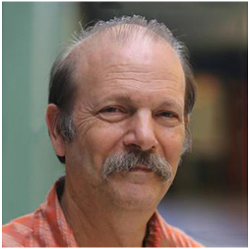
2015: “The jury is still out ...”



2008: “You’re barking up the wrong tree”

2015: “The jury is still out . . . ”

2017: “Hmm, we need one of your results!
– How about writing a paper together??”



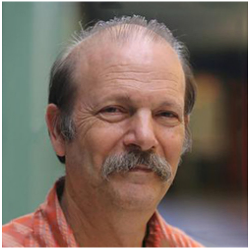
2008: "You're barking up the wrong tree"

2015: "The jury is still out . . . "

2017: "Hmm, we need one of your results!
– How about writing a paper together??"

$\Longrightarrow$ *Sequential Relational Decomposition*

LICS 2018 / LMCS 2022



2008: "You're barking up the wrong tree"

2015: "The jury is still out . . ."

2017: "Hmm, we need one of your results!
– How about writing a paper together??"

$\Longrightarrow$ *Sequential Relational Decomposition*

LICS 2018 / LMCS 2022

We are now in a position to proceed with our equivalence:

Theorem 5.11. *EBP is Equivalent to Positivity.*

Proof. We first show that Positivity reduces to EBP. Let $\langle u_n \rangle_{n=0}^{\infty}$ be an LRS of order d; we

Very nice — but why should *you* care??

Very nice — but why should *you* care??

You don't have to be a complexity theorist to make use of NP-completenss or SAT solvers!

Very nice — but why should *you* care??

You don't have to be a complexity theorist to make use of NP-completenss or SAT solvers!

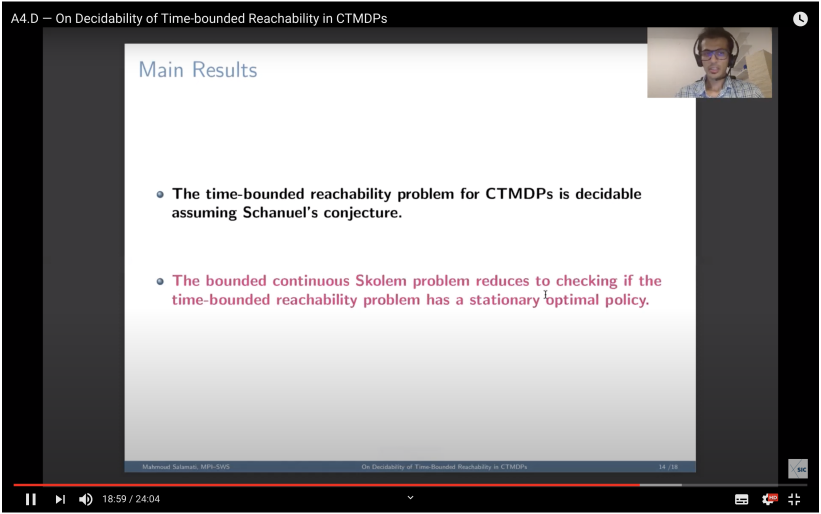
In the world of Verification:

$$\boxed{\begin{array}{rcl} \text{Skolem} & \approx & \text{NP} \\ \text{Positivity} & \approx & \text{PSPACE} \end{array}}$$

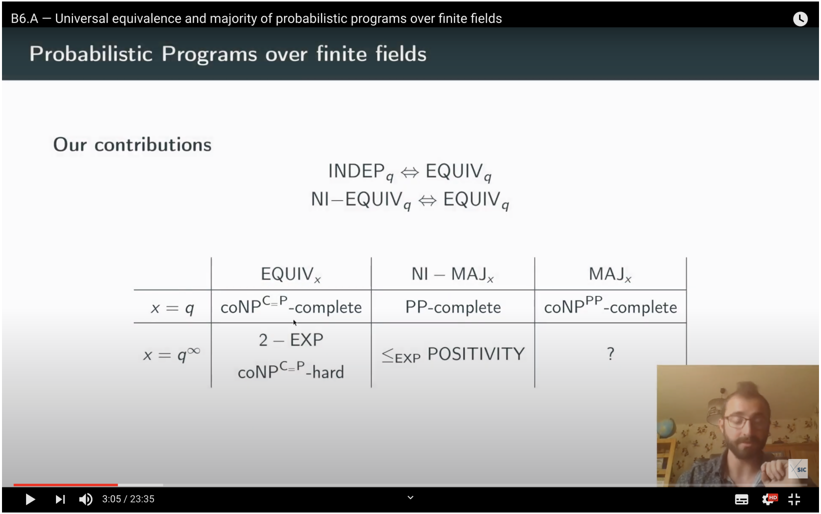
On Skolem-hardness and saturation points in Markov decision processes

Summary

optimization problem on MDPs	threshold problem Skolem-hard (Positivity-hard) for	exponential-time algorithm using a saturation point for
partial SSPP	weights in $\mathbb{Z}$	weights in $\mathbb{N}$ [Chen et al., 2013]
conditional SSPP	weights in $\mathbb{Z}$	weights in $\mathbb{N}$ [Baier et al., 2017]
conditional value-at-risk for the classical SSPP	weights in $\mathbb{Z}$	weights in $\mathbb{N}$
long-run probability	regular co-safety properties	constrained reachability $a \, \mathrm{U} \, b$ [Baier, Bertrand, Piribauer, Sankur, 2019]
model checking of frequency-LTL	$\mathrm{Pr}^{\max}_{\mathcal{M}}(G^{>\vartheta}_{\inf}(\varphi)) = 1?$ for an LTL-formula φ	$\mathrm{Pr}^{\max}_{\mathcal{M}}(G^{>\vartheta}_{\inf}(a \, \mathrm{U} \, b)) = 1?$


A4.D — On Decidability of Time-bounded Reachability in CTMDPs
Main Results
The time-bounded reachability problem for CTMDPs is decidable assuming Schanuel's conjecture.
The bounded continuous Skolem problem reduces to checking if the time-bounded reachability problem has a stationary optimal policy.
Mahmoud Salamati, MPI-SWS
On Decidability of Time-Bounded Reachability in CTMDPs
14 /18
18:59 / 24:04

G. Barthe, C. Jacomme, S. Kremer @ LICS 2020



Highlights 2022
of Logic, Games and Automata

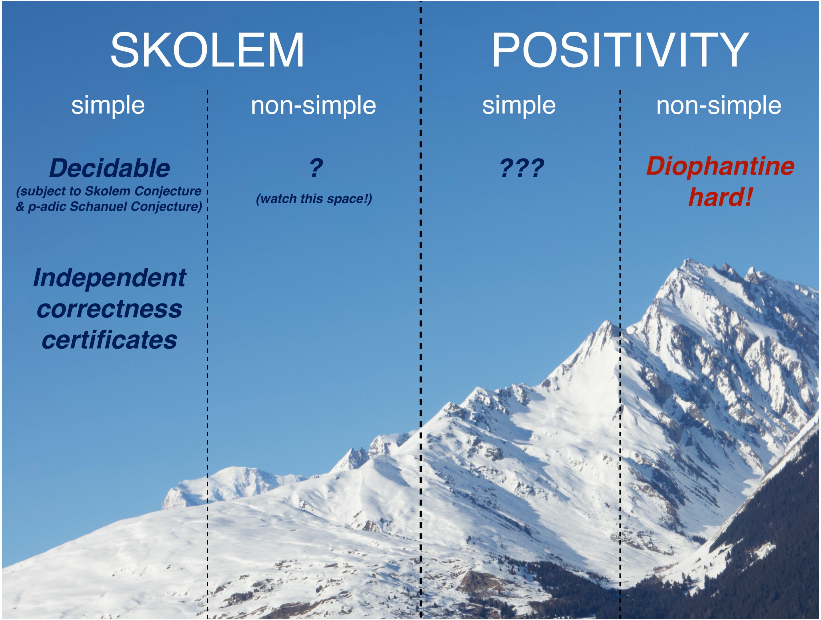
Wednesday 16h10-17h40: Contributed talks II

Skolem Problem (Amphitheatre 2A)

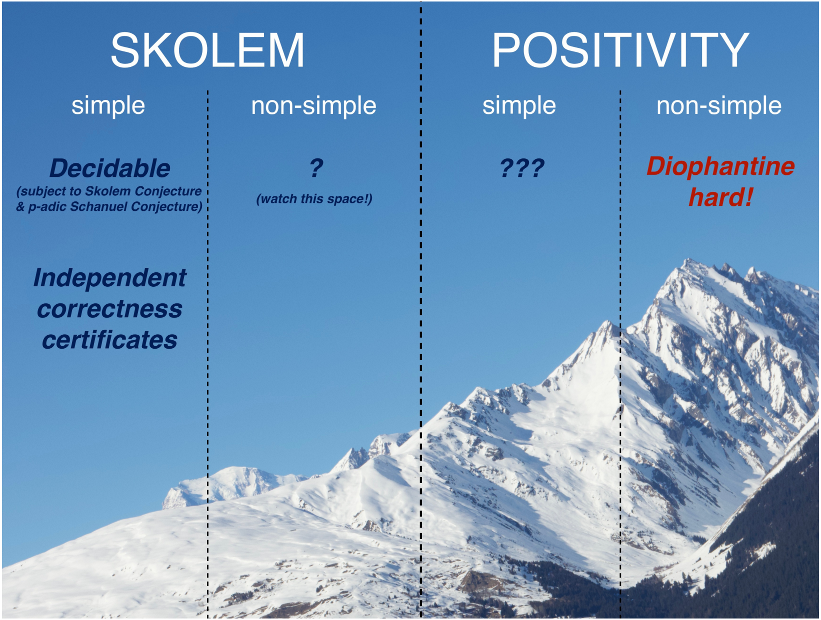
- ▶ Joris Nieuwveld: Progress on the Skolem Problem
- ▶ George Kenison: On the Skolem Problem for Reversible Sequences
- ▶ Arka Ghosh: Orbit-Finite Systems of Linear Equations
- ▶ James Worrell: The Pseudo-Reachability Problem for Linear Dynamical Systems
- ▶ Isa Vialard: On the Cartesian Product of Well-Orderings
- ▶ Edon Kelmendi: Computing the Density of the Positivity Set for Linear Recurrence Sequences
- ▶ Klara Nosan: The Membership Problem for Hypergeometric Sequences with Rational Parameters
- ▶ Nikhil Balaji: Identity Testing for Radical Expressions

The Skolem Landscape

The Skolem Landscape



Want more? Come to our LICS talk, Tuesday 10am!



https://skolem.mpi-sws.org/

skolem.mpi-sws.org

Accounts Teams

SKOLEM: Solves the Skolem Problem for simple integer LRS

System Explanation

Show/Hide

- On the first line write the coefficients of the recurrence relation, separated by spaces.
- On the second line write an equal number of space-separated initial values.
- The LRS must be simple, non-degenerate, and not the zero LRS.
- The tool will output all zeros (at both positive and negative indices), along with a completeness certificate.

Input Format

$a_1\ a_2\ \dots\ a_k$

$u_0\ u_1\ \dots\ u_{k-1}$

where:

$u_{n+k} = a_1 \cdot u_{n+k-1} + a_2 \cdot u_{n+k-2} + \dots + a_k \cdot u_n$

Input area

Auto-fill examples: Show/Hide

Zero LRS | Degenerate LRS | Non-simple LRS | Trivial | Fibonacci | Tribonacci | Berstel sequence [1] | Order 5 [3] | Order 6 [3] | Reversible order 8 [3]

Manual input:

```
6 -25 66 -120 150 -89 18 -1
0 0 -48 -120 0 520 624 -2016
```

- Always render full LRS (otherwise restricted to 400 characters)
- I solemnly swear the LRS is non-degenerate (skips degeneracy check, it will timeout or break if the LRS is degenerate!)
- Factor subcases (merges subcases into single linear set, sometimes requires higher modulo classes)
- Use GCD reduction (reduces initial values by GCD)
- Use fast identification of mod-m (requires GCD reduction) (may result in non-minimal mod-m argument)

Go | Clear | Stop

Output area

Zeros: 0, 1, 4

Zero at 0 in $(0+ 1\mathbb{Z})$ hide/show

- p-adic non-zero in $(0+ 136\mathbb{Z}_{\neq 0})$
- Zero at 1 in $(1+ 136\mathbb{Z})$ hide/show
  - p-adic non-zero in $(1+ 680\mathbb{Z}_{\neq 0})$ $((0+ 5\mathbb{Z}_{\neq 0})$ of parent)
  - Non-zero mod 3 in $(137+ 680\mathbb{Z})$ $((1+ 5\mathbb{Z})$ of parent)
  - Non-zero mod 3 in $(273+ 680\mathbb{Z})$ $((2+ 5\mathbb{Z})$ of parent)
  - Non-zero mod 9 in $(409+ 680\mathbb{Z})$ $((3+ 5\mathbb{Z})$ of parent)
  - Non-zero mod 3 in $(545+ 680\mathbb{Z})$ $((4+ 5\mathbb{Z})$ of parent)
- Non-zero mod 7 in $(2+ 136\mathbb{Z})$

```
================
LRS: u_{n} =
-27161311617120974485866352055894634704015095508906419136363354546754097691
1} +
-50875717942553060846492761332069658239718750163652943951247535707239324495
2} +
-10206640015864118991519942651944720249221599840966743554793056867782008052
3} +
-14120956624060003103644967151812606672989015750648229312685175908046543759
4} +
1906955894773207103609842658940914223756942339091587019654461069437273467027
5} +
```