# Verification of Linear Dynamical Systems

James Worrell

Department of Computer Science
Oxford University

Marktoberdorf 2023

# A Landscape

# Overview

Verification of linear systems (Markov chains, linear constraint loops, probabilistic and quantum automata, affine programs, linear recurrences, . . . )

# Overview

Verification of linear systems (Markov chains, linear constraint loops, probabilistic and quantum automata, affine programs, linear recurrences, . . . )

1. **Halting Problem**:
   - Skolem's Problem as the Halting Problem for linear loops

# Overview

Verification of linear systems (Markov chains, linear constraint loops, probabilistic and quantum automata, affine programs, linear recurrences, . . . )

1. **Halting Problem**:
   - Skolem's Problem as the Halting Problem for linear loops

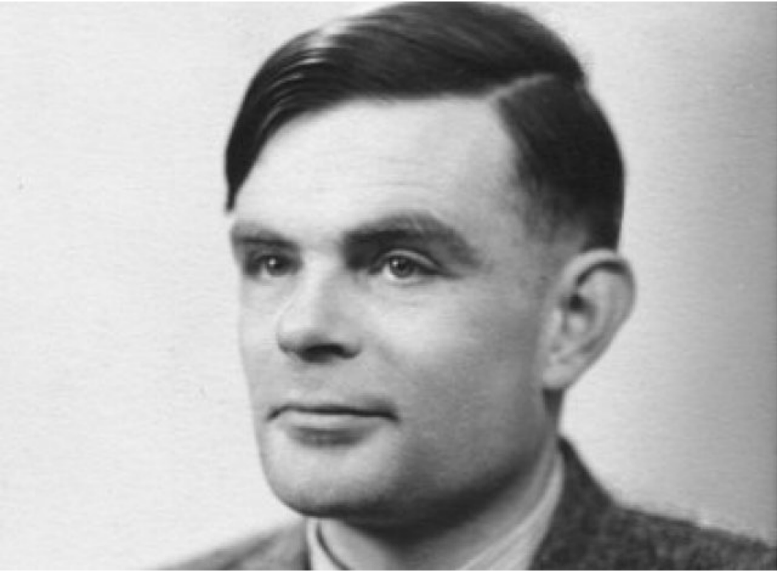
2. **Termination analysis**:
   - Termination for linear constraint loops

# Overview

Verification of linear systems (Markov chains, linear constraint loops, probabilistic and quantum automata, affine programs, linear recurrences, . . . )

1. **Halting Problem**:
    - Skolem's Problem as the Halting Problem for linear loops
2. **Termination analysis**:
    - Termination for linear constraint loops
3. **Invariant synthesis**:
    - Computing polynomial invariants for affine programs

# Part I: Halting Problem



*What is the simplest class of programs for which decidability of the Halting Problem is open?*

# Halting Problem for Simple Linear Loops!

# Halting Problem for Simple Linear Loops!

$$
\begin{aligned}
& x := 1; \\
& y := 0; \\
& z := 0; \\
& \text{while} \quad x \neq 0 \quad \text{do} \\
& \qquad x := 2x + y; \\
& \qquad y := y + 3 - z; \\
& \qquad z := -4z + 6;
\end{aligned}
$$

# Halting Problem for Simple Linear Loops!

$$
\begin{aligned}
&x := 1;\\
&y := 0;\\
&z := 0;\\
&\text{while} \quad x \neq 0 \quad \text{do}\\
&\qquad x := 2x + y;\\
&\qquad y := y + 3 - z;\\
&\qquad z := -4z + 6;
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{x} := \mathbf{a};\\
&\text{while} \quad x_1 \neq 0 \quad \text{do}\\
&\qquad \mathbf{x} := \mathbf{M}\mathbf{x};
\end{aligned}
$$

# Halting Problem for Simple Linear Loops!

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

**Skolem Problem:**

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

# Halting Problem for Simple Linear Loops!

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

**Skolem Problem:**

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

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

# Halting Problem for Simple Linear Loops!

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

**Skolem Problem:**

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

**Positivity Problem:**

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

# Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence $\langle u_0, u_1, u_2, \ldots \rangle$ in $\mathbb{Q}$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

# Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence $\langle u_0, u_1, u_2, \ldots \rangle$ in $\mathbb{Q}$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n$.

- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$

# Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence $\langle u_0, u_1, u_2, \ldots \rangle$ in $\mathbb{Q}$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0: \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n$.

- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- $k$ is the **order** of the sequence
  - Fibonacci has order 2 $(u_{n+2} = u_{n+1} + u_n)$

# Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence $\langle u_0, u_1, u_2, \ldots \rangle$ in $\mathbb{Q}$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0: \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n$.

- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- $k$ is the **order** of the sequence
  - Fibonacci has order 2 $(u_{n+2} = u_{n+1} + u_n)$
  - Binet formula: $u_n = \sum_{i=1}^{s} P_i(n) \lambda_i^n$

# Classical Formulation

A **linear recurrence sequence (LRS)** is a sequence $\langle u_0, u_1, u_2, \ldots \rangle$ in $\mathbb{Q}$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0: \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n$.

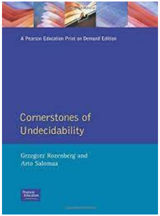
- e.g. the Fibonacci numbers $\langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$
- $k$ is the **order** of the sequence
  - Fibonacci has order 2 $(u_{n+2} = u_{n+1} + u_n)$
  - Binet formula: $u_n = \sum_{i=1}^{s} P_i(n) \lambda_i^n$

**Problem SKOLEM**

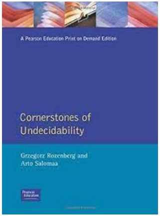
*Instance:* An LRS $\langle u_0, u_1, u_2, \ldots \rangle$

*Question:* Does $\exists n \geq 0$ such that $u_n = 0$?

# The Positivity Problem



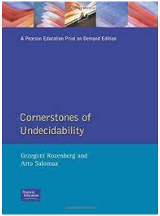
# The Positivity Problem




**Problem POSITIVITY**

*Instance:* An LRS $\langle u_0, u_1, u_2, \ldots \rangle$
*Question:* Is $u_n \geq 0$ for all $n$?

# The Positivity Problem




**Problem POSITIVITY**

*Instance*: An LRS $\langle u_0, u_1, u_2, \ldots \rangle$
*Question*: Is $u_n \geq 0$ for all $n$?

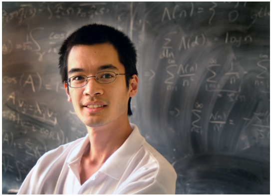
**Problem ULTIMATE POSITIVITY**

*Instance*: An LRS $\langle u_0, u_1, u_2, \ldots \rangle$
*Question*: Is $u_n \geq 0$ for all but finitely many $n$?

# The Skolem Problem is Open

*"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!"*

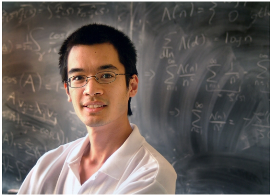
Terence Tao



# The Skolem Problem is Open

*"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 . . . "*

Richard Lipton

# The Skolem-Mahler-Lech Theorem

**Fact:** any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

# The Skolem-Mahler-Lech Theorem

**Fact:** any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

**Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)**

*The set of zeros* $\{n \in \mathbb{N} : u_n = 0\}$ *of a non-degenerate LRS* $\langle u_0, u_1, u_2, \ldots \rangle$ *is finite.*

# The Skolem-Mahler-Lech Theorem

**Fact:** any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

**Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)**

*The set of zeros* $\{n \in \mathbb{N} : u_n = 0\}$ *of a non-degenerate LRS* $\langle u_0, u_1, u_2, \ldots \rangle$ *is finite.*

- Decidability of the Skolem Problem is equivalent to being able to compute the finite set of zeros of any given non-degenerate LRS

# The Skolem-Mahler-Lech Theorem

**Fact:** any LRS can be effectively decomposed into finitely many *non-degenerate* LRS.

**Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)**

*The set of zeros* $\{n \in \mathbb{N} : u_n = 0\}$ *of a non-degenerate LRS* $\langle u_0, u_1, u_2, \ldots \rangle$ *is finite.*

- Decidability of the Skolem Problem is equivalent to being able to compute the finite set of zeros of any given non-degenerate LRS
- Unfortunately, all known proofs of the Skolem-Mahler-Lech Theorem make use of *non-constructive* $p$-adic techniques

# Quiz on Computational Complexity

- Given two NFA $A$ and $B$, is every word accepted by $A$ also accepted by $B$?

- Given two NFA $A$ and $B$, does every word have at least as many accepting runs in $B$ as in $A$?

- Given two NFA $A$ and $B$, for every $n$, does $B$ accept at least as many words of length $n$ as $A$?

- Given a Markov chain over states $s_1, \ldots, s_k$ with initial state $s_1$, is there some timepoint from which the probabiity to be in state $s_k$ is always greater than $1/2$?

# Quiz on Computational Complexity

- Given two NFA $A$ and $B$, is every word accepted by $A$ also accepted by $B$?
    - **PSPACE-COMPLETE**

- Given two NFA $A$ and $B$, does every word have at least as many accepting runs in $B$ as in $A$?

- Given two NFA $A$ and $B$, for every $n$, does $B$ accept at least as many words of length $n$ as $A$?

- Given a Markov chain over states $s_1, \ldots, s_k$ with initial state $s_1$, is there some timepoint from which the probabiity to be in state $s_k$ is always greater than $1/2$?

# Quiz on Computational Complexity

- Given two NFA $A$ and $B$, is every word accepted by $A$ also accepted by $B$?
  - **PSPACE-COMPLETE**
- Given two NFA $A$ and $B$, does every word have at least as many accepting runs in $B$ as in $A$?
  - **UNDECIDABLE**
- Given two NFA $A$ and $B$, for every $n$, does $B$ accept at least as many words of length $n$ as $A$?
- Given a Markov chain over states $s_1, \ldots, s_k$ with initial state $s_1$, is there some timepoint from which the probabiity to be in state $s_k$ is always greater than $1/2$?

# Quiz on Computational Complexity

- Given two NFA $A$ and $B$, is every word accepted by $A$ also accepted by $B$?
  - **PSPACE-COMPLETE**
- Given two NFA $A$ and $B$, does every word have at least as many accepting runs in $B$ as in $A$?
  - **UNDECIDABLE**
- Given two NFA $A$ and $B$, for every $n$, does $B$ accept at least as many words of length $n$ as $A$?
  - **POSITIVITY-COMPLETE**
- Given a Markov chain over states $s_1, \ldots, s_k$ with initial state $s_1$, is there some timepoint from which the probabiity to be in state $s_k$ is always greater than $1/2$?

# Quiz on Computational Complexity

- Given two NFA $A$ and $B$, is every word accepted by $A$ also accepted by $B$?
  - **PSPACE-COMPLETE**
- Given two NFA $A$ and $B$, does every word have at least as many accepting runs in $B$ as in $A$?
  - **UNDECIDABLE**
- Given two NFA $A$ and $B$, for every $n$, does $B$ accept at least as many words of length $n$ as $A$?
  - **POSITIVITY-COMPLETE**
- Given a Markov chain over states $s_1, \ldots, s_k$ with initial state $s_1$, is there some timepoint from which the probabiity to be in state $s_k$ is always greater than $1/2$?
  - **ULTIMATE POSITIVITY-COMPLETE**

# Some Other Application Areas

SKOLEM and POSITIVITY arise in many other areas (often in hardness results), e.g.:

# Some Other Application Areas

SKOLEM and POSITIVITY arise in many other areas (often in hardness results), e.g.:

- Theoretical biology
  - analysis of L-systems
  - population dynamics
- Software verification / program analysis
- Dynamical systems
- Differential privacy
- (Weighted) automata and games
- Analysis of stochastic systems
- Control theory
- Quantum computing
- Statistical physics
- Formal power series
- Combinatorics
- ...

# The Skolem Problem at Low Orders

**Skolem Problem**

Does $\exists n$ such that $u_n = 0$ ?

Let $u_n$ be a linear recurrence sequence of fixed order

# The Skolem Problem at Low Orders

**Skolem Problem**

Does $\exists n$ such that $u_n = 0$ ?

Let $u_n$ be a linear recurrence sequence of fixed order

**Theorem (folklore)**

*For orders 1 and 2, Skolem is decidable.*

# The Skolem Problem at Low Orders

**Skolem Problem**

Does $\exists n$ such that $u_n = 0$ ?

Let $u_n$ be a linear recurrence sequence of fixed order

**Theorem (folklore)**

*For orders 1 and 2, Skolem is decidable.*

**Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)**

*For orders 3 and 4, Skolem is decidable.*

# The Skolem Problem at Low Orders

**Skolem Problem**

Does $\exists n$ such that $u_n = 0$ ?

Let $u_n$ be a linear recurrence sequence of fixed order

**Theorem (folklore)**

*For orders 1 and 2, Skolem is decidable.*

**Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)**

*For orders 3 and 4, Skolem is decidable.*

Critical ingredient is Baker's theorem for linear forms in logarithms, which earned Baker the Fields Medal in 1970.

# *Simple* Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

# *Simple* Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

- e.g., the Fibonacci sequence:

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

# *Simple* Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

- e.g., the Fibonacci sequence:

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

- The "vast majority" of LRS are simple...

# *Simple* Linear Recurrence Sequences

An LRS is **simple** if its *characteristic roots* are simple (non-repeated)

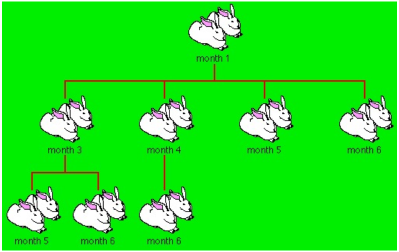
- e.g., the Fibonacci sequence:

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

- The "vast majority" of LRS are simple...

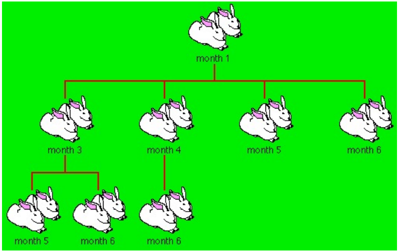
Simple LRS correspond precisely to **diagonalisable** matrices

# Counting Rabbits Modulo $m$




$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

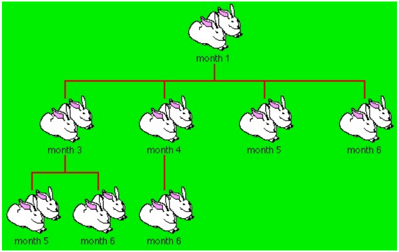
# Counting Rabbits Modulo $m$




$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod{2}$

# Counting Rabbits Modulo $m$

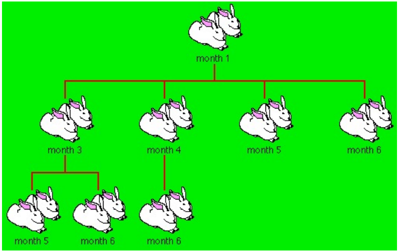



$$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$$

$$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod 2$$

$$\langle 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \ldots \rangle \pmod 3$$

# Counting Rabbits Modulo $m$



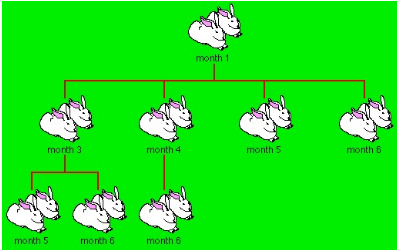

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod 2$

$\langle 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \ldots \rangle \pmod 3$

$\langle 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, \ldots \rangle \pmod 4$

# Counting Rabbits Modulo $m$




$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

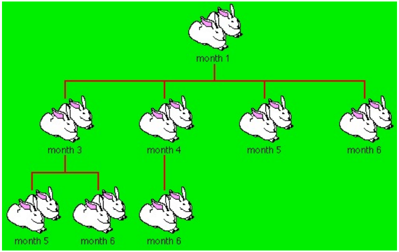
$\langle 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \rangle \pmod{2}$

$\langle 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \ldots \rangle \pmod{3}$

$\langle 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, \ldots \rangle \pmod{4}$

$\langle 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, 2, \ldots \rangle \pmod{5}$

# Counting Rabbits Modulo $m$




$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

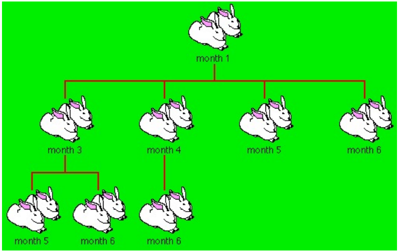
$\langle 1, 1, \mathbf{0}, 1, 1, \mathbf{0}, 1, 1, \mathbf{0}, 1, 1, \mathbf{0}, \ldots \rangle \pmod 2$

$\langle 1, 1, 2, \mathbf{0}, 2, 2, 1, \mathbf{0}, 1, 1, 2, \mathbf{0}, \ldots \rangle \pmod 3$

$\langle 1, 1, 2, 3, 1, \mathbf{0}, 1, 1, 2, 3, 1, \mathbf{0}, \ldots \rangle \pmod 4$

$\langle 1, 1, 2, 3, \mathbf{0}, 3, 3, 1, 4, \mathbf{0}, 4, 4, 3, 2, \mathbf{0}, 2, 2, 4, 1, \mathbf{0}, 1, 1, 2, \ldots \rangle \pmod 5$

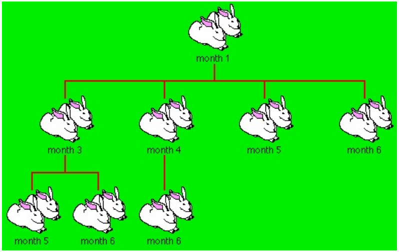
# Reversibility




$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

- The Fibonacci sequence has a zero mod $m$ for every $m$

# Reversibility



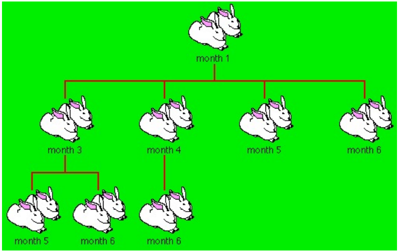

$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

- The Fibonacci sequence has a zero mod $m$ for every $m$
- The sequence has bi-infinite extension

$$\langle \ldots, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8 \ldots \rangle$$

that contains a zero

# Reversibility




$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots \rangle$

- The Fibonacci sequence has a zero mod *m* for every *m*
- The sequence has bi-infinite extension

$$\langle \ldots, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8 \ldots \rangle$$

  that contains a zero
- The bi-infinite extension is periodic modulo *m* for every *m*

# Skolem Conjecture

ANWENDUNG EXPONENTIELLER KONGRUENZEN ZUM BEWEIS DER UNLÖSBARKEIT GEWISSER DIOPHANTISCHER GLEICHUNGEN

VON

TH. SKOLEM

AVHANDLINGER UTGITT AV DET NORSKE VIDENSKAPS-AKADEMI I OSLO
I. MAT.-NATURV. KLASSE. 1937. No. 12

- If a **simple bi-infinite** LRS over the rationals has no zeros, then it has no zeros modulo *some* integer $m$.

# Skolem Conjecture

ANWENDUNG EXPONENTIELLER KONGRUENZEN ZUM BEWEIS DER UNLÖSBARKEIT GEWISSER DIOPHANTISCHER GLEICHUNGEN

VON

TH. SKOLEM

Avhandlinger utgitt av Det Norske Videnskaps-Akademi i Oslo
I. Mat.-Naturv. Klasse. 1937. No. 12

- If a **simple bi-infinite** LRS over the rationals has no zeros, then it has no zeros modulo *some* integer $m$.
- Why simple?

# Skolem Conjecture

ANWENDUNG EXPONENTIELLER KONGRUENZEN ZUM BEWEIS DER UNLÖSBARKEIT GEWISSER DIOPHANTISCHER GLEICHUNGEN

VON

TH. SKOLEM

AVHANDLINGER UTGITT AV DET NORSKE VIDENSKAPS-AKADEMI I OSLO
I. MAT.-NATURV. KLASSE. 1937. No. 12

- If a **simple bi-infinite** LRS over the rationals has no zeros, then it has no zeros modulo *some* integer $m$.
- Why simple? Consider $u_n = 2^n(2n+1)$

# Skolem Conjecture

ANWENDUNG EXPONENTIELLER KONGRUENZEN ZUM BEWEIS DER UNLÖSBARKEIT GEWISSER DIOPHANTISCHER GLEICHUNGEN

VON

TH. SKOLEM

AVHANDLINGER UTGITT AV DET NORSKE VIDENSKAPS-AKADEMI I OSLO
I. MAT.-NATURV. KLASSE. 1937. No. 12

- If a **simple bi-infinite** LRS over the rationals has no zeros, then it has no zeros modulo *some* integer $m$.
- Why simple? Consider $u_n = 2^n(2n+1)$
- One-way version fails to hold

# Skolem Problem for Bi-Infinite Sequences

**Problem BI-SKOLEM**

*Instance*: A bi-LRS $\langle \ldots, u_{-2}, u_{-1}, u_0, u_1, u_2, \ldots \rangle$ over $\mathbb{Q}$

*Question*: Does $\exists n \in \mathbb{Z}$ such that $u_n = 0$?

# Skolem Problem for Bi-Infinite Sequences

**Problem BI-SKOLEM**

*Instance:* A bi-LRS $\langle \ldots, u_{-2}, u_{-1}, u_0, u_1, u_2, \ldots \rangle$ over $\mathbb{Q}$
*Question:* Does $\exists n \in \mathbb{Z}$ such that $u_n = 0$?

- Decidable for simple LRS assuming Skolem's Conjecture.

# Skolem Problem for Bi-Infinite Sequences

**Problem BI-SKOLEM**

*Instance:* A bi-LRS $\langle \ldots, u_{-2}, u_{-1}, u_0, u_1, u_2, \ldots \rangle$ over $\mathbb{Q}$
*Question:* Does $\exists n \in \mathbb{Z}$ such that $u_n = 0$?

- Decidable for simple LRS assuming Skolem's Conjecture.
- How are the Skolem and Bi-Skolem Problems related?

# Skolem Problem for Bi-Infinite Sequences

**Problem BI-SKOLEM**

*Instance:* A bi-LRS $\langle \dots, u_{-2}, u_{-1}, u_0, u_1, u_2, \dots \rangle$ over $\mathbb{Q}$
*Question:* Does $\exists n \in \mathbb{Z}$ such that $u_n = 0$?

- Decidable for simple LRS assuming Skolem's Conjecture.
- How are the Skolem and Bi-Skolem Problems related?
- Can one use an oracle for Bi-Skolem to compute all zeros of a bi-LRS?

# Reducing Skolem to Bi-Skolem

**Theorem (Bilu, Luca, Pursar, Ouaknine, Nieuwveld, W. 22)**

*For LRS of order 5 the Skolem and Bi-Skolem Problems are interreducible.*

# Reducing Skolem to Bi-Skolem

**Theorem (Bilu, Luca, Pursar, Ouaknine, Nieuwveld, W. 22)**

*For LRS of order 5 the Skolem and Bi-Skolem Problems are interreducible. For LRS of all orders the Skolem and Bi-Skolem problems are irreducible assuming the p-adic Schanuel conjecture.*

# Reducing Skolem to Bi-Skolem

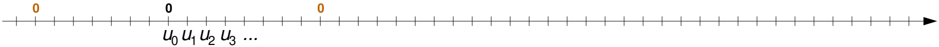
**Theorem (Bilu, Luca, Pursar, Ouaknine, Nieuwveld, W. 22)**

*For LRS of order 5 the Skolem and Bi-Skolem Problems are interreducible. For LRS of all orders the Skolem and Bi-Skolem problems are irreducible assuming the p-adic Schanuel conjecture.*

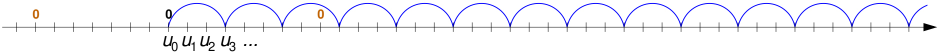
**Lemma (Zero Isolation)**

*Assuming the p-adic Schanuel Conjecture, given a bi-infinite LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ one can compute $L$ such that $u_{Ln} \neq 0$ for all $n \neq 0$.*

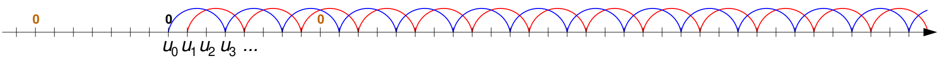
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



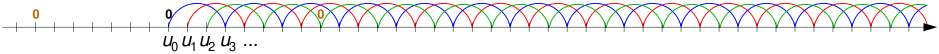
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



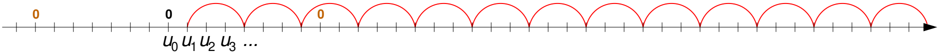
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



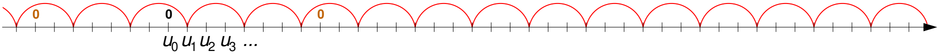
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



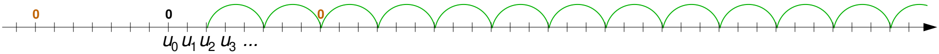
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



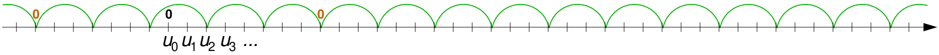
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



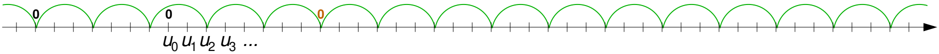
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



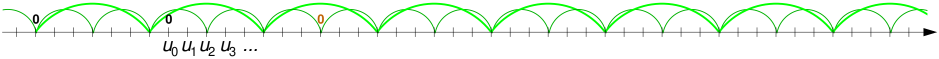
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



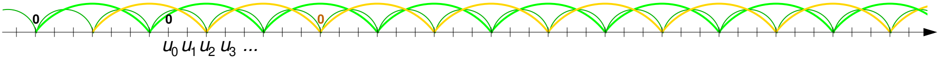
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



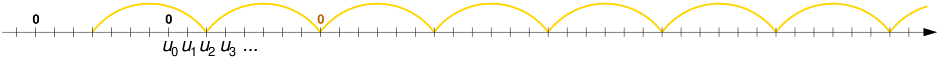
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



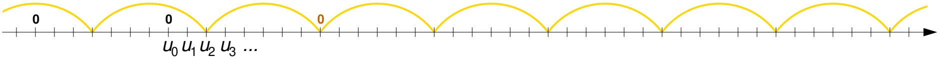
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



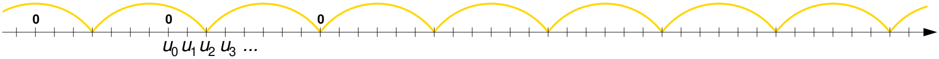
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



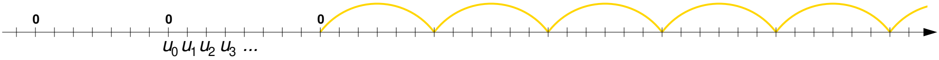
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



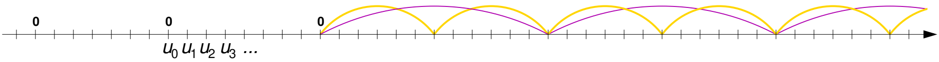
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



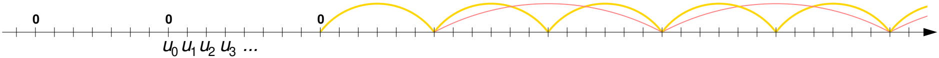
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



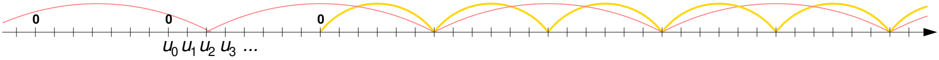
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



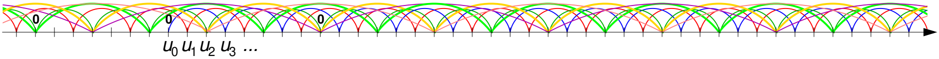
# Computing Zero Set of an LRS with Oracle to Bi-Skolem



# Computing Zero Set of an LRS with Oracle to Bi-Skolem



# Computing Zero Set of an LRS with Oracle to Bi-Skolem



# Schanuel's Conjecture

**Schanuel's Conjecture (early 1960s)**

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$. Then $\{\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}\}$, contains (at least) $n$ numbers that are algebraically independent over $\mathbb{Q}$.

# Schanuel's Conjecture

**Schanuel's Conjecture (early 1960s)**

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$. Then $\{\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}\}$, contains (at least) $n$ numbers that are algebraically independent over $\mathbb{Q}$.

In other words: for any polynomial $P(x_1, \ldots, x_n)$ with rational (or algebraic) coefficients, if $P(\beta_1, \ldots, \beta_n) = 0$, then $P$ must be the zero polynomial.

# Schanuel's Conjecture — Example

- $e$ is transcendental (Charles Hermite, 1873)
- $\pi$ is transcendental (Ferdinand von Lindemann, 1882)

# Schanuel's Conjecture — Example

- $e$ is transcendental (Charles Hermite, 1873)
- $\pi$ is transcendental (Ferdinand von Lindemann, 1882)
- What about $e + \pi$ and $e\pi$?

# Schanuel's Conjecture — Example

- $e$ is transcendental (Charles Hermite, 1873)
- $\pi$ is transcendental (Ferdinand von Lindemann, 1882)
- What about $e + \pi$ and $e\pi$?

Consider

$$\begin{aligned} p(x) &= (x - e)(x - \pi) \\ &= x^2 - (e + \pi)x + e\pi \end{aligned}$$

# Schanuel's Conjecture — Example

- $e$ is transcendental (Charles Hermite, 1873)
- $\pi$ is transcendental (Ferdinand von Lindemann, 1882)
- What about $e + \pi$ and $e\pi$?

Consider

$$\begin{aligned} p(x) &= (x - e)(x - \pi) \\ &= x^2 - (e + \pi)x + e\pi \end{aligned}$$

If *both* $e + \pi$ and $e\pi$ were rational, then $e$ and $\pi$ would be algebraic, contradiction.

# Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

# Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

# Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

# Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

So (assuming Schanuel's Conjecture), $\beta_1 = i\pi$ and $\beta_2 = e$ must be algebraically independent, and therefore $\pi$ and $e$ must be algebraically independent.

# Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

So (assuming Schanuel's Conjecture), $\beta_1 = i\pi$ and $\beta_2 = e$ must be algebraically independent, and therefore $\pi$ and $e$ must be algebraically independent.

Thus for *any* non-zero polynomial $P(x, y)$ with rational (or algebraic) coefficients, we have that $P(e, \pi)$ cannot be zero.

# Schanuel's Conjecture — Example

- So what about $e + \pi$ and $e\pi$ or (say) $e^5\pi^3 - e^2\pi^7 + e$?

Apply Schanuel's Conjecture with $\alpha_1 = 1$ and $\alpha_2 = i\pi$:

$$\{1, i\pi, e^1, e^{i\pi}\} = \{1, i\pi, e, -1\}$$

So (assuming Schanuel's Conjecture), $\beta_1 = i\pi$ and $\beta_2 = e$ must be algebraically independent, and therefore $\pi$ and $e$ must be algebraically independent.

Thus for *any* non-zero polynomial $P(x, y)$ with rational (or algebraic) coefficients, we have that $P(e, \pi)$ cannot be zero.

Therefore $e + \pi$, $e\pi$, and $e^5\pi^3 - e^2\pi^7 + e$ must all be irrational (in fact, transcendental).

# Zero Isolation

**Lemma (Zero Isolation)**

*Assuming the p-adic Schanuel Conjecture, given a bi-infinite LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ one can compute $L$ such that $u_{Ln} \neq 0$ for all $n \neq 0$.*

# Zero Isolation

**Lemma (Zero Isolation)**

*Assuming the p-adic Schanuel Conjecture, given a bi-infinite LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ one can compute $L$ such that $u_{Ln} \neq 0$ for all $n \neq 0$.*

- Solve the equation $x^2 - 5 = 0$ in 11-adic integers $\mathbb{Z}_{11}$

$$\sqrt{5} = 4 + 4 \cdot 11 + 10 \cdot 11^2 + \cdots$$

# Zero Isolation

**Lemma (Zero Isolation)**

*Assuming the p-adic Schanuel Conjecture, given a bi-infinite LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ one can compute $L$ such that $u_{Ln} \neq 0$ for all $n \neq 0$.*

- Solve the equation $x^2 - 5 = 0$ in 11-adic integers $\mathbb{Z}_{11}$

$$\sqrt{5} = 4 + 4 \cdot 11 + 10 \cdot 11^2 + \cdots$$

- Binet formula

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

makes sense in $\mathbb{Z}_{11}$

# Zero Isolation

**Lemma (Zero Isolation)**

*Assuming the p-adic Schanuel Conjecture, given a bi-infinite LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ one can compute $L$ such that $u_{Ln} \neq 0$ for all $n \neq 0$.*

- Solve the equation $x^2 - 5 = 0$ in 11-adic integers $\mathbb{Z}_{11}$

$$\sqrt{5} = 4 + 4 \cdot 11 + 10 \cdot 11^2 + \cdots$$

- Binet formula

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

  makes sense in $\mathbb{Z}_{11}$

- Extend to analytic function $f : \mathbb{Z}_{11} \to \mathbb{Z}_{11}$.

# Zero Isolation

**Lemma (Zero Isolation)**

*Assuming the p-adic Schanuel Conjecture, given a bi-infinite LRS $\langle u_n \rangle_{n=-\infty}^{\infty}$ one can compute $L$ such that $u_{Ln} \neq 0$ for all $n \neq 0$.*

- Solve the equation $x^2 - 5 = 0$ in 11-adic integers $\mathbb{Z}_{11}$

$$\sqrt{5} = 4 + 4 \cdot 11 + 10 \cdot 11^2 + \cdots$$

- Binet formula

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

  makes sense in $\mathbb{Z}_{11}$

- Extend to analytic function $f : \mathbb{Z}_{11} \to \mathbb{Z}_{11}$.
- There is a punctuated disk around zero in which $f$ is non-zero.

# Decision Procedure for the Skolem Problem

**Theorem (Bilu, Luca, Nieuwveld, Ouaknine, Pursar, W., 22)**

*There is a decision procedure for the Skolem Problem for simple LRS that terminates subject to the p-adic Schanuel Conjecture and the Skolem Conjecture.*

# Decision Procedure for the Skolem Problem

**Theorem (Bilu, Luca, Nieuwveld, Ouaknine, Pursar, W., 22)**

*There is a decision procedure for the Skolem Problem for simple LRS that terminates subject to the p-adic Schanuel Conjecture and the Skolem Conjecture.*

- Search in parallel for a zero or a “modulo witness” of no zeroes.

# Decision Procedure for the Skolem Problem

**Theorem (Bilu, Luca, Nieuwveld, Ouaknine, Pursar, W., 22)**

*There is a decision procedure for the Skolem Problem for simple LRS that terminates subject to the p-adic Schanuel Conjecture and the Skolem Conjecture.*

- Search in parallel for a zero or a "modulo witness" of no zeroes.
- If a zero is found, use Zero-Isolation Lemma to split input into subsequences and then recurse

# Decision Procedure for the Skolem Problem

**Theorem (Bilu, Luca, Nieuwveld, Ouaknine, Pursar, W., 22)**

*There is a decision procedure for the Skolem Problem for simple LRS that terminates subject to the p-adic Schanuel Conjecture and the Skolem Conjecture.*

- Search in parallel for a zero or a "modulo witness" of no zeroes.
- If a zero is found, use Zero-Isolation Lemma to split input into subsequences and then recurse
- Output is a list of zeroes and certificate that there are no more zeroes

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} =
-271613116171209744858663520558946347040150955089064191363633545467540976915
1} +
-508757179425530608464927613320696582397187501636529439512475357072393244955
2} +
-102066400158641189915199426519447202492215998409667435547930568677820080526
3} +
-141209566240600031036449671518126066729890157506482293126851759080465437598
4} +
190695589477320710360984265894091422375694233909158701965446106943727346702
5} +
```