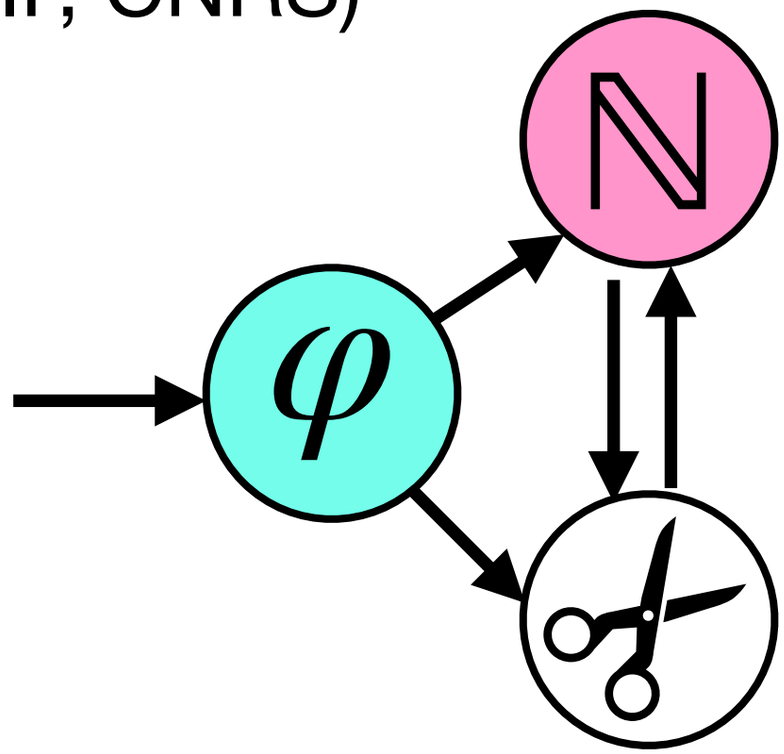
On the Monadic Second-Order Theory of Arithmetic Predicates

- Valérie Berthé (Université de Paris, IRIF, CNRS)
- Toghrul Karimov (MPI-SWS)
- Joris Nieuwveld (MPI-SWS)
- Joël Ouaknine (MPI-SWS)
- **Mihir Vahanwala (MPI-SWS)**
- James Worrell (University of Oxford)



SymDynAr Workshop, Roscoff
September 2024

Research questions can often be exposed through playful riddles

Are there infinitely many n, m such that:

1. n is a power of 3; m is a power of 2
2. The units place digits of n, m are $9, 8$ respectively
3. m is the smallest power of 2 larger than n, and their difference is at least 100

$$n = 4782969, m = 8388608$$

… ?

The riddle is an example of
how we can push the expressive limits of
Monadic Second-Order (MSO) Theory of
the natural numbers with order

$$\langle \mathbb{N}; < \rangle$$

But what is MSO Logic?

(over the structure of the natural numbers with order)

Statements in MSO logic have two kinds of variables: those that refer to numbers, and those that refer to sets of numbers

So why is MSO Logic important?

To practitioners:
for its ability to serve as a framework to reason about systems' execution traces

To theoreticians:
for its profound connections to formal language theory, and its place at the frontiers of decidability

Our research question

What expressive power can be added to the MSO Theory of the natural numbers with order while retaining its decidability?

MSO Theory of $\langle \mathbb{N}; < \rangle$

$$x = y$$

$$\neg(x < y) \wedge \neg(y < x)$$

MSO Theory of $\langle \mathbb{N}; < \rangle$

$$x = 0$$

$$\forall y \,.\, x \leq y$$

$$y = x+1$$

$$x < y \wedge \neg \exists z \,.\, (x < z < y)$$

MSO Theory of $\langle \mathbb{N}; < \rangle$

Variables can refer to numbers $x, y, \ldots$
or to sets $X, Y, \ldots$ of numbers

The logic allows us to express that
x is an element of X

X is the empty set

$$\forall y \,.\, y \notin X$$

MSO Theory of $\langle \mathbb{N}; < \rangle$

$$X \subseteq Y$$

$$\forall x \,.\, (x \in X \Rightarrow x \in Y)$$

X has infinitely many elements

$$\forall x \,.\, \exists y \,.\, (x < y \wedge y \in X)$$

MSO Theory of $\langle \mathbb{N}; < \rangle$

Second-Order variables $X, Y, \ldots$ allow us to define some interesting unary *predicates*

x is even

$$\exists X\,.\,(x \in X \wedge 0 \in X \wedge \forall y\,.\,(y \in X \Leftrightarrow y{+}1 \notin X))$$

MSO Theory of $\langle \mathbb{N}; < \rangle$: Sentences

Variables occurring in a formula are either free or bound to a quantifier

A formula with only bound variables is called a **sentence**

$$\forall X \,.\, (\exists x \,.\, x \in X) \Rightarrow \big(\exists x \,.\, x \in X \wedge \forall y \,.\, (y \in X \Rightarrow x \leq y)\big)$$

Every non-empty set has a minimum element

Deciding an MSO Theory

$$\forall X \,.\, (\exists x \,.\, x \in X) \Rightarrow \big(\exists x \,.\, x \in X \wedge \forall y \,.\, (y \in X \Rightarrow x \leq y)\big)$$

Every non-empty set has a minimum element

Büchi (1962) showed how to decide:

Context	MSO Theory of $\langle \mathbb{N}; < \rangle$
Input	A sentence
Output	Whether the input sentence is true

Büchi's work

Expanding the MSO Theory of $\langle \mathbb{N}; < \rangle$

However, the expressive power is not enough to assert, for instance:

x is a perfect square

x is a power of 2

Adding such predicates results in an expanded theory $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$

Deciding expanded MSO Theories
[Elgot and Rabin, 1966]

It is known how to decide:

Context	MSO Theory of $\langle \mathbb{N}; <, \mathrm{Pow}_2 \rangle$
Input	A sentence
Output	Whether the input sentence is true

and also:

Context	MSO Theory of $\langle \mathbb{N}; <, \mathrm{Pow}_3 \rangle$
Input	A sentence
Output	Whether the input sentence is true

State of the art

[Carton and Thomas, 2002]

Sentence in MSO Theory of

$$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$$

There are infinitely many n, m such that:

$$\forall x \exists n \exists m \,.\, x < n < m \wedge \ldots$$

n is a power of 3; m is a power of 2

$$n \in \mathrm{Pow}_3 \wedge m \in \mathrm{Pow}_2 \wedge \ldots$$

The units place digits of n, m are of $9, 8$ respectively

$$n \in \mathrm{Units}_9 \wedge m \in \mathrm{Units}_8 \wedge \ldots$$

m is the smallest power of 2 larger than n,
and their difference is at least 100

$$(n+100 \leq m) \wedge \neg \exists k \,.\, (k \in \mathrm{Pow}_2 \wedge n < k < m)$$

We show that…

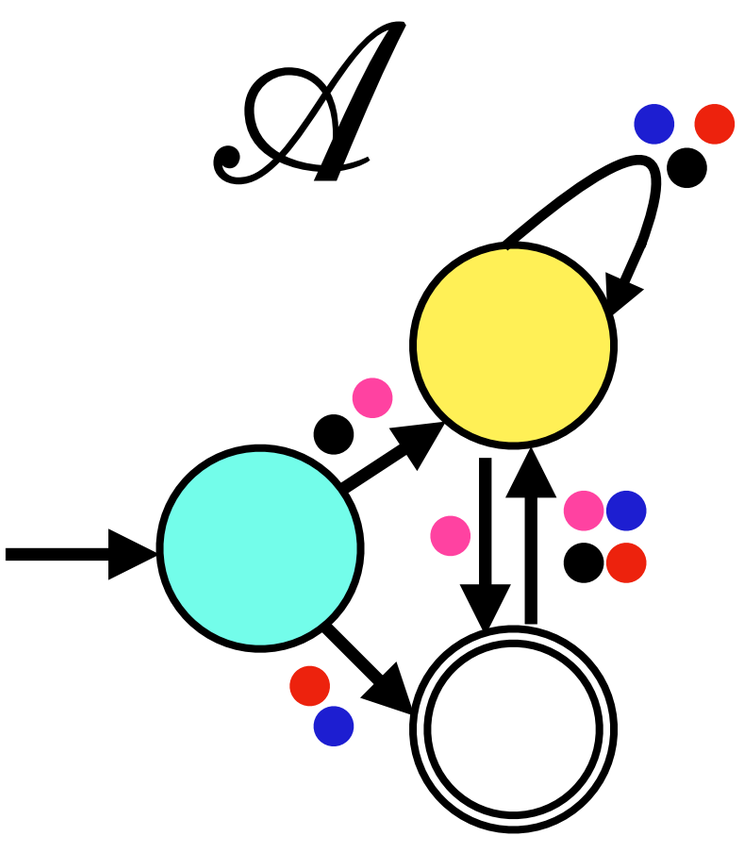
The MSO Theory of $\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$ is decidable.

Context	MSO Theory of $\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$
Input	A sentence
Output	Whether the input sentence is true

Our contribution

Sentence holds in Theory

$$\varphi \qquad \langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$$



Turing-equivalent

Due to Büchi, McNaughton, …

$$\begin{array}{ccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \binom{0}{0} & \binom{1}{1} & \binom{1}{0} & \binom{0}{1} & \binom{1}{0} & \binom{0}{0} & \binom{0}{0} & \binom{0}{0} & \binom{1}{0} & \binom{0}{1} & \binom{0}{0} \end{array} \ldots$$

Automaton accepts characteristic word

Characteristic word

$$\alpha = \binom{0}{0}\binom{1}{1}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{0}{0}\binom{0}{0}\binom{0}{0}\binom{1}{0}\binom{0}{1}\binom{0}{0}\ldots$$

Acceptance Problem

$\mathrm{Acc}_\alpha :=$ Does the run of a given automaton $\mathscr{A}$ on α visit state q infinitely often?

trivially reduces to ↑

↓ when is this reduction possible?

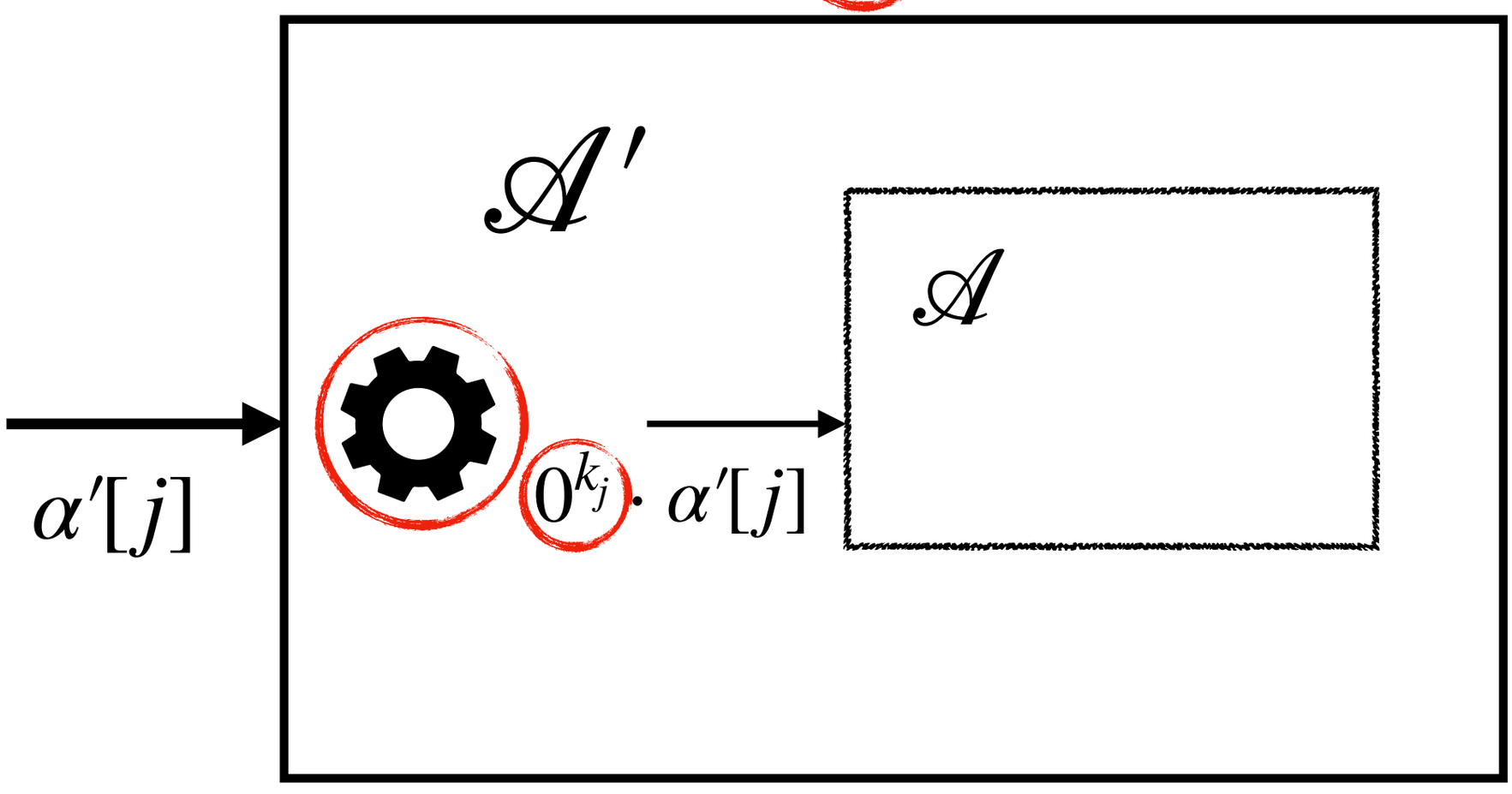
$\mathrm{Acc}_{\alpha'}$

Order word

$$\alpha' = \binom{1}{1}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{1}{0}\binom{0}{1}\ldots$$

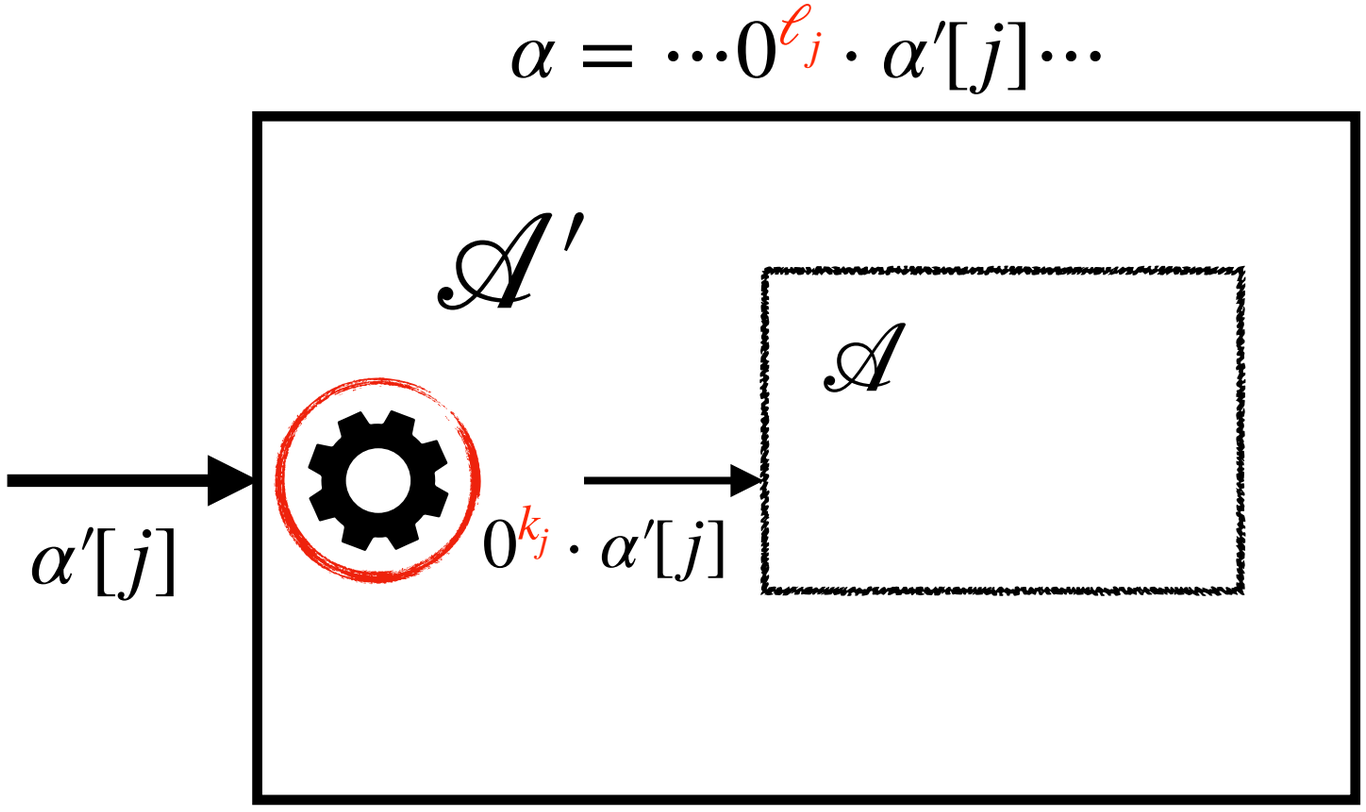
Reduction: Idea

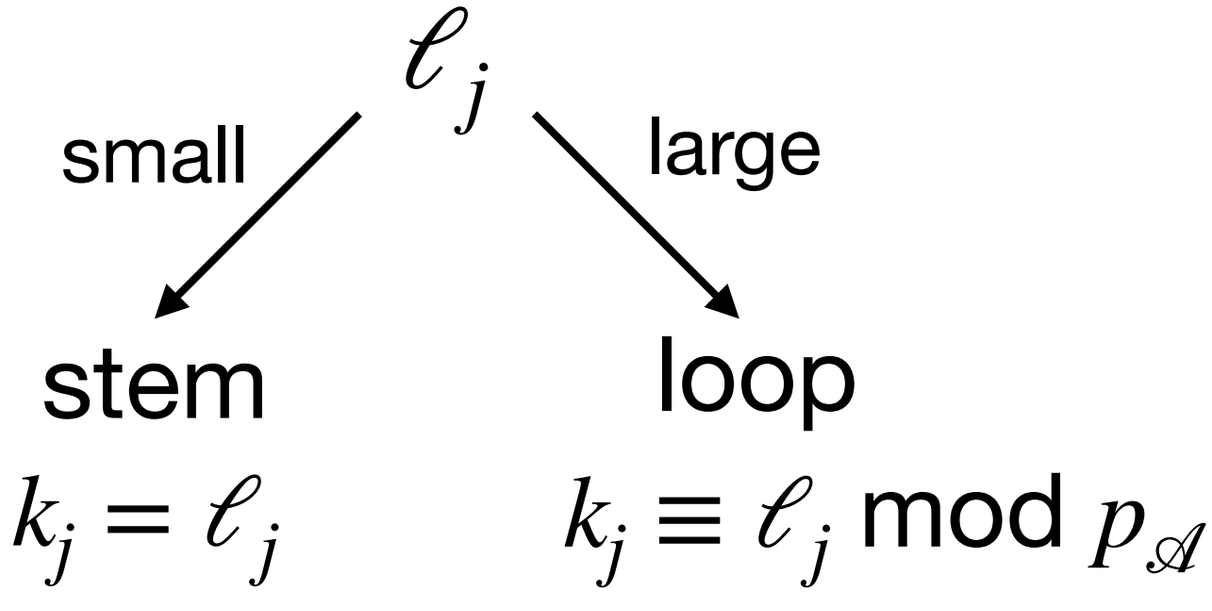
$$\alpha = \cdots 0^{\ell_j} \cdot \alpha'[j] \cdots$$

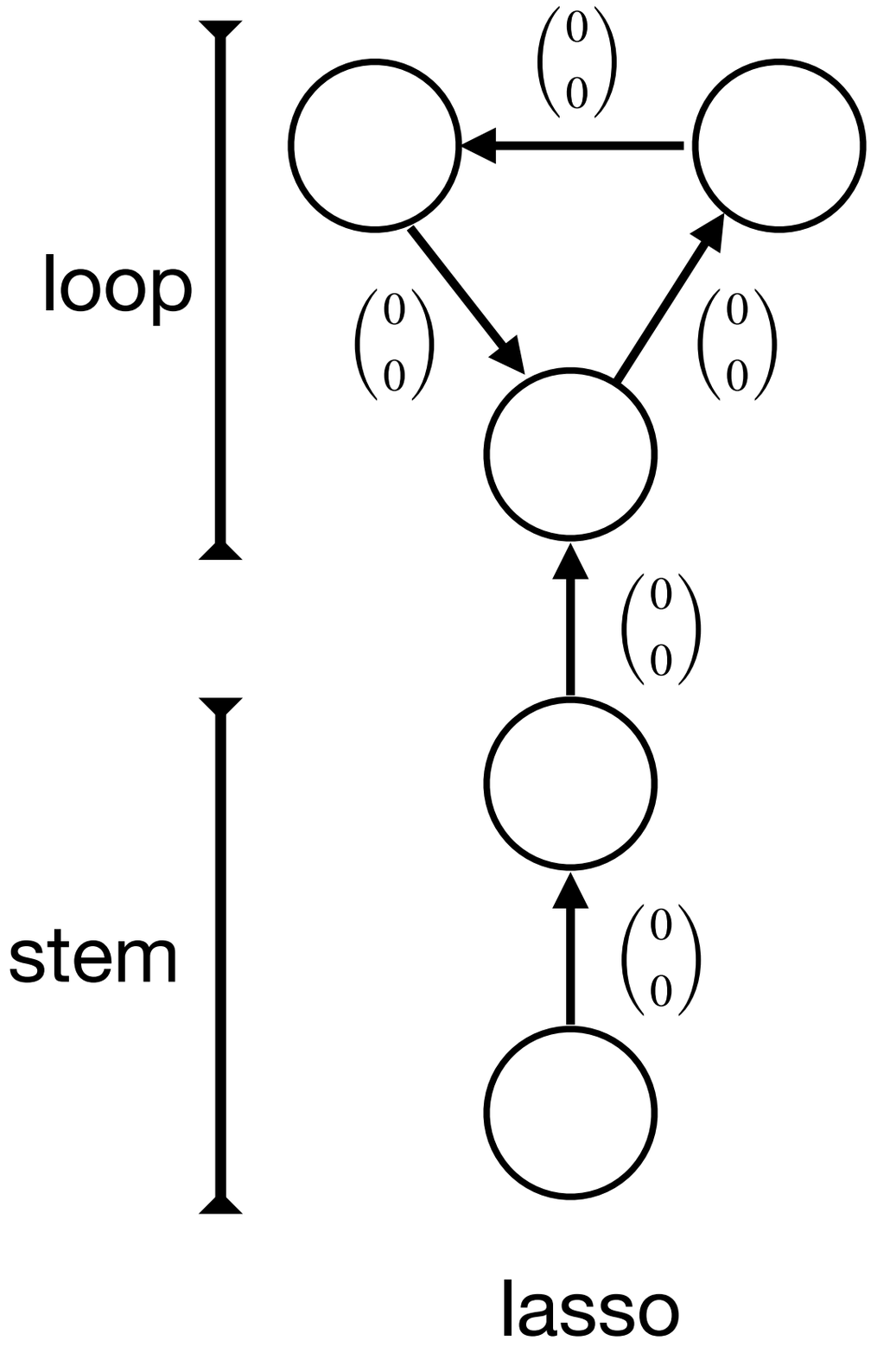


Construct $\mathscr{A}'$ such that the run of $\mathscr{A}'$ on α' simulates the run of $\mathscr{A}$ on α

Automata are inherently periodic







Our predicates are sparse

For our predicates,
we can compute $n_{\mathscr{A}}$ such that for all $j \geq n_{\mathscr{A}}$,
ℓ_j is large enough to enter a loop in $\mathscr{A}$

Corollary of Baker's Theorem

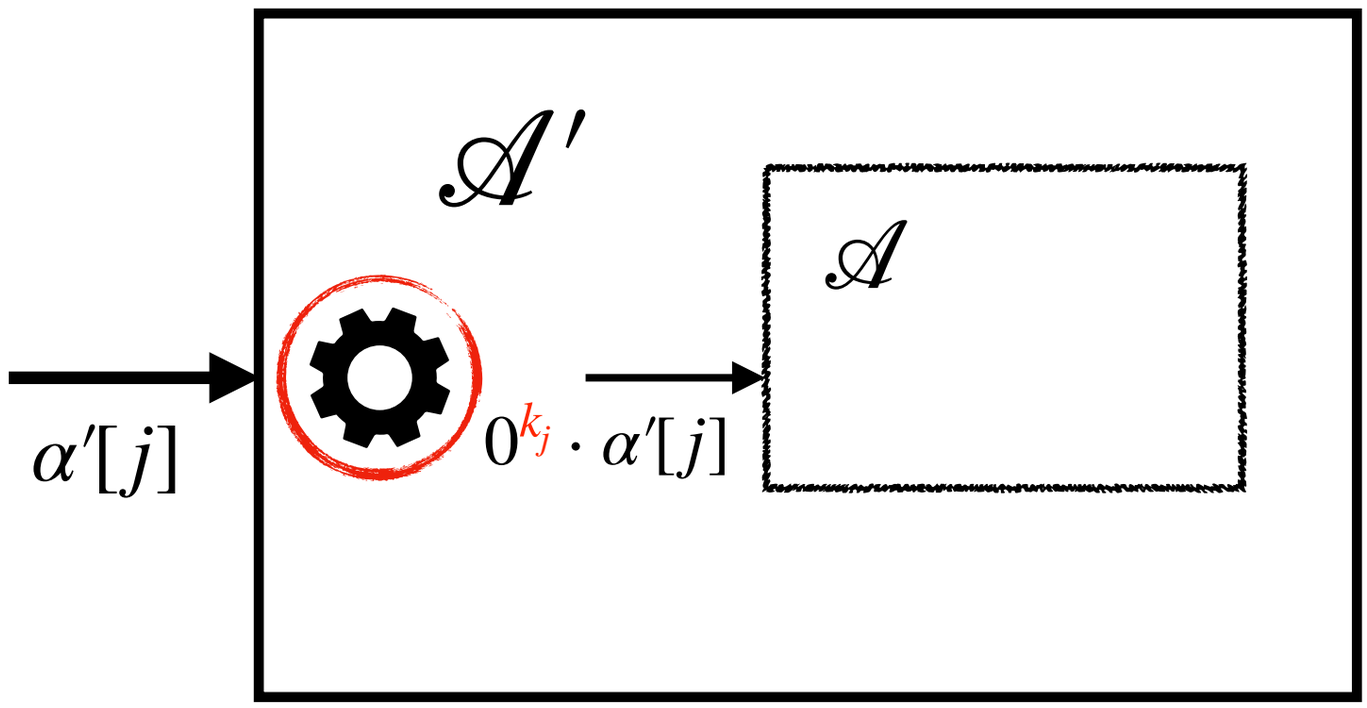
For all $N \in \mathbb{N}$, the inequality in n, m

$$|2^n - 3^m| \leq N$$

has finitely many solutions which can moreover be effectively enumerated.

The simulation only needs modular arithmetic

$$\alpha = \cdots 0^{\ell_j} \cdot \alpha'[j] \cdots$$



ℓ_j

small → stem

$k_j = \ell_j$

first $n_{\mathscr{A}}$ blocks

large → loop

$k_j \equiv \ell_j \bmod p_{\mathscr{A}}$

infinite suffix

Our predicates are periodic

As an example, let $p_{\mathscr{A}} = 10$

What remainders do the powers of 2
leave when divided by 10?

$(1, 2, 4, 8, 16, 32, 64, 128, 256, \ldots)$

Remainders eventually cycle between $2, 4, 8, 6$

Similarly, remainders left by the powers of 3
cycle between $1, 3, 9, 7$

The pattern is eventually periodic for any $p_{\mathscr{A}}$

We use this to track ℓ_j mod $p_{\mathscr{A}}$

How do we track ℓ_j mod $p_{\mathscr{A}}$? $\alpha = \cdots 0^{\ell_j} \cdot \alpha'[j] \cdots$

We keep track of:

A) The remainder left by the last seen power of 2
e.g. $512 \equiv 2 \bmod 10$

B) The remainder left by the last seen power of 3
e.g. $729 \equiv 9 \bmod 10$

C) The remainder left by the last seen letter $\alpha'[j-1]$
e.g. $729 \equiv 9 \bmod 10$

Upon reading the current letter $\alpha'[j]$:

1) The letter indicates whether it is a power of 2 or 3
e.g. $1024 = 2^{10}$

2) Our memory lets us deduce its remainder
e.g. $1024 \equiv 4 \bmod 10$, because 4 follows 2 in the cycle

3) Our memory lets us deduce ℓ_j mod $p_{\mathscr{A}}$
e.g. $\ell_j \equiv (4 - 9 - 1) \bmod 10 \equiv 4 \bmod 10$

Characteristic word

$$\alpha = \binom{0}{0}\binom{1}{1}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{0}{0}\binom{0}{0}\binom{0}{0}\binom{1}{0}\binom{0}{1}\binom{0}{0}\ldots$$

Acceptance Problem

$\mathrm{Acc}_\alpha :=$ Does the run of a given automaton $\mathscr{A}$ on α visit state q infinitely often?

trivially reduces to ↑

↓ when is this reduction possible?

↓ predicates periodic and sparse

$\mathrm{Acc}_{\alpha'}$

Order word

$$\alpha' = \binom{1}{1}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{1}{0}\binom{0}{1}\ldots$$

Deciding whether…

A given sentence holds in a theory

Turing-equivalent

A given automaton accepts the characteristic word

Turing-equivalent for sparse, periodic predicates

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_6 \rangle$

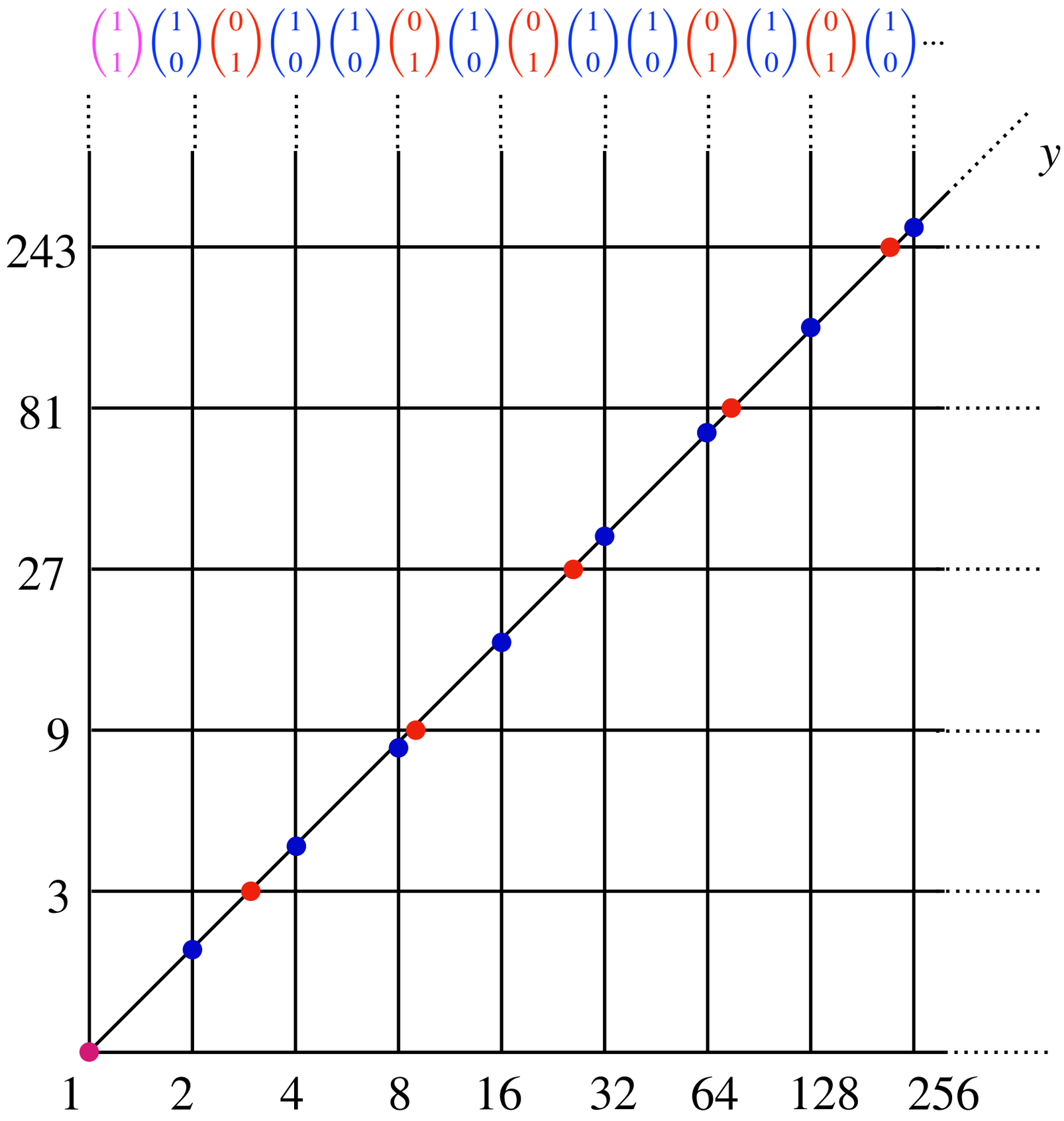
$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Fibonacci} \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_5 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Squares} \rangle$

A given automaton accepts the order word

Our order word is a cutting sequence



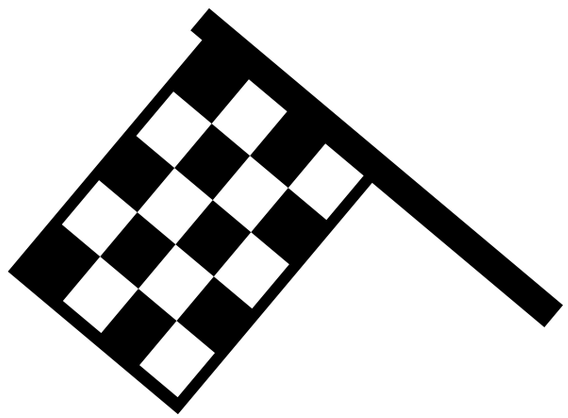
Cutting sequences are almost-periodic: a crucial combinatorial property

For every finite word w, there exists $R \in \mathbb{N}$ such that either:

1) w does not occur in the suffix $\alpha'[R\ldots]$

2) For all $j \in \mathbb{N}$, w occurs in the segment $\alpha'[j\ldots(j+R)]$

Our α' is effectively almost-periodic, because we can compute $R(w)$



Theorem (Semenov)

If α' is effectively almost-periodic, then $\mathrm{Acc}_{\alpha'}$ is decidable.

Deciding whether…

A given sentence holds in a theory

Turing-equivalent

A given automaton accepts the characteristic word

Turing-equivalent for sparse, periodic predicates

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_6 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Fibonacci} \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_5 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Squares} \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Factorials} \rangle$

A given automaton accepts the order word

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_6 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Fibonacci} \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_5 \rangle$ *

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Squares} \rangle$ * *

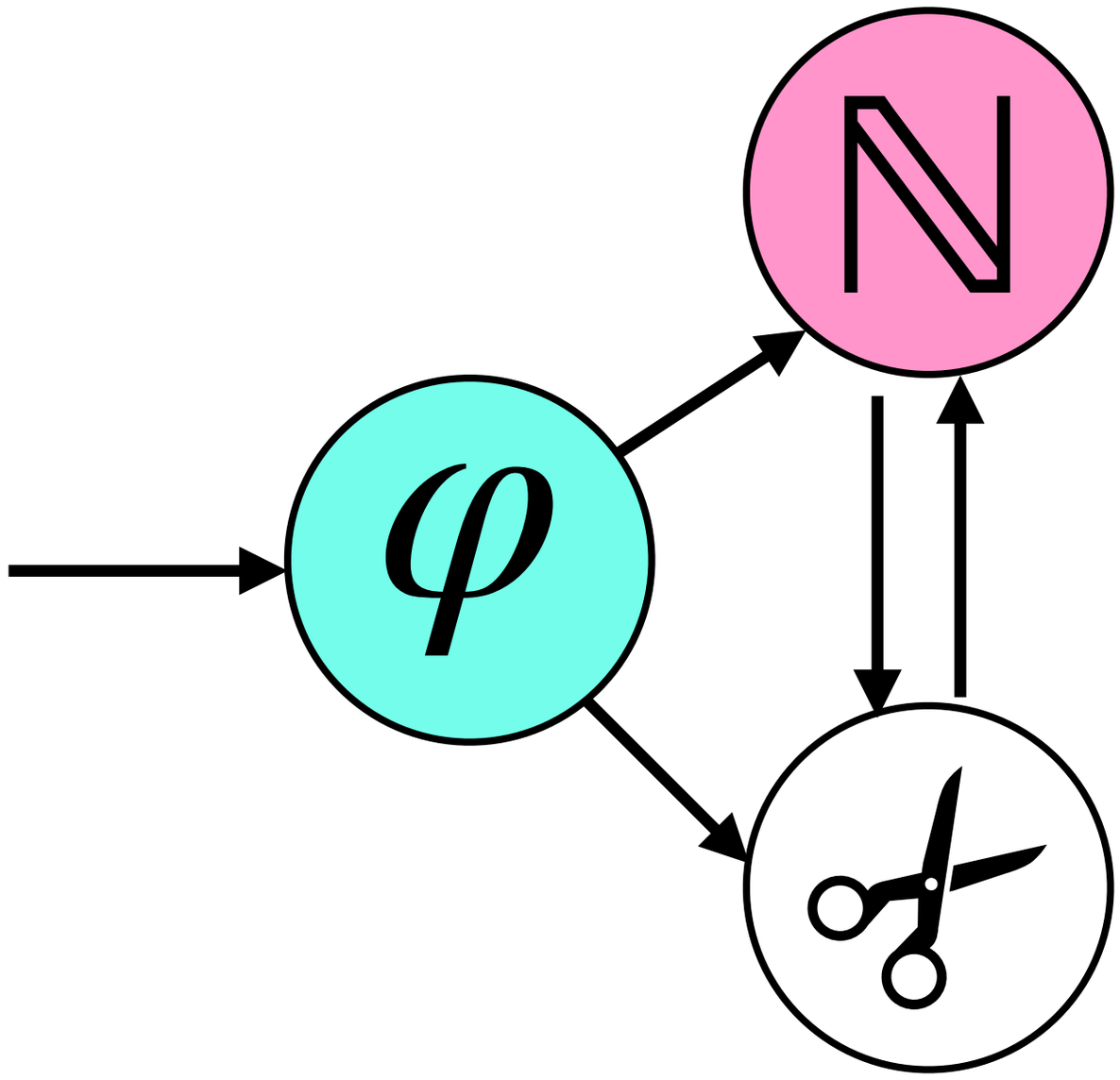
$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Factorials} \rangle$?

* Subject to Schanuel's conjecture

* Assuming the binary expansion of $\sqrt{2}$ is weakly normal

Our contribution

Thank You!



Thank You!

A given sentence holds in a theory

Turing-equivalent

A given automaton accepts the characteristic word

Turing-equivalent for sparse, periodic predicates

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_6 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Fibonacci} \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_5 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Squares} \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Factorials} \rangle$

A given automaton accepts the order word

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_6 \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Fibonacci} \rangle$

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3, \mathrm{Pow}_5 \rangle$ *

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Squares} \rangle$ * *

$\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Factorials} \rangle$?

* Subject to Schanuel's conjecture

* Assuming the binary expansion of $\sqrt{2}$ is weakly normal

Thank You!

Combinatorics

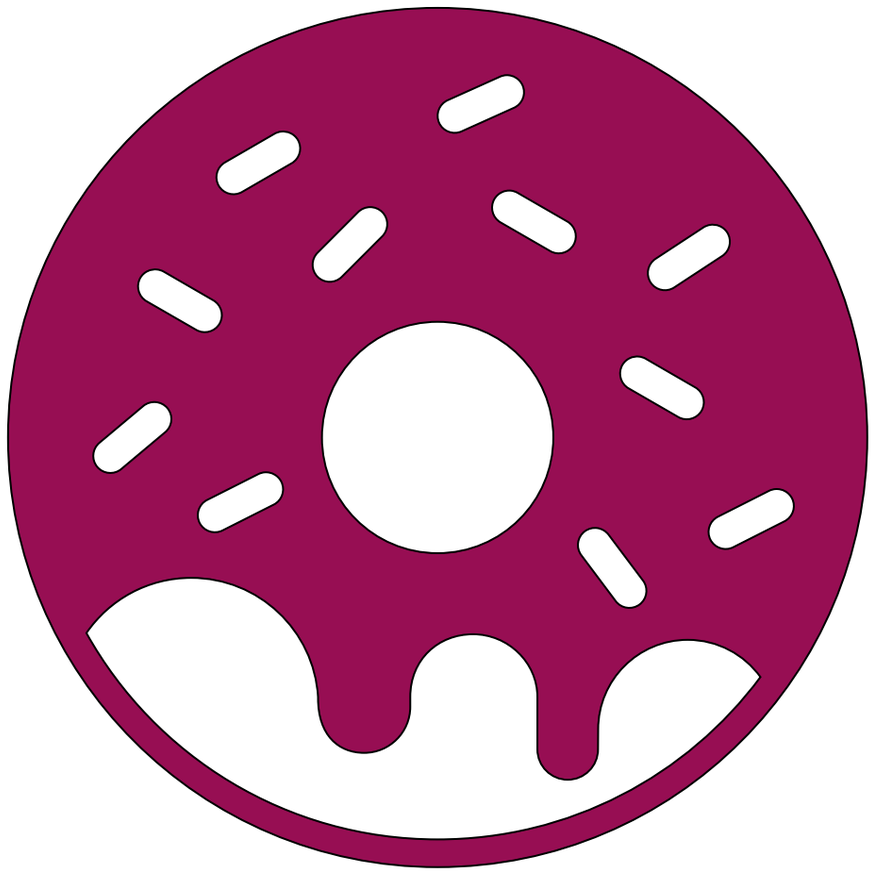
Dynamical Systems

Number Theory

Algebra

Automata

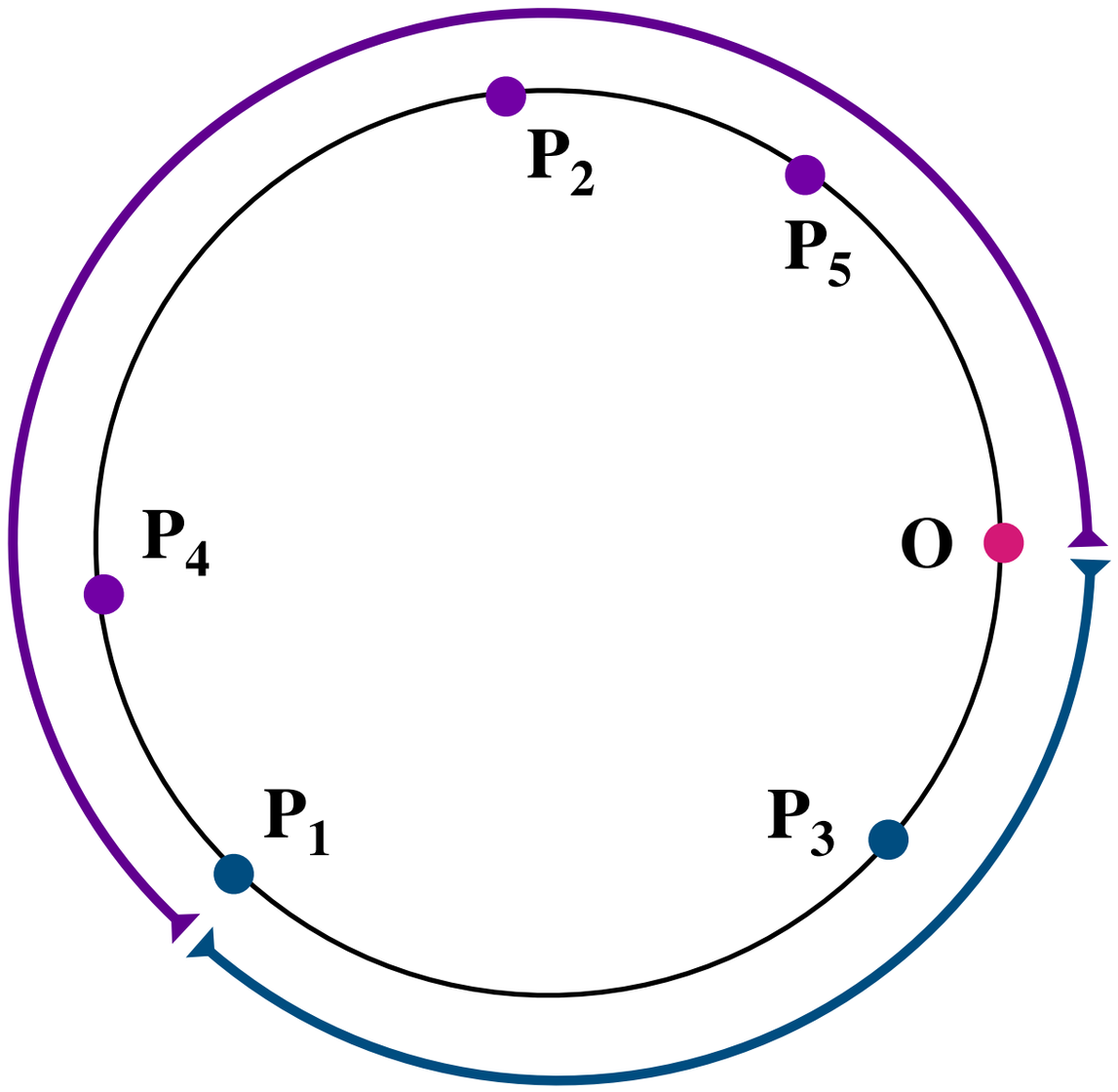
We need a donut.



More technically, a torus

Order word through a compact dynamical system

A point starts at $\mathbf{O}$ and travels around torus in steps of $\log_3 2$



Number line perspective

one revolution $\equiv$ triple the number

arc $\theta \equiv 3^\theta \times$

one step $\equiv$ double the number

trajectory $\equiv$ powers of 2

cross $\mathbf{O} \equiv$ cross a power of 3

purple arc $\equiv \binom{0}{1}\binom{1}{0}$

blue arc $\equiv \binom{1}{0}$

$\binom{1}{1} \cdot \binom{1}{0} \cdot \binom{0}{1}\binom{1}{0} \cdot \binom{1}{0} \cdot \binom{0}{1}\binom{1}{0} \cdot \binom{0}{1}\binom{1}{0} \cdots$