

# The universal algorithm and arithmetic potentialism

Kameryn J. Williams

University of Hawai'i at Mānoa

Analysis, Logic, and Physics Seminar  
Virginia Commonwealth University  
2020 October 30



# Undecidability

- In the 1930s Alan Turing formalized the concept of **algorithm**, as part of a project investigating the limits of computability. Others gave equivalent formalizations, but it is the **Turing machine** which has become the standard in computability theory.

# Undecidability

- In the 1930s Alan Turing formalized the concept of **algorithm**, as part of a project investigating the limits of computability. Others gave equivalent formalizations, but it is the **Turing machine** which has become the standard in computability theory.
- One advantage of talking about this in 2020 is you all have experience with computers, so you don't need to see the definition. You can think of Turing machines as your favorite programming language (abstracting away things like limited memory).

# Undecidability

- In the 1930s Alan Turing formalized the concept of **algorithm**, as part of a project investigating the limits of computability. Others gave equivalent formalizations, but it is the **Turing machine** which has become the standard in computability theory.
- One advantage of talking about this in 2020 is you all have experience with computers, so you don't need to see the definition. You can think of Turing machines as your favorite programming language (abstracting away things like limited memory).
- Turing showed that there are some questions which are **undecidable**—there is no algorithm to decide all instances.

# Undecidability

- In the 1930s Alan Turing formalized the concept of **algorithm**, as part of a project investigating the limits of computability. Others gave equivalent formalizations, but it is the **Turing machine** which has become the standard in computability theory.
- One advantage of talking about this in 2020 is you all have experience with computers, so you don't need to see the definition. You can think of Turing machines as your favorite programming language (abstracting away things like limited memory).
- Turing showed that there are some questions which are **undecidable**—there is no algorithm to decide all instances. For example:
  - Does a Turing machine halt on a given input?
  - Hilbert's *Entscheidungsproblem*. (Turing, Church)
  - Does a Diophantine equation have an integer solution? (MRDP theorem)

# The incompleteness theorems

# The incompleteness theorems

**Peano arithmetic** (PA) axiomatizes natural number arithmetic: axioms of discretely ordered semirings + induction axioms.

## Theorem (Gödel's first and second incompleteness theorems)

- 1 *No computably axiomatizable extension of PA is complete. There must be an arithmetic statement it neither proves nor disproves.*
- 2 *PA can neither prove nor disprove the consistency of PA.*

# The incompleteness theorems

**Peano arithmetic** (PA) axiomatizes natural number arithmetic: axioms of discretely ordered semirings + induction axioms.

## Theorem (Gödel's first and second incompleteness theorems)

- 1 *No computably axiomatizable extension of PA is complete. There must be an arithmetic statement it neither proves nor disproves.*
  - 2 *PA can neither prove nor disprove the consistency of PA.*
- **Hard part!** (Arithmetization) Gödel showed that logical formulae can be coded as natural numbers, so statements about logic and proof can be coded as statements about natural numbers.
  - **Easy part!** (Self-reference) Do a diagonalization argument.



# The incompleteness theorems

**Peano arithmetic** (PA) axiomatizes natural number arithmetic: axioms of discretely ordered semirings + induction axioms.

## Theorem (Gödel's first and second incompleteness theorems)

- 1 No *computably axiomatizable* extension of PA is complete. There must be an arithmetic statement it neither proves nor disproves.
  - 2 PA can neither prove nor disprove the consistency of PA.
- **Hard part!** (Arithmetization) Gödel showed that logical formulae can be coded as natural numbers, so statements about logic and proof can be coded as statements about natural numbers.
  - **Easy part!** (Self-reference) Do a diagonalization argument.

We need the restriction. True arithmetic TA—the set of all truths of  $\mathbb{N}$ —is a complete extension of PA.

(Moreover, the **low basis theorem** implies that there are complete extensions of PA which are arithmetically definable, specifically,  $\Delta_2$  in the arithmetical hierarchy.)

# Arithmetization

- Gödel's beta lemma states that arbitrary finite sequences can be coded as a single number, and this is provable within PA.
- Thus any finite mathematical object can be coded in arithmetic.
- Relevant to this talk, objects like Turing machines or logical formulae can be coded in arithmetic.
- And so statements like “PA does not prove  $0 = 1$ ” or “such and such Turing machine halts” can be cast as statements in arithmetic.

# Arithmetization

0 substituted for  $[s]_0$ , and  $\varphi$  with  $[s]_0 + 1$  substituted for  $[s]_0$ . Now for the gory details. We define the relation  $\text{PA}(x)$ , expressing that  $x$  is the Gödel-number of a Peano axiom by the formula

$$x = n_1 \vee \dots \vee x = n_{15} \vee \left( \exists y, s \subseteq x \exists n \leq s \left( \begin{array}{l} \text{Form}(y) \wedge \text{len}(s) = n \wedge \\ \forall i < \text{len}(n) \text{Free}(y, [s]_i) \wedge \forall j \leq y (\text{Free}(y, j) \rightarrow \exists k \leq s [s]_k = j) \wedge \\ \exists t \subseteq s \exists u, w \left( \begin{array}{l} \text{len}(t) = \text{len}(s) - 1 \wedge \forall i < \text{len}(t) [t]_i = [s]_{i+1} \wedge \\ u = \text{Sub}(y, [s]_0, \ulcorner 0 \urcorner) \wedge w = \text{Sub}(y, [s]_0, \ulcorner [s]_0 + 1 \urcorner) \wedge \\ x = \ulcorner (\forall t (u \wedge (\forall [s]_0 (y \rightarrow w) \rightarrow \forall [s]_0 y)) \urcorner) \end{array} \right) \end{array} \right) \right).$$

(Taken with permission from Victoria Gitman's lecture notes for Mathematical Logic, Spring 2013.)

# Self-reference

- The **Gödel fixed-point lemma** states that a form of self-reference is possible for logical formulae.

(Formally: for any formula  $\varphi(x)$  there's a sentence  $\sigma$  so that  $\sigma$  is PA-provably equivalent to  $\varphi(\sigma)$ .)

# Self-reference

- The **Gödel fixed-point lemma** states that a form of self-reference is possible for logical formulae.

(Formally: for any formula  $\varphi(x)$  there's a sentence  $\sigma$  so that  $\sigma$  is PA-provably equivalent to  $\varphi(\sigma)$ .)

- You can now prove a form of the first incompleteness theorem by considering  $\sigma$  PA-provably equivalent to “ $\sigma$  is not PA-provable”.

# Self-reference

- The **Gödel fixed-point lemma** states that a form of self-reference is possible for logical formulae.

(Formally: for any formula  $\varphi(x)$  there's a sentence  $\sigma$  so that  $\sigma$  is PA-provably equivalent to  $\varphi(\sigma)$ .)

- You can now prove a form of the first incompleteness theorem by considering  $\sigma$  PA-provably equivalent to “ $\sigma$  is not PA-provable”.
- Suppose PA proves  $\sigma$ . Then PA proves that  $\sigma$  is not provable. Whence PA does not prove  $\sigma$ .  $\nexists$

Suppose PA proves  $\neg\sigma$ . Then PA proves that  $\sigma$  is provable. Whence PA does prove  $\sigma$ .  $\nexists$

(You need an additional lemma for those whences, one we will see on Slide 13. If you've heard of “ $\omega$ -consistency”, this is where it shows up.)

# Self-reference

- The **Gödel fixed-point lemma** states that a form of self-reference is possible for logical formulae.

(Formally: for any formula  $\varphi(x)$  there's a sentence  $\sigma$  so that  $\sigma$  is PA-provably equivalent to  $\varphi(\sigma)$ .)

- You can now prove a form of the first incompleteness theorem by considering  $\sigma$  PA-provably equivalent to “ $\sigma$  is not PA-provable”.
- Suppose PA proves  $\sigma$ . Then PA proves that  $\sigma$  is not provable. Whence PA does not prove  $\sigma$ .  $\nexists$

Suppose PA proves  $\neg\sigma$ . Then PA proves that  $\sigma$  is provable. Whence PA does prove  $\sigma$ .  $\nexists$

(You need an additional lemma for those whences, one we will see on Slide 13. If you've heard of “ $\omega$ -consistency”, this is where it shows up.)

Some people say the incompleteness theorems are difficult to prove. But if you handwave over the actual hard parts you can fit the proof on one slide. :)

# Self-reference

- Also have self-reference for computability theory, via the **Kleene recursion theorem**. Informally, Turing machines can refer to themselves.

(Formally: for any partial computable function  $F(x, y)$  there's a TM  $p$  so that  $p$  computes the function  $y \mapsto F(p, y)$ .)



# Self-reference

- Also have self-reference for computability theory, via the **Kleene recursion theorem**. Informally, Turing machines can refer to themselves.

(Formally: for any partial computable function  $F(x, y)$  there's a TM  $p$  so that  $p$  computes the function  $y \mapsto F(p, y)$ .)

A fun application: programming languages admit **quines**—programs that output their own source code.

```
;; Quine in Common Lisp
((lambda (x) (list x (list 'quote x))))
'(lambda (x) (list x (list 'quote x))))
```

# Incompleteness and Turing machines

The incompleteness theorems can be recast as saying that whether certain Turing machines halt is undecidable.

A TM  $p$ :

- Look at all length 1 proofs from the first 1 axiom of PA.
- Then look at all length 2 proofs from the first 2 axioms of PA.
- $\vdots$
- If at any point you see a proof that ends with  $0 = 1$ , halt and output affirmatively.

Whether  $p$  halts is independent of PA.

# Incompleteness and Turing machines

The incompleteness theorems can be recast as saying that whether certain Turing machines halt is undecidable.

A TM  $p$ :

- Look at all length 1 proofs from the first 1 axiom of PA.
- Then look at all length 2 proofs from the first 2 axioms of PA.
- $\vdots$
- If at any point you see a proof that ends with  $0 = 1$ , halt and output affirmatively.
- Adam Yedidia and Scott Aaronson do even better.
- They constructed a TM of size 7910 so that whether it halts is independent of ZFC, but ZFC + large cardinals does prove it halts.  
(Specifically an ineffable cardinal will do.)

Whether  $p$  halts is independent of PA.

# If you liked Gödel's incompleteness theorems, you'll love his completeness theorem

## Theorem (Gödel's Completeness Theorem)

- 1 *A set of axioms  $T$  is consistent if and only if there is a structure satisfying  $T$ .*
- 2  *$\varphi$  is true in every structure satisfying  $T$  if and only if  $\varphi$  is a theorem of  $T$ .*

*(This is for axioms in first-order logic.)*

- This lets us translate talk about proofs, consistency, etc. to talk about structures.
- The incompleteness theorems plus the completeness theorem together imply there must be non-isomorphic structures satisfying the axioms of arithmetic.

# If you liked Gödel's incompleteness theorems, you'll love his completeness theorem

## Theorem (Gödel's Completeness Theorem)

- 1 *A set of axioms  $T$  is consistent if and only if there is a structure satisfying  $T$ .*
- 2  *$\varphi$  is true in every structure satisfying  $T$  if and only if  $\varphi$  is a theorem of  $T$ .*

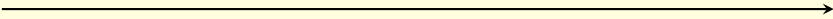
*(This is for axioms in first-order logic.)*

- This lets us translate talk about proofs, consistency, etc. to talk about structures.
- The incompleteness theorems plus the completeness theorem together imply there must be non-isomorphic structures satisfying the axioms of arithmetic.

What could these even look like???

# Nonstandard models of arithmetic

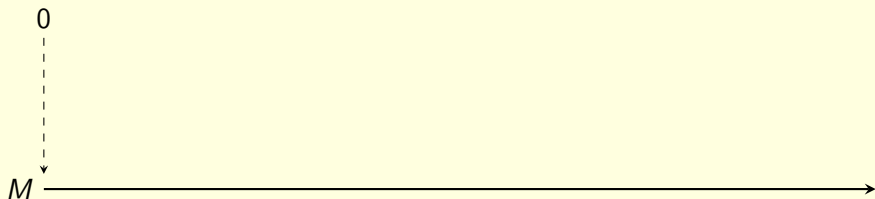
A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.

$M$  

- $X \subseteq M$  is **definable** if you can express  $x \in X$  just by quantifying over the elements of  $M$  and using the semiring operations and order of  $M$ .
- $X \subseteq M$  is **inductive** if  $0 \in X$  and  $a \in X \Rightarrow a + 1 \in X$  implies  $X = M$ .

# Nonstandard models of arithmetic

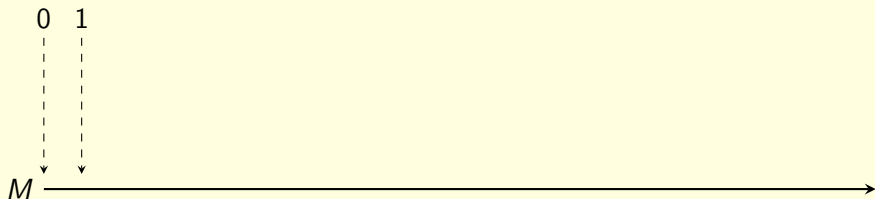
A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



$M$  has a least element  $0^M$  (= the additive identity for  $M$ ) because the set  $\{x \in M : x \geq 0^M\}$  satisfies the inductive hypotheses.

# Nonstandard models of arithmetic

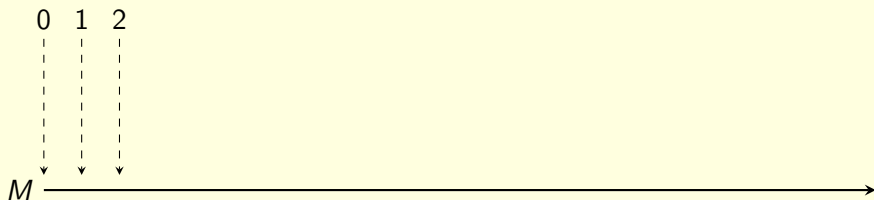
A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.





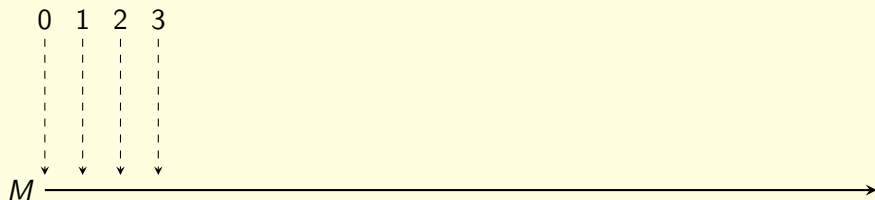
# Nonstandard models of arithmetic

A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



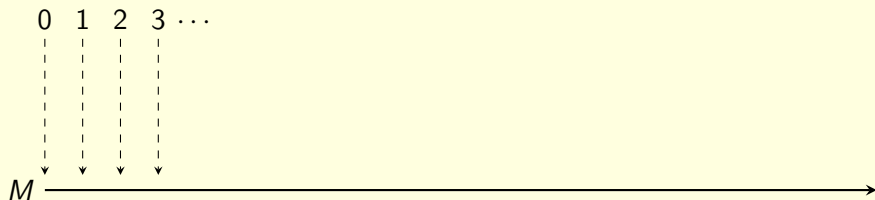
# Nonstandard models of arithmetic

A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



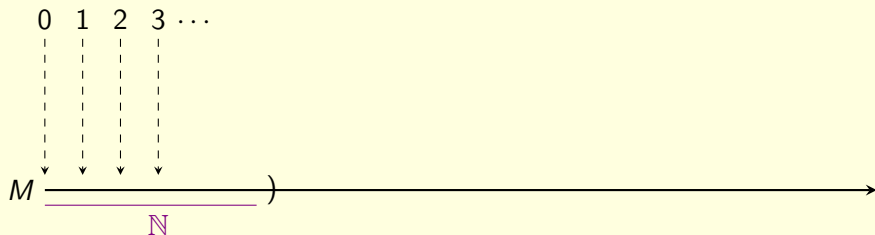
# Nonstandard models of arithmetic

A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



# Nonstandard models of arithmetic

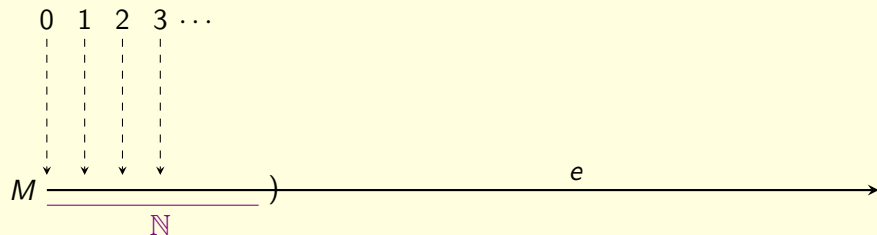
A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



$\mathbb{N}$  embeds as an initial segment on any model of arithmetic.

# Nonstandard models of arithmetic

A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



If  $e \in M \setminus \mathbb{N}$  then  $e > n$  for all  $n \in \mathbb{N}$ .

# Nonstandard models of arithmetic

A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



All non-zero elements have a predecessor because

$$\{0\} \cup \{a \in M : a \text{ has a predecessor}\}$$

satisfies the induction hypotheses.

# Nonstandard models of arithmetic

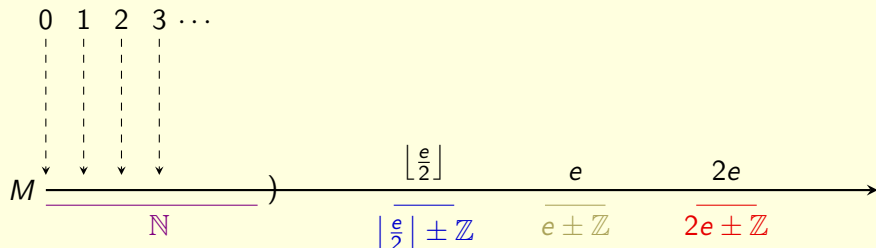
A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



$e + n < e + e = 2e$  for all  $n \in \mathbb{N}$ .

# Nonstandard models of arithmetic

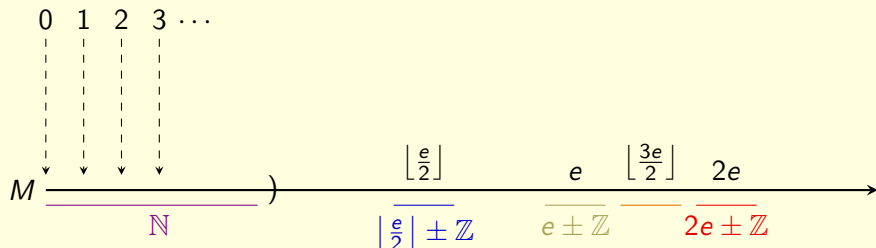
A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.





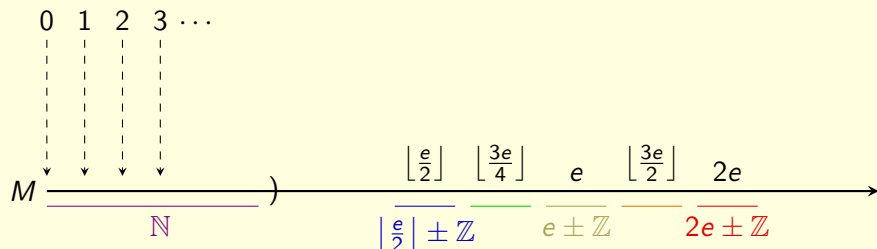
# Nonstandard models of arithmetic

A **model of (Peano) arithmetic** is a discretely ordered semiring whose **definable** subsets are **inductive**.



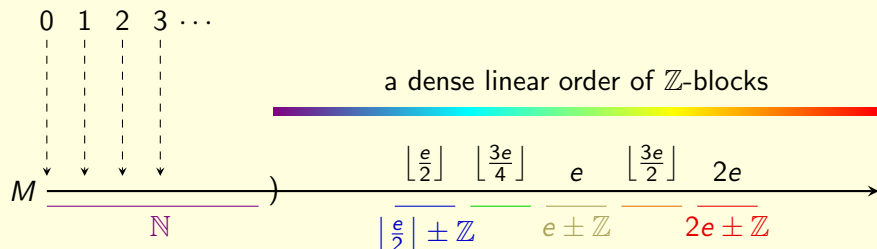
# Nonstandard models of arithmetic

A model of (Peano) arithmetic is a discretely ordered semiring whose definable subsets are inductive.



# Nonstandard models of arithmetic

A model of (Peano) arithmetic is a discretely ordered semiring whose definable subsets are inductive.



# Facts about nonstandard models of arithmetic

- First constructed by Thoralf Skolem. (Skolem used an ultrapower construction.)
- There are many different nonisomorphic models of arithmetic of any infinite cardinality. In particular, there are  $2^{\aleph_0}$  isomorphism classes for countable models of arithmetic.

# Facts about nonstandard models of arithmetic

- First constructed by Thoralf Skolem. (Skolem used an ultrapower construction.)
- There are many different nonisomorphic models of arithmetic of any infinite cardinality. In particular, there are  $2^{\aleph_0}$  isomorphism classes for countable models of arithmetic.
- If  $M$  is countable, then its ordertype is exactly  $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$ . (Because  $\mathbb{Q}$  is the unique countable dense linear order without endpoints.)
- In particular, all countable nonstandard models of arithmetic are order-isomorphic.

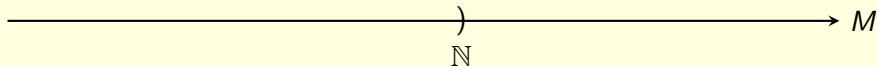
# Facts about nonstandard models of arithmetic

- First constructed by Thoralf Skolem. (Skolem used an ultrapower construction.)
- There are many different nonisomorphic models of arithmetic of any infinite cardinality. In particular, there are  $2^{\aleph_0}$  isomorphism classes for countable models of arithmetic.
- If  $M$  is countable, then its ordertype is exactly  $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$ . (Because  $\mathbb{Q}$  is the unique countable dense linear order without endpoints.)
- In particular, all countable nonstandard models of arithmetic are order-isomorphic.
- **Open Question** (Harvey Friedman):  $\mathbb{N}$  has the property that if a model of arithmetic is order-isomorphic to it then they are fully isomorphic. Does any other model of arithmetic have this property?

# Facts about nonstandard models of arithmetic

- First constructed by Thoralf Skolem. (Skolem used an ultrapower construction.)
- There are many different nonisomorphic models of arithmetic of any infinite cardinality. In particular, there are  $2^{\aleph_0}$  isomorphism classes for countable models of arithmetic.
- If  $M$  is countable, then its ordertype is exactly  $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$ . (Because  $\mathbb{Q}$  is the unique countable dense linear order without endpoints.)
- In particular, all countable nonstandard models of arithmetic are order-isomorphic.
- **Open Question** (Harvey Friedman):  $\mathbb{N}$  has the property that if a model of arithmetic is order-isomorphic to it then they are fully isomorphic. Does any other model of arithmetic have this property?
- (Stanley Tennenbaum) If  $M$  is nonstandard then neither the  $+$  nor  $\times$  of  $M$  is a computable function.

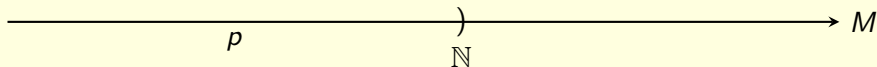
# Turing machines in a nonstandard world



- Consider  $p$  the TM which enumerates the theorems of arithmetic.

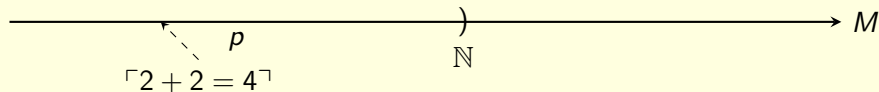


# Turing machines in a nonstandard world



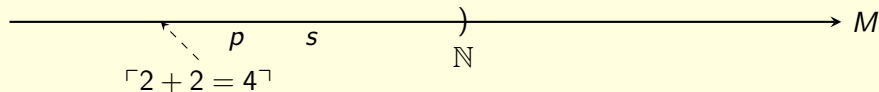
- Consider  $p$  the TM which enumerates the theorems of arithmetic.

# Turing machines in a nonstandard world



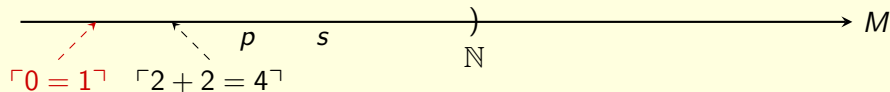
- Consider  $p$  the TM which enumerates the theorems of arithmetic.

# Turing machines in a nonstandard world



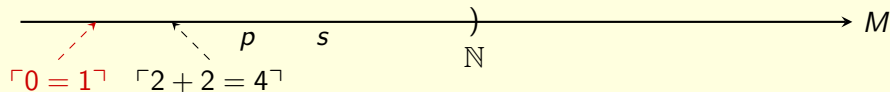
- Consider  $p$  the TM which enumerates the theorems of arithmetic.
- $s$  is a computation log witnessing that  $p$  outputs  $\ulcorner 2 + 2 = 4 \urcorner$ .  
( $s$  is a number coding the sequence of computation steps. Checking that  $s$  has this property only requires looking in  $\mathbb{N}$ .)

# Turing machines in a nonstandard world



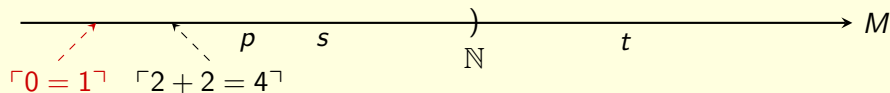
- Consider  $p$  the TM which enumerates the theorems of arithmetic.
- $s$  is a computation log witnessing that  $p$  outputs  $\ulcorner 2 + 2 = 4 \urcorner$ .  
( $s$  is a number coding the sequence of computation steps. Checking that  $s$  has this property only requires looking in  $\mathbb{N}$ .)
- If we run  $p$  in  $\mathbb{N}$ , then we never output  $\ulcorner 0 = 1 \urcorner$ .

# Turing machines in a nonstandard world



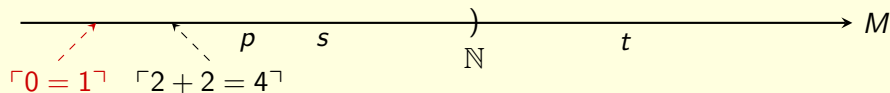
- Consider  $p$  the TM which enumerates the theorems of arithmetic.
- $s$  is a computation log witnessing that  $p$  outputs  $\ulcorner 2 + 2 = 4 \urcorner$ .  
( $s$  is a number coding the sequence of computation steps. Checking that  $s$  has this property only requires looking in  $\mathbb{N}$ .)
- If we run  $p$  in  $\mathbb{N}$ , then we never output  $\ulcorner 0 = 1 \urcorner$ .
- But what if we run  $p$  in nonstandard  $M$  which thinks arithmetic is inconsistent?

# Turing machines in a nonstandard world



- Consider  $p$  the TM which enumerates the theorems of arithmetic.
- $s$  is a computation log witnessing that  $p$  outputs  $\lceil 2 + 2 = 4 \rceil$ .  
( $s$  is a number coding the sequence of computation steps. Checking that  $s$  has this property only requires looking in  $\mathbb{N}$ .)
- If we run  $p$  in  $\mathbb{N}$ , then we never output  $\lceil 0 = 1 \rceil$ .
- But what if we run  $p$  in nonstandard  $M$  which thinks arithmetic is inconsistent?
- Then there is a computation log  $t$  witnessing that  $p$  outputs  $\lceil 0 = 1 \rceil$ . But  $t$  must be nonstandard! In other words, we had to run  $p$  for a nonstandard number of steps to output  $\lceil 0 = 1 \rceil$ .

# Turing machines in a nonstandard world



- Consider  $p$  the TM which enumerates the theorems of arithmetic.
- $s$  is a computation log witnessing that  $p$  outputs  $\lceil 2 + 2 = 4 \rceil$ .  
( $s$  is a number coding the sequence of computation steps. Checking that  $s$  has this property only requires looking in  $\mathbb{N}$ .)
- If we run  $p$  in  $\mathbb{N}$ , then we never output  $\lceil 0 = 1 \rceil$ .
- But what if we run  $p$  in nonstandard  $M$  which thinks arithmetic is inconsistent?
- Then there is a computation log  $t$  witnessing that  $p$  outputs  $\lceil 0 = 1 \rceil$ . But  $t$  must be nonstandard! In other words, we had to run  $p$  for a nonstandard number of steps to output  $\lceil 0 = 1 \rceil$ .
- **The point:** By moving to a larger world we made  $p$  output more numbers.

# The absoluteness of computability

In summary:

- The statement “the TM  $p$  outputs  $n$  for some input” is **upward absolute**—if it’s true it stays true if we **end-extend** to a larger model.  
(Logicians call this sort of statement a  $\Sigma_1$  statement. By the MRDP theorem, these are the statements equivalent to one whose only quantifiers are a block of  $\exists$ s.)
- But the statement “the TM  $p$  does **not** output  $n$  for some input” is not upward absolute. (It is **downward absolute** though.)  
(Logicians call this sort of statement a  $\Pi_1$  statement.)



# The absoluteness of computability

In summary:

- The statement “the TM  $p$  outputs  $n$  for some input” is **upward absolute**—if it’s true it stays true if we **end-extend** to a larger model.

(Logicians call this sort of statement a  $\Sigma_1$  statement. By the MRDP theorem, these are the statements equivalent to one whose only quantifiers are a block of  $\exists$ s.)

By Gödel’s completeness theorem plus the last slide, Peano arithmetic proves every true (i.e. in  $\mathbb{N}$ ) statement of this form.

- But the statement “the TM  $p$  does **not** output  $n$  for some input” is not upward absolute. (It is **downward absolute** though.)

(Logicians call this sort of statement a  $\Pi_1$  statement.)

Both the first and second incompleteness theorems are about statements of this form.

# Woodin's universal algorithm

We've seen that the behavior of a Turing machine can be undecidable.

- **Proof theoretic:** It may be independent of PA how  $p$  behaves.
- **Model theoretic:** Running  $p$  in different nonstandard models of arithmetic may produce different behavior.

I want to talk about a striking case of the undecidability of how Turing machines behave, due to W. Hugh Woodin, where  $p$  can output anything at all if run in the right universe!

**DISTINGUISHED LECTURE SERIES**

**NUS** National University of Singapore | **IMS** Institute for Mathematical Sciences

**W. HUGH WOODIN**

W. Hugh Woodin is Professor of Philosophy and of Mathematics at Harvard University. Woodin has been an ICM speaker three times, is a member of the American Academy of Arts and Sciences, and for nearly 20 years has been a Distinguished Visiting Professor in the Mathematics Department at NUS.

**Lecture 1: A new basis theorem for  $\Sigma_1^1$  sets**  
Thursday, 6 June 2019, 9.30-10.30am

This is the first lecture in a two part series on recent applications of the fine-structure of inner models to problems in descriptive set theory. The focus of this first lecture will lie on the projective sets and simple generalizations. The context will be determinacy hypotheses.

**Lecture 2: Counting Woodin cardinals in HOD**  
Monday, 10 June 2019, 9.30-10.30am

The final synthesis of fine-structure and determinacy will yield a number of theorems about HOD in the context of the Axiom of Determinacy. However, there are some of these expected theorems which can be proved now before that fine synthesis is achieved. We focus on one such recent theorem which concerns the relationship between the number of Woodin cardinals in HOD and the descriptive set theory of the universe within which HOD is defined.

One application shows that the axiom  $V = \text{Ultimate L}$  implies the  $\mathcal{Q}$  Conjecture.

**Venue:**  
Auditorium  
Institute for Mathematical Sciences  
3 Prince George's Park, Singapore 118402

[ims.nus.edu.sg](http://ims.nus.edu.sg) | [ims@nus.edu.sg](mailto:ims@nus.edu.sg) | [Follow us on Facebook facebook.com/imsnusag](https://www.facebook.com/imsnusag) | [Find us on Youtube bitJy2HEXeY6](https://www.youtube.com/watch?v=bitJy2HEXeY6)

# Woodin's universal algorithm, first form

## Theorem (Woodin)

*There is a Turing machine  $p$  with the following properties.*

- 1  *$p$  provably enumerates a finite sequence.*
- 2 *Running  $p$  inside  $\mathbb{N}$  never produces any output, i.e. it enumerates the empty sequence.*
- 3 *But, for any finite sequence  $s$  of natural numbers there is a nonstandard model of arithmetic  $M$  so that running  $p$  in  $M$  enumerates exactly  $s$ .*

# Woodin's algorithm

(This construction for Woodin's theorem is due to Joel David Hamkins.)

The Turing machine  $p$ :

- $p$  searches through the proofs of Peano arithmetic, looking at the theorems they prove.
- $p$  is looking for a theorem of the form “ $p$  does **not** enumerate the sequence  $s$ ”, for  $s$  some nonempty finite sequence of numbers.  
( $p$  can refer to itself by the Kleene Recursion theorem.)
- If  $p$  ever sees this, then  $p$  outputs the sequence  $s$ .

# Woodin's algorithm

(This construction for Woodin's theorem is due to Joel David Hamkins.)

The Turing machine  $p$ :

- $p$  searches through the proofs of Peano arithmetic, looking at the theorems they prove.
- $p$  is looking for a theorem of the form “ $p$  does **not** enumerate the sequence  $s$ ”, for  $s$  some nonempty finite sequence of numbers.  
( $p$  can refer to itself by the Kleene Recursion theorem.)
- If  $p$  ever sees this, then  $p$  outputs the sequence  $s$ .

**Claim:** Run in  $\mathbb{N}$ ,  $p$  outputs the empty sequence.

Otherwise  $p$  outputs some  $s$ . So Peano arithmetic proves this true  $\Sigma_1$  statement. But by the definition of  $p$ , this also means that Peano arithmetic proves that  $p$  does not output  $s$ . This would mean that Peano arithmetic is inconsistent. But it's not.

# Checking the extension property

## Definition (The Turing machine $p$ )

- $p$  searches through the proofs of Peano arithmetic, looking for a theorem of the form “ $p$  does **not** enumerate the sequence  $s$ ”, for  $s$  some nonempty sequence of numbers.
- If  $p$  ever sees this, then  $p$  outputs the sequence  $s$ .

Fix a finite sequence of natural numbers  $s$ . We want to find a nonstandard model of arithmetic  $M$  in which running  $p$  outputs  $s$ .

# Checking the extension property

## Definition (The Turing machine $p$ )

- $p$  searches through the proofs of Peano arithmetic, looking for a theorem of the form “ $p$  does **not** enumerate the sequence  $s$ ”, for  $s$  some nonempty sequence of numbers.
- If  $p$  ever sees this, then  $p$  outputs the sequence  $s$ .

Fix a finite sequence of natural numbers  $s$ . We want to find a nonstandard model of arithmetic  $M$  in which running  $p$  outputs  $s$ .

**Claim:** Peano arithmetic + “ $p$  outputs  $s$ ” is consistent.

# Checking the extension property

## Definition (The Turing machine $p$ )

- $p$  searches through the proofs of Peano arithmetic, looking for a theorem of the form “ $p$  does **not** enumerate the sequence  $s$ ”, for  $s$  some nonempty sequence of numbers.
- If  $p$  ever sees this, then  $p$  outputs the sequence  $s$ .

Fix a finite sequence of natural numbers  $s$ . We want to find a nonstandard model of arithmetic  $M$  in which running  $p$  outputs  $s$ .

**Claim:** Peano arithmetic + “ $p$  outputs  $s$ ” is consistent.

Otherwise “ $p$  does not output  $s$ ” is a theorem of Peano arithmetic. But then running  $p$  in  $\mathbb{N}$  would output a nonempty sequence. We just saw that is not the case.



# Checking the extension property

## Definition (The Turing machine $p$ )

- $p$  searches through the proofs of Peano arithmetic, looking for a theorem of the form “ $p$  does **not** enumerate the sequence  $s$ ”, for  $s$  some nonempty sequence of numbers.
- If  $p$  ever sees this, then  $p$  outputs the sequence  $s$ .

Fix a finite sequence of natural numbers  $s$ . We want to find a nonstandard model of arithmetic  $M$  in which running  $p$  outputs  $s$ .

**Claim:** Peano arithmetic + “ $p$  outputs  $s$ ” is consistent.

Otherwise “ $p$  does not output  $s$ ” is a theorem of Peano arithmetic. But then running  $p$  in  $\mathbb{N}$  would output a nonempty sequence. We just saw that is not the case.

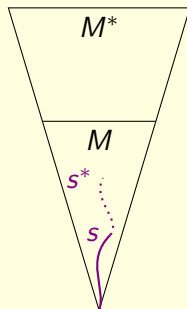
So by Gödel’s completeness theorem we can find a model of arithmetic in which  $p$  outputs  $s$ . □

# Woodin's universal algorithm, general form

## Theorem (Woodin)

Let  $PA^+$  be a computably axiomatizable extension of PA. There is a Turing machine  $p$  with the following properties.

- 1  $p$  provably enumerates a finite sequence.
- 2 Running  $p$  inside  $\mathbb{N}$  never produces any output, i.e. it enumerates the empty sequence.
- 3 Suppose  $M$  is a model of  $PA^+$  in which  $p$  enumerates  $s$  and that  $s^*$  is a sequence in  $M$  which extends  $s$ . Then we can end-extend  $M$  to  $M^*$ , a larger model of  $PA^+$  in which  $p$  enumerates  $s^*$ .

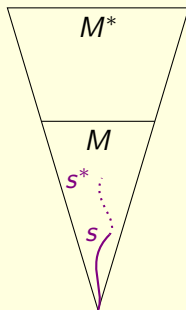


# Woodin's universal algorithm, general form

## Theorem (Woodin)

Let  $PA^+$  be a computably axiomatizable extension of PA. There is a Turing machine  $p$  with the following properties.

- 1  $p$  provably enumerates a finite sequence.
- 2 Running  $p$  inside  $\mathbb{N}$  never produces any output, i.e. it enumerates the empty sequence.
- 3 Suppose  $M$  is a model of  $PA^+$  in which  $p$  enumerates  $s$  and that  $s^*$  is a sequence in  $M$  which extends  $s$ . Then we can end-extend  $M$  to  $M^*$ , a larger model of  $PA^+$  in which  $p$  enumerates  $s^*$ .



**Proof idea:** Do a similar argument, but internally to  $M$ . Need some more technical lemmata to check that the argument can be [arithmetized](#).

# Potentialist systems

The general form of Woodin's theorem isn't about a single mathematical structure, but rather a collection of structures ordered by end-extension. Let's look at this in more generality.

# Potentialist systems

The general form of Woodin's theorem isn't about a single mathematical structure, but rather a collection of structures ordered by end-extension. Let's look at this in more generality.

## Definition

A **potentialist system** is a collection  $\mathcal{M}$  of structures  $M$  in a fixed signature, ordered by a reflexive, transitive relation  $\subseteq$  which extends the substructure relation.

So named because they formalize concepts that are never fully completed, but there is always the potential to extend.

# Aristotle's potential infinite

Aristotle distinguished between the **actual infinite**—a completed infinite whole—versus the **potential infinite**—a process which always has the potential to be extended.

# Aristotle's potential infinite

Aristotle distinguished between the **actual infinite**—a completed infinite whole—versus the **potential infinite**—a process which always has the potential to be extended.

Formalizing:

- The actualist view: study the structure  $(\mathbb{N}, +, \cdot, <)$ .

# Aristotle's potential infinite

Aristotle distinguished between the **actual infinite**—a completed infinite whole—versus the **potential infinite**—a process which always has the potential to be extended.

Formalizing:

- The actualist view: study the structure  $(\mathbb{N}, +, \cdot, <)$ .
- The potentialist view: study the structures  $\mathbb{N}_k = \{0, 1, \dots, k\}$ , ordered by extension.



# Aristotle's potential infinite

Aristotle distinguished between the **actual infinite**—a completed infinite whole—versus the **potential infinite**—a process which always has the potential to be extended.

Formalizing:

- The actualist view: study the structure  $(\mathbb{N}, +, \cdot, <)$ .
- The potentialist view: study the structures  $\mathbb{N}_k = \{0, 1, \dots, k\}$ , ordered by extension.

(Linnebo and Shapiro, Mirroring Theorem) You can translate statements about one perspective to the other. (The mirroring theorem applies in a more general context.)

Example: How to express the falsity of the Goldbach conjecture.

- Actualist: there's an even number which isn't the sum of two primes.
- Potentialist: we can extend to a larger world in which there's an even number which isn't the sum of two primes.

# Aristotle's potential infinite

Aristotle distinguished between the **actual infinite**—a completed infinite whole—versus the **potential infinite**—a process which always has the potential to be extended.

Formalizing:

- The actualist view: study the structure  $(\mathbb{N}, +, \cdot, <)$ .
- The potentialist view: study the structures  $\mathbb{N}_k = \{0, 1, \dots, k\}$ , ordered by extension.

(Linnebo and Shapiro, Mirroring Theorem) You can translate statements about one perspective to the other. (The mirroring theorem applies in a more general context.)

Example: How to express the falsity of the Goldbach conjecture.

- Actualist: there's an even number which isn't the sum of two primes.
- Potentialist: we can extend to a larger world in which there's an even number which isn't the sum of two primes.

For the potentialist we need to expand our logical tools to allow us to talk about what happens in extensions.

# Potentialism and modal logic

Introduce two new logical operators:

- $\Box\varphi$ , “ $\varphi$  is **necessary**”, says that  $\varphi$  holds in *every* extension.
- $\Diamond\varphi$ , “ $\varphi$  is **possible**”, says that  $\varphi$  holds in *some* extension.

# Potentialism and modal logic

Introduce two new logical operators:

- $\Box\varphi$ , “ $\varphi$  is **necessary**”, says that  $\varphi$  holds in *every* extension.
- $\Diamond\varphi$ , “ $\varphi$  is **possible**”, says that  $\varphi$  holds in *some* extension.

Every potentialist system satisfies:

$$\Box\varphi \Rightarrow \varphi \quad (\text{because } \subseteq \text{ is reflexive})$$

$$\Box\varphi \Rightarrow \Box\Box\varphi \quad (\text{because } \subseteq \text{ is transitive})$$

# Potentialism and modal logic

Introduce two new logical operators:

- $\Box\varphi$ , “ $\varphi$  is **necessary**”, says that  $\varphi$  holds in *every* extension.
- $\Diamond\varphi$ , “ $\varphi$  is **possible**”, says that  $\varphi$  holds in *some* extension.

Every potentialist system satisfies:

$$\Box\varphi \Rightarrow \varphi \quad (\text{because } \subseteq \text{ is reflexive})$$

$$\Box\varphi \Rightarrow \Box\Box\varphi \quad (\text{because } \subseteq \text{ is transitive})$$

These two formulae, plus the following two—also true in any potentialist system—axiomatize the modal theory **S4**.

$$\Box(\varphi \Rightarrow \psi) \Rightarrow (\Box\varphi \Rightarrow \Box\psi)$$

$$\neg\Diamond\varphi \Leftrightarrow \Box\neg\varphi$$

# The modal logic of a potentialist system

A question to ask about any potentialist system: which modal assertions are valid?

# The modal logic of a potentialist system

A question to ask about any potentialist system: which modal assertions are valid?

- (Forcing potentialism) Look at the forcing extensions of a model of set theory. Has modal validities precisely S4.2.

$$\diamond \Box \varphi \Rightarrow \Box \diamond \varphi \quad (.2)$$

- (Aristotelean potentialism) Look at worlds  $\mathbb{N}_k$ . Has modal validities precisely S4.3.

$$(\diamond \varphi \wedge \diamond \psi) \Rightarrow [(\varphi \wedge \diamond \psi) \vee (\diamond \varphi \wedge \psi)] \quad (.3)$$

# The modal logic of a potentialist system

The modal validities of a potentialist system express something about the structure of its truths.

- S4.2 expresses **directedness**.
- S4.3 expresses **linearity**.
- Just S4 expresses **essential branching**.



# The modal logic of a potentialist system

The modal validities of a potentialist system express something about the structure of its truths.

- S4.2 expresses **directedness**.
- S4.3 expresses **linearity**.
- Just S4 expresses **essential branching**.

Note that this can be distinct from the properties of the underlying partial order.

- Forcing potentialism has S4.2 as its modal validities.
- But as a partially ordered set, it's not directed.
- (Mostowski) If  $V$  is a countable model of ZF then there are Cohen reals  $c$  and  $d$  generic over  $V$  so that  $V[c]$  and  $V[d]$  cannot be amalgamated into a common extension.

## Theorem (Hamkins)

*Consider the potentialist system consisting of models of arithmetic, ordered by end-extension. The modal validities for this potentialist system are precisely S4.*

*(For the general case you need to allow a parameter in formulae, for the length of the sequence output by the universal algorithm.)*

## Theorem (Hamkins)

*Consider the potentialist system consisting of models of arithmetic, ordered by end-extension. The modal validities for this potentialist system are precisely S4.*

*(For the general case you need to allow a parameter in formulae, for the length of the sequence output by the universal algorithm.)*

We already saw that S4 is a lower bound, so all that remains is to check it is an upper bound.

The intuition: You get incompatible branching via statements like “the  $n$ th number output by the universal algorithm is 7”. Combine this with some facts about modal logic and you can show that any assertion not in S4 is invalid.

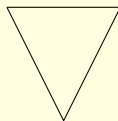
Can we extend this analysis to the transfinite?

Can we extend this analysis to the transfinite?

Yes.

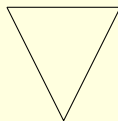
# Models of set theory

- A universe of sets is built up by iterating the powerset operation, starting from the empty set.



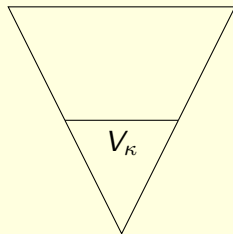
# Models of set theory

- A universe of sets is built up by iterating the powerset operation, starting from the empty set.
- Every set has an ordinal **rank**—how many times you must iterate  $\mathcal{P}$  to reach the set.



# Models of set theory

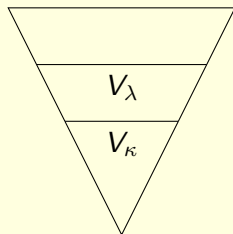
- A universe of sets is built up by iterating the powerset operation, starting from the empty set.
- Every set has an ordinal **rank**—how many times you must iterate  $\mathcal{P}$  to reach the set.
- Unlike with arithmetic, there's more than one well-founded universe of sets. E.g. if  $\kappa$  is an **inaccessible cardinal** then the sets of rank  $< \kappa$  form a model of ZF.





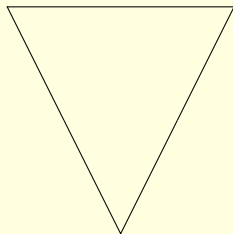
# Models of set theory

- A universe of sets is built up by iterating the powerset operation, starting from the empty set.
- Every set has an ordinal **rank**—how many times you must iterate  $\mathcal{P}$  to reach the set.
- Unlike with arithmetic, there's more than one well-founded universe of sets. E.g. if  $\kappa$  is an **inaccessible cardinal** then the sets of rank  $< \kappa$  form a model of ZF.



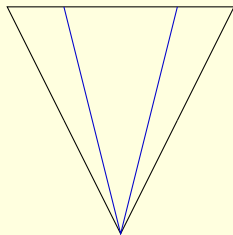
# Models of set theory

- A universe of sets is built up by iterating the powerset operation, starting from the empty set.
- Every set has an ordinal **rank**—how many times you must iterate  $\mathcal{P}$  to reach the set.
- Unlike with arithmetic, there's more than one well-founded universe of sets. E.g. if  $\kappa$  is an **inaccessible cardinal** then the sets of rank  $< \kappa$  form a model of ZF.
- You can also get new universes by changing the width, going thinner to an **inner model** or wider via Cohen's method of **forcing**.



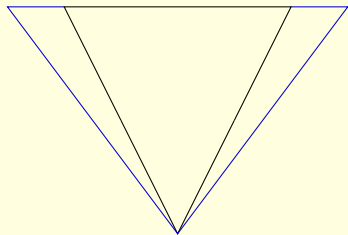
# Models of set theory

- A universe of sets is built up by iterating the powerset operation, starting from the empty set.
- Every set has an ordinal **rank**—how many times you must iterate  $\mathcal{P}$  to reach the set.
- Unlike with arithmetic, there's more than one well-founded universe of sets. E.g. if  $\kappa$  is an **inaccessible cardinal** then the sets of rank  $< \kappa$  form a model of ZF.
- You can also get new universes by changing the width, going thinner to an **inner model** or wider via Cohen's method of **forcing**.



# Models of set theory

- A universe of sets is built up by iterating the powerset operation, starting from the empty set.
- Every set has an ordinal **rank**—how many times you must iterate  $\mathcal{P}$  to reach the set.
- Unlike with arithmetic, there's more than one well-founded universe of sets. E.g. if  $\kappa$  is an **inaccessible cardinal** then the sets of rank  $< \kappa$  form a model of ZF.
- You can also get new universes by changing the width, going thinner to an **inner model** or wider via Cohen's method of **forcing**.

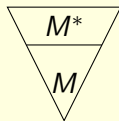


# Extensions of models of set theory

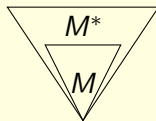
Unlike with arithmetic where there's only one sensible notion of adding new elements to the end, in set theory we have multiple notions.

- $M^*$  **end-extends**  $M$  if  $M^*$  doesn't add any new elements to sets from  $M$ . (For example, a forcing extension is an end-extension.)
- $M^*$  **rank-extends**  $M$  if the new sets in  $M^*$  have higher rank than all elements in  $M$ .

Note that every rank-extension is an end-extension but not vice versa.



rank-extension



end-extension

# The $\Sigma_2$ universal finite sequence for rank-extensions

There is a universal “algorithm” for rank-extensions.

## Theorem (Hamkins–Woodin)

*Let  $ZF^+$  be any computably axiomatizable extension of  $ZF$ . There is a  $\Sigma_2$  definition for a finite sequence  $s$  with the following properties:*

- 1  *$ZF$  proves  $s$  is a finite sequence.*
- 2 *If  $M$  is a well-founded model of  $ZF^+$  then its  $s$  is the empty sequence.*
- 3 *If  $M$  is a countable model of  $ZF^+$  with  $s$  as its sequence and  $s^*$  is any finite sequence in  $M$  extending  $s$  then there is a rank-extension  $M^* \models ZF^+$  of  $M$  whose sequence is  $s^*$ .*

( $\Sigma_2$  assertions are precisely those that are upward absolute for rank-extensions.)

# The $\Sigma_1$ universal finite sequence for end-extensions

There is also a universal “algorithm” for end-extensions.

## Theorem (Hamkins–W.)

*Let  $ZF^+$  be any computably axiomatizable extension of  $ZF$ . There is a  $\Sigma_1$  definition for a finite sequence  $s$  with the following properties:*

- 1  $ZF$  proves  $s$  is a finite sequence.
- 2 If  $M$  is a well-founded model of  $ZF^+$  then its  $s$  is the empty sequence.
- 3 If  $M$  is a countable model of  $ZF^+$  with  $s$  as its sequence and  $s^*$  is any finite sequence in  $M$  extending  $s$  then there is a end-extension  $M^* \models ZF^+$  of  $M$  whose sequence is  $s^*$ .

( $\Sigma_1$  assertions are precisely those that are upward absolute for end-extensions.)

# The $\Sigma_1$ universal finite sequence for end-extensions

There is also a universal “algorithm” for end-extensions.

## Theorem (Hamkins–W.)

*Let  $ZF^+$  be any computably axiomatizable extension of ZF. There is a  $\Sigma_1$  definition for a finite sequence  $s$  with the following properties:*

- 1  $ZF$  proves  $s$  is a finite sequence.
- 2 If  $M$  is a well-founded model of  $ZF^+$  then its  $s$  is the empty sequence.
- 3 If  $M$  is a countable model of  $ZF^+$  with  $s$  as its sequence and  $s^*$  is any finite sequence in  $M$  extending  $s$  then there is a end-extension  $M^* \models ZF^+$  of  $M$  whose sequence is  $s^*$ .
- 4 For (3), it is enough that  $M$  be a model of ZF and  $M$  have an inner model of  $ZF^+$ .

( $\Sigma_1$  assertions are precisely those that are upward absolute for end-extensions.)



# Set theoretic potentialism

Corollary (Hamkins–Woodin, Hamkins–W.)

*The modal validities for both rank-extension potentialism and end-extension potentialism are precisely S4.*

# Set theoretic potentialism

Corollary (Hamkins–Woodin, Hamkins–W.)

*The modal validities for both rank-extension potentialism and end-extension potentialism are precisely S4.*

Same proof as before works.

# Resurrection in end-extensions

If you forget the stuff about universal algorithms, the end-extension result says that you can resurrect properties of inner models in end-extensions.

## Theorem (Hamkins–W.)

*Let  $ZF^+$  and  $ZF^\dagger$  be computably axiomatizable extensions of  $ZF$ . Let  $M$  be a countable model of  $ZF^+$  with an inner model of  $ZF^\dagger$ . Then there is a model of  $ZF^\dagger$  which end-extends  $M$ .*

# Resurrection in end-extensions

If you forget the stuff about universal algorithms, the end-extension result says that you can resurrect properties of inner models in end-extensions.

## Theorem (Hamkins–W.)

*Let  $ZF^+$  and  $ZF^\dagger$  be computably axiomatizable extensions of ZF. Let  $M$  be a countable model of  $ZF^+$  with an inner model of  $ZF^\dagger$ . Then there is a model of  $ZF^\dagger$  which end-extends  $M$ .*

## Corollary

- *(Barwise Extension Theorem) Every countable model of ZF end-extends to a model of  $ZF + V = L$ .*
- *Every countable model of  $ZFC +$  “there is a measurable cardinal” end-extends to a model of  $ZFC + V = L[\mu]$ .*
- *Every countable model of  $ZFC +$  “there are infinitely many Woodin cardinals with a measurable above” end-extends to a model of  $ZF + V = L(\mathbb{R}) + AD$ .*

Thank you!