Introduction to nonstandard models of arithmetic

Victoria Gitman

vgitman@nylogic.org
http://boolesrings.org/victoriagitman

VCU Analysis, Logic, and Physics Seminar

April 24, 2015

Flashback: first number theory course

"Your assumptions are your windows on the world. Scrub them off every once in a while, or the light won't come in." –Isaac Asimov

Theorem: The greatest common divisor g of a and b has the form $g = ax + by$.

Proof:

- Let $S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$, and note $S \neq \emptyset$.
- Let $l = ax_0 + by_0$ be the least element of S.
- If $l \nmid b$, then $b = lq + r$ with $0 < r < l$.
- So $r = b - lq = b - (ax_0 + by_0)q = a(-x_0q) + b(1 - y_0)$ is in S.
- But this contradicts that l is least!
- Suppose $c \mid a$ and $c \mid b$, and let $a = xl$ and $b = yl$.
- $l = x_0(xc) + y_0(yc) = c(x_0x + y_0y)$, so $c \leq l$. $\square$

Flashback: first number theory course

"Your assumptions are your windows on the world. Scrub them off every once in a while, or the light won't come in." –Isaac Asimov

Theorem: The greatest common divisor g of a and b has the form $g = ax + by$.

Proof:

- Let $S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$, and note $S \neq \emptyset$.
- Let $l = ax_0 + by_0$ be the least element of S.
- If $l \nmid b$, then $b = lq + r$ with $0 < r < l$.
- So $r = b - lq = b - (ax_0 + by_0)q = a(-x_0 q) + b(1 - y_0)$ is in S.
- But this contradicts that l is least!
- Suppose $c \mid a$ and $c \mid b$, and let $a = xl$ and $b = yl$.
- $l = x_0(xc) + y_0(yc) = c(x_0 x + y_0 y)$, so $c \leq l$. $\square$

Question: What assumptions did the proof use?

- g is the greatest common divisor of a and b.

Flashback: first number theory course

"Your assumptions are your windows on the world. Scrub them off every once in a while, or the light won't come in." –Isaac Asimov

Theorem: The greatest common divisor g of a and b has the form $g = ax + by$.

Proof:

- Let $S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$, and note $S \neq \emptyset$.
- Let $l = ax_0 + by_0$ be the least element of S.
- If $l \nmid b$, then $b = lq + r$ with $0 < r < l$.
- So $r = b - lq = b - (ax_0 + by_0)q = a(-x_0q) + b(1 - y_0)$ is in S.
- But this contradicts that l is least!
- Suppose $c \mid a$ and $c \mid b$, and let $a = xl$ and $b = yl$.
- $l = x_0(xc) + y_0(yc) = c(x_0x + y_0y)$, so $c \leq l$. $\square$

Question: What assumptions did the proof use?

- g is the greatest common divisor of a and b.
- Peano axioms!

The axiomatic method

Question: What is the epistemology of mathematics? How do we know that a mathematical statement is true?

The axiomatic method

Question: What is the epistemology of mathematics? How do we know that a mathematical statement is true?

The (naive) axiomatic method

- Introduced by Euclid in the *Elements* around 300 BC, it revolutionizes how mathematics is done.
- All mathematical statements are derivable from a few self-evident truths by logical inference.
- The "self-evident truths" are called axioms.

The axiomatic method

Question: What is the epistemology of mathematics? How do we know that a mathematical statement is true?

The (naive) axiomatic method

- Introduced by Euclid in the *Elements* around 300 BC, it revolutionizes how mathematics is done.
- All mathematical statements are derivable from a few self-evident truths by logical inference.
- The "self-evident truths" are called axioms.

Peano axioms

- Two millennia later, in 1889, Giuseppe Peano (building on an earlier work of Dedekind) proposed an axiomatization of arithmetic.
- A modern version of the Peano axioms is taught to every high school student (without the subtleties).
- Peano is better known for proving that there is a space filling curve, a continuous map from the unit interval onto the unit square.

Peano axioms

Addition and Multiplication

- $\forall x \forall y \forall z\ (x+y)+z = x+(y+z)$ (associativity of addition)
- $\forall x \forall y\ x+y = y+x$ (commutativity of addition)
- $\forall x \forall y \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)
- $\forall x \forall y\ x \cdot y = y \cdot x$ (commutativity of multiplication)
- $\forall x \forall y \forall z\ x \cdot (y+z) = x \cdot y + x \cdot z.$ (distributive law)
- $\forall x\ (x+0 = x \wedge x \cdot 1 = x)$ (additive and multiplicative identity)

Peano axioms

Addition and Multiplication

- $\forall x \forall y \forall z\ (x+y)+z = x+(y+z)$ (associativity of addition)
- $\forall x \forall y\ x+y = y+x$ (commutativity of addition)
- $\forall x \forall y \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)
- $\forall x \forall y\ x \cdot y = y \cdot x$ (commutativity of multiplication)
- $\forall x \forall y \forall z\ x \cdot (y+z) = x \cdot y + x \cdot z.$ (distributive law)
- $\forall x\ (x+0 = x \wedge x \cdot 1 = x)$ (additive and multiplicative identity)

Order

- $\forall x \forall y \forall z\ ((x<y \wedge y<z) \to x<z)$ (transitive)
- $\forall x\ \neg x < x$ (anti-reflexive)
- $\forall x \forall y\ ((x<y \vee x=y) \vee y<x)$ (linear)
- $\forall x \forall y \forall z\ (x<y \to x+z < y+z)$ (respects addition)
- $\forall x \forall y \forall z\ ((0<z \wedge x<y) \to x \cdot z < x \cdot z)$ (respects multiplication)
- $\forall x \forall y\ (x<y \leftrightarrow \exists z\ (z>0 \wedge x+z=y))$
- $\forall x\ (x \geq 0 \wedge (x>0 \to x \geq 1))$ (discrete)

Peano axioms

Addition and Multiplication

- $\forall x \forall y \forall z\ (x+y)+z = x+(y+z)$ (associativity of addition)
- $\forall x \forall y\ x+y = y+x$ (commutativity of addition)
- $\forall x \forall y \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)
- $\forall x \forall y\ x \cdot y = y \cdot x$ (commutativity of multiplication)
- $\forall x \forall y \forall z\ x \cdot (y+z) = x \cdot y + x \cdot z.$ (distributive law)
- $\forall x\ (x+0 = x \wedge x \cdot 1 = x)$ (additive and multiplicative identity)

Order

- $\forall x \forall y \forall z\ ((x < y \wedge y < z) \to x < z)$ (transitive)
- $\forall x\ \neg x < x$ (anti-reflexive)
- $\forall x \forall y\ ((x < y \vee x = y) \vee y < x)$ (linear)
- $\forall x \forall y \forall z\ (x < y \to x+z < y+z)$ (respects addition)
- $\forall x \forall y \forall z\ ((0 < z \wedge x < y) \to x \cdot z < x \cdot z)$ (respects multiplication)
- $\forall x \forall y\ (x < y \leftrightarrow \exists z\ (z > 0 \wedge x+z = y))$
- $\forall x\ (x \geq 0 \wedge (x > 0 \to x \geq 1))$ (discrete)

Induction Scheme

For every statement $\varphi(x)$: $(\varphi(0) \wedge \forall x\ (\varphi(x) \to \varphi(x+1))) \to \forall x \varphi(x)$

Codifying the axiomatic method

- A formal treatment of mathematics was necessitated by the increasingly abstract character it assumed in the 18-19$^{\text{th}}$ centuries.
- The most robust formal mathematical system is first-order logic.

Codifying the axiomatic method

- A formal treatment of mathematics was necessitated by the increasingly abstract character it assumed in the 18-19$^{\text{th}}$ centuries.
- The most robust formal mathematical system is first-order logic.

Language of first-order logic

- General: variables, logical connectives, quantifiers
- Subject specific: functions, relations, constants
  - language of group theory: $\mathcal{L}_G = (\circ, {}^{-1}, e)$
  - language of arithmetic: $\mathcal{L}_A = (+, \cdot, <, 0, 1)$

Codifying the axiomatic method

- A formal treatment of mathematics was necessitated by the increasingly abstract character it assumed in the 18-19th centuries.
- The most robust formal mathematical system is first-order logic.

Language of first-order logic

- General: variables, logical connectives, quantifiers
- Subject specific: functions, relations, constants
  - language of group theory: $\mathcal{L}_G = (\circ, {}^{-1}, e)$
  - language of arithmetic: $\mathcal{L}_A = (+, \cdot, <, 0, 1)$

Axioms: A collection of statements in a first-order language defining fundamental structural properties

- common to many different mathematical objects, e.g., group axioms,
- of a single mathematical object, e.g., Peano axioms.

Codifying the axiomatic method

- A formal treatment of mathematics was necessitated by the increasingly abstract character it assumed in the 18-19$^{\text{th}}$ centuries.
- The most robust formal mathematical system is first-order logic.

Language of first-order logic

- General: variables, logical connectives, quantifiers
- Subject specific: functions, relations, constants
  - language of group theory: $\mathcal{L}_G = (\circ, {}^{-1}, e)$
  - language of arithmetic: $\mathcal{L}_A = (+, \cdot, <, 0, 1)$

Axioms: A collection of statements in a first-order language defining fundamental structural properties

- common to many different mathematical objects, e.g., group axioms,
- of a single mathematical object, e.g., Peano axioms.

Rules of logical inference

- Logical axioms, e.g.,
  - $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$,
  - $x = y \to f(x) = f(y)$.
- Modus ponens: if φ and $\varphi \to \psi$, then conclude ψ.

Models for group axioms

A model is a group: $(G, \circ, {}^{-1}, e)$

- G is a set,
- $\circ$ is a function on $G \times G$, ${}^{-1}$ is a function on G, e is a fixed element in G,

such that the group axioms are satisfied.

- Symmetric group S_3 - all permutations on 3 objects
  - $\circ$ is function composition, ${}^{-1}$ inverts the permutation, e is the identity permutation
  - finite, non-abelian
- Integers $\mathbb{Z}$
  - $\circ$ is addition, ${}^{-1}$ negates, e is 0
  - infinite, abelian group

Models for group axioms

A model is a group: $(G, \circ, {}^{-1}, e)$

- G is a set,
- $\circ$ is a function on $G \times G$, ${}^{-1}$ is a function on G, e is a fixed element in G,

such that the group axioms are satisfied.

- Symmetric group S_3 - all permutations on 3 objects
  - $\circ$ is function composition, ${}^{-1}$ inverts the permutation, e is the identity permutation
  - finite, non-abelian
- Integers $\mathbb{Z}$
  - $\circ$ is addition, ${}^{-1}$ negates, e is 0
  - infinite, abelian group

There are vastly different models of the group axioms!

- local properties (expressible in $\mathcal{L}_G$): abelian/non-abelian, divisible/non-divisible
- global properties (not expressible in $\mathcal{L}_G$): cyclic/non-cyclic, nilpotent/non-nilpotent
- sizes: finite/countable/uncountable

Models for Peano axioms

A model is $(M, +, \cdot, <, 0, 1)$:

- M is a set,
- $+$, $\cdot$ are functions on $M \times M$, $<$ is a relation on $M \times M$, 0, 1 are fixed elements in M,

such that the Peano axioms are satisfied.

- $(\mathbb{N}, +, \cdot, <, 0, 1)$

Models for Peano axioms

A model is $(M, +, \cdot, <, 0, 1)$:

- M is a set,
- $+$, $\cdot$ are functions on $M \times M$, $<$ is a relation on $M \times M$, 0, 1 are fixed elements in M,

such that the Peano axioms are satisfied.

- $(\mathbb{N}, +, \cdot, <, 0, 1)$

Euclid's world

- $(\mathbb{N}, +, \cdot, <, 0, 1)$ should be the unique model of the Peano axioms.
- Every true arithmetic statement should be provable from the Peano axioms.

Models for Peano axioms

A model is $(M, +, \cdot, <, 0, 1)$:

- M is a set,
- $+$, $\cdot$ are functions on $M \times M$, $<$ is a relation on $M \times M$, 0, 1 are fixed elements in M,

such that the Peano axioms are satisfied.

- $(\mathbb{N}, +, \cdot, <, 0, 1)$

Euclid's world

- $(\mathbb{N}, +, \cdot, <, 0, 1)$ should be the unique model of the Peano axioms.
- Every true arithmetic statement should be provable from the Peano axioms.

The real world: Peano axioms (or any other reasonable axioms) cannot

- determine the size of a model,
- decide the truth of all arithmetic statements.

Models in general

Definition: A model for a collection of statements $\mathcal{C}$ in a first-order language $\mathcal{L}$ is a set S together with definitions on S of all functions, relations, constants in $\mathcal{L}$ such that all statements in $\mathcal{C}$ are satisfied.

Models in general

Definition: A model for a collection of statements $\mathcal{C}$ in a first-order language $\mathcal{L}$ is a set S together with definitions on S of all functions, relations, constants in $\mathcal{L}$ such that all statements in $\mathcal{C}$ are satisfied.

- Variables in first-order statements apply only to elements of S.
  - Induction cannot be expressed as a single statement in $\mathcal{L}_A$ because we cannot quantify over subsets.
  - Divisibility of a group requires infinitely many statements in $\mathcal{L}_G$.

Models in general

Definition: A model for a collection of statements $\mathcal{C}$ in a first-order language $\mathcal{L}$ is a set S together with definitions on S of all functions, relations, constants in $\mathcal{L}$ such that all statements in $\mathcal{C}$ are satisfied.

- Variables in first-order statements apply only to elements of S.
  - Induction cannot be expressed as a single statement in $\mathcal{L}_A$ because we cannot quantify over subsets.
  - Divisibility of a group requires infinitely many statements in $\mathcal{L}_G$.

Definition: A collection of statements is consistent if we cannot prove from it any statement of the form $\varphi \wedge \neg\varphi$.

Inconsistent collections of statements cannot have models!

The glories and the frailties of formal mathematics

" ...the point of philosophy is to start with something so simple as not to seem worth stating, and to end with something so paradoxical that no one will believe it." –Bertrand Russell

Completeness Theorem: (Gödel, Maltsev, 1930-36) Every consistent collection of statements has a model.

- If every finite fragment of a collection of statements has a model, then the whole collection has a model.

The glories and the frailties of formal mathematics

" ...the point of philosophy is to start with something so simple as not to seem worth stating, and to end with something so paradoxical that no one will believe it." –Bertrand Russell

Completeness Theorem: (Gödel, Maltsev, 1930-36) Every consistent collection of statements has a model.

- If every finite fragment of a collection of statements has a model, then the whole collection has a model.

Lowenheim-Skolem Theorem: (Lowenheim, Skolem, Maltsev, 1920-36) If a collection of statements has an infinite model, then it has a model of every possible infinite cardinality.

- Axioms cannot determine the size of a model.
- There are uncountable models of the Peano axioms!

The glories and the frailties of formal mathematics

" ...the point of philosophy is to start with something so simple as not to seem worth stating, and to end with something so paradoxical that no one will believe it." –Bertrand Russell

Completeness Theorem: (Gödel, Maltsev, 1930-36) Every consistent collection of statements has a model.

- If every finite fragment of a collection of statements has a model, then the whole collection has a model.

Lowenheim-Skolem Theorem: (Lowenheim, Skolem, Maltsev, 1920-36) If a collection of statements has an infinite model, then it has a model of every possible infinite cardinality.

- Axioms cannot determine the size of a model.
- There are uncountable models of the Peano axioms!

First Incompleteness Theorem: (Gödel, 1931) No reasonable axioms can prove all true statements of arithmetic (and similarly complex subjects).

- Reasonable means expressible algorithmically.
- "All true statements of arithmetic" is not reasonable.
- There is a true arithmetic statement that cannot be proved from the Peano axioms.

A nonstandard model of arithmetic

A nonstandard model of arithmetic is any model of the Peano axioms that is not the standard model $(\mathbb{N}, +, \cdot, <, 0, 1)$.

The existence of a countable nonstandard model of arithmetic (even satisfying all true arithmetic statements) follows from the completeness theorem.

- Expand $\mathcal{L}_A$ by adding a constant c to obtain the language $\mathcal{L}_{A^*} = (+, \cdot, <, 0, 1, c)$.
- Let $\mathcal{C}$ be any collection of true arithmetic statements, e.g., the Peano axioms.
- Let $\mathcal{C}^*$ consist of:
  - $\mathcal{C}$,
  - $\{c > 0, c > 1, c > 2, \ldots, c > n, \ldots\}$ (note: $n = \underbrace{1 + \cdots + 1}_{n}$)

A nonstandard model of arithmetic

A nonstandard model of arithmetic is any model of the Peano axioms that is not the standard model $(\mathbb{N}, +, \cdot, <, 0, 1)$.

The existence of a countable nonstandard model of arithmetic (even satisfying all true arithmetic statements) follows from the completeness theorem.

- Expand $\mathcal{L}_A$ by adding a constant c to obtain the language $\mathcal{L}_{A^*} = (+, \cdot, <, 0, 1, c)$.
- Let $\mathcal{C}$ be any collection of true arithmetic statements, e.g., the Peano axioms.
- Let $\mathcal{C}^*$ consist of:
  - $\mathcal{C}$,
  - $\{c > 0, c > 1, c > 2, \ldots, c > n, \ldots\}$ (note: $n = \underbrace{1 + \cdots + 1}_{n}$)

Observation: Every finite fragment F of $\mathcal{C}^*$ has a model.

Proof:

- There is the largest n such that $c > n$ is in F.
- $(\mathbb{N}, +, \cdot, <, 0, 1, n+1)$ is a model of F.

By completeness theorem, $\mathcal{C}^*$ has a model $(M, +, \cdot, <, 0, 1, c)$! $\square$

A nonstandard model of arithmetic

A nonstandard model of arithmetic is any model of the Peano axioms that is not the standard model $(\mathbb{N}, +, \cdot, <, 0, 1)$.

The existence of a countable nonstandard model of arithmetic (even satisfying all true arithmetic statements) follows from the completeness theorem.

- Expand $\mathcal{L}_A$ by adding a constant c to obtain the language $\mathcal{L}_{A^*} = (+, \cdot, <, 0, 1, c)$.
- Let $\mathcal{C}$ be any collection of true arithmetic statements, e.g., the Peano axioms.
- Let $\mathcal{C}^*$ consist of:
  - $\mathcal{C}$,
  - $\{c > 0, c > 1, c > 2, \ldots, c > n, \ldots\}$ (note: $n = \underbrace{1 + \cdots + 1}_{n}$)

Observation: Every finite fragment F of $\mathcal{C}^*$ has a model.

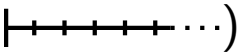
Proof:

- There is the largest n such that $c > n$ is in F.
- $(\mathbb{N}, +, \cdot, <, 0, 1, n+1)$ is a model of F.

By completeness theorem, $\mathcal{C}^*$ has a model $(M, +, \cdot, <, 0, 1, c)$! $\square$

Question: What does it look like?

A countable nonstandard model of arithmetic



- $\mathbb{N}$ is the initial segment of M.

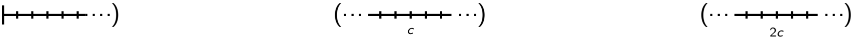
A countable nonstandard model of arithmetic

- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).

A countable nonstandard model of arithmetic

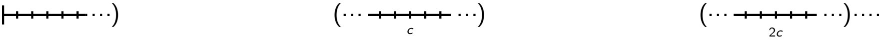
- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.

A countable nonstandard model of arithmetic



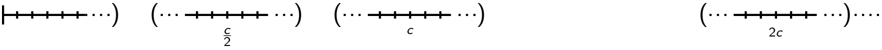
- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c + n$ for all $n \in \mathbb{N}$.

A countable nonstandard model of arithmetic



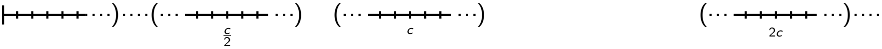
- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.

A countable nonstandard model of arithmetic



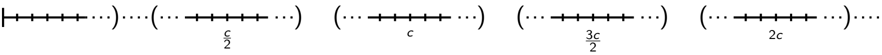
- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- M has $\frac{c}{2}$: $\frac{c}{2} < c-n$ for all $n \in \mathbb{N}$

A countable nonstandard model of arithmetic



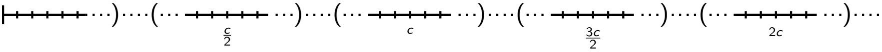
- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- M has $\frac{c}{2}$: $\frac{c}{2} < c-n$ for all $n \in \mathbb{N}$

A countable nonstandard model of arithmetic



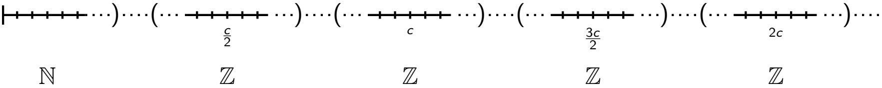
- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- M has $\frac{c}{2}$: $\frac{c}{2} < c-n$ for all $n \in \mathbb{N}$
- M has $\frac{3c}{2}$: $c+n < \frac{3c}{2} < 2c-n$ for all $n \in \mathbb{N}$.

A countable nonstandard model of arithmetic



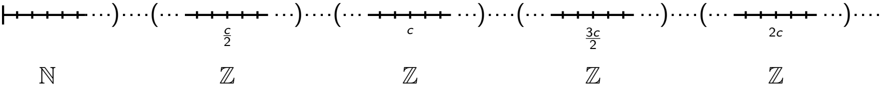
- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- M has $\frac{c}{2}$: $\frac{c}{2} < c-n$ for all $n \in \mathbb{N}$
- M has $\frac{3c}{2}$: $c+n < \frac{3c}{2} < 2c-n$ for all $n \in \mathbb{N}$.

A countable nonstandard model of arithmetic



- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- M has $\frac{c}{2}$: $\frac{c}{2} < c-n$ for all $n \in \mathbb{N}$
- M has $\frac{3c}{2}$: $c+n < \frac{3c}{2} < 2c-n$ for all $n \in \mathbb{N}$.

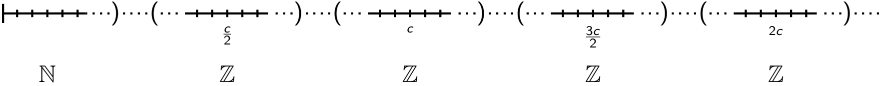
A countable nonstandard model of arithmetic



$\mathbb{Q}$ many copies of $\mathbb{Z}$

- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- M has $\frac{c}{2}$: $\frac{c}{2} < c - n$ for all $n \in \mathbb{N}$
- M has $\frac{3c}{2}$: $c+n < \frac{3c}{2} < 2c - n$ for all $n \in \mathbb{N}$.

A countable nonstandard model of arithmetic



$\mathbb{Q}$ many copies of $\mathbb{Z}$

- $\mathbb{N}$ is the initial segment of M.
- M has an element $c > \mathbb{N}$ (assume c is even).
- M has $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M has $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- M has $\frac{c}{2}$: $\frac{c}{2} < c-n$ for all $n \in \mathbb{N}$
- M has $\frac{3c}{2}$: $c+n < \frac{3c}{2} < 2c-n$ for all $n \in \mathbb{N}$.

Paradox? Induction is equivalent to every subset has a least element, but clearly this is false!

An Android app for a nonstandard model of arithmetic?

Question: Can we compute inside a nonstandard model of arithmetic?
Is there a nonstandard model of arithmetic for which there an algorithm to compute addition and multiplication?

An Android app for a nonstandard model of arithmetic?

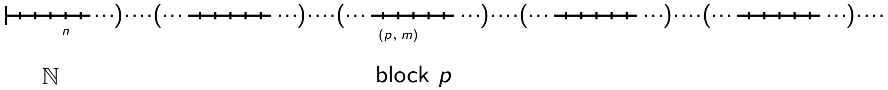
Question: Can we compute inside a nonstandard model of arithmetic?
Is there a nonstandard model of arithmetic for which there an algorithm to compute addition and multiplication?

- It is natural to think of elements of a nonstandard model as $\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}$.

An Android app for a nonstandard model of arithmetic?

Question: Can we compute inside a nonstandard model of arithmetic?
Is there a nonstandard model of arithmetic for which there an algorithm to compute addition and multiplication?

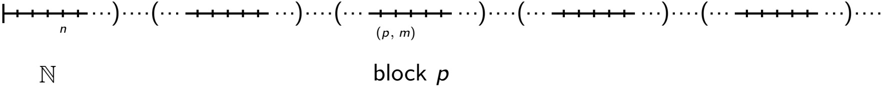
- It is natural to think of elements of a nonstandard model as $\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}$.
- $(p, m) + n = (p, m + n)$. How about $(p, m) \cdot n$?



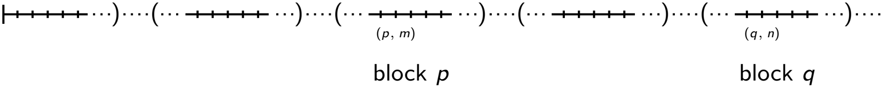
An Android app for a nonstandard model of arithmetic?

Question: Can we compute inside a nonstandard model of arithmetic?
Is there a nonstandard model of arithmetic for which there an algorithm to compute addition and multiplication?

- It is natural to think of elements of a nonstandard model as $\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}$.
- $(p, m) + n = (p, m + n)$. How about $(p, m) \cdot n$?



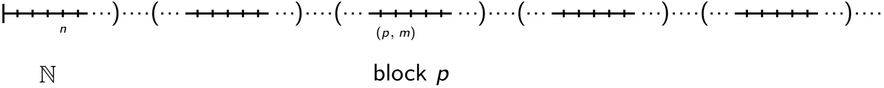
- How about $(p, m) + (q, n)$, $(p, n) \cdot (q, m)$?



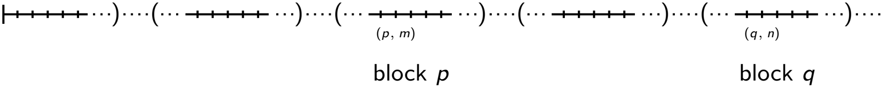
An Android app for a nonstandard model of arithmetic?

Question: Can we compute inside a nonstandard model of arithmetic?
Is there a nonstandard model of arithmetic for which there an algorithm to compute addition and multiplication?

- It is natural to think of elements of a nonstandard model as $\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}$.
- $(p, m) + n = (p, m + n)$. How about $(p, m) \cdot n$?



- How about $(p, m) + (q, n)$, $(p, n) \cdot (q, m)$?



- Is there a nonstandard model of arithmetic for which there is algorithm to compute
  - $(p, m) + (q, n)$,
  - $(p, m) \cdot n$,
  - $(p, m) \cdot (q, n)$?

Tennenbaum's Theorem

"All you really need to know for the moment is that the universe is a lot more complicated than you might think, even if you start from a position of thinking it's pretty damn complicated in the first place." – Douglas Adams

Theorem: (Tennenbaum, 1959) There is no nonstandard model of arithmetic for which there is an algorithm to compute any of the following $(p, m) + (q, n)$, $(p, m) \cdot n$, $(p, m) \cdot (q, n)$.

Tennenbaum's Theorem

"All you really need to know for the moment is that the universe is a lot more complicated than you might think, even if you start from a position of thinking it's pretty damn complicated in the first place." – Douglas Adams

Theorem: (Tennenbaum, 1959) There is no nonstandard model of arithmetic for which there is an algorithm to compute any of the following $(p, m) + (q, n)$, $(p, m) \cdot n$, $(p, m) \cdot (q, n)$.

- We cannot hope to compute inside a nonstandard model of arithmetic!
- Every nonstandard model of arithmetic contains non-algorithmic information.
- $(\mathbb{N}, +, \cdot, <, 0, 1)$ is the unique computable model of arithmetic!

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.
- Every finite set of numbers is coded by some natural number, e.g., the set $\{0, 5, 7\}$ is coded by $161 = 2^0 + 2^5 + 2^7$.

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.
- Every finite set of numbers is coded by some natural number, e.g., the set $\{0, 5, 7\}$ is coded by $161 = 2^0 + 2^5 + 2^7$.

Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic.

- Every $c \in M$ has a unique binary expansion.

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.
- Every finite set of numbers is coded by some natural number, e.g., the set $\{0, 5, 7\}$ is coded by $161 = 2^0 + 2^5 + 2^7$.

Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic.

- Every $c \in M$ has a unique binary expansion.
- Every $c \in M$ codes a (possibly infinite) subset of $\mathbb{N}$!

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.
- Every finite set of numbers is coded by some natural number, e.g., the set $\{0, 5, 7\}$ is coded by $161 = 2^0 + 2^5 + 2^7$.

Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic.

- Every $c \in M$ has a unique binary expansion.
- Every $c \in M$ codes a (possibly infinite) subset of $\mathbb{N}$!
  - $c = 2^1 + 2^3 + 2^5 + \cdots + 2^{2b+1}$ $(b > \mathbb{N})$ codes the odd numbers.

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.
- Every finite set of numbers is coded by some natural number, e.g., the set $\{0, 5, 7\}$ is coded by $161 = 2^0 + 2^5 + 2^7$.

Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic.

- Every $c \in M$ has a unique binary expansion.
- Every $c \in M$ codes a (possibly infinite) subset of $\mathbb{N}$!
  - $c = 2^1 + 2^3 + 2^5 + \cdots + 2^{2b+1}$ ($b > \mathbb{N}$) codes the odd numbers.
  - $c = 2^2 + 2^3 + 2^5 + 2^7 + \cdots + 2^p$ ($p > \mathbb{N}$ is a nonstandard prime) codes the prime numbers.

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.
- Every finite set of numbers is coded by some natural number, e.g., the set $\{0, 5, 7\}$ is coded by $161 = 2^0 + 2^5 + 2^7$.

Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic.

- Every $c \in M$ has a unique binary expansion.
- Every $c \in M$ codes a (possibly infinite) subset of $\mathbb{N}$!
  - $c = 2^1 + 2^3 + 2^5 + \cdots + 2^{2b+1}$ ($b > \mathbb{N}$) codes the odd numbers.
  - $c = 2^2 + 2^3 + 2^5 + 2^7 + \cdots + 2^p$ ($p > \mathbb{N}$ is a nonstandard prime) codes the prime numbers.

Definition: A subset A of $\mathbb{N}$ is coded in a nonstandard model $(M, +, \cdot, <, 0, 1)$ if there is $c \in M$ coding A.

Coding sets of natural numbers into a nonstandard model

Theorem: Every natural number has a unique binary expansion.

- This follows from the Peano axioms, and therefore extends to nonstandard models.
- Every natural number codes a finite set of numbers, e.g., $1288 = 2^3 + 2^8 + 2^{10}$ codes the set $\{3, 8, 10\}$.
- Every finite set of numbers is coded by some natural number, e.g., the set $\{0, 5, 7\}$ is coded by $161 = 2^0 + 2^5 + 2^7$.

Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic.

- Every $c \in M$ has a unique binary expansion.
- Every $c \in M$ codes a (possibly infinite) subset of $\mathbb{N}$!
  - $c = 2^1 + 2^3 + 2^5 + \cdots + 2^{2b+1}$ ($b > \mathbb{N}$) codes the odd numbers.
  - $c = 2^2 + 2^3 + 2^5 + 2^7 + \cdots + 2^p$ ($p > \mathbb{N}$ is a nonstandard prime) codes the prime numbers.

Definition: A subset A of $\mathbb{N}$ is coded in a nonstandard model $(M, +, \cdot, <, 0, 1)$ if there is $c \in M$ coding A.

Question: What can we say about subsets of $\mathbb{N}$ coded in a nonstandard model M?

Computable sets of natural numbers

Definition: A subset A of $\mathbb{N}$ is computable if there is an algorithm to determine membership in A.

- There is a computer program which outputs 1 if $n \in A$ and 0 if $n \notin A$.

Computable sets of natural numbers

Definition: A subset A of $\mathbb{N}$ is computable if there is an algorithm to determine membership in A.

- There is a computer program which outputs 1 if $n \in A$ and 0 if $n \notin A$.

Computable sets:

- the set of odd numbers

Computable sets of natural numbers

Definition: A subset A of $\mathbb{N}$ is computable if there is an algorithm to determine membership in A.

- There is a computer program which outputs 1 if $n \in A$ and 0 if $n \notin A$.

Computable sets:

- the set of odd numbers
- the set of prime numbers

Computable sets of natural numbers

Definition: A subset A of $\mathbb{N}$ is computable if there is an algorithm to determine membership in A.

- There is a computer program which outputs 1 if $n \in A$ and 0 if $n \notin A$.

Computable sets:

- the set of odd numbers
- the set of prime numbers
- the set of codes of the Peano axioms
  - fix a reasonable coding of strings into numbers
  - in practice, this is done by any text editor

Computable sets of natural numbers

Definition: A subset A of $\mathbb{N}$ is computable if there is an algorithm to determine membership in A.

- There is a computer program which outputs 1 if $n \in A$ and 0 if $n \notin A$.

Computable sets:

- the set of odd numbers
- the set of prime numbers
- the set of codes of the Peano axioms
  - fix a reasonable coding of strings into numbers
  - in practice, this is done by any text editor

Non-computable sets:

- the set of codes of true arithmetic statements

Sets of natural numbers coded in a nonstandard model

Theorem: Every nonstandard model of arithmetic codes all computable sets.

Sets of natural numbers coded in a nonstandard model

Theorem: Every nonstandard model of arithmetic codes all computable sets.

Theorem: Every set of natural numbers is coded in some countable nonstandard model.

Sets of natural numbers coded in a nonstandard model

Theorem: Every nonstandard model of arithmetic codes all computable sets.

Theorem: Every set of natural numbers is coded in some countable nonstandard model.

Proof:

- Every finite initial segment of A is coded by some natural number.

Sets of natural numbers coded in a nonstandard model

Theorem: Every nonstandard model of arithmetic codes all computable sets.

Theorem: Every set of natural numbers is coded in some countable nonstandard model.

Proof:

- Every finite initial segment of A is coded by some natural number.
- Write down a collection of statements in $\mathcal{L}_A$ together with a new constant c:
  - If $n \in A$, then the n^{th}-digit in the binary expansion of c is 1.
  - If $n \notin A$, then n^{th}-digit in the binary expansion of c is 0.

Sets of natural numbers coded in a nonstandard model

Theorem: Every nonstandard model of arithmetic codes all computable sets.

Theorem: Every set of natural numbers is coded in some countable nonstandard model.

Proof:

- Every finite initial segment of A is coded by some natural number.
- Write down a collection of statements in $\mathcal{L}_A$ together with a new constant c:
  - If $n \in A$, then the n^{th}-digit in the binary expansion of c is 1.
  - If $n \notin A$, then n^{th}-digit in the binary expansion of c is 0.
- Use completeness theorem. $\square$

Sets of natural numbers coded in a nonstandard model

Theorem: Every nonstandard model of arithmetic codes all computable sets.

Theorem: Every set of natural numbers is coded in some countable nonstandard model.

Proof:

- Every finite initial segment of A is coded by some natural number.
- Write down a collection of statements in $\mathcal{L}_A$ together with a new constant c:
  - If $n \in A$, then the n^{th}-digit in the binary expansion of c is 1.
  - If $n \notin A$, then n^{th}-digit in the binary expansion of c is 0.
- Use completeness theorem. $\square$

Theorem: Every nonstandard model of arithmetic codes some non-computable set.

- Every nonstandard model of arithmetic contains non-algorithmic information.

Some nonstandard facts about nonstandard models

"If you think this Universe is bad, you should see some of the others." – Philip K. Dick

Theorem: There are continuum many countable non-isomorphic models of arithmetic.

Proof: Every subset of $\mathbb{N}$ is coded in some countable model of arithmetic.

Some nonstandard facts about nonstandard models

"If you think this Universe is bad, you should see some of the others." – Philip K. Dick

Theorem: There are continuum many countable non-isomorphic models of arithmetic.

Proof: Every subset of $\mathbb{N}$ is coded in some countable model of arithmetic.

Theorem: (Friedman, 1973) Every nonstandard countable model of arithmetic is isomorphic to an initial segment of itself.

Some nonstandard facts about nonstandard models

"If you think this Universe is bad, you should see some of the others." – Philip K. Dick

Theorem: There are continuum many countable non-isomorphic models of arithmetic.

Proof: Every subset of $\mathbb{N}$ is coded in some countable model of arithmetic.

Theorem: (Friedman, 1973) Every nonstandard countable model of arithmetic is isomorphic to an initial segment of itself.

Theorem: There are countable models of arithmetic with continuum many automorphisms.

- $(\mathbb{N}, +, \cdot, <, 0, 1)$ has no automorphisms!
- A nonstandard model of arithmetic can have indiscernible numbers - satisfying the exact same first-order properties.

Goodstein sequences

Hereditary base *n* notation

Example: Write 3003 in hereditary base 3 notation.

- $3^7 + 3^6 + 3^4 + 2 \cdot 3^1$
- $3^{2\cdot 3+1} + 3^{2\cdot 3} + 3^{3+1} + 2 \cdot 3^1$
- $3^{3+3+1} + 3^{3+3} + 3^{3+1} + 3^1 + 3^1$

Hereditary base n notation

Example: Write 3003 in hereditary base 3 notation.

- $3^7 + 3^6 + 3^4 + 2 \cdot 3^1$
- $3^{2\cdot 3+1} + 3^{2\cdot 3} + 3^{3+1} + 2 \cdot 3^1$
- $3^{3+3+1} + 3^{3+3} + 3^{3+1} + 3^1 + 3^1$

To write a number in hereditary base n notation:

- Write the number in base n: $a_k n^k + a_{k-1} n^{k_1} + \cdots + a_1 n + a_0$ where each $a_i < n$.
- Replace each $a_i n^i$ with $\underbrace{n^i + \cdots + n^i}_{a_i \text{ times}}$
- Write every exponent in hereditary base n notation.
- You are done when every digit appearing in the expression is either n or 1.

Goodstein sequences (continued)

Goodstein sequence G_m:

- $G_m(1)$: m

Goodstein sequences (continued)

Goodstein sequence G_m:

- $G_m(1)$: m
- $G_m(2)$
  - write $G_m(1)$ in hereditary base 2 notation
  - replace all 2's by 3's
  - subtract 1

Goodstein sequences (continued)

Goodstein sequence G_m:

- $G_m(1)$: m
- $G_m(2)$
  - write $G_m(1)$ in hereditary base 2 notation
  - replace all 2's by 3's
  - subtract 1
- $G_m(n+1)$
  - write $G_m(n)$ in hereditary base $n+1$ notation
  - replace all $n+1$ by $n+2$
  - subtract 1

Goodstein sequences (continued)

Goodstein sequence G_m:

- $G_m(1)$: m
- $G_m(2)$
  - write $G_m(1)$ in hereditary base 2 notation
  - replace all 2's by 3's
  - subtract 1
- $G_m(n+1)$
  - write $G_m(n)$ in hereditary base $n+1$ notation
  - replace all $n+1$ by $n+2$
  - subtract 1

Example: $G_3 = \{3, 3, 3, 2, 1, 0\}$

$G_3(1)$			3
$G_3(2)$	2^1+1	3^1+1	3
$G_3(3)$	3^1	4^1	3
$G_3(4)$	$1+1+1$	$1+1+1$	2
$G_3(5)$	$1+1$	$1+1$	1
$G_3(6)$	1	1	0

Goodstein sequences: G_4

$G_4(1)$			4
$G_4(2)$	2^2	3^3	26
$G_4(3)$	$3^{1+1}+3^{1+1}+3+3+1+1$	$4^{1+1}+4^{1+1}+4+4+1+1$	41
$G_4(4)$	$4^{1+1}+4^{1+1}+4+4+1$	$5^{1+1}+5^{1+1}+5+5+1$	60
$G_4(5)$	$5^{1+1}+5^{1+1}+5+5$	$6^{1+1}+6^{1+1}+6+6$	83
$G_4(6)$	$6^{1+1}+6^{1+1}+6+1+1+1+1+1$	$7^{1+1}+7^{1+1}+7+1+1+1+1+1$	109
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$G_4(11)$	$11^{1+1}+11^{1+1}+11$	$12^{1+1}+12^{1+1}+12$	253
$G_4(11)$	$12^{1+1}+12^{1+1}+1+1+\cdots+1$	$13^{1+1}+13^{1+1}+1+1+\cdots+1$	299
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Goodstein sequences: G_4

$G_4(1)$			4
$G_4(2)$	2^2	3^3	26
$G_4(3)$	$3^{1+1}+3^{1+1}+3+3+1+1$	$4^{1+1}+4^{1+1}+4+4+1+1$	41
$G_4(4)$	$4^{1+1}+4^{1+1}+4+4+1$	$5^{1+1}+5^{1+1}+5+5+1$	60
$G_4(5)$	$5^{1+1}+5^{1+1}+5+5$	$6^{1+1}+6^{1+1}+6+6$	83
$G_4(6)$	$6^{1+1}+6^{1+1}+6+1+1+1+1+1$	$7^{1+1}+7^{1+1}+7+1+1+1+1+1$	109
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$G_4(11)$	$11^{1+1}+11^{1+1}+11$	$12^{1+1}+12^{1+1}+12$	253
$G_4(11)$	$12^{1+1}+12^{1+1}+1+1+\cdots+1$	$13^{1+1}+13^{1+1}+1+1+\cdots+1$	299
$\vdots$	$\vdots$	$\vdots$	$\vdots$

"Elements of G_4 continue to increase for a while, but at base $3\cdot 2^{402653209}$, they reach a maximum of $3\cdot 2^{402653210}-1$, stay there for the next $3\cdot 2^{402653209}$ steps, then begin their first and final descent to 0." – Wikipedia

Theorem: (Goodstein, 1944) For every m, the sequence G_m is eventually 0.

- The proof uses Zermelo-Fraenkel set theory.
- Zermelo-Fraenkel set theory is a much stronger axiomatic system.

Applications of nonstandard models: Goodstein's Theorem

Theorem: (Goodstein, 1944) For every m, the sequence G_m is eventually 0.

- The proof uses Zermelo-Fraenkel set theory.
- Zermelo-Fraenkel set theory is a much stronger axiomatic system.

Theorem: (Kirby, Paris, 1982) Goodstein's Theorem cannot be proved from the Peano axioms.

- The proof uses nonstandard models of arithmetic!

Applications of nonstandard models: logician's dreamland

Twin prime conjecture: (Polignac, 1849) There are infinitely many primes p such that $p+2$ is also prime.

- largest known twin primes: $3756801695685 \cdot 2^{666669} \pm 1$ (Wikipedia)

Applications of nonstandard models: logician's dreamland

Twin prime conjecture: (Polignac, 1849) There are infinitely many primes p such that $p+2$ is also prime.

- largest known twin primes: $3756801695685 \cdot 2^{666669} \pm 1$ (Wikipedia)

Theorem: (Zhang, Polymath project, 2013-14) There is $n < 246$ such that there are infinitely many primes separated by n numbers.

Applications of nonstandard models: logician's dreamland

Twin prime conjecture: (Polignac, 1849) There are infinitely many primes p such that $p+2$ is also prime.

- largest known twin primes: $3756801695685 \cdot 2^{666669} \pm 1$ (Wikipedia)

Theorem: (Zhang, Polymath project, 2013-14) There is $n < 246$ such that there are infinitely many primes separated by n numbers.

Observation: Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic satisfying all true statements about $\mathbb{N}$. If M has a twin prime pair above $\mathbb{N}$, then the twin prime conjecture is true.

Applications of nonstandard models: logician's dreamland

Twin prime conjecture: (Polignac, 1849) There are infinitely many primes p such that $p+2$ is also prime.

- largest known twin primes: $3756801695685 \cdot 2^{666669} \pm 1$ (Wikipedia)

Theorem: (Zhang, Polymath project, 2013-14) There is $n < 246$ such that there are infinitely many primes separated by n numbers.

Observation: Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic satisfying all true statements about $\mathbb{N}$. If M has a twin prime pair above $\mathbb{N}$, then the twin prime conjecture is true.

Proof:

- Suppose p and $p+2$ are prime in M with $p > \mathbb{N}$.

Applications of nonstandard models: logician's dreamland

Twin prime conjecture: (Polignac, 1849) There are infinitely many primes p such that $p+2$ is also prime.

- largest known twin primes: $3756801695685 \cdot 2^{666669} \pm 1$ (Wikipedia)

Theorem: (Zhang, Polymath project, 2013-14) There is $n < 246$ such that there are infinitely many primes separated by n numbers.

Observation: Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic satisfying all true statements about $\mathbb{N}$. If M has a twin prime pair above $\mathbb{N}$, then the twin prime conjecture is true.

Proof:

- Suppose p and $p+2$ are prime in M with $p > \mathbb{N}$.
- For every $n \in \mathbb{N}$, M satisfies that there is a twin prime pair above n.

Applications of nonstandard models: logician's dreamland

Twin prime conjecture: (Polignac, 1849) There are infinitely many primes p such that $p+2$ is also prime.

- largest known twin primes: $3756801695685 \cdot 2^{666669} \pm 1$ (Wikipedia)

Theorem: (Zhang, Polymath project, 2013-14) There is $n < 246$ such that there are infinitely many primes separated by n numbers.

Observation: Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic satisfying all true statements about $\mathbb{N}$. If M has a twin prime pair above $\mathbb{N}$, then the twin prime conjecture is true.

Proof:

- Suppose p and $p+2$ are prime in M with $p > \mathbb{N}$.
- For every $n \in \mathbb{N}$, M satisfies that there is a twin prime pair above n.
- M and $\mathbb{N}$ satisfy the same arithmetic statements.

Applications of nonstandard models: logician's dreamland

Twin prime conjecture: (Polignac, 1849) There are infinitely many primes p such that $p+2$ is also prime.

- largest known twin primes: $3756801695685 \cdot 2^{666669} \pm 1$ (Wikipedia)

Theorem: (Zhang, Polymath project, 2013-14) There is $n < 246$ such that there are infinitely many primes separated by n numbers.

Observation: Suppose that $(M, +, \cdot, <, 0, 1)$ is a nonstandard model of arithmetic satisfying all true statements about $\mathbb{N}$. If M has a twin prime pair above $\mathbb{N}$, then the twin prime conjecture is true.

Proof:

- Suppose p and $p+2$ are prime in M with $p > \mathbb{N}$.
- For every $n \in \mathbb{N}$, M satisfies that there is a twin prime pair above n.
- M and $\mathbb{N}$ satisfy the same arithmetic statements.
- For every n, $\mathbb{N}$ satisfies that there is a twin prime pair above n. $\square$

Applications of nonstandard models: logician's dreamland

$P = NP$**?**

- If there is a fast algorithm to verify whether a solution to a problem is correct, is there a fast algorithm to compute the solution?
- This is an arithmetic statement (algorithms are coded by numbers).

A very Bold Conjecture: One day, we will use nonstandard models of arithmetic to show that $P = NP$ cannot be proved from the Peano axioms!

In the meantime, I like to study nonstandard models of arithmetic for the sake of their own uniquely beautiful properties.

Thank you!