Nonstandard Numbers

Athar Abdul-Quader

Purchase College, SUNY

Hofstra Mathematics Department Seminar
April 9, 2025

Formalization

- 1700s / 1800s: formalizing notions of calculus (Bolzano, Weierstrauss, Cauchy: limits, continuity)
- Development of set theory (Cantor, late 1800s)
- Foundational crises!
- Axiomatic theories (Late 1800s Dedekind-Peano, early 1900s Zermelo)
- Early 1900s: Hilbert's program

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. What exactly does "..." mean? Aren't mathematical definitions supposed to be precise?

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. What exactly does "..." mean? Aren't mathematical definitions supposed to be precise?

Definition

$\mathbb{N}$ is the smallest set containing 0 that is closed under the operation of adding 1.

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. What exactly does "..." mean? Aren't mathematical definitions supposed to be precise?

Definition

$\mathbb{N}$ is the smallest set containing 0 that is closed under the operation of adding 1.

The word "smallest" is key here. One can imagine a set containing $\mathbb{N}$ and an "infinite element" c, together with all of its successors: $\{0, 1, 2, 3, \ldots, c, c+1, c+2, c+3, \ldots\}$. Such a set would contain 0 and be closed under adding 1. c is kind of "unreachable" from 0.

Arithmetic: $+$, $\times$ and $<$

The definition in the previous slide just describes the *set* of natural numbers; it doesn't describe the arithmetical structure. This can be described with the (Dedekind-)Peano axioms:

- For all natural numbers a and b, $a+b$ is a natural number ($\mathbb{N}$ is closed under addition).
- For all natural numbers a and b, ab is a natural number ($\mathbb{N}$ is closed under multiplication).
- For all natural numbers a, b and c, $a(b+c) = ab + ac$ (multiplication distributes over addition).
- Addition and multiplication are commutative, associative, etc.
- For all natural numbers a and b, $a < b$ or $b < a$ or $a = b$.
- ... (There are many more: Every natural number has a unique "successor", every non-zero natural number has a unique "predecessor", etc.)

First Order Logic

We can use the first order language of arithmetic $(0, 1, +, \times, <)$ to formalize the statements in the previous slide.

First Order Logic

We can use the first order language of arithmetic $(0, 1, +, \times, <)$ to formalize the statements in the previous slide.

- Formulas are built using variables, $0, 1$, $+, \times, <$ and $=$.

First Order Logic

We can use the first order language of arithmetic $(0, 1, +, \times, <)$ to formalize the statements in the previous slide.

- Formulas are built using variables, $0, 1$, $+$, $\times$, $<$ and $=$.
- If ϕ and ψ are formulas, then so are $\phi \wedge \psi$ ("ϕ and ψ"), $\phi \vee \psi$ ("ϕ or ψ"), $\neg\phi$ ("Not ϕ"), and $\phi \to \psi$ ("If ϕ, then ψ.")

First Order Logic

We can use the first order language of arithmetic $(0, 1, +, \times, <)$ to formalize the statements in the previous slide.

- Formulas are built using variables, $0, 1$, $+$, $\times$, $<$ and $=$.
- If ϕ and ψ are formulas, then so are $\phi \wedge \psi$ ("ϕ and ψ"), $\phi \vee \psi$ ("ϕ or ψ"), $\neg\phi$ ("Not ϕ"), and $\phi \to \psi$ ("If ϕ, then ψ.")
- Formulas can have free variables: e.g. $\psi(y) = 1 < y$ expresses "y is greater than 1."

First Order Logic

We can use the first order language of arithmetic $(0, 1, +, \times, <)$ to formalize the statements in the previous slide.

- Formulas are built using variables, $0, 1$, $+$, $\times$, $<$ and $=$.
- If ϕ and ψ are formulas, then so are $\phi \wedge \psi$ ("ϕ and ψ"), $\phi \vee \psi$ ("ϕ or ψ"), $\neg\phi$ ("Not ϕ"), and $\phi \rightarrow \psi$ ("If ϕ, then ψ.")
- Formulas can have free variables: e.g. $\psi(y) = 1 < y$ expresses "y is greater than 1."
- We can also quantify over variables in a formula using $\forall$ ("For all") and $\exists$ ("There exists").
  $\phi(y) = 1 < y \wedge \forall a \forall b(a \times b = y \rightarrow (a = y \vee b = y))$ expresses "y is a prime number".
- For the above formula $\phi(y)$, $\mathbb{N} \models \phi(2)$ and $\mathbb{N} \models \neg\phi(6)$.

Categoricity

Many mathematical structures that have those same properties. What makes $\mathbb{N}$ unique? We already said this: $\mathbb{N}$ is the smallest set containing 0 and closed under successors!

How do we express this formally?

Dedekind-Peano

Dedekind (1888) / Peano (1889): axiomatization of $\mathbb{N}$ using just 0 and S (for "successor"):

- $0 \in \mathbb{N}$
- For every $n \in \mathbb{N}$, $S(n) \in \mathbb{N}$ ($\mathbb{N}$ is closed under successors).
- For all $m, n \in \mathbb{N}$, if $S(m) = S(n)$, then $m = n$ (S is an injection).
- For all $n \in \mathbb{N}$, $S(n) \neq 0$ (0 is not a successor).

Dedekind-Peano

Dedekind (1888) / Peano (1889): axiomatization of $\mathbb{N}$ using just 0 and S (for "successor"):

- $0 \in \mathbb{N}$
- For every $n \in \mathbb{N}$, $S(n) \in \mathbb{N}$ ($\mathbb{N}$ is closed under successors).
- For all $m, n \in \mathbb{N}$, if $S(m) = S(n)$, then $m = n$ (S is an injection).
- For all $n \in \mathbb{N}$, $S(n) \neq 0$ (0 is not a successor).

(So far this defines 0, successors, and says that $\mathbb{N}$ is closed under successors. Now how do we say it's the smallest?)

Dedekind-Peano

Dedekind (1888) / Peano (1889): axiomatization of $\mathbb{N}$ using just 0 and S (for "successor"):

- $0 \in \mathbb{N}$
- For every $n \in \mathbb{N}$, $S(n) \in \mathbb{N}$ ($\mathbb{N}$ is closed under successors).
- For all $m, n \in \mathbb{N}$, if $S(m) = S(n)$, then $m = n$ (S is an injection).
- For all $n \in \mathbb{N}$, $S(n) \neq 0$ (0 is not a successor).

(So far this defines 0, successors, and says that $\mathbb{N}$ is closed under successors. Now how do we say it's the smallest?)

- If K is a set with the properties that $0 \in K$ and whenever $n \in K$, then $S(n) \in K$, then $\mathbb{N} \subseteq K$.

Categoricity

Dedekind proved that $\mathbb{N}$ is categorical for these axioms: that is, if any structure $(M, 0', S')$ satisfies these same axioms, then $(\mathbb{N}, 0, S) \cong (M, 0', S')$.

Proof.

The isomorphism $f : \mathbb{N} \to M$ is defined inductively so that:

- $0 \mapsto 0'$
- If $m \mapsto n$, then $S(m) \mapsto S'(n)$.

(Need to prove this is an isomorphism; ie that this defines a function that is one to one, onto, and commutes with successors.) □

Formalizing

The Dedekind-Peano axiomatization can be formalized in first-order logic, with one major caveat.

Notice the difference between a sentence like

$$\forall n \forall m (S(n) = S(m) \to n = m)$$

and

$$\forall K (0 \in K \wedge (n \in K \to S(n) \in K)) \to \forall n (n \in K)?$$

First and Second Order

The distinction: what *objects* are we quantifying over?

- The ones in the set $\mathbb{N}$?
- The *subsets* of $\mathbb{N}$?

The Dedekind-Peano axiomatization is a *second-order* axiomatization of $\mathbb{N}$. Can we translate it to first-order logic?

Scheme

Let's go back to the language with $0, 1, +, \times, <$.

Instead of quantifying over *all* sets K, we can add an infinite scheme of axioms, one for each formula $\phi(x, \bar{y})$ in this language:

$$\forall \bar{v}(\phi(0, \bar{v}) \wedge \forall x(\phi(x, \bar{v}) \rightarrow \phi(x+1, \bar{v})) \rightarrow \forall x(\phi(x, \bar{v})))$$

This is the axiom schema of induction. Now we have a first-order axiomatization of arithmetic!

Scheme

Let's go back to the language with $0, 1, +, \times, <$.

Instead of quantifying over *all* sets K, we can add an infinite scheme of axioms, one for each formula $\phi(x, \bar{y})$ in this language:

$$\forall \bar{v}(\phi(0, \bar{v}) \wedge \forall x(\phi(x, \bar{v}) \rightarrow \phi(x+1, \bar{v})) \rightarrow \forall x(\phi(x, \bar{v})))$$

This is the axiom schema of induction. Now we have a first-order axiomatization of arithmetic!

Is this good enough?

Aside: Models and Theories

A statement is a formula without free variables. A theory is a consistent collection of statements (in some fixed "language").

Aside: Models and Theories

A statement is a formula without free variables. A theory is a consistent collection of statements (in some fixed “language”).

- Can reason axiomatically: start with a theory, and see what we can prove from that theory (need a proof system).
- Alternatively, start with a mathematical structure (a set with some operations like $+$ and/or relations like $<$), describe the properties that are true about that structure.
- The interplay between these two approaches is the heart of model theory, a branch of mathematical logic.

Aside: Models and Theories

A statement is a formula without free variables. A theory is a consistent collection of statements (in some fixed "language").

- Can reason axiomatically: start with a theory, and see what we can prove from that theory (need a proof system).
- Alternatively, start with a mathematical structure (a set with some operations like $+$ and/or relations like $<$), describe the properties that are true about that structure.
- The interplay between these two approaches is the heart of model theory, a branch of mathematical logic.

Definition

- A model of a theory is a set M such that every statement in the theory is true in M.

Aside: Models and Theories

A statement is a formula without free variables. A theory is a consistent collection of statements (in some fixed "language").

- Can reason axiomatically: start with a theory, and see what we can prove from that theory (need a proof system).
- Alternatively, start with a mathematical structure (a set with some operations like $+$ and/or relations like $<$), describe the properties that are true about that structure.
- The interplay between these two approaches is the heart of model theory, a branch of mathematical logic.

Definition

- A model of a theory is a set M such that every statement in the theory is true in M.
- Given a structure M $\mathrm{Th}(M)$ is the set of all first-order statements that are true about M.

Completeness / Compactness

Fix a first-order language $\mathcal{L}$. Let T be a theory and ϕ a sentence.

- If there is a proof of ϕ from T, we write $T \vdash \phi$.
- If M is a model and ϕ is true in M, we write $M \models \phi$.
- If, in *every* model M of T, it happens that $M \models \phi$, then we write $T \models \phi$.

Theorem (Gödel's Completeness Theorem)

Fix a language $\mathcal{L}$. For every theory T and sentence ϕ, $T \vdash \phi$ if and only if $T \models \phi$.

Importantly: proofs are finite! This implies:

Theorem (Compactness Theorem)

A theory T has a model if and only if every finite subset $T_0 \subseteq T$ has a model.

Nonstandardness

- PA is the first-order theory including the axioms for arithmetic (in the language $0, 1, +, \times, <$).
- Describes the algebraic structure (commutativity, associativity, etc), ordering, and the induction scheme.
- Consider the theory T (in an expanded language which has a new symbol c) consisting of PA as well as all statements of the form $c > n$ for each natural number n.

Nonstandardness

- PA is the first-order theory including the axioms for arithmetic (in the language $0, 1, +, \times, <$).
- Describes the algebraic structure (commutativity, associativity, etc), ordering, and the induction scheme.
- Consider the theory T (in an expanded language which has a new symbol c) consisting of PA as well as all statements of the form $c > n$ for each natural number n.
- Take any finite subset T_0 of T: there is natural number $c \in \mathbb{N}$ satisfying all those statements.

Nonstandardness

- PA is the first-order theory including the axioms for arithmetic (in the language $0, 1, +, \times, <$).
- Describes the algebraic structure (commutativity, associativity, etc), ordering, and the induction scheme.
- Consider the theory T (in an expanded language which has a new symbol c) consisting of PA as well as all statements of the form $c > n$ for each natural number n.
- Take any finite subset T_0 of T: there is natural number $c \in \mathbb{N}$ satisfying all those statements.
- By the compactness theorem, there is a model M of T.

Nonstandardness

- PA is the first-order theory including the axioms for arithmetic (in the language $0, 1, +, \times, <$).
- Describes the algebraic structure (commutativity, associativity, etc), ordering, and the induction scheme.
- Consider the theory T (in an expanded language which has a new symbol c) consisting of PA as well as all statements of the form $c > n$ for each natural number n.
- Take any finite subset T_0 of T: there is natural number $c \in \mathbb{N}$ satisfying all those statements.
- By the compactness theorem, there is a model M of T.
- But in this model, c cannot be any natural number n! So this model M must contain non-standard elements.

M is called a non-standard model of arithmetic!

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.
- If $c \in M$ is nonstandard, then $c+1, c+2, \ldots$ are all in M

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.
- If $c \in M$ is nonstandard, then $c+1, c+2, \ldots$ are all in M
- $c \neq 0$, so it is a successor: $c-1, c-2, \ldots$ are all in M.

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.
- If $c \in M$ is nonstandard, then $c+1, c+2, \dots$ are all in M
- $c \neq 0$, so it is a successor: $c-1, c-2, \dots$ are all in M.
- That is: $\{c+n : n \in \mathbb{Z}\} \subseteq M$.

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.
- If $c \in M$ is nonstandard, then $c+1, c+2, \ldots$ are all in M
- $c \neq 0$, so it is a successor: $c-1, c-2, \ldots$ are all in M.
- That is: $\{c+n : n \in \mathbb{Z}\} \subseteq M$.
- $2c$? $3c$? c^2?

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.
- If $c \in M$ is nonstandard, then $c+1, c+2, \ldots$ are all in M
- $c \neq 0$, so it is a successor: $c-1, c-2, \ldots$ are all in M.
- That is: $\{c+n : n \in \mathbb{Z}\} \subseteq M$.
- $2c$? $3c$? c^2?
- Can prove via induction: every number is either even or odd (congruent to 0 or 1 mod 2). So $\lfloor \frac{c}{2} \rfloor \in M$.

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.
- If $c \in M$ is nonstandard, then $c+1, c+2, \ldots$ are all in M
- $c \neq 0$, so it is a successor: $c-1, c-2, \ldots$ are all in M.
- That is: $\{c+n : n \in \mathbb{Z}\} \subseteq M$.
- $2c$? $3c$? c^2?
- Can prove via induction: every number is either even or odd (congruent to 0 or 1 mod 2). So $\lfloor \frac{c}{2} \rfloor \in M$.
- But also, same reasoning holds about $\{\lfloor \frac{c}{2} \rfloor + n : n \in \mathbb{Z}\}$, $\{\lfloor \frac{3c}{2} \rfloor + n : n \in \mathbb{Z}\}, \ldots$

What do they look like?

Suppose M is a nonstandard model of PA.

- $0 \in M$, $1 \in M$, etc. That is: $\mathbb{N} \subseteq M$.
- If $c \in M$ is nonstandard, then $c+1, c+2, \ldots$ are all in M
- $c \neq 0$, so it is a successor: $c-1, c-2, \ldots$ are all in M.
- That is: $\{c+n : n \in \mathbb{Z}\} \subseteq M$.
- $2c$? $3c$? c^2?
- Can prove via induction: every number is either even or odd (congruent to 0 or 1 mod 2). So $\lfloor \frac{c}{2} \rfloor \in M$.
- But also, same reasoning holds about $\{\lfloor \frac{c}{2} \rfloor + n : n \in \mathbb{Z}\}$, $\{\lfloor \frac{3c}{2} \rfloor + n : n \in \mathbb{Z}\}$, ...

Every countable, non-standard model of PA looks like a copy of $\mathbb{N}$, followed by $\mathbb{Q}$-many copies of $\mathbb{Z}$ (ie a dense ordering of $\mathbb{Z}$-chains above $\mathbb{N}$)!

What do they think?

Euclidean division: if $M \models \mathrm{PA}$, and $b, c \in M$ with $b \neq 0$, then $M \models \exists q \exists r (r < b \wedge c = qb + r)$. How do we see this?

Proof.

Fix $b \neq 0$ and let $\phi(x)$ be the formula $\exists q \exists r (r < b \wedge x = qb + r)$. Then $\phi(0)$ is true. (Why?)

Suppose $x \in M$ and $M \models \phi(x)$. Then there are q, r such that $M \models x = qb + r$. Then $M \models x + 1 = qb + r + 1$. If $r + 1 < b$, we are done.

If not? Then $r + 1 = b$, and so $M \models x + 1 = qb + b = (q + 1)b + 0$, and therefore $M \models \phi(x + 1)$. $\square$

What do they think?

What else is true in M?

- Almost any number-theoretic statement you can think of.
- Chinese Remainder Theorem
- Binary representations: there is a formula $b(x, y)$ that is true if the x-th bit of y is 1.
- Fundamental Theorem of Arithmetic
- Infinitude of the primes
- ...

Elementarity

Definition

If $M \subseteq N$ and M and N agree on $+$, $\times$, and the $<$ relation for elements of M, then M is a substructure of N and N is an extension of M.

Elementarity

Definition

If $M \subseteq N$ and M and N agree on $+$, $\times$, and the $<$ relation for elements of M, then M is a substructure of N and N is an extension of M.

If $M \subseteq N$ is a substructure, then they agree on the truth of any quantifier-free statements involving parameters from M.

If, for every formula $\phi(x_0, \ldots, x_{n-1})$ and all $a_0, \ldots, a_{n-1} \in M$, $M \models \phi(\bar{a})$ if and only if $N \models \phi(\bar{a})$, the extension is elementary, written $M \prec N$. M is called an elementary substructure of N, and N is called an elementary extension of M. We write $M \prec N$.

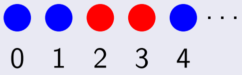
Colorings

$\mathbb{N}$ is the set of natural numbers: $\{0, 1, 2, 3, \ldots\}$

A two-coloring of a set X is a function $f : X \to \{$ red, blue $\}$.

Example

A two-coloring of $\mathbb{N}$:



Ramsey's Theorem

Definition

Let X be a set and $n > 0$ a natural number. The set $[X]^n$ is the set $\{A \subseteq X : |A| = n\}$, the set of all n-element subsets of X.

Ramsey's Theorem

Definition

Let X be a set and $n > 0$ a natural number. The set $[X]^n$ is the set $\{A \subseteq X : |A| = n\}$, the set of all n-element subsets of X.

For example, $[\mathbb{N}]^2$ is the set containing
$\{0,1\}, \{0,2\}, \{1,2\}, \{0,3\}, \{1,3\}, \{2,3\}, \ldots$

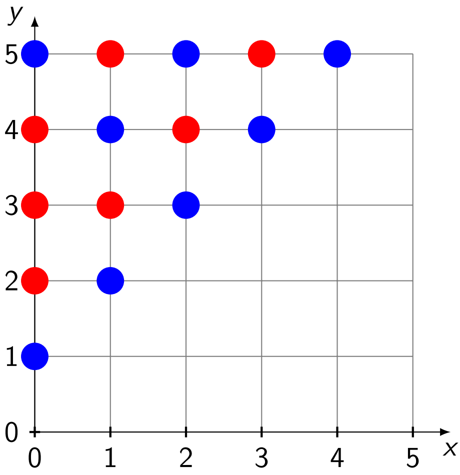
Theorem (Ramsey's Theorem for Pairs)

Let f be a two-coloring of $[\mathbb{N}]^2$. There is an infinite $H \subseteq \mathbb{N}$ such that $f \restriction [H]^2$ is constant.

A set H satisfying the theorem above is called homogeneous for the coloring f.

Ramsey's Theorem

A two-coloring of $[\mathbb{N}]^2$



Ramsey's Theorem for Singletons

A significantly easier result is the following:

Theorem (Ramsey's Theorem for Singletons)

Let f be a two-coloring of $\mathbb{N}$. There is an infinite $H \subseteq \mathbb{N}$ such that $f \restriction H$ is constant.

Ramsey's Theorem for Singletons

A significantly easier result is the following:

Theorem (Ramsey's Theorem for Singletons)

Let f be a two-coloring of $\mathbb{N}$. There is an infinite $H \subseteq \mathbb{N}$ such that $f \upharpoonright H$ is constant.

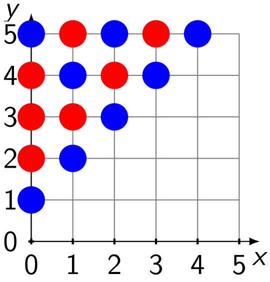
Proof.

Let $B = \{a \in \mathbb{N} : f(a) = \text{blue}\}$, and $R = \{a : f(a) = \text{red}\}$. If both are finite, then their union is finite, but of course $B \cup R = \mathbb{N}$ is infinite. $\square$

Similar "Proof"?

Argument does not directly generalize to pairs.

- Certainly either $B = \{\{x,y\} : f(\{x,y\}) = \text{blue}\}$ or $R = \{\{x,y\} : f(\{x,y\}) = \text{red}\}$ is infinite.
- But it could be that $B = \{\{0,1\},\{1,2\},\{2,3\},\ldots\}$, so that $\{0,3\} \notin B$. So any homogeneous H should not contain 0, 1, and 3.



- We want an infinite set of numbers, not pairs!

Ramsey

Ramsey's Theorem for Pairs, again:

Theorem

Let f be a two-coloring of $[\mathbb{N}]^2$. There is an infinite $H \subseteq \mathbb{N}$ such that $f \restriction [H]^2$ is constant.

Ramsey

Ramsey's Theorem for Pairs, again:

Theorem

Let f be a two-coloring of $[\mathbb{N}]^2$. There is an infinite $H \subseteq \mathbb{N}$ such that $f \restriction [H]^2$ is constant.

Let f be a two-coloring of $[\mathbb{N}]^2$. We expand the language of arithmetic to allow our formulas to talk about f; in other words, we allow build our formulas using $+, \times, <, =$, and f.

Let M be an elementary extension of $\mathbb{N}$ (in this language containing f). Let $b \in M \setminus \mathbb{N}$. So b is nonstandard ($b > n$ for each $n \in \mathbb{N}$).

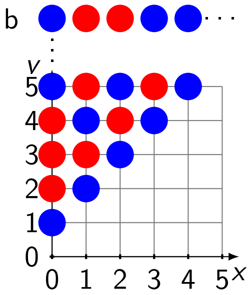
Proof

Define a sequence inductively in M as follows:

- $a_0 = 0$.
- $a_{n+1} =$ the least $a \in M$ such that for every $i \leq n$, $a > a_i$ and $f(a_i, a) = f(a_i, b)$.

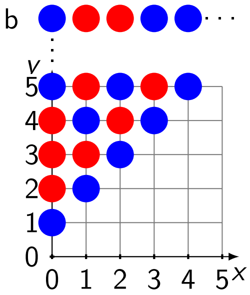
In other words: $f(\cdot, a_{n+1})$ should agree with $f(\cdot, b)$ on $\{a_0, \ldots, a_n\}$.

Proof, Part II



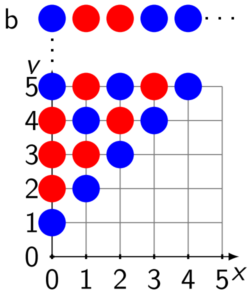
Let $X = \{a_i : i \in M\} \cap \mathbb{N}$. Using elementarity, we show that X is infinite:

Proof, Part II



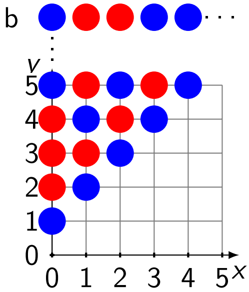
Let $X = \{a_i : i \in M\} \cap \mathbb{N}$. Using elementarity, we show that X is infinite: First, we see that $a_1 \in \mathbb{N}$.

Proof, Part II



Let $X = \{a_i : i \in M\} \cap \mathbb{N}$. Using elementarity, we show that X is infinite: First, we see that $a_1 \in \mathbb{N}$. Suppose $M \models f(0, b) = \text{blue}$. Then $M \models \exists x(f(0, x) = \text{blue})$. By elementarity, $\mathbb{N} \models \exists x(f(0, x) = \text{blue})$, so $a_1 \in \mathbb{N}$.

Proof, Part II



- Similar argument: $a_n \in \mathbb{N}$ for each $n \in \mathbb{N}$.
- Since they are all different, X is infinite.
- Split X into $R = \{a \in X : f(a, b) = \mathrm{red}\}$ and $B = \{a \in X : f(a, b) = \mathrm{blue}\}$.
- One of these is infinite, and both are homogeneous!

Set Theory

Models of PA can be thought of as models of finite set theory:

- Use binary representations and define $x \in y$ to mean the x-th bit of y is 1.
- Can prove that M satisfies all the axioms of set theory (ZFC) except the axiom of infinity!

So we can use the full power of (finite) set theory: we can code sequences, formulas[1], proofs[2], ...

[1] a formula is just a sequence of symbols

[2] a proof is a sequence of formulas with some special properties

Proofs

Just to re-iterate, there is a formula $Pr(x, y)$ which says:

- x codes a sequence of (codes of) statements
- each of which is either an axiom or follows from previous statements in the sequence by the usual rules of proof,
- and that sequence concludes with the statement coded by y.

Let $\theta(y)$ be the formula $\neg\exists x(Pr(x, y))$. What does this say?

Self-reference

Theorem (Gödel 1931 / Carnap 1934)

For every formula $\theta(x)$ in the language of arithmetic, there is a statement P such that $\theta(\ulcorner P \urcorner) \leftrightarrow P$ is true.

In other words, P asserts that it, itself, has the property described by θ.

Self-reference

Theorem (Gödel 1931 / Carnap 1934)

For every formula $\theta(x)$ in the language of arithmetic, there is a statement P such that $\theta(\ulcorner P \urcorner) \leftrightarrow P$ is true.

In other words, P asserts that it, itself, has the property described by θ.

> "How shocking it is to find that self-reference, the stuff of paradox and nonsense, is fundamentally embedded in our beautiful number theory! The fixed point lemma shows that every elementary property F admits a statement of arithmetic asserting 'this statement has property F'."
>
> — Joel David Hamkins

Apply the fixed point lemma

Let $\theta(y)$ be the formula $\neg\exists x(Pr(x, y))$. Suppose P is the fixed point of θ. Then:

- If P is true, then there is no proof of P.
- If P is false, then there is a proof of P.
- Therefore, P *must* be true!
- But there cannot be a proof of P from the axioms of arithmetic!

In other words: there are arithmetic statements that are true (ie, $\mathbb{N} \models P$), but there is no proof of P from the axioms of PA[3]! This is, essentially, Gödel's First Incompleteness Theorem!

[3] What does this mean about nonstandard models of PA?

Hydra

The hydra game is played as follows:

- Begin with a finite tree (with the root at the bottom). This is your hydra. The "heads" of the hydra are the leaves of the tree.
- At stage n: Hercules chooses a head to chop off.
- If the head was attached to the root, nothing else happens (just continue).
- Otherwise, go down one level from the chopped off head, and sprout n copies of that part of the tree.

Hercules wins if, at some finite stage, he has chopped off all of the heads.

Hydra Results

Theorem (Kirby-Paris 1982)

For any finite tree:

1. *Every strategy for Hercules is a winning strategy. (No matter what order he chops the heads off, he will eventually win!)*
2. *We can formalize the notion of winning strategies in* PA, *but* PA *does not prove that Hercules has a winning strategy!*

(Another true but unprovable statement!)

Could Goldbach be independent?

Goldbach's conjecture: every even integer $x \geq 4$ can be expressed as a sum of two primes. Exercises:

1. Write the formula $P(x)$ asserting that x is prime.
2. Write the statement G, using $P(x)$, expressing Goldbach's conjecture.
3. Could G be unprovable from PA?
4. Then there would be $M_1, M_2 \models$ PA where $M_1 \models G$ and $M_2 \models \neg G$.
5. What about $\mathbb{N}$? Can $\mathbb{N} \models G$? Can $\mathbb{N} \models \neg G$?

Thank you!

Questions?