The countable reals

Andrej Bauer (University of Ljubljana)

James E. Hanson (University of Maryland)

Topos Institute Colloquium, May 12th 2022

This is work in progress.

Talk overview

1. Uncountability and $\mathbb{R}$
2. Beating diagonalization
3. The parametric realizability topos

Talk overview

1. **Uncountability and** $\mathbb{R}$
2. Beating diagonalization
3. The parametric realizability topos

Definition

A set A is **countable** if there is a surjection $\mathbb{N} \to 1 + A$.
It is **uncountable** if it is not countable.

Remark

An inhabited set A is countable if, and only if, there is a surjection $\mathbb{N} \to A$.

The essence of diagonalization

Theorem

If there is a surjection $e : \mathbb{N} \to A^{\mathbb{N}}$ then every $f : A \to A$ has a fixed point.

Proof. There is $n \in \mathbb{N}$ such that $e(n) = (k \mapsto f(e(k)(k)))$, therefore $e(n)(n) = f(e(n)(n))$. □

Corollary

If $f : A \to A$ does not have a fixed point then $A^{\mathbb{N}}$ is not countable.

Some uncountable sets

Let Ω be the set of truth values, i.e., the subobject classifier.
Let $2 = \{0, 1\}$ be the Booleans.

Some uncountable sets

Let $\mathbb{\Omega}$ be the set of truth values, i.e., the subobject classifier.
Let $\mathbb{2} = \{0, 1\}$ be the Booleans.

The following sets are uncountable:

- $\mathbb{N}^{\mathbb{N}}$ because $n \mapsto n + 1$ has no fixed points.
- $\mathbb{2}^{\mathbb{N}}$ because $\neg : \mathbb{2} \to \mathbb{2}$ has no fixed points.
- $\mathbb{\Omega}^{\mathbb{N}}$ because $\neg : \mathbb{\Omega} \to \mathbb{\Omega}$ has no fixed points.

Some uncountable sets

Let Ω be the set of truth values, i.e., the subobject classifier.
Let $2 = \{0, 1\}$ be the Booleans.

The following sets are uncountable:

- $\mathbb{N}^{\mathbb{N}}$ because $n \mapsto n + 1$ has no fixed points.
- $2^{\mathbb{N}}$ because $\neg : 2 \to 2$ has no fixed points.
- $\Omega^{\mathbb{N}}$ because $\neg : \Omega \to \Omega$ has no fixed points.

Observations:

- Ω^A is the powerset $\mathcal{P}A$.
- 2^A is the set of *decidable* subsets of A.
- Constructive taboos:

$$2 \cong \Omega \qquad \mathbb{R} \cong 2^{\mathbb{N}} \qquad \mathbb{R} \cong \Omega^{\mathbb{N}}$$

Diagonalization for $\mathbb{R}$ – with excluded middle

Theorem (classical)

Every sequence $a : \mathbb{N} \to \mathbb{R}$ is avoided by some $x \in \mathbb{R}$.

Proof. Define $[u_0, v_0] = [0, 1]$ and recursively

$$[u_{n+1}, v_{n+1}] = \begin{cases} [u_n, {}^4\!/\!_5 \cdot u_n + {}^1\!/\!_5 \cdot v_n] & \text{if } a_n > {}^1\!/\!_2 \cdot u_n + {}^1\!/\!_2 \cdot v_n \\ [{}^1\!/\!_5 \cdot u_n + {}^4\!/\!_5 \cdot v_n, v_n] & \text{if } a_n \leq {}^1\!/\!_2 \cdot a_n + {}^1\!/\!_2 \cdot v_n. \end{cases}$$

Then take $x = \lim_n u_n = \lim_n v_n$. □

Diagonalization for $\mathbb{R}$ – with Dependent Choice

Theorem (intuitionistic with Dependent Choice)

Every sequence $a : \mathbb{N} \to \mathbb{R}$ is avoided by some $x \in \mathbb{R}$.

Proof. Define $[u_0, v_0] = [0, 1]$ and choose

$$[u_{n+1}, v_{n+1}] = \begin{cases} [u_n, {}^4\!/\!_5 \cdot u_n + {}^1\!/\!_5 \cdot v_n] & \text{if } a_n > {}^3\!/\!_5 \cdot u_n + {}^2\!/\!_5 \cdot v_n \\ [{}^1\!/\!_5 \cdot u_n + {}^4\!/\!_5 \cdot v_n, v_n] & \text{if } a_n < {}^2\!/\!_5 \cdot a_n + {}^3\!/\!_2 \cdot v_n. \end{cases}$$

Then take $x = \lim_n u_n = \lim_n v_n$. □

The proof can be improved to use just Countable Choice.

Diagonalization breaks down intuitionistically

Theorem
The topos $\mathsf{Sh}(\mathbb{R})$ *does not validate the internal statement*

$$\forall a \in \mathbb{R}^{\mathbb{N}} . \exists x \in \mathbb{R} . \forall n \in \mathbb{N} . |a_n - x| > 0.$$

Proof. See "Constructive algebraic integration theory without choice" (Appendix A) by Bas Spitters. □

Diagonalization breaks down intuitionistically

Theorem

The topos $\mathsf{Sh}(\mathbb{R})$ *does not validate the internal statement*

$$\forall a \in \mathbb{R}^{\mathbb{N}} \,.\, \exists x \in \mathbb{R} \,.\, \forall n \in \mathbb{N} \,.\, |a_n - x| > 0.$$

Proof. See "Constructive algebraic integration theory without choice" (Appendix A) by Bas Spitters. □

However, $\mathsf{Sh}(\mathbb{R})$ validates $\neg \exists e \in \mathbb{R}^{\mathbb{N}} \,.\, \forall x \in \mathbb{R} \,.\, \exists n \in \mathbb{N} \,.\, e(n) = x$.

Uncountability of $[0, 1]$

Lemma (intuitionistic)

If $[0, 1]$ is countable then so is $\mathbb{R}$.

Proof. Given an enumeration $e : \mathbb{N} \to [0, 1]$, we show surjectivity of $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{R}$, defined by $f(k, n) = k + 2 \cdot e(n)$ Given any $x \in \mathbb{R}$, there is $k \in \mathbb{Z}$ such that $k < x < k + 2$, and $n \in \mathbb{N}$ such that $e(n) = 1/2 \cdot (x - k)$, hence $f(k, n) = x$. □

Subcountability of $\mathbb{R}$

Definition

A set S is

- **subcountable** if there is an injection $S \to \mathbb{N}$,
- **subquotient** of $\mathbb{N}$ if it is a quotient of a subset of $\mathbb{N}$.

Subcountability of $\mathbb{R}$

Definition

A set S is

- **subcountable** if there is an injection $S \to \mathbb{N}$,
- **subquotient** of $\mathbb{N}$ if it is a quotient of a subset of $\mathbb{N}$.

Theorem

In the effective topos $\mathbb{R}$ is a subquotient of $\mathbb{N}$.

Subcountability of $\mathbb{R}$

Definition

A set S is

- **subcountable** if there is an injection $S \to \mathbb{N}$,
- **subquotient** of $\mathbb{N}$ if it is a quotient of a subset of $\mathbb{N}$.

Theorem

In the effective topos $\mathbb{R}$ is a subquotient of $\mathbb{N}$.

Theorem

In the realizability topos over infinite-time Turing machines $\mathbb{R}$ is subcountable.

Subcountability of $\mathbb{R}$

Definition

A set S is

- **subcountable** if there is an injection $S \to \mathbb{N}$,
- **subquotient** of $\mathbb{N}$ if it is a quotient of a subset of $\mathbb{N}$.

Theorem

In the effective topos $\mathbb{R}$ is a subquotient of $\mathbb{N}$.

Theorem

In the realizability topos over infinite-time Turing machines $\mathbb{R}$ is subcountable.

However, in both toposes $\mathbb{R}$ is uncountable because realizability toposes validate Dependent choice.

Cauchy, Dedekind and MacNeille reals

Notions of completeness:

- Cauchy reals $\mathbb{R}_C$: Cauchy sequences have limits.
- Dedekind reals $\mathbb{R}_D$: Dedekind cuts straddle reals.
- MacNeille reals $\mathbb{R}_M$: bounded inhabited subsets have infima and suprema.

In general $\mathbb{R}_C \subseteq \mathbb{R}_D \subseteq \mathbb{R}_M$, and the inclusions may be proper.

MacNeille reals are uncountable, but ...

Theorem (intuitionistic)

The MacNeille reals $\mathbb{R}_M$ are uncountable.

Proof. See "A constructive Knaster-Tarski proof of the uncountability of the reals" by Ingo Blechschmidt and Matthias Hutzler. □

MacNeille reals are uncountable, but ...

Theorem (intuitionistic)

The MacNeille reals $\mathbb{R}_M$ *are uncountable.*

Proof. See "A constructive Knaster-Tarski proof of the uncountability of the reals" by Ingo Blechschmidt and Matthias Hutzler. □

Theorem (intuitionistic)

If MacNeille reals satisfy $\forall x \in \mathbb{R}_M \,.\, 0 < x \lor x < 1$ *then excluded middle holds.*

Proof. See On complete ordered fields, summarizing an argument by Toby Bartels. □

What about uncountability of $\mathbb{R}_C$ and $\mathbb{R}_D$?

Talk overview

1. Uncountability and $\mathbb{R}$
2. **Beating diagonalization**
3. The parametric realizability topos

Ideas that do not work

Find a magical sequence $a : \mathbb{N} \to \mathbb{R}$ such that no Turing machine can diagonalize against it when given a as an oracle.

Ideas that do not work

Find a magical sequence $a : \mathbb{N} \to \mathbb{R}$ such that no Turing machine can diagonalize against it when given a as an oracle.

How about a enumerating all computable reals?

- No, diagonalization relativizes to any oracle.

Ideas that do not work

Find a magical sequence $a : \mathbb{N} \to \mathbb{R}$ such that no Turing machine can diagonalize against it when given a as an oracle.

How about a enumerating all computable reals?

- No, diagonalization relativizes to any oracle.

How about a enumerating all reals definable in some strong theory?

- No! Diagonalization relativizes to **any single oracle**.

Ideas that do not work

Find a magical sequence $a : \mathbb{N} \to \mathbb{R}$ such that no Turing machine can diagonalize against it when given a as an oracle.

How about a enumerating all computable reals?

- No, diagonalization relativizes to any oracle.

How about a enumerating all reals definable in some strong theory?

- No! Diagonalization relativizes to **any single oracle**.

What if we design a special model of computation?

Ideas that do not work

Find a magical sequence $a : \mathbb{N} \to \mathbb{R}$ such that no Turing machine can diagonalize against it when given a as an oracle.

How about a enumerating all computable reals?

- No, diagonalization relativizes to any oracle.

How about a enumerating all reals definable in some strong theory?

- No! Diagonalization relativizes to **any single oracle**.

What if we design a special model of computation?

- No, every realizability topos validates Dependent choice.

Oracles for $x \in [0, 1]$

- There is a computable proper quotient map $q : 2^{\mathbb{N}} \to [0, 1]$.
- Say that $\beta : \mathbb{N} \to 2$ *represents* $x \in [0, 1]$ when $q(\beta) = x$.
- Let $\mathcal{O}_x = \{\beta \in 2^{\mathbb{N}} \mid q(\beta) = x\}$.

Think of $\beta \in \mathcal{O}_x$ as an *oracle* for x.

Note: $\mathcal{O}_x \subseteq 2^{\mathbb{N}}$ is compact because q is proper.

Oracles for $a \in [0,1]^{\mathbb{N}}$

- Let $\langle -, - \rangle : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a computable bijection.
- Define $r : 2^{\mathbb{N}} \to [0,1]^{\mathbb{N}}$ by $r(\alpha)(n) = q(k \mapsto \alpha(\langle n, k \rangle))$.
- Say that $\alpha : \mathbb{N} \to 2$ *represents* $a \in [0,1]^{\mathbb{N}}$ when $r(\alpha) = a$.
- Let $\mathcal{O}_a = \{\alpha \in 2^{\mathbb{N}} \mid q(\alpha) = a\}$.

Think of $\alpha \in \mathcal{O}_a$ as an *oracle* for a.

Note: $\mathcal{O}_a \subseteq 2^{\mathbb{N}}$ is compact because r is proper.

Sequences that beat diagonalization

- Diagonalization works against any **single** $\alpha \in \mathcal{O}_a$.
- But can it work against **many** oracles, parametrically?

Let φ_n^α be the partial map $\mathbb{N} \rightharpoonup \mathbb{N}$ computed by the n-th Turing machine with oracle α.

Definition

Given a set of oracles $S \subseteq 2^{\mathbb{N}}$, say that $n \in \mathbb{N}$ is:

- an *S-index* for $x \in [0, 1]$ when $\varphi_n^\beta \in \mathcal{O}_x$ for all $\beta \in S$,
- an *S-index* for $a \in [0, 1]^{\mathbb{N}}$ when $\varphi_n^\alpha \in \mathcal{O}_a$ for all $\alpha \in S$.

A generalization of Brouwer's fixed point theorem

Let $\mathfrak{C}[0,1]^{\mathbb{N}} = \{S \subseteq [0,1]^{\mathbb{N}} \mid S \text{ is non-empty and convex}\}$.

Theorem

If the graph of $f : [0,1]^{\mathbb{N}} \to \mathfrak{C}[0,1]^{\mathbb{N}}$ is closed then there is $a \in [0,1]^{\mathbb{N}}$ such that $a \in f(a)$.

Theorem (J. Miller, classical)

There is a sequence $\boldsymbol{\mu} : \mathbb{N} \to [0, 1]$ *such that, for all* $x \in [0, 1]$*, if* $n \in \mathbb{N}$ *is an* $\mathcal{O}_{\boldsymbol{\mu}}$*-index for* x *then* $\boldsymbol{\mu}(n) = x$*.*

Theorem (J. Miller, classical)

There is a sequence $\boldsymbol{\mu} : \mathbb{N} \to [0,1]$ *such that, for all* $x \in [0,1]$*, if* $n \in \mathbb{N}$ *is an* $\mathcal{O}_{\boldsymbol{\mu}}$*-index for* x *then* $\boldsymbol{\mu}(n) = x$*.*

Proof. Let $\mathbb{I} = \{[u,v] \mid 0 \le u \le v \le 1\}$ be the interval domain.

Steps of the construction:

1. Define $\Psi : [0,1]^{\mathbb{N}} \to \mathbb{I}^{\mathbb{N}} \subseteq \mathfrak{C}[0,1]^{\mathbb{N}}$ such that, for all $a \in [0,1]^{\mathbb{N}}$ and $n \in \mathbb{N}$, if n is an $\mathcal{O}_a$-index for $x \in [0,1]$ then $\Psi(a)(n) = \{x\}$.

Theorem (J. Miller, classical)

There is a sequence $\boldsymbol{\mu} : \mathbb{N} \to [0,1]$ *such that, for all* $x \in [0,1]$*, if* $n \in \mathbb{N}$ *is an* $\mathcal{O}_{\boldsymbol{\mu}}$*-index for* x *then* $\boldsymbol{\mu}(n) = x$*.*

Proof. Let $\mathbb{I} = \{[u,v] \mid 0 \leq u \leq v \leq 1\}$ be the interval domain.

Steps of the construction:

1. Define $\Psi : [0,1]^{\mathbb{N}} \to \mathbb{I}^{\mathbb{N}} \subseteq \mathfrak{C}[0,1]^{\mathbb{N}}$ such that, for all $a \in [0,1]^{\mathbb{N}}$ and $n \in \mathbb{N}$, if n is an $\mathcal{O}_a$-index for $x \in [0,1]$ then $\Psi(a)(n) = \{x\}$.
2. Verify that Ψ has a closed graph and apply the fixed-point theorem to obtain $\boldsymbol{\mu} \in [0,1]^{\mathbb{N}}$ such that $\boldsymbol{\mu} \in \Psi(\boldsymbol{\mu})$.

Theorem (J. Miller, classical)

There is a sequence $\boldsymbol{\mu} : \mathbb{N} \to [0,1]$ *such that, for all* $x \in [0,1]$, *if* $n \in \mathbb{N}$ *is an* $\mathcal{O}_{\boldsymbol{\mu}}$*-index for* x *then* $\boldsymbol{\mu}(n) = x$.

Proof. Let $\mathbb{I} = \{[u,v] \mid 0 \le u \le v \le 1\}$ be the interval domain.

Steps of the construction:

1. Define $\Psi : [0,1]^{\mathbb{N}} \to \mathbb{I}^{\mathbb{N}} \subseteq \mathfrak{C}[0,1]^{\mathbb{N}}$ such that, for all $a \in [0,1]^{\mathbb{N}}$ and $n \in \mathbb{N}$, if n is an $\mathcal{O}_a$-index for $x \in [0,1]$ then $\Psi(a)(n) = \{x\}$.
2. Verify that Ψ has a closed graph and apply the fixed-point theorem to obtain $\boldsymbol{\mu} \in [0,1]^{\mathbb{N}}$ such that $\boldsymbol{\mu} \in \Psi(\boldsymbol{\mu})$.
3. If $n \in \mathbb{N}$ is an $\mathcal{O}_{\boldsymbol{\mu}}$-index for $x \in [0,1]$ then $\boldsymbol{\mu}(n) \in \Psi(\boldsymbol{\mu})(n) = \{x\}$, therefore $\boldsymbol{\mu}(n) = x$.

See "Degrees of unsolvability of continuous functions" by Joseph S. Miller for details. □

Talk overview

1. Uncountability and $\mathbb{R}$
2. Beating diagonalization
3. **The parametric realizability topos**

It is just a matter of technique

- Let $\boldsymbol{\mu}$ be Miller's sequence.
- A tripos for $\mathcal{O}_{\boldsymbol{\mu}}$-computability.
- The tripos-to-topos construction yields a topos $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$.
- Show that $\boldsymbol{\mu} : \mathbb{N} \to [0, 1]$ is epi in $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$.

The parametric realizability tripos & topos

Let $\mathcal{O} \subseteq 2^{\mathbb{N}}$ be a non-empty set of oracles.

Define the tripos $\mathsf{Pred}_{\mathcal{O}} : \mathsf{Set}^{\mathsf{op}} \to \mathsf{Heyt}$ by $\mathsf{Pred}_{\mathcal{O}}(X) = (\mathcal{P}\mathbb{N}^X, \leq_X)$ where for $\phi, \psi \in \mathcal{P}\mathbb{N}^X$

$$\phi \leq_X \psi \iff \exists e \in \mathbb{N} \,.\, \forall x \in X \,.\, \forall n \in \phi(x) \,.\, \forall \alpha \in \mathcal{O} \,.\, \varphi_e^{\alpha}(n) \in \psi(x).$$

The parametric realizability tripos & topos

Let $\mathcal{O} \subseteq 2^{\mathbb{N}}$ be a non-empty set of oracles.

Define the tripos $\mathsf{Pred}_{\mathcal{O}} : \mathsf{Set}^{\mathsf{op}} \to \mathsf{Heyt}$ by $\mathsf{Pred}_{\mathcal{O}}(X) = (\mathcal{P}\mathbb{N}^X, \leq_X)$ where for $\phi, \psi \in \mathcal{P}\mathbb{N}^X$

$$\phi \leq_X \psi \iff \exists e \in \mathbb{N} \,.\, \forall x \in X \,.\, \forall n \in \phi(x) \,.\, \forall \alpha \in \mathcal{O} \,.\, \varphi_e^{\alpha}(n) \in \psi(x).$$

The **parametric realizability topos** $\mathsf{PRT}(\mathcal{O})$ is the topos arising from the tripos $\mathsf{Pred}_{\mathcal{O}}$.

The Dedekind reals in $\mathsf{PRT}(\mathcal{O})$

For $m \in \mathbb{N}$ and $x \in [0,1]$, let

$$n \Vdash_I x \iff \forall \alpha \in \mathcal{O} \,.\, \varphi_n^\alpha \in \mathcal{O}_x.$$

Let $I = \{x \in [0,1] \mid \exists n \in \mathbb{N} \,.\, n \Vdash_I x\}$.

Theorem
$(I, \Vdash_I)$ is the Dedekind unit interval $[0,1] \subseteq \mathbb{R}_D$ in $\mathsf{PRT}(\mathcal{O})$.

Theorem

$\boldsymbol{\mu} : \mathbb{N} \to [0,1]$ is epi in $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$.

Proof. Let $m \Vdash \boldsymbol{\mu} \in [0,1]^{\mathbb{N}}$, so that $\boldsymbol{\varphi}_m^{\alpha}(k) \Vdash \boldsymbol{\mu}(k) \in [0,1]$ for all $k \in \mathbb{N}$ and $\alpha \in \mathcal{O}_{\boldsymbol{\mu}}$.

We seek a realizer $e \in \mathbb{N}$ for the statement

$$\forall x \in [0,1] \,.\, \exists n \in \mathbb{N} \,.\, \boldsymbol{\mu}(n) = x.$$

Take e such that $\boldsymbol{\varphi}_e^{\alpha}(k) = \langle k, 0 \rangle$ for all $k \in \mathbb{N}$ and $\alpha \in \mathcal{O}_{\boldsymbol{\mu}}$.

If $n \Vdash x \in [0,1]$ then for every $\alpha \in \mathcal{O}_{\boldsymbol{\mu}}$ we have $\boldsymbol{\varphi}_n^{\alpha} \in \mathcal{O}_x$, hence $\boldsymbol{\mu}(n) = x$. It follows that $\boldsymbol{\varphi}_e^{\alpha}(n) = \langle n, 0 \rangle$ realizes $\exists n \in \mathbb{N} \,.\, \boldsymbol{\mu}(n) = x$, as required. $\square$

Concluding remarks

- In $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$ the object $[0,1]^{\mathbb{N}}$ is countable as well. Therefore Lawvere's fixed point theorem implies Brouwer's fixed point theorem in the form "Every $f : [0,1]^n \to [0,1]^n$ has a fixed point."

Concluding remarks

- In $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$ the object $[0,1]^{\mathbb{N}}$ is countable as well. Therefore Lawvere's fixed point theorem implies Brouwer's fixed point theorem in the form "Every $f : [0,1]^n \to [0,1]^n$ has a fixed point."
- It remains to explore $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$ even further.

Concluding remarks

- In $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$ the object $[0,1]^{\mathbb{N}}$ is countable as well. Therefore Lawvere's fixed point theorem implies Brouwer's fixed point theorem in the form "Every $f : [0,1]^n \to [0,1]^n$ has a fixed point."
- It remains to explore $\mathsf{PRT}(\mathcal{O}_{\boldsymbol{\mu}})$ even further.
- We defined a notion of a **parameterized partial combinatory algebra** which generalizes Turing machines parameterized by a set of oracles $\mathcal{O}$. The tripos construction carries over.