Excluded middle considered as a mathematical problem

Martín Escardó
University of Birmingham, UK

Proof, Structure and Computation Workshop (PSC)
Vienna Summer of Logic, 16th July 2014

The problem we investigate

1. Classical mathematics postulates excluded middle (EM).

2. Constructive mathematics (successfully) tries to redevelop the main results of classical mathematics without this postulate.

   (Especially Bishop's School of mathematics.)

3. Logic meta-proves that EM and some of its instances (e.g. LPO, WLPO, LLPO) are not mathematically provable.

4. This talk mathematically proves, hopefully surprising, instances of EM.

   We *remove* the postulate, and we try to see how much of it we can prove.

   We need to remove general choice too, of course, because it gives EM.

   And in fact we don't postulate any form of choice.

   Crucially, we *don't add* any postulate. (Such as e.g. continuity axioms.)

The problem we investigate

1. Classical mathematics. Any decision is possible, by decree.

2. Constructive mathematics. Try to live without this decree.

3. Logic. Decisions involving infinitely many cases are not always possible.

4. This talk. Some decisions involving infinitely many cases are actually mathematically and (hence) computationally possible.

Sample mathematical theorem

Fix an arbitrary function $p : 2^{\mathbb{N}} \to 2$.

Let P be the proposition $\forall n : \mathbb{N}.\, p(1^n 0^\omega) = 1$.

Then P or not P.

$$\forall p : 2^{\mathbb{N}} \to 2.\, (\forall n : \mathbb{N}.\, p(1^n 0^\omega) = 1) \vee \neg(\forall n : \mathbb{N}.\, p(1^n 0^\omega) = 1).$$

Why should this be surprising? There are infinitely many cases to check.

This is an instance of WLPO (the weak limited principle of omniscience),

$$\forall q : \mathbb{N} \to 2.\, (\forall n : \mathbb{N}.\, q(n) = 1) \vee \neg(\forall n : \mathbb{N}.\, q(n) = 1),$$

which, logicians tell us, is not mathematically provable.

But in the particular case where $q(n)$ is $p(1^n 0^\omega) = 1$, we have a proof!

Another one

Let $\mathbb{N}_\infty$ be the set of decreasing binary sequences $\alpha : 2^{\mathbb{N}}$.

They include sequences of the form $1^n 0^\omega$ and 1^ω, and *nothing else*.

Which is quite different from saying that any $\alpha : \mathbb{N}_\infty$ is of the form $1^n 0^\omega$ or 1^ω.

This last claim is equivalent to LPO (the limited principle of omniscience),

$$\forall q : \mathbb{N} \to 2. (\exists n : \mathbb{N}. q(n) = 0) \vee \neg(\exists n : \mathbb{N}. q(n) = 0),$$

which mathematically implies WLPO, and hence is not provable either.

However, the following, which looks like LPO, has a mathematical proof:

$$\forall p : \mathbb{N}_\infty \to 2. (\exists \alpha : \mathbb{N}_\infty. p(\alpha) = 0) \vee \neg(\exists \alpha : \mathbb{N}_\infty. p(\alpha) = 0).$$

Yet another one

Let P be the proposition that a given function $f : \mathbb{N}_\infty \to \mathbb{N}$ fails to be continuous.

Then P or not P.

Side remark: Then $\neg$WLPO and Markov's Principle (MP) together imply that all functions $\mathbb{N}_\infty \to \mathbb{N}$ are continuous.

But our development in this talk is $\neg$-WLPO- and MP-neutral.

We leave them undecided (they certainly are not (dis)provable).

References for this talk

I won't be able to prove everything mentioned above, and other things mentioned below, but their proofs, and proofs of more theorems like that, can be found here:

1. Infinite sets that satisfy the principle of omniscience in any variety of constructive mathematics. JSL, 2013.

2. Constructive decidability of classical continuity. MSCS, to appear.

3. Agda files with formal proofs of (un)published theorems, at my web page.

4. *Seemingly impossible constructive proofs.* Blog post at Andrej Bauer's *Mathematics and Computation*.

I will, however, prove one example to illustrate the main technical ideas.

Principle of omniscience

$$\forall p\colon X \to 2.\, (\exists x : X.\, p(x) = 0) \vee (\forall x : X.\, p(x) = 1).$$

Can be proved for X finite (not for X subfinite in general).

For $X = \mathbb{N}$ this is LPO, so can't be proved.

For $X = 2^{\mathbb{N}}$ can be proved from Brouwerian assumptions.
(Continuity, fan theorem. We don't do this in this talk.)

Omniscience can be proved for plenty of infinite sets

In spartan (contructive) mathematics

We'll look at omniscient subsets of the Cantor space $2^{\mathbb{N}}$.

They will be ordinals with respect to the lexicographical order.

Spartan mathematics

Don't assume (or reject), among other things:

0. Excluded middle.
1. Choice.
2. Powerset.
3. Markov's principle.
4. Continuity, bar induction, fan theorem, double-negation shift.
5. Church's thesis.
7. Extensionality (with respect to extensional equality).

But we do need extensionality to prove omniscience theorems

We use extensionality as a hypothesis of theorems rather than as axiom.

$$\forall \text{ extensional } p\colon X \to 2\, (\exists x : X.\, p(x) = 0) \vee (\forall x : X.\, p(x) = 1).$$

Drinker paradox

In every pub there is a person a such that if a drinks then everybody drinks.

$$\forall \text{ extensional } p\colon X \to 2(\exists a : X(p(a) = 1 \implies \forall x : X(p(x) = 1))).$$

For X inhabited, this is equivalent to the omniscience of X.

Selection of roots of 2-valued functions

A selection function for a set X is a functional $\varepsilon\colon (X \to 2) \to X$ such that for all extensional $p\colon X \to 2$,

$$\boxed{p(\varepsilon(p)) = 1 \implies \forall x : X (p(x) = 1).}$$

Equivalently, the function p has a root if and only if $\varepsilon(p)$ is a root.

$$\boxed{p(\varepsilon(p)) = 0 \Longleftarrow \exists x : X (p(x) = 0).}$$

Searchable sets

We say that a set is searchable if it has a selection function.

The generic convergent sequence

$$\mathbb{N}_\infty = \{x : 2^{\mathbb{N}} \mid \forall i : \mathbb{N}(x_i \geq x_{i+1})\}.$$

Also known as the one-point compactification of the natural numbers.
It is the final co-algebra of the functor $X \mapsto 1 + X$.

The set $\mathbb{N}_\infty$ has elements $\underline{n} = 1^n 0^\omega$ and $\infty = 1^\omega$.

Lemma. $\forall x : \mathbb{N}_\infty (\forall n : \mathbb{N}(x \neq \underline{n})) \implies x = \infty$.

Proof. For any i, if we had $x_i = 0$, then we would have $x = \underline{n}$ for some $n < i$, and so we must have $x_i = 1$.

Warning

$$\mathbb{N}_\infty \subseteq \underline{\mathbb{N}} \cup \{\infty\} \iff \text{LPO}.$$

However

Lemma (Density). For all extensional $p\colon \mathbb{N}_\infty \to 2$, if

1. $p(\underline{n}) = 1$ for every $n : \mathbb{N}$, and

2. $p(\infty) = 1$,

then

3. $p(x) = 1$ for every $x : \mathbb{N}_\infty$.

Proof. If we had $p(x) \neq 1$, then the extensionality of p would give $x \neq \underline{n}$ for every $n : \mathbb{N}$ and $p(x) \neq \infty$, which is impossible.

$\mathbb{N}_\infty$ is searchable and hence omniscient

Proof. Given $p\colon \mathbb{N}_\infty \to 2$ extensional, let

$$\varepsilon(p) = \lambda i. \min_{n \le i} p(\underline{n}).$$

Clearly $\varepsilon(p) : \mathbb{N}_\infty$ (it is a decreasing sequence). Also

$$(0) \qquad \forall n : \mathbb{N}(\varepsilon(p) = \underline{n} \implies p(\underline{n}) = 0),$$

$$(1) \qquad \varepsilon(p) = \infty \implies \forall n : \mathbb{N}(p(\underline{n}) = 1).$$

We need to show that $p(\varepsilon(p)) = 1 \implies \forall x : \mathbb{N}_\infty(p(x) = 1)$.

Claim 0. $p(\varepsilon(p)) = 1 \implies \forall n : \mathbb{N}(\varepsilon(p) \neq \underline{n}).$

Proof. We know that $\forall n : \mathbb{N}(\varepsilon(p) = \underline{n} \implies p(\underline{n}) = 0)$.

But, for any $n : \mathbb{N}$, if we had $\varepsilon(p) = \underline{n}$, we would have $p(\underline{n}) = 1$ by extensionality.

Claim 1. $p(\varepsilon(p)) = 1 \implies \varepsilon(p) = \infty.$

Proof. This follows from Claim 0 and the previous lemma that

$$\forall x : \mathbb{N}_\infty (\forall n : \mathbb{N}(x \neq \underline{n})) \implies x = \infty.$$

Claim 2. $p(\varepsilon(p)) = 1 \implies \forall n : \mathbb{N}(p(\underline{n}) = 1).$

Proof. This follows from the previous fact $\varepsilon(p) = \infty \implies \forall n : \mathbb{N}(p(\underline{n}) = 1)$.

Claim 1. $\boxed{p(\varepsilon(p)) = 1 \implies \varepsilon(p) = \infty.}$

Claim 2. $\boxed{p(\varepsilon(p)) = 1 \implies \forall n : \mathbb{N}(p(\underline{n}) = 1).}$

Claim 3. $\boxed{p(\varepsilon(p)) = 1 \implies p(\infty) = 1.}$

Proof. This follows from Claim 1 and the extensionality of p.

Claim 4. $\boxed{p(\varepsilon(p)) = 1 \implies \forall x : \mathbb{N}_\infty(p(x) = 1).}$

Proof. This follows from Claims 2 and 3 and the density Lemma.

Q.E.D.

Addendum to the omniscience theorem

$\varepsilon(p)$ is the infimum of the set of roots of p.

So it is the least root if p has a some root.

We work with the lexicographical order of the Cantor space and hence $\mathbb{N}_\infty$.

Easy closure properties of omniscient sets

1. Finite products.

2. Images.

3. Unions with an omniscient index set.

Omniscient sets are not closed under finite intersections.

A more powerful closure property will be discussed later.

Reformulations of previous theorems

1 . Every decidable subset of $\mathbb{N}_\infty$ is either empty or inhabited.

2 . Every decidable subset of $\mathbb{N}_\infty$ has an infimum.

3 . Every inhabited decidable subset of $\mathbb{N}_\infty$ has a least element.

3'. Every non-empty decidable subset of $\mathbb{N}_\infty$ has a least element.

Transfinite induction

For every decidable predicate A on $\mathbb{N}_\infty$,

$$\forall x : \mathbb{N}_\infty(\forall y < x(Ay)) \implies Ax,$$

implies

$$\forall x : \mathbb{N}_\infty(Ax).$$

Proof. Density Lemma and case analysis on $\underline{\mathbb{N}} \cup \{\infty\}$.

So $\mathbb{N}_\infty$ is an ordinal

But with respect to decidable (extensional) predicates only.

Ordinal for our purposes

1. Linearly ordered set.
2. Any inhabited, decidable, extensional subset has a least element.
3. Any decidable, extensional subset satisfies transfinite induction.

We construct plenty of omniscient ordinal in $2^{\mathbb{N}}$.

Countable sums of omniscient ordinals

Not possible.

E.g. $\mathbb{N}$ is a countable sum.

But $\sum_i X_i + 1$ works if we define it properly.

Squashed sums

The crude definition, with $X_n \subseteq 2^{\mathbb{N}}$, is

$$\overline{\sum}_n X_n = \bigcup_n 1^n 0 X_n \cup \{\infty\}.$$

The refined definition is written down in the accompanying references.

Theorem. The searchable subsets of $2^{\mathbb{N}}$ are closed under squashed sums.

Theorem. So are the ordinal subsets of $2^{\mathbb{N}}$.

Can reach any ordinal below ϵ_0

And higher using richer type systems.

We apply Coquand, Hancock and Setzer (CSL 1997).

Question. How far can we get?

Meta-mathematics

HA^ω is a canonical example of formal spartan constructive mathematics.

Let's work with HA^ω in this slide.

Here are some results I conjectured, and that Dag Normann proved.

Definition. A set is called full if its complement is empty.

Definition. A set is called classically countable if it has a full countable subset.

Meta-Theorem. Any definable searchable subset of $2^{\mathbb{N}}$ is classically countable.

Meta-Theorem. Moreover, its Cantor-Bendixon rank has to be smaller than ϵ_0.