

# Seemingly impossible programs & proofs

Martin Escardó

School of Computer Science

University of Birmingham, UK

CSL 2022

Online, hosted by Göttingen University.

19<sup>th</sup> February

# The problem addressed here

$$\mathbb{Z} = \{0, 1\}$$

Given a set  $X$  and  $p: X \rightarrow \mathbb{Z}$ ,

- either find  $x \in X$  such that  $p(x) = 0$  ( $x$  is root of  $p$ )
- or else report that  $P$  has no root.

## Exhaustive search

| when  $X$  is finitely enumerated this is possible, of course.

↑↑  
we generalize to  
 $X$  infinite

# Previous work

- Scott Model
- Model of Kleene-Kreisel etc functionals
- & their relationship

## 1. Plotek-Scott-Plotkin PCF

(i) Turing universal for total higher-type computation in the sense of Kleene & Kreisel (Dag Normann JSL'2000)

(ii) Search over the Cantor space  $\mathbb{N} \rightarrow 2$  is PCF definable. (Ulrich Berger 1990.)

(iii) {  
• Searchable sets are compact in the Kleene-Kreisel topology.  
• A non-empty set is searchable  
     $\iff$  it is a computable image of the Cantor space.

(M.E. LICS'2007 & LMCS'2008.)

(iv) Crucially, the above work with continuous  $p: X \rightarrow 2$ .

Previous work ctd.

- topos models
- Set-theoretical model
- Model of Kleene-Kreisel cts functionals

## 2. Gödel's System T.

(i) Search over the Cantor type  $\mathbb{N} \rightarrow 2$  is not System T definable.  
(Folklore - use Kleene Tree.)

(ii) However, many infinite sets  $X \subseteq (\mathbb{N} \rightarrow 2)$  are System T searchable.

For any ordinal  $\alpha < \varepsilon_0$  there is an ordinal  $\alpha'$  with  
 $\alpha \leq \alpha' < \varepsilon_0$  and  $\exists$  System T searchable set  $X \subseteq (\mathbb{N} \rightarrow 2)$   
of order type  $\alpha'$  w.r.t. the lexicographic order.  
(M.E. JSL'2013)

(iii) Any System T searchable subset of  $\mathbb{N} \rightarrow 2$  has Cantor-Bendixson rank  $< \varepsilon_0$ . (Dag Normann, JOC'2016.)

(iv) We don't assume any more that  $p: X \rightarrow 2$  is continuous.

Work reported in this talk writing in progress, preliminary  
2-page abstract at Types' 2019

### 3. Searchable sets in MLTT (Martin-Löf type theory)

- (i) Like in (2), we don't assume continuity. The results hold in all models.
- (ii) Unlike (2), we consider sets beyond  $X \subseteq (\mathbb{N} \rightarrow \mathbb{Z})$ .
- (iii) The searchable sets we get are still well ordered. Not by the axiom of choice,  
but by explicit constructions.  
But we get much higher than  $\epsilon_0$ .
- (iv) Unlike (1) and (2), we reason within the system rather than externally to the system with the aid of a model.  
In particular, this forces the use of constructive proofs.
- (v) Theantor type  $\mathbb{N} \rightarrow \mathbb{Z}$  is not searchable, like in (2).
- (vi) The constructions and proofs are implemented in Agda.  
( [github.com/martinescardo/TypeTopology](https://github.com/martinescardo/TypeTopology) )

# Our system

MLTT  $\mathbb{O}, \mathbb{1}, \mathbb{N}, +, \times, \Sigma, \Pi, \text{Id}, \mathcal{U}, \mathcal{W}$

+  
funext function extensionality (we could use setoids instead)

↖ This computes in Cubical Agda

(There are some results for MLTT + HoTT/UF features,  
not discussed in this talk.)

Many models

Our results hold in all models.

- Types are sets.
- Types are "spaces".
- Types are homotopy types.
- Types are "sets with computational structure" (realizability).
- Types are the objects of a topos.

# Mathematical expression of the problem in our system

Every  $p: X \rightarrow \mathbb{2}$   
has a root or  
it doesn't.

$$\forall p: X \rightarrow \mathbb{2} \left( \exists x: X, px = 0 \right) \vee \left( \forall x: X, px = 1 \right)$$

$\neg \exists x: X, px = 0$

- In classical mathematics this is a non-problem.

It is just an instance of the principle of excluded middle.

Excluded middle  
considered as an open  
problem. → •

In this talk we are going to establish instances of the principle of excluded middle in MLTT.

## Searchable set

- We say that a set  $X$  is searchable if for every  $p: X \rightarrow \mathbb{Z}$ ,

$$\left( \exists x: X. p x = 0 \right) \vee \left( \forall x: X. p x = 1 \right)$$

- Weaker notion:

$$\left( \neg \forall x: X. p x = 1 \right) \vee \left( \forall x: X. p x = 1 \right)$$

For the purposes of this talk, let's say that  $X$  is weakly searchable.





## Counter example

- The set  $\mathbb{N}$  of natural numbers fails to be searchable.
- The searchability of  $\mathbb{N}$  amounts to Bishop's LPO (Limited Principle of Omniscience).

→ More precisely, LPO is independent of MLTT

- False in realizability models (not computable)
- False in topological models (not continuous)
- True in the model of classical sets (by excluded middle)

Our constructive mathematics doesn't have anticlassical axioms (such as "all functions are continuous").

Probably the simplest infinite example

$$\mathbb{N}_\infty := \{ \alpha = 2^{\mathbb{N}} \mid \forall i. \alpha_i \geq \alpha_{i+1} \}$$

That is, the set of decreasing binary sequences.

$$\underline{n} := 1^n 0^\omega$$

$$\infty := 1^\omega$$

We have an injection

$$\mathbb{N} \longrightarrow \mathbb{N}_\infty$$

$$n \longmapsto \underline{n}$$

Theorem. The set  $\mathbb{N}_\infty$  is system T searchable (JSL '2013)

It is also MLTT searchable with an MLTT+funext proof of the algorithm.

## Proof sketch (with the difficult part omitted)

• Given  $p: \mathbb{N}_\infty \rightarrow 2$ , (not assumed to be continuous)

define  $\beta_n = \min(p_0, p_1, \dots, p_n)$

Formula for the infimum of the set of roots.

• This is clearly decreasing.

• Now we check whether  $p_\beta = 0$  or  $p_\beta = 1$ .

(0) If  $p_\beta = 0$  then we've found a root.

(1) If  $p_\beta = 1$  then  $p_\alpha = 1$  for all  $\alpha: \mathbb{N}_\infty$  and so

there is no root. (This is easy classically and less so constructively.)

| In the pub  $\mathbb{N}_\infty$  there is a person  $\beta: \mathbb{N}_\infty$  such that if  $\beta$  drinks, then everybody drinks.

Some consequences (decision procedures)

(1) For every  $p: \mathbb{N}_\infty \rightarrow 2$  either  $\forall n: \mathbb{N}, p_n = 1$  or  $\neg \forall n: \mathbb{N}, p_n = 1$   
(JSL'2013)

quantification over the natural numbers! Not over  $\mathbb{N}_\infty$ .

(2) Every  $p: \mathbb{N}_\infty \rightarrow 2$  is continuous or not.

(3) There is some discontinuous  $p: \mathbb{N}_\infty \rightarrow 2$  iff WLPO holds

(Bishop's principle of Weak Limited Omniscience,  
or the weak searchability of  $\mathbb{N}$ , which is also independent.)

(MSCS'2015)

# Some applications of the searchability of $\aleph_\infty$

1. Pierre Pradic & Chad E. Brown. Arxiv '2019  
Cantor-Bernstein implies excluded middle  
arxiv 1904.09193  
(Also implemented in Coq.)

2. Dag Normann & William Tait. Springer '2017  
On the computability of the Fan Functional  
(They use the system T searchability of  $\aleph_\infty$   
to fill a gap in an unpublished but widely  
circulated 1958 manuscript by Tait.)

# Searchable sets in our type theory

- (1)  $0$ ,  $1$  and  $\mathbb{N}_\infty$  are searchable.
- (2) If  $X$  and  $Y$  are searchable then so are  $X+Y$  and  $X \times Y$ .
- (3) If  $X$  is a searchable set and  $A$  is a family of searchable sets indexed by  $X$ , then its disjoint union  $\sum_{x:X} A_x$  is a searchable set.
- (4) If furthermore (a) we have a function that picks an element of  $A_x$  for any given  $x:X$ , and (b) the set  $X$  has at most one element, then the cartesian product  $\prod_{x:X} A_x$  is searchable. (Mico-Tychonoff)

# Building more searchable sets

- The searchable sets that we have constructed so far are all well-ordered.

(1)  $\mathbb{1}$

$\uparrow$

$\mathbb{N}_\infty$  (requires some thought)

(2)  $X + Y$

$X \times Y$

(baby Tychonoff)

(3)  $\sum x: X, \Delta x$

(lexicographic order - also requires thought)

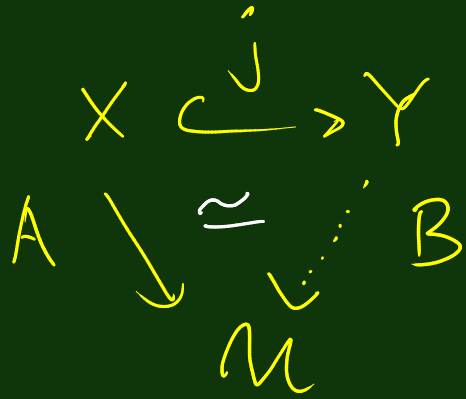
→ we use the notion adopted in the HoTT book, which agrees with the classical one under the principle of excluded middle.

- But we can't get very high, ordinally speaking, with just the above.
- This is what we address next.





# Family extension problem



(MSCS'2021. "Injective types in univalent mathematics")

This set has at most one element. (because  $j$  is an embedding)

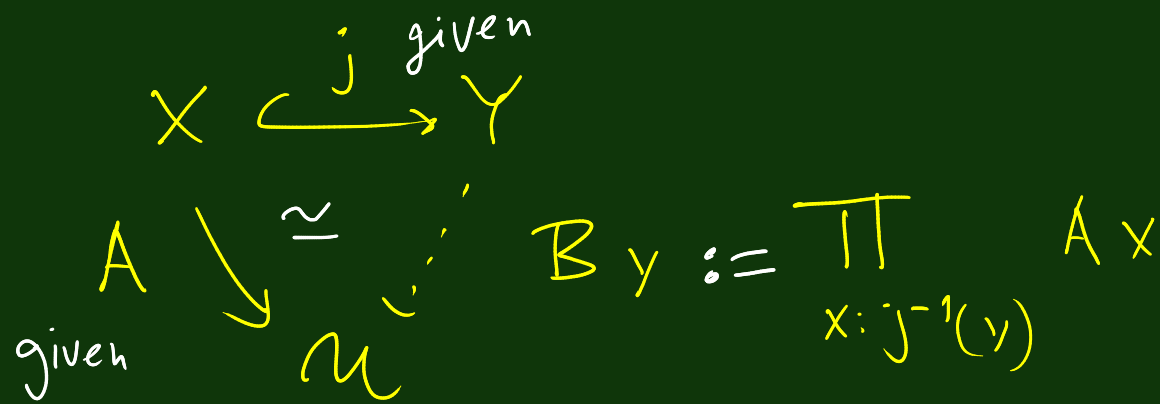
Smallest solution (left Kan extension):  $B y := \sum_{x: j^{-1}(y)} A x$

Largest solution (right Kan extension):  $B y := \prod_{x: j^{-1}(y)} A x$

It is this that works for the wish of the previous board.

why? By Micro-Tychonoff

# Summary of the previous reasoning



Special case  
of interest:

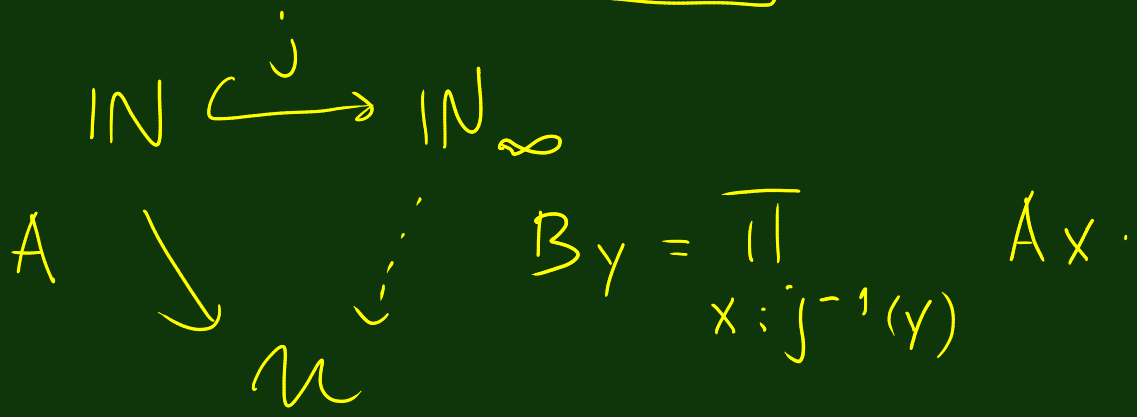


**Theorem** If the set  $A_x$  is searchable for every  $x: X$ , then  
then set  $B_y$  is searchable for every  $y: Y$ .

**Corollary** If additionally  $Y$  is searchable, then so is  $\sum_{y: Y} B_y$ .

In the special case of interest we have  $B(\infty) \simeq \mathbb{1}$

More

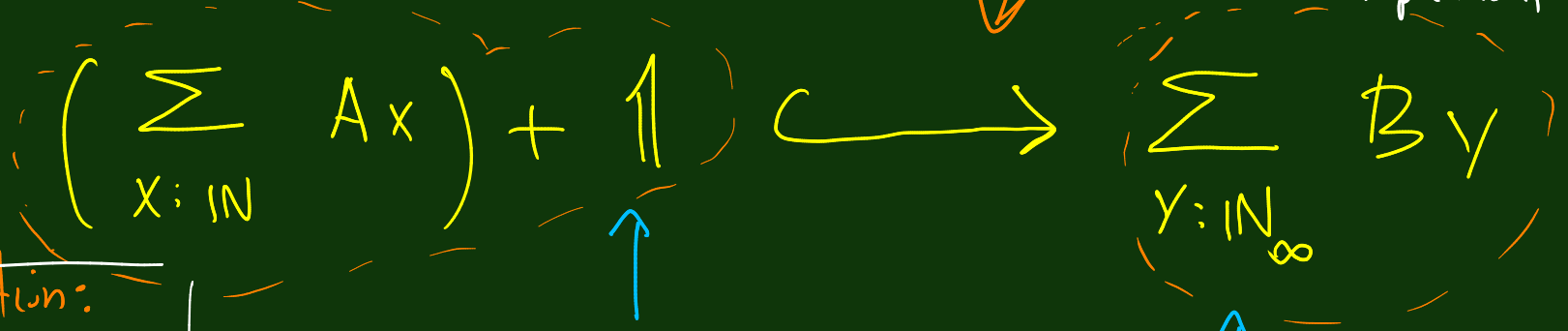


Classically

This is a bijection  
(with noncomputable inverse)

Constructively

This is an injection  
whose image has empty  
complement.



Notation:

$$\sum_{x: X} A_x$$

adds "isolated"  
point

adds point "at infinity".

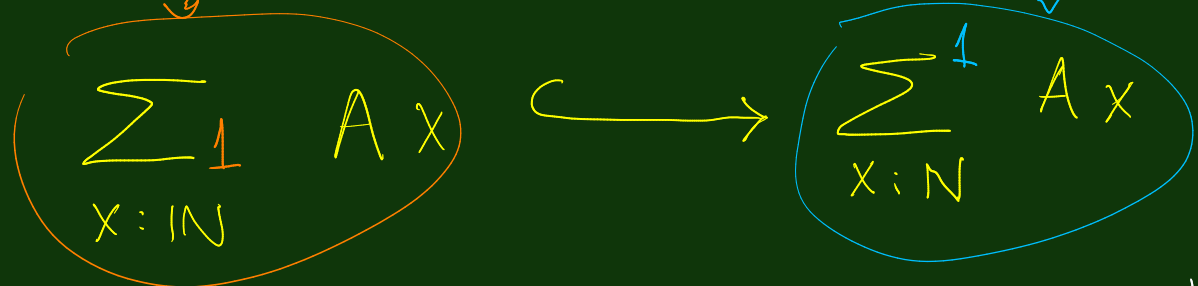
Notation:

$$\sum_{x: X}^1 A_x$$

What is the point of the previous discussion?

The well-ordered set  $(\sum_{x:\mathbb{N}} Ax) + \mathbb{1}$  is not searchable in general, even if  $Ax$  is searchable for every  $x:\mathbb{N}$ .

However, the (classically isomorphic) set  $\sum_{y:\mathbb{N}_\infty} By$  is searchable.



Constructively, this embedding has empty complement.

# Ordinal expressions

 OE

Inductively defined (z w type)

We can get much higher than  $\epsilon_0$  (c.f. Anton Setzer's work)

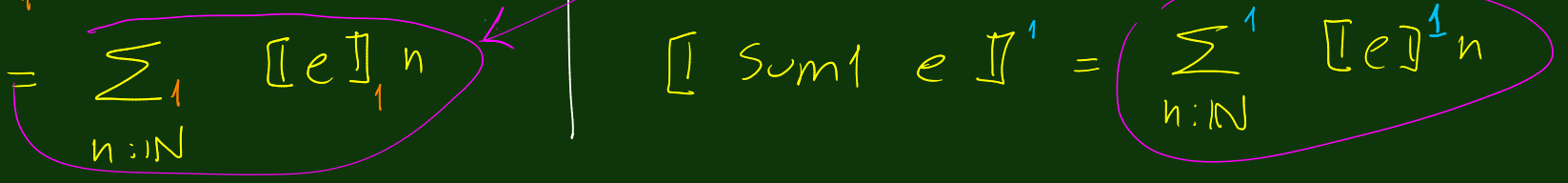
- One : OE
- Add : OE  $\rightarrow$  OE  $\rightarrow$  OE
- Mul : OE  $\rightarrow$  OE  $\rightarrow$  OE
- Sum1 : (IN  $\rightarrow$  OE)  $\rightarrow$  OE

Two interpretations

$$\begin{aligned} \llbracket \text{one} \rrbracket_1 &= 1 \\ \llbracket \text{Add } e \ e' \rrbracket_1 &= \llbracket e \rrbracket_1 + \llbracket e' \rrbracket_1 \\ \llbracket \text{Mul } e \ e' \rrbracket_1 &= \llbracket e \rrbracket_1 \times \llbracket e' \rrbracket_1 \\ \llbracket \text{sum1 } e \rrbracket_1 &= \sum_{n \in \mathbb{N}} \llbracket e \rrbracket_1^n \end{aligned}$$

$$\begin{aligned} \llbracket \text{one} \rrbracket^1 &= 1 \\ \llbracket \text{Add } e \ e' \rrbracket^1 &= \llbracket e \rrbracket^1 + \llbracket e' \rrbracket^1 \\ \llbracket \text{Mul } e \ e' \rrbracket^1 &= \llbracket e \rrbracket^1 \times \llbracket e' \rrbracket^1 \\ \llbracket \text{sum1 } e \rrbracket^1 &= \sum_{n \in \mathbb{N}} \llbracket e \rrbracket^1^n \end{aligned}$$

only difference



Theorems

The ordinal

$$\mathbb{I}e\mathbb{I}_1$$

- has decidable equality
- is a retract of  $\mathbb{N}$
- so countable
- Not searchable unless LPO holds

The ordinal

$$\mathbb{I}e\mathbb{I}^1$$

- is searchable
- is a retract of  $\mathbb{N} \rightarrow 2$
- is totally separated (discussed later)
- Not countable unless LPO holds
- doesn't have decidable equality unless LPO

Even better:  
 Every decidable subset is either empty or has a least element.

There is an order-preserving-reflecting embedding

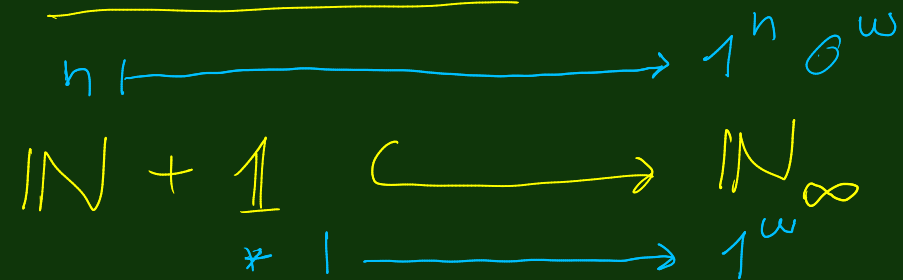
$$\mathbb{I}e\mathbb{I}_1 \hookrightarrow \mathbb{I}e\mathbb{I}^1$$

whose image has empty complement

(but is a bijection iff LPO holds)

The embedding doesn't have a computable inverse.

# Illustration The ordinal $\omega+1$



- Decidable equality
- Searchable iff **LPO**
- Countable

- Searchable
- Decidable equality iff **WLPO**
- Countable iff **LPO**

- bijection iff **LPO**,
- but its image has empty complement.

Every decreasing sequence is of one of the forms  $1^n 0^\omega$  and  $1^\omega$ .

There is no decreasing sequence other than  $1^\omega 0$  and  $1^\omega$ .



## Totally separated sets

In some models, all maps  $\mathbb{R} \rightarrow 2$  are constant, and so the set  $\mathbb{R}$  is trivially searchable, in a useless way.

A type  $X$  is totally separated if there are plenty of functions  $X \rightarrow 2$ :

**Definition.** A type  $X$  is called totally separated if

$$\left( \forall p : X \rightarrow 2, p^x = p^y \right) \rightarrow x = y$$

"The functions into the booleans separate the points".

(A totally separated type is automatically a set in the sense of HoTT/UF.)

The searchable ordinals discussed before  
are totally separated.

Because  $\mathbb{N} \rightarrow \mathbb{Z}$  is a total separatedness  
is inherited by retracts.

Moreover

1. Any type has a totally separated reflection.
2. A type is searchable iff its t-s. reflection is.

# Summary & discussion

1. Plenty of searchable sets in a constructive setting compatible with classical mathematics.  
(A "neutral" mathematics.)
2. In particular, continuity axioms are not used.
3. But there are connections with topology that we didn't discuss.  
(e.g. searchable sets correspond to compact spaces).  
And which inspire & guide the constructions we have performed.
4. The searchable sets constructed here are well-ordered & and decidable subsets are either empty or have a least element.
5. Anton Setzer (1998, 2015) describes the proof-theoretic strength of our system.
6. Can Dag Normann's result for system T be adapted to MLTT or HoTT/UF, in connection with (5)?