Seemingly impossible programs & proofs

Martín Escardó
School of Computer Science
University of Birmingham, UK

CSL 2022

Online, hosted by Göttingen University.

19th February

The problem addressed here

$2 = \{0,1\}$

Given a set X and $p : X \longrightarrow 2$,

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

$$\boxed{\text{Exhaustive search}}$$

When X is finitely enumerated this is possible, of course.

we generalize to X infinite

Previous work

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

1. Platek-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 $\mathbb{N} \to 2$ 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 $p : X \to 2$.

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 $\mathbb{N} \to 2$ is not system T definable.
(Folklore – use Kleene Tree.)

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

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

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

(iv) We don't assume any more that $p : X \to 2$ 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 $X \subseteq (\mathbb{N} \to 2)$.

(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 ε_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) The Cantor type $\mathbb{N} \to 2$ is not searchable, like in (2).

(vi) The constructions and proofs are implemented in Agda.
(github.com/martinescardo/TypeTopology)

Our system

MLTT $\quad \mathbb{0}, \mathbb{1}, \mathbb{N}, +, \times, \Sigma, \Pi, \mathrm{Id}, \mathcal{U}, W$

\+

funext $\quad$ 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 $\qquad$ 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 $p : X \to 2$ has a root or it doesn't.

$$\forall p : X \to 2 \; (\exists x : X ,\ p x = 0) \vee \underbrace{(\forall x : X .\ p x = 1)}_{\neg \exists x : X .\ p x = 0}$$

- 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 $p : X \to 2$,

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

- **Weaker notion:**

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

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

Discussion for HoTT/UF practitioners

(There are some in the audience)

$$\left(\underset{\Sigma}{\exists} x : X .\ p\,x \underset{\mathrm{Id}}{=} 0\right) \underset{+}{\vee} \left(\underset{\Pi}{\forall} x : X .\ p\,x = 1\right)$$

- But the notion with propositionally truncated Σ is also relevant.
  - E.g. $\mathrm{Fin}\ n$ is searchable with Σ.
  - But (kuratowski) finite sets are searchable only with truncated Σ.
- However, the results discussed here use the Σ version.

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

  define $\beta_n = \min(p\,\underline{0}, p\,\underline{1}, \ldots, p\,\underline{n})$ 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 β drinks, then everybody drinks.

Some consequences (decision procedures)

(1) For every $p : \mathbb{N}_\infty \to 2$ either $\forall n : \mathbb{N},\ p\ \underline{n} = 1$ or $\neg \forall n : \mathbb{N}.\ p\ \underline{n} = 1$

(JSL'2013)

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

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

(3) There is some discontinuous $p : \mathbb{N}_\infty \to 2$ 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 $\mathbb{N}_\infty$

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 $\mathbb{N}_\infty$ to fill a gap in an unpublished but widely circulated 1958 manuscript by Tait.)

Searchable sets in our type theory

(1) $\mathbb{0}$, $\mathbb{1}$ 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. (Micro-Tychonoff)

Building more searchable sets

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

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

  (1) $\mathbb{1}$

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

  (2) $X+Y$

  $X \times Y$ (baby Tychonoff)

  (3) $\Sigma\, x : X,\, A\, x$ (lexicographic order – also requires thought)

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

Extending families of searchable sets

General situation:

$$\begin{tikzcd} X \arrow[r, hook, "j"] \arrow[dr, "A"'] & Y \arrow[d, dotted, "B"] \\ & \mathcal{U} \end{tikzcd}$$

embedding

$\simeq$

type family

type universe

extension of A along j up to bijection

Interested in:

$$\begin{tikzcd} \mathbb{N} \arrow[r, hook] \arrow[dr, "A"'] & \mathbb{N}_\infty \arrow[d, dotted, "B"] \\ & \mathcal{U} \end{tikzcd}$$

canonical embedding

Want: If $A\,x$ searchable for every $x : X$, then $B\,y$ searchable for every $y : Y$.

Because then: By (3), if Y is also searchable, then $\Sigma\, y : Y,\ B\,y$ searchable too.

Family extension problem

$$\begin{tikzcd} X \arrow[r, hook, "j"] \arrow[dr, "A"', "\simeq"] & Y \arrow[d, dotted, "B"] \\ & \mathcal{U} \end{tikzcd}$$

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

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

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

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

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

why? By Micro-Tychonoff

Summary of the previous reasoning

$$\begin{tikzcd} X \arrow[r, hook, "j"] \arrow[dr, "A"'] & Y \arrow[d, dotted] \\ & \mathcal{U} \end{tikzcd}$$

j given, A given, $\simeq$

$$B\,y := \prod_{x : j^{-1}(y)} A\,x$$

Special case of interest:

$$\begin{tikzcd} \mathbb{N} \arrow[r, hook] \arrow[dr, "A"'] & \mathbb{N}_\infty \arrow[d, dotted, "B"] \\ & \mathcal{U} \end{tikzcd}$$

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

$$\begin{tikzcd} \mathbb{N} \arrow[r, hook, "j"] \arrow[dr, "A"'] & \mathbb{N}_\infty \arrow[d, dotted] \\ & \mathcal{U} \end{tikzcd} \qquad B_y = \prod_{x : j^{-1}(y)} A_x$$

Classically

This is a bijection (with noncomputable inverse)

Constructively

This is an injection whose image has empty complement.

$$\left(\sum_{x : \mathbb{N}} A_x \right) + 1 \hookrightarrow \sum_{y : \mathbb{N}_\infty} B_y$$

adds "isolated" point

adds point "at infinity".

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

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

$\boxed{\text{what is the point of the previous discussion ?}}$

- The well-ordered set $\left(\sum_{x:\mathbb{N}} Ax\right)+1$ 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.

$$\underset{x:\mathbb{N}}{\Sigma_1} Ax \hookrightarrow \sum_{x:\mathbb{N}}^{1} Ax$$

Constructively, this embedding has empty complement.

Ordinal expressions OE

Inductively defined (a W type)

We can get much higher than ε_0 (c.f. Anton Setzer's work)

$$\mathrm{One} : OE$$
$$\mathrm{Add} : OE \to OE \to OE$$
$$\mathrm{Mul} : OE \to OE \to OE$$
$$\mathrm{Sum1} : (\mathbb{N} \to OE) \to OE$$

Two interpretations

$$[\![\mathrm{one}]\!]_1 = 1$$
$$[\![\mathrm{Add}\ e\ e']\!]_1 = [\![e]\!]_1 + [\![e']\!]_1$$
$$[\![\mathrm{Mul}\ e\ e']\!]_1 = [\![e]\!]_1 \times [\![e']\!]_1$$
$$[\![\mathrm{Sum1}\ e]\!]_1 = \sum_{n:\mathbb{N}}{}_1\ [\![e]\!]_1\, n$$

$$[\![\mathrm{one}]\!]^1 = 1$$
$$[\![\mathrm{Add}\ e\ e']\!]^1 = [\![e]\!]^1 + [\![e']\!]^1$$
$$[\![\mathrm{Mul}\ e\ e']\!]^1 = [\![e]\!]^1 \times [\![e']\!]^1$$
$$[\![\mathrm{Sum1}\ e]\!]^1 = \sum_{n:\mathbb{N}}^1 [\![e]\!]^1\, n$$

only difference

Theorems

The ordinal $[\![e]\!]_1$

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

The ordinal $[\![e]\!]^1$

- is searchable
- is a retract of $\mathbb{N} \to 2$
- 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

$$[\![e]\!]_1 \hookrightarrow [\![e]\!]^1$$

whose image has empty complement (but is a bijection iff LPO holds)

The embedding doesn't have a **computable** inverse.

$\boxed{\text{Illustration}}$ The ordinal $\omega+1$

$$n \longmapsto 1^n 0^\omega$$

$$\mathbb{N} + \mathbb{1} \hookrightarrow \mathbb{N}_\infty$$

$$* \longmapsto 1^\omega$$

- 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^ω.

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

Totally separated sets

In some models, all maps $\mathbb{R} \to 2$ 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 $X \to 2$:

Definition. A type X is called totally separated if

$$(\forall p : X \to 2,\ p\,x = p\,y) \longrightarrow x = y$$

"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 $\mathbb{N} \to 2$ is and 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 motivate & 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, 2019) 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)?