Synthetic Computability

Sander Suverkropp

s1019051

MFoCS Seminar — Radboud University Nijmegen

23rd February 2023

Introduction

- First Steps in Synthetic Computability Theory
- On Synthetic Undecidability in Coq, with an Application to the Entscheidungsproblem

Motivation

- Models of computation:
  - Turing machines
  - Partial recursive functions
- Gödel encodings
- Alternative: more abstract

Synthetic Computability Theory

- Constructive set theory
- All functions and sets have computability structure
- For example, enumerable sets are computably enumerable

Intuitionistic set theory

- Intuitionistic logic
- No excluded middle

$$\phi \vee \neg\phi$$

Truth values

- Represented by sentences: $\top$, $\bot$, $\forall x \in \mathbb{R}.(x = 0 \vee x \neq 0)$
- Truth values p, q are equal iff $p \iff q$

Truth values

- Represented by sentences: $\top$, $\bot$, $\forall x \in \mathbb{R}.(x = 0 \vee x \neq 0)$
- Truth values p, q are equal iff $p \iff q$
- Identification with *subsingletons*: $\{\_ \in 1 \mid p\}$
- Then the set of truth values is:

$$\Omega = \mathcal{P}(1)$$

Truth values

- Represented by sentences: $\top$, $\bot$, $\forall x \in \mathbb{R}.(x = 0 \vee x \neq 0)$
- Truth values p, q are equal iff $p \iff q$
- Identification with *subsingletons*: $\{\_ \in 1 \mid p\}$
- Then the set of truth values is:

$$\Omega = \mathcal{P}(1)$$

- Decidable truth values:

$$2 = \{p \in \Omega \mid p \vee \neg p\} = \{\top, \bot\}$$

- Classical truth values:

$$\Omega_{\neg\neg} = \{p \in \Omega \mid \neg\neg p \implies p\}$$

Axiom of Choice

Definition (Projective sets)

Choice holds for A and B, written $AC(A, B)$, if for all relations $R \subseteq A \times B$,

$$(\forall x \in A.\exists y \in B.R(x, y)) \Rightarrow \exists f \in B^A.\forall x \in A.(x, f(x)) \in R$$

A set A is *projective* if for all sets B, $AC(A, B)$ holds.

- Number Choice Axiom: The set $\mathbb{N}$ is projective.
- Dependent Choice Axiom: If R is a total relation on A, and $x \in A$, then there is function $f : \mathbb{N} \to A$ such that $f(0) = x$ and $R(f(n), f(n+1))$ holds for all $n \in \mathbb{N}$

Enumerability

Definition (Enumerability)

A set A is *enumerable* if there is a surjection $e : \mathbb{N} \to 1 + A$.

- $\mathcal{E}$ is the set of enumerable subsets of $\mathbb{N}$

$$\mathcal{E} = \{A \subseteq \mathbb{N} \mid \exists e : \mathbb{N} \to 1 + A\}$$

Projection theorem

Theorem (Projection theorem)

A subset of $\mathbb{N}$ is enumerable if and only if it is the projection of a decidable subset of $\mathbb{N} \times \mathbb{N}$.

Projection theorem

Theorem (Projection theorem)

A subset of $\mathbb{N}$ is enumerable if and only if it is the projection of a decidable subset of $\mathbb{N} \times \mathbb{N}$.

Proof.

If A is enumerated by $e : \mathbb{N} \to 1 + A$, then A is the projection of the decidable set $\{\langle n, m\rangle \in \mathbb{N} \times \mathbb{N} \mid e(n) = m\}$.

Projection theorem

Theorem (Projection theorem)

A subset of $\mathbb{N}$ is enumerable if and only if it is the projection of a decidable subset of $\mathbb{N} \times \mathbb{N}$.

Proof.

If A is enumerated by $e : \mathbb{N} \to 1 + A$, then A is the projection of the decidable set $\{\langle n, m\rangle \in \mathbb{N} \times \mathbb{N} \mid e(n) = m\}$.
If $D \subseteq \mathbb{N} \times \mathbb{N}$ is decidable, and $A = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}. \langle n, m\rangle \in D\}$, then the following enumerates A:

$$e\langle n, m\rangle = \begin{cases} n & \text{if } \langle n, m\rangle \in D \\ \star & \text{if } \langle n, m\rangle \notin D \end{cases}$$

□

Semidecidable truth values

- Idea: truth values $\Sigma \subseteq \Omega$ such that $\mathcal{E} = \Sigma^{\mathbb{N}}$
- By the projection theorem, $A \in \mathcal{E}$ is the projection of a decidable subset $D \subseteq \mathbb{N} \times \mathbb{N}$
- So $m \in A$ iff $\exists n \in \mathbb{N}.\chi_D(m, n)$
- Define $f_m(n) = \chi_D(m, n)$
- Then $m \in A$ if and only if $\exists n \in \mathbb{N}.f_m(n)$

Definition (Semidecidable truth values)

The *semidecidable truth values* are the truth values of the form $\exists f \in 2^{\mathbb{N}}.(p \iff \exists n \in \mathbb{N}.f(n))$

Markov's Principle

Axiom (Markov's Principle)

A binary sequence which is not constantly 0 contains a 1.

Equivalent statements:

- Semidecidable truth values are classical: $\Sigma \subseteq \Omega_{\neg\neg}$
- Semidecidable subsets are classical
- Semidecidable subsets of $\mathbb{N}$ are classical

Post's Theorem

Theorem (Post's Theorem)

A subset B of a set A is decidable if and only if B and $A \setminus B$ are enumerable.

Post's Theorem

Theorem (Post's Theorem)

A subset B of a set A is decidable if and only if B and $A \setminus B$ are enumerable.

Proof.

We look only at the truth values $x \in B$.
We will prove that p is decidable if and only if $p, \neg p$ are semidecidable.
Since $2 \subseteq \Sigma$, if p is decidable, then $p, \neg p$ are semidecidable.
Suppose p and $\neg p$ are semidecidable. Then $p \vee \neg p \in \Sigma \subseteq \Omega_{\neg\neg}$.
Since $\neg\neg(p \vee \neg p)$ is always true, it follows that $p \in 2$. □

Partial functions

Definition (Partial functions and partial values)

A *partial function* $f : A \rightharpoonup B$ is a function $f : A \to \tilde{B}$, where

$$\tilde{B} = \{s \in \mathcal{P}(B) \mid \forall x, y \in s. x = y\}$$

Here $\tilde{B}$ is the set of *partial values* of B.

- Partial values are subsingletons, like truth values
- $\emptyset = \bot_B \in \tilde{B}$
- $\forall x \in B. \{x\} \in \tilde{B}$

Σ-partial functions

- The equivalent of partial computable functions are partial functions with a semidecidable graph:

$$\Gamma(f) = \{\langle x, y\rangle \in A \times B \mid f(x) = \{y\}\}$$

- Those are exactly the functions for which $f(x)\downarrow$ is semidecidable

Σ-partial functions

- The equivalent of partial computable functions are partial functions with a semidecidable graph:

$$\Gamma(f) = \{\langle x, y\rangle \in A \times B \mid f(x) = \{y\}\}$$

- Those are exactly the functions for which $f(x)\downarrow$ is semidecidable

Definition (Σ-partial functions)

The *lifting* $A_\perp$ of a set A is the set of Σ*-partial values*,

$$A_\perp = \{s \in \tilde{A} \mid s\downarrow \in \Sigma\}$$

A Σ*-partial function* is a partial function $f : A \to B_\perp$.

Enumerability Axiom

Axiom (Enumerability Axiom)

There are enumerably many enumberable subsets of $\mathbb{N}$.

Enumerability Axiom

Axiom (Enumerability Axiom)

There are enumerably many enumberable subsets of $\mathbb{N}$.

- This is incompatible with classical logic

Enumerability Axiom

Axiom (Enumerability Axiom)

There are enumerably many enumberable subsets of $\mathbb{N}$.

- This is incompatible with classical logic

Proposition

$\mathbb{N} \to \mathbb{N}_\perp$ is enumerable.

Synthetic computability in Coq

- Coq's type theory (also intuitionistic)
- All definable functions computable
- Avoids proving computability with explicit models of computation

Synthetic Undecidability

- Consistent with all functions are computable
- Solution: axiom for undecidability of a known problem
- PCP

PCP

Definition (PCP)

A *stack* is a list of cards, where each card is a pair of strings of booleans.

$$\mathbb{S} = \mathcal{L}(\mathcal{L}(2) \times \mathcal{L}(2))$$

A card is written s/t. PCP asks whether a card of the form s/s can be derived from a given stack S.

$$\frac{s/t \in S}{S \triangleright s/t} \qquad \frac{S \triangleright u/v \quad s/t \in S}{S \triangleright s +\!\!+ u/t +\!\!+ v} \qquad \frac{S \triangleright s/s}{\text{PCP } S}$$

Axiom of undecidability of PCP

- PCP S is enumerable

Axiom (Axiom of undecidability of PCP)

PCP S is not co-enumerable.

Reducing the Entscheidungsproblem to PCP

- The Entscheidungsproblem asks whether formulas in first-order logic are valid
- This can be reduced to PCP by translating each derivation rule to a formula
- Idea: translate each derivation rule into a formula

Reducing the Entscheidungsproblem to PCP

$$\frac{s/t \in S}{S \triangleright s/t} \qquad \frac{S \triangleright u/v \quad s/t \in S}{S \triangleright s \mathbin{+\!\!+} u/t \mathbin{+\!\!+} v} \qquad \frac{S \triangleright s/s}{\text{PCP } S}$$

$$\varphi_1 := \bigwedge_{s/t \in S} Pst$$

$$\varphi_2 := \bigwedge_{s/t \in S} \forall xy. Pxy \to P(s \mathbin{+\!\!+} x)(t \mathbin{+\!\!+} y)$$

$$\varphi_3 := \forall x. Pxx \to Q$$

$$\varphi_S := \varphi_1 \to \varphi_2 \to \varphi_3 \to Q$$

Questions

Are there any questions?