Reverse mathematics in constructive set theory

Hajime Ishihara

School of Information Science
Japan Advanced Institute of Science and Technology
(JAIST)
Nomi, Ishikawa 923-1292, Japan

Proof and Computation, Fischbachau,
26 September – 1 October, 2022

Overview

- Lecture 1
  - Reverse mathematics and set theory
  - Intuitionistic logic
- Lecture 2
  - Classical Zermelo-Fraenkel set theory ZF
  - Basic constructive set theory BCST
  - Elementary constructive set theory ECST
  - Constructive Zermelo-Fraenkel set theory CZF
- Lecture 3
  - Set-generated classes and NID principles
  - Equivalents of the nullary NID
  - Equivalents of the elementary NID
  - Equivalents of the finitary NID

Lecture 2

- Classical Zermelo-Fraenkel set theory ZF
- Basic constructive set theory BCST
- Elementary constructive set theory ECST
- Constructive Zermelo-Fraenkel set theory CZF

Classical Zermelo-Fraenkel set theory ZF

Set theory

- The language of a set theory contains variables for sets and the binary predicates $=$ and $\in$.
- The axioms and rules are those of classical/intuitionistic predicate logic with equality.
- The axioms for equality:

  Reflexivity: $\forall x(x = x)$;

  Replacement schema:

$$\forall xy(\varphi(x) \wedge x = y \to \varphi(y))$$

  for every formula $\varphi(x)$.

Set theory

Notation 1

- $\forall x \in a\, \varphi(x) \equiv \forall x(x \in a \to \varphi(x))$;
- $\exists x \in a\, \varphi(x) \equiv \exists x(x \in a \wedge \varphi(x))$;
- $a \subseteq b \equiv \forall x \in a\, (x \in b) \equiv \forall x(x \in a \to x \in b)$;
- $0 \equiv \emptyset$;
- $x + 1 \equiv x \cup \{x\}$.

Note that $n = \{0, \ldots, n-1\}$.

Class notation and terminology

Given a formula $\varphi(x)$, we may form a class, that is, a collection of the form

$$\{x \mid \varphi(x)\}.$$

- Not all classes are sets; hence we can not quantify over classes.
- We write $a \in \{x \mid \varphi(x)\}$ for $\varphi(a)$.
- For a set C, we write $C = \{x \mid \varphi(x)\}$ for

$$\forall x(x \in C \leftrightarrow x \in \{x \mid \varphi(x)\}) \equiv \forall x(x \in C \leftrightarrow \varphi(x)).$$

- A class $\{x \mid \varphi(x)\}$ is a set if

$$\exists y \forall x(x \in y \leftrightarrow x \in \{x \mid \varphi(x)\}) \equiv \exists y \forall x(x \in y \leftrightarrow \varphi(x)).$$

The classical Zermelo-Fraenkel set theory, ZF

The axioms and rules of ZF are those of classical predicate logic with equality. In addition, ZF has the following set theoretic axioms:

Extensionality: $\forall a \forall b[\forall x(x \in a \leftrightarrow x \in b) \rightarrow a = b]$;

Pairing: $\forall a \forall b \exists c \forall x(x \in c \leftrightarrow x = a \vee x = b)$;

Emptyset: $\exists a \forall x(x \notin a)$;

Union: $\forall a \exists b \forall x[x \in b \leftrightarrow \exists y \in a\,(x \in y)]$;

Separation:

$$\forall a \exists b \forall x[x \in b \leftrightarrow x \in a \wedge \varphi(x)]$$

for every formula $\varphi(x)$;

The classical Zermelo-Fraenkel set theory, ZF

Replacement:

$$\forall a[\forall x \in a \exists ! y \varphi(x,y) \rightarrow \exists b \forall y(y \in b \leftrightarrow \exists x \in a\, \varphi(x,y))]$$

for every formula $\varphi(x,y)$;

Powerset: $\forall a \exists b \forall x[x \in b \leftrightarrow x \subseteq a]$;

Infinity: $\exists a[0 \in a \wedge \forall x(x \in a \rightarrow x+1 \in a)]$;

Foundation:

$$\exists x \varphi(x) \rightarrow \exists x[\varphi(x) \wedge \forall y(y \in x \rightarrow \neg \varphi(y))]$$

for every formula $\varphi(x)$.

The axiom of choice

We consider the following form of the axiom of choice:

$$\forall a[\forall x \in a \exists y(y \in x) \to \exists f \in (\bigcup a)^a \, \forall x \in a \, (f(x) \in x)].$$

Theorem 2

The axiom of choice implies DNE, *constructively.*

The axiom of choice

Proof.

For each formula A with $\neg\neg A$, define sets x_0 and x_1 as follows:

$$x_0 = \{y \in \{0,1\} \mid y = 0 \vee A\}, \quad x_1 = \{y \in \{0,1\} \mid y = 1 \vee A\},$$

and let $a = \{x_0, x_1\}$. Then, since $0 \in x_0$ and $1 \in x_1$, we have

$$\forall x \in a \, \exists y (y \in x).$$

Hence, by the axiom of choice, there exists a function $f : a \to \bigcup a = \{0,1\}$ such that

$$\forall x \in a \, (f(x) \in x).$$

Note that if A, then, since $x_0 = x_1$, we have $f(x_0) = f(x_1)$. If $f(x_0) = 0$ and $f(x_1) = 1$, then $\neg A$, a contradiction. Therefore either $f(x_0) = 1$ or $f(x_1) = 0$, and so $1 \in x_0$ or $0 \in x_1$. Thus A. $\square$

Basic constructive set theory BCST

Basic constructive set theory, BCST

The axioms and rules of BCST are those of intuitionistic predicate logic with equality. In addition, BCST has the following set theoretic axioms:

Extensionality: $\forall a \forall b [\forall x (x \in a \leftrightarrow x \in b) \rightarrow a = b]$;

Pairing: $\forall a \forall b \exists c \forall x (x \in c \leftrightarrow x = a \vee x = b)$;

Emptyset: $\exists a \forall x (x \notin a)$;

Union: $\forall a \exists b \forall x [x \in b \leftrightarrow \exists y \in a \, (x \in y)]$;

Basic constructive set theory, BCST

Bounded Separation:

$$\forall a \exists b \forall x [x \in b \leftrightarrow x \in a \wedge \varphi(x)]$$

for every bounded formula $\varphi(x)$. Here a formula $\varphi(x)$ is bounded, or Δ_0, if all the quantifiers occurring in it are bounded, i.e. of the form $\forall x \in c$ or $\exists x \in c$;

Replacement:

$$\forall a [\forall x \in a\, \exists! y \varphi(x, y) \rightarrow \exists b \forall y (y \in b \leftrightarrow \exists x \in a\, \varphi(x, y))]$$

for every formula $\varphi(x, y)$.

Sets in BCST

Extensionality: for each formula $\varphi(x)$ and each A and B,

- $\{x \mid \varphi(x)\}$ corresponds to at most one set:

$$A = \{x \mid \varphi(x)\} \wedge B = \{x \mid \varphi(x)\} \to A = B;$$

- $\subseteq$ is anti-symmetric:

$$A \subseteq B \wedge B \subseteq A \to A = B.$$

Pairing: for each a and b,

- $\{a, b\} = \{x \mid x = a \vee x = b\}$ is a set;
- $\{a\} = \{x \mid x = a\}$ is a set;
- $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$ is a set;

Emptyset:

- $\emptyset = \{x \mid \bot\}$ is a set.

Sets in BCST

Union: for each C, A and B,

- $\bigcup C = \{x \mid \exists y \in C\,(x \in y)\}$ is a set;
- $A \cup B = \bigcup\{A, B\} = \{x \mid x \in A \vee x \in B\}$ is a set.

Bounded Separation: for each A and B,

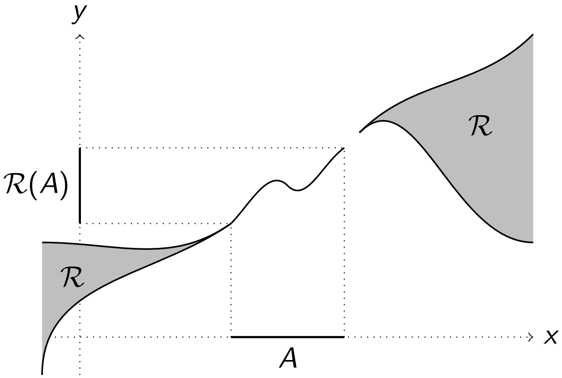
- $A \cap B = \{x \mid x \in A \wedge x \in B\}$ is a set;
- $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$ is a set.

Sets in BCST

Replacement:

$$\forall a[\forall x \in a \exists! y \varphi(x,y) \rightarrow \exists b \forall y (y \in b \leftrightarrow \exists x \in a\, \varphi(x,y))].$$

says that if a class relation $\mathcal{R} = \{\langle x,y\rangle \mid \varphi(x,y)\}$ is total and single valued on a set A, then the image $\mathcal{R}(A) = \{y \mid \exists x \in A\, \varphi(x,y)\}$ of A under $\mathcal{R}$ is a set.



Sets in BCST

For each A and B,

- for each $a \in A$, since $\forall x \in B \, \exists! y (y = \langle a, x \rangle)$,

  $$\{a\} \times B = \{y \mid \exists x \in B \, (y = \langle a, x \rangle)\}$$

  is a set, by Replacement;
- since $\forall x \in A \, \exists! z (z = \{x\} \times B)$,

  $$C = \{z \mid \exists x \in A \, (z = \{x\} \times B)\}$$

  is a set, by Replacement;
- $$A \times B = \bigcup C = \bigcup \{z \mid \exists x \in A \, (z = \{x\} \times B)\}$$

  is a set, by Union.

Russell set

For each set A, define a set R_A, called the Russell set of A, by Bounded Separation as follows:

$$\mathrm{R}_A = \{x \in A \mid x \notin x\}.$$

Proposition 3

For each A, $\mathrm{R}_A \notin A$.

Proof.

Suppose that $\mathrm{R}_A \in A$. If $\mathrm{R}_A \in \mathrm{R}_A$, then $\mathrm{R}_A \notin \mathrm{R}_A$, a contradiction. Therefore $\mathrm{R}_A \notin \mathrm{R}_A$, and so $\mathrm{R}_A \in \mathrm{R}_A$, a contradiction. $\square$

Remark 4

The class $U = \{x \mid \top\}$ is not a set: for if U is a set, then $\mathrm{R}_U \in U$, a contradiction.

Relations

- A relation r between A and B is a subset of $A \times B$; A and B are called the initial set and the final set of R, respectively.
- The inverse relation r^{-1} of a relation $r \subseteq A \times B$ is a relation between B and A given by

$$r^{-1} = \{\langle y, x\rangle \in B \times A \mid \langle x, y\rangle \in r\}.$$

- For a relation $r \subseteq A \times B$ and a subset C of A, the image $r(C)$ of C under r is a subset of B given by

$$r(C) = \{y \in B \mid \exists x \in C\,(\langle x, y\rangle \in r)\}.$$

- For a relation $r \subseteq A \times B$ and a subset D of B, the inverse image $r^{-1}(D)$ of D under r is a subset of A given by

$$r^{-1}(D) = \{x \in A \mid \exists y \in D\,(\langle x, y\rangle \in r)\}.$$

Relations

- For relations $r \subseteq A \times B$ and $s \subseteq B \times C$, their composition $s \circ r$ is the relation between A and C given by

$$s \circ r = \{\langle x, z \rangle \in A \times C \mid \exists y \in B\,(\langle x, y \rangle \in r \wedge \langle y, z \rangle \in s)\}.$$

Proposition 5

For $r \subseteq A \times B$ and $s \subseteq B \times C$,

1. $(r^{-1})^{-1} = r$,
2. $(s \circ r)^{-1} = r^{-1} \circ s^{-1}$.

Relations

A category C consists of

- A class of objects;
- for each object X and Y, a class $\hom_C(X, Y)$ of morphisms; we write $f : X \to Y$ or $X \xrightarrow{f} Y$ for $f \in \hom_C(X, Y)$;
- for each object X, Y and Z, an operation, called composition:

$$\circ : \hom_C(X, Y) \times \hom_C(Y, Z) \to \hom_C(X, Z);$$

- for each object X, a morphism $1_X : X \to X$, called identity;

where composition and identity satisfy

1. for all $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$,

$$h \circ (g \circ f) = (h \circ g) \circ f;$$

2. for all $f : X \to Y$, $f \circ 1_X = 1_Y \circ f = f$.

Relations

- For a set A, the diagonal set Δ_A is the relation between A and A given by

$$\Delta_A = \{\langle x, y\rangle \in A \times A \mid x = y\}.$$

Proposition 6

For $r \subseteq A \times B$, $s \subseteq B \times C$ and $t \subseteq C \times D$,

1. $t \circ (s \circ r) = (t \circ s) \circ r$,
2. $r \circ \Delta_A = \Delta_B \circ r = r$.

We write Rel for the category of sets and relations.

Relations

- A relation $r \subseteq A \times B$ is total (or is a multivalued function) if
$$\forall x \in A \, \exists y \in B \, (\langle x, y \rangle \in r).$$
- A relation $r \subseteq A \times B$ is single valued if
$$\forall x \in A \, \forall y, z \in B \, (\langle x, y \rangle \in r \wedge \langle x, z \rangle \in r \rightarrow y = z).$$

Theorem 7

Let $r \subseteq A \times B$ be a relation. Then

1. *r is total if and only if $\Delta_A \subseteq r^{-1} \circ r$;*
2. *r is single valued if and only if $r \circ r^{-1} \subseteq \Delta_B$.*

Functions

- A function f from A into B is a total and single valued relation $f \subseteq A \times B$; we then write $f : A \to B$ or $A \xrightarrow{f} B$; we write $f(a)$ for b such that $f(\{a\}) = \{b\}$.
- A function $f : A \to B$ is surjective if

$$\forall y \in B \, \exists x \in A \, (y = f(x)).$$

- A function $f : A \to B$ is injective if

$$\forall x, y \in A \, (f(x) = f(y) \to x = y).$$

Lemma 8

Let $f : A \to B$. Then

1. *f is surjective if and only if $f^{-1} \subseteq B \times A$ is total;*
2. *f is injective if and only if $f^{-1} \subseteq B \times A$ is single valued.*

Functions

We write Set for the category of sets and functions.
A morphism $f : X \to Y$ of a category C is

- epic if for all $g, h : Y \to Z$, $g = h$ whenever $g \circ f = h \circ f$;
- monic if for all $g, h : Z \to X$, $g = h$ whenever $f \circ g = f \circ h$.

Theorem 9
Let $f : A \to B$. Then

1. *f is surjective if and only if f is epic in* Set*;*
2. *f is injective if and only if f is monic in* Set*.*

Functions

Proof.

Suppose that for all $g, h : B \to C$, if $g \circ f = h \circ f$, then $g = h$. For each $b \in B$, let $c_b = \{u \in 1 \mid \exists x \in A\,(b = f(x))\}$. Then, since $\forall y \in B\,\exists! z(z = c_y)$,

$$C_0 = \{z \mid \exists y \in B\,(z = c_y)\}$$

is a set by Replacement. Let $C = C_0 \cup \{1\}$, and define $g, h : B \to C$ by $g(b) = c_b$ and $h(b) = 1$ for all $b \in B$. Then

$$(g \circ f)(a) = g(f(a)) = c_{f(a)} = 1 = h(f(a)) = (h \circ f)(a)$$

for all $a \in A$; hence $g \circ f = h \circ f$. Therefore $g = h$, and so $c_b = g(b) = h(b) = 1$ for all $b \in B$. Thus $\forall y \in B\,\exists x \in A\,(y = f(x))$, that is, f is surjective. $\square$

Quotients

Let A be a set. A subset r of $A \times A$ is an equivalence relation on A if

1. $a \; r \; a$,
2. if $a \; r \; b$, then $b \; r \; a$,
3. if $a \; r \; b$ and $b \; r \; c$ then $a \; r \; c$;

for all $a, b, c \in A$, where $a \; r \; b \Leftrightarrow \langle a, b \rangle \in r$.
Then for each $a \in A$, its equivalence class

$$[a]_r = \{x \in A \mid a \; r \; x\}$$

is a set by Bounded Separation. Since $\forall x \in A \, \exists ! y (y = [x]_r)$, the quotient of A by r

$$A/r = \{[x]_r \mid x \in A\}$$

is a set by Replacement.

Notations for some classes

- The class of total relations between A and B is denoted by $\mathrm{mv}(A, B)$:

$$r \in \mathrm{mv}(A, B) \Leftrightarrow r \subseteq A \times B \wedge \forall x \in A \, \exists y \in B \, (\langle x, y \rangle \in r);$$

- the class of functions from A to B is denoted by B^A:

$$\begin{aligned} f \in B^A \Leftrightarrow {} & f \in \mathrm{mv}(A, B) \\ & \wedge \forall x \in A \, \forall y, z \in B \, (\langle x, y \rangle \in f \wedge \langle x, z \rangle \in f \to y = z); \end{aligned}$$

- the class of subsets of S is denoted by $\mathrm{Pow}(S)$:

$$a \in \mathrm{Pow}(S) \Leftrightarrow a \subseteq S.$$

Elementary constructive set theory ECST

Elementary constructive set theory, ECST

The axioms and rules of ECST are those of intuitionistic predicate logic with equality. In addition, ECST has the set theoretic axioms of BCST and

Strong Infinity:

$$\exists a[0 \in a \wedge \forall x(x \in a \rightarrow x+1 \in a)$$
$$\wedge \forall y(0 \in y \wedge \forall x(x \in y \rightarrow x+1 \in y) \rightarrow a \subseteq y)].$$

Infinity and Strong Infinity

By Infinity: $\exists a[0 \in a \wedge \forall x(x \in a \rightarrow x+1 \in a)]$, there exists a set A_0 such that

$$0 \in A_0 \wedge \forall x(x \in A_0 \rightarrow x+1 \in A_0).$$

Hence, by (full) Separation, there exists a set A given by

$$A = \{z \in A_0 \mid \forall y(0 \in y \wedge \forall x(x \in y \rightarrow x+1 \in y) \rightarrow z \in y)\}.$$

Then it is straghtforward to show that

$$\begin{aligned} &0 \in A \wedge \forall x(x \in A \rightarrow x+1 \in A) \\ &\qquad\qquad \wedge \forall y(0 \in y \wedge \forall x(x \in y \rightarrow x+1 \in y) \rightarrow A \subseteq y). \end{aligned}$$

However, ECST dose not have (full) Separation.
We have to adopt Strong Infinity instead of Infinity.

Dedekind-Peano axioms

Lemma 10
In ECST,

$$\exists! a[0 \in a \land \forall x(x \in a \to x+1 \in a) \\ \land \forall y(0 \in y \land \forall x(x \in y \to x+1 \in y) \to a \subseteq y)].$$

We write ω *for the unique such set* a*.*

Dedekind-Peano axioms

Let $(\omega, 0, S)$ be a structure with $0 = \emptyset$ and $S : \omega \to \omega$ given by $S(x) = x + 1$ for all $x \in \omega$.

Proposition 11

In ECST*, the structure* $(\omega, 0, S)$ *satisfies the Dedekind-Peano axioms:*

1. $0 \neq S(x)$ *for all* $x \in \omega$*;*
2. S *is injective;*
3. *if* X *is a subset of* ω *such that* $0 \in X$ *and* $S(x) \in X$ *for all* $x \in X$*, then* $X = \omega$*.*

Finite Power Axiom

Finite Powers Axiom (FPA):

$$\forall a \forall n \in \omega \, \exists b (b = a^n).$$

Lemma 12

In ECST, *(full) Separation implies* FPA.

Proof.

Let B be a set defined by (full) Separation as follows:

$$B = \{x \in \omega \mid \exists b (b = a^x)\}.$$

Then it is straghtforward to show that

$$0 \in B \wedge \forall x (x \in B \rightarrow x + 1 \in B);$$

hence $\omega \subseteq B$. $\square$

Finitely enumerable sets

- A set A is finitely enumerable if there exist $n \in \omega$ and a surjection $f : n \to A$;
- For a set S, we write $\mathrm{Fin}(S)$ for the class of finitely enumerable subsets of S.

Lemma 13

In ECST, FPA *implies that for each set* S, $\mathrm{Fin}(S)$ *is a set.*

Constructive Zermelo-Fraenkel set theory CZF

Constructive Zermelo-Fraenkel set theory CZF

The axioms and rules of CZF are those of intuitionistic predicate logic with equality. CZF is obtained from ECST by replacing Replacement by

Strong Collection:

$$\forall a[\forall x \in a\, \exists y \varphi(x,y) \rightarrow \exists b(\forall x \in a\, \exists y \in b\, \varphi(x,y) \\ \wedge \forall y \in b\, \exists x \in a\, \varphi(x,y))]$$

for every formula $\varphi(x,y)$,

Constructive Zermelo-Fraenkel set theory CZF

and adding

Subset Collection:

$$\begin{aligned}\forall a \forall b \exists c \forall u [\forall x \in a\, \exists y \in b\, \varphi(x,y,u) \rightarrow \\ \exists d \in c\, (\forall x \in a\, \exists y \in d\, \varphi(x,y,u) \\ \wedge\, \forall y \in d\, \exists x \in a\, \varphi(x,y,u))]\end{aligned}$$

for every formula $\varphi(x,y,u)$, and

$\in$-Induction:

$$\forall a(\forall x \in a\, \varphi(x) \rightarrow \varphi(a)) \rightarrow \forall a \varphi(a)$$

for every formula $\varphi(x)$.

Fullness

We consider the following additional axiom.

Fullness:

$$\forall a \forall b \exists c (c \subseteq \mathrm{mv}(a, b) \\ \land \forall r \in \mathrm{mv}(a, b) \, \exists s \in c \, (s \subseteq r)).$$

Lemma 14

In ECST, *Subset Collection implies Fullness.*

Lemma 15

In ECST, *Fullness and Strong Collection imply Subset Collection.*

Fullness

Lemma 16

In ECST, *Fullness implies*

Exponentiation: $\forall a \forall b \exists c \forall f (f \in c \leftrightarrow f \in b^a)$.

Proof.

Let A and B be sets. Then, by Fullness, there exists C_0 such that

$$C_0 \subseteq \mathrm{mv}(A, B) \wedge \forall r \in \mathrm{mv}(A, B) \, \exists s \in C_0 \, (s \subseteq r).$$

Let

$$C = \{r \in C_0 \mid \forall x \in A \forall y, z \in B \, (\langle x, y \rangle \in r \wedge \langle x, z \rangle \in r \to y = z)\},$$

by Bounded Separation. Then $\forall f (f \in C \leftrightarrow f \in B^A)$. $\square$

Corollary 17

In ECST, *Fullness implies* FPA.

References

- P. Aczel and M. Rathjen, *Notes on constructive set theory*, Technical Report 40, Institut Mittag-Leffler, 200/2001.
- P. Aczel and M. Rathjen, *CST Book draft*, http://www1.maths.leeds.ac.uk/~rathjen/book.pdf, August, 2010.
- K. Devlin, *The joy of sets: Fundamentals of contemporary set theory*, Second edition, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1993.
- R. Diaconescu, *Axiom of choice and complementation*, Proc. Amer. Math. Soc. **51** (1975), 176–178.
- N. Goodman and J. Myhill, *Choice implies excluded middle*, Z. Math. Logik Grundlagen Math. **24** (1978), 461.

References

- A. S. Troelstra and D. van Dalen, *Constructivism in mathematics: An introduction*, Vol. I, Studies in Logic and the Foundations of Mathematics **121**, North-Holland Publishing Co., Amsterdam, 1988.
- A. S. Troelstra and D. van Dalen, *Constructivism in mathematics: An introduction*, Vol. II, Studies in Logic and the Foundations of Mathematics **123**, North-Holland Publishing Co., Amsterdam, 1988.