Constructive analysis

Philosophy, Proof and Fundamentals

Hajime Ishihara

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

Interval Analysis and Constructive Mathematics,
Oaxaca, 13 – 18 November, 2016

Contents

A history of constructivism

- History
  - Arithmetization of mathematics (Kronecker, 1887)
  - Three kinds of intuition (Poincaré, 1905)
  - French semi-intuitionism (Borel, 1914)
  - Intuitionism (Brouwer, 1914)
  - Predicativity (Weyl, 1918)
  - Finitism (Skolem, 1923; Hilbert-Bernays, 1934)
  - Constructive recursive mathematics (Markov, 1954)
  - Constructive mathematics (Bishop, 1967)
- Logic
  - Intuitionistic logic (Heyting, 1934; Kolmogorov, 1932)

Mathematical theory

A mathematical theory consists of

- axioms describing mathematical objects in the theory, such as
  - natural numbers,
  - sets,
  - groups, etc.
- logic being used to derive theorems from the axioms

	objects	logic
Interval analysis	intervals	classical logic
Constructive analysis	arbitrary reals	intuitionistic logic
Computable analysis	computable reals	classical logic

Language

We use the standard language of (many-sorted) first-order predicate logic based on

- primitive logical operators $\wedge, \vee, \rightarrow, \perp, \forall, \exists$.

We introduce the abbreviations

- $\neg A \equiv A \rightarrow \perp$;
- $A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$.

The BHK interpretation

The Brouwer-Heyting-Kolmogorov (BHK) interpretation of the logical operators is the following.

- A proof of $A \wedge B$ is given by presenting a proof of A and a proof of B.
- A proof of $A \vee B$ is given by presenting either a proof of A or a proof of B.
- A proof of $A \rightarrow B$ is a construction which transform any proof of A into a proof of B.
- Absurdity $\perp$ has no proof.
- A proof of $\forall x A(x)$ is a construction which transforms any t into a proof of $A(t)$.
- A proof of $\exists x A(x)$ is given by presenting a t and a proof of $A(t)$.

Natural Deduction System

We shall use $\mathcal{D}$, possibly with a subscript, for arbitrary deduction.

We write

$$\begin{array}{c} \Gamma \\ \mathcal{D} \\ A \end{array}$$

to indicate that $\mathcal{D}$ is deduction with conclusion A and assumptions Γ.

Deduction (Basis)

For each formula A,

$$A$$

is a deduction with conclusion A and assumptions $\{A\}$.

Deduction (Induction step, $\to$I)

If

$$\begin{array}{c}\Gamma\\ \mathcal{D}\\ B\end{array}$$

is a deduction, then

$$\dfrac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ B\end{array}}{A \to B}\ \to\mathrm{I}$$

is a deduction with conclusion $A \to B$ and assumptions $\Gamma \setminus \{A\}$.
We write

$$\dfrac{\begin{array}{c}[A]\\ \mathcal{D}\\ B\end{array}}{A \to B}\ \to\mathrm{I}$$

Deduction (Induction step, $\to$E)

If

$$\begin{array}{ccc} \Gamma_1 & & \Gamma_2 \\ \mathcal{D}_1 & & \mathcal{D}_2 \\ A \to B & & A \end{array}$$

are deductions, then

$$\dfrac{\begin{array}{cc} \Gamma_1 & \Gamma_2 \\ \mathcal{D}_1 & \mathcal{D}_2 \\ A \to B & A \end{array}}{B} \to\mathrm{E}$$

is a deduction with conclusion B and assumptions $\Gamma_1 \cup \Gamma_2$.

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg\neg A] \quad \dfrac{\dfrac{[\neg\neg(A\to B)] \quad \dfrac{\dfrac{[\neg B] \quad \dfrac{[A\to B] \quad [A]}{B}\,{\to}\mathrm{E}}{\bot}\,{\to}\mathrm{E}}{\neg(A\to B)}\,{\to}\mathrm{I}}{\bot}\,{\to}\mathrm{E}}{\neg A}\,{\to}\mathrm{I}}{\bot}\,{\to}\mathrm{E}}{\neg\neg B}\,{\to}\mathrm{I}}{\neg\neg A\to\neg\neg B}\,{\to}\mathrm{I}}{\neg\neg(A\to B)\to(\neg\neg A\to\neg\neg B)}\,{\to}\mathrm{I}$$

Minimal logic

$$\dfrac{\begin{matrix}[A]\\ \mathcal{D}\\ B\end{matrix}}{A \to B}\ \to\mathrm{I} \qquad \dfrac{\begin{matrix}\mathcal{D}_1\\ A \to B\end{matrix} \quad \begin{matrix}\mathcal{D}_2\\ A\end{matrix}}{B}\ \to\mathrm{E}$$

$$\dfrac{\begin{matrix}\mathcal{D}_1\\ A\end{matrix} \quad \begin{matrix}\mathcal{D}_2\\ B\end{matrix}}{A \wedge B}\ \wedge\mathrm{I} \qquad \dfrac{\begin{matrix}\mathcal{D}\\ A \wedge B\end{matrix}}{A}\ \wedge\mathrm{E}_r \quad \dfrac{\begin{matrix}\mathcal{D}\\ A \wedge B\end{matrix}}{B}\ \wedge\mathrm{E}_l$$

$$\dfrac{\begin{matrix}\mathcal{D}\\ A\end{matrix}}{A \vee B}\ \vee\mathrm{I}_r \quad \dfrac{\begin{matrix}\mathcal{D}\\ B\end{matrix}}{A \vee B}\ \vee\mathrm{I}_l \qquad \dfrac{\begin{matrix}\mathcal{D}_1\\ A \vee B\end{matrix} \quad \begin{matrix}[A]\\ \mathcal{D}_2\\ C\end{matrix} \quad \begin{matrix}[B]\\ \mathcal{D}_3\\ C\end{matrix}}{C}\ \vee\mathrm{E}$$

Minimal logic

$$\dfrac{\begin{matrix}\mathcal{D}\\ A\end{matrix}}{\forall y A[x/y]}\ \forall\mathrm{I} \qquad \dfrac{\begin{matrix}\mathcal{D}\\ \forall x A\end{matrix}}{A[x/t]}\ \forall\mathrm{E}$$

$$\dfrac{\begin{matrix}\mathcal{D}\\ A[x/t]\end{matrix}}{\exists x A}\ \exists\mathrm{I} \qquad \dfrac{\begin{matrix}\mathcal{D}_1\\ \exists y A[x/y]\end{matrix} \quad \begin{matrix}[A]\\ \mathcal{D}_2\\ C\end{matrix}}{C}\ \exists\mathrm{E}$$

- In $\forall\mathrm{E}$ and $\exists\mathrm{I}$, t must be free for x in A.
- In $\forall\mathrm{I}$, $\mathcal{D}$ must not contain assumptions containing x free, and $y \equiv x$ or $y \notin \mathrm{FV}(A)$.
- In $\exists\mathrm{E}$, $\mathcal{D}_2$ must not contain assumptions containing x free except A, $x \notin \mathrm{FV}(C)$, and $y \equiv x$ or $y \notin \mathrm{FV}(A)$.

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[(A \to B) \land (A \to C)]}{A \to B}\ \land\mathrm{E}_r \qquad [A]}{B}\ \to\mathrm{E} \qquad \dfrac{\dfrac{[(A \to B) \land (A \to C)]}{A \to C}\ \land\mathrm{E}_l \qquad [A]}{C}\ \to\mathrm{E}}{B \land C}\ \land\mathrm{I}}{A \to B \land C}\ \to\mathrm{I}}{(A \to B) \land (A \to C) \to (A \to B \land C)}\ \to\mathrm{I}$$

Example

$$
\dfrac{
  \dfrac{\dfrac{\dfrac{}{[A \vee B]}\quad
    \dfrac{\dfrac{[(A \to C) \wedge (B \to C)]}{A \to C}\,\wedge\mathrm{E}_r \quad [A]}{C}\,{\to}\mathrm{E} \quad
    \dfrac{\dfrac{[(A \to C) \wedge (B \to C)]}{B \to C}\,\wedge\mathrm{E}_l \quad [B]}{C}\,{\to}\mathrm{E}
  }{C}\,\vee\mathrm{E}}{A \vee B \to C}\,{\to}\mathrm{I}
}{(A \to C) \wedge (B \to C) \to (A \vee B \to C)}\,{\to}\mathrm{I}
$$

Example

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A \to \forall x B] \quad [A]}{\forall x B}\ \to\mathrm{E}}{B}\ \forall\mathrm{E}}{A \to B}\ \to\mathrm{I}}{\forall x (A \to B)}\ \forall\mathrm{I}}{(A \to \forall x B) \to \forall x (A \to B)}\ \to\mathrm{I}
$$

where $x \notin \mathrm{FV}(A)$.

Example

$$
\dfrac{[\exists x(A \to B)] \qquad \dfrac{\dfrac{[A \to B] \quad [A]}{B}\ \to\mathrm{E}}{\exists x B}\ \exists\mathrm{I}}{\dfrac{\dfrac{\exists x B}{A \to \exists x B}\ \to\mathrm{I}}{\exists x(A \to B) \to (A \to \exists x B)}\ \to\mathrm{I}}\ \exists\mathrm{E}
$$

where $x \notin \mathrm{FV}(A)$.

Intuitionistic logic

Intuitionistic logic is obtained from minimal logic by adding the intuitionistic absurdity rule (ex falso quodlibet).

If

$$\begin{array}{c}\Gamma\\ \mathcal{D}\\ \bot\end{array}$$

is a deduction, then

$$\dfrac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ \bot\end{array}}{A}\ \bot_i$$

is a deduction with conclusion A and assumptions Γ.

Example

$$
\dfrac{\dfrac{\dfrac{[\neg\neg A \to \neg\neg B] \qquad \dfrac{\dfrac{[\neg(A \to B)] \qquad \dfrac{\dfrac{\dfrac{[\neg A] \quad [A]}{\bot}\ {\to}\mathrm{E}}{B}\ {\color{red}\bot_i}}{A \to B}\ {\to}\mathrm{I}}{\bot}\ {\to}\mathrm{E}}{\neg\neg A}\ {\to}\mathrm{I}}{\neg\neg B}\ {\to}\mathrm{E} \qquad \dfrac{\dfrac{[\neg(A \to B)] \quad \dfrac{[B]}{A \to B}\ {\to}\mathrm{I}}{\bot}\ {\to}\mathrm{E}}{\neg B}\ {\to}\mathrm{I}}{\dfrac{\bot}{\neg\neg(A \to B)}\ {\to}\mathrm{I}}}{(\neg\neg A \to \neg\neg B) \to \neg\neg(A \to B)}\ {\to}\mathrm{I}
$$

Example

$$\dfrac{[A \vee B] \qquad \dfrac{\dfrac{[\neg A] \quad [A]}{\bot}\,\to\mathrm{E}}{B}\,{\color{red}\bot_i} \qquad [B]}{\dfrac{\dfrac{B}{\neg A \to B}\,\to\mathrm{I}}{A \vee B \to (\neg A \to B)}\,\to\mathrm{I}}\,\vee\mathrm{E}$$

Classical logic

Classical logic is obtained from intuitionistic logic by strengthening the absurdity rule to the classical absurdity rule (reductio ad absurdum).

If

$$\begin{array}{c}\Gamma\\ \mathcal{D}\\ \bot\end{array}$$

is a deduction, then

$$\dfrac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ \bot\end{array}}{A}\ \bot_c$$

is a deduction with conclusion A and assumption $\Gamma \setminus \{\neg A\}$.

Example (classical logic)

The double negation elimination (DNE):

$$\dfrac{\dfrac{\dfrac{[\neg\neg A] \quad [\neg A]}{\bot}\ {\to}\mathrm{E}}{A}\ \bot_c}{\neg\neg A \to A}\ {\to}\mathrm{I}$$

Example (classical logic)

The principle of excluded middle (PEM):

$$\dfrac{\dfrac{[\neg(A \vee \neg A)] \qquad \dfrac{\dfrac{\dfrac{[\neg(A \vee \neg A)] \quad \dfrac{[A]}{A \vee \neg A}\ \vee\mathrm{I}_r}{\bot}\ \to\mathrm{E}}{\neg A}\ \to\mathrm{I}}{A \vee \neg A}\ \vee\mathrm{I}_l}{\bot}\ \to\mathrm{E}}{A \vee \neg A}\ \bot_c$$

Example (classical logic)

De Morgan's law (DML):

$$
\dfrac{\dfrac{\dfrac{[\neg(\neg A\vee\neg B)] \quad \dfrac{\dfrac{\dfrac{[\neg(\neg A\vee\neg B)] \quad \dfrac{\dfrac{\dfrac{[\neg(A\wedge B)] \quad \dfrac{[A] \quad [B]}{A\wedge B}\wedge\mathrm{I}}{\bot}\to\mathrm{E}}{\neg A}\to\mathrm{I}}{\neg A\vee\neg B}\vee\mathrm{I}_r}{\bot}\to\mathrm{E}}{\neg B}\to\mathrm{I}}{\neg A\vee\neg B}\vee\mathrm{I}_l}{\bot}\to\mathrm{E}}{\neg A\vee\neg B}{\color{red}\bot_c}}{\neg(A\wedge B)\to\neg A\vee\neg B}\to\mathrm{I}
$$

RAA vs $\rightarrow$I

$\bot_c$: deriving A by deducing absurdity ($\bot$) from $\neg A$.

$$\cfrac{\begin{matrix}[\neg A] \\ \mathcal{D} \\ \bot\end{matrix}}{A}\ \bot_c$$

$\rightarrow$I: deriving $\neg A$ by deducing absurdity ($\bot$) from A.

$$\cfrac{\begin{matrix}[A] \\ \mathcal{D} \\ \bot\end{matrix}}{\neg A}\ \rightarrow\mathrm{I}$$

Notations

- $m, n, i, j, k, \ldots \in \mathbf{N}$
- $\alpha, \beta, \gamma, \delta, \ldots \in \mathbf{N}^{\mathbf{N}}$
  - $\mathbf{0} = \lambda n.0$
  - $\alpha \# \beta \Leftrightarrow \exists n(\alpha(n) \neq \beta(n))$

Omniscience principles

- The limited principle of omniscience (LPO, Σ^0_1-PEM):

$$\forall\alpha[\alpha \# \mathbf{0} \vee \neg\alpha \# \mathbf{0}]$$

- The weak limited principle of omniscience (WLPO, Π^0_1-PEM):

$$\forall\alpha[\neg\neg\alpha \# \mathbf{0} \vee \neg\alpha \# \mathbf{0}]$$

- The lesser limited principle of omniscience (LLPO, Σ^0_1-DML):

$$\forall\alpha\beta[\neg(\alpha \# \mathbf{0} \wedge \beta \# \mathbf{0}) \rightarrow \neg\alpha \# \mathbf{0} \vee \neg\beta \# \mathbf{0}]$$

Markov's principle

- Markov's principle (MP, Σ^0_1-DNE):

$$\forall\alpha[\neg\neg\alpha \# \mathbf{0} \to \alpha \# \mathbf{0}]$$

- Markov's principle for disjunction ($\mathrm{MP}^\vee$, Π^0_1-DML):

$$\forall\alpha\beta[\neg(\neg\alpha \# \mathbf{0} \wedge \neg\beta \# \mathbf{0}) \to \neg\neg\alpha \# \mathbf{0} \vee \neg\neg\beta \# \mathbf{0}]$$

- Weak Markov's principle (WMP):

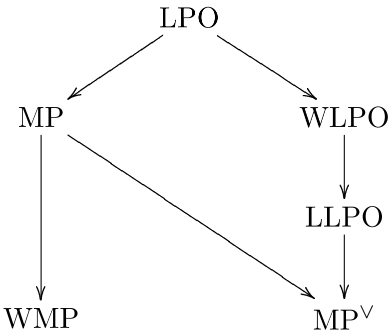
$$\forall\alpha[\forall\beta(\neg\neg\beta \# \mathbf{0} \vee \neg\neg\beta \# \alpha) \to \alpha \# \mathbf{0}]$$

Remark

We may assume without loss of generality that α (and β) are ranging over

- binary sequences,
- nondecreasing sequences,
- sequences with at most one nonzero term, or
- sequences with $\alpha(0) = 0$.

Relationship among principles



- $\mathrm{LPO} \Leftrightarrow \mathrm{WLPO} + \mathrm{MP}$
- $\mathrm{MP} \Leftrightarrow \mathrm{WMP} + \mathrm{MP}^{\vee}$

Remark

- MP (and hencce WMP and $\mathrm{MP}^{\vee}$) holds in constructive recuresive mathematics.
- WMP holds in intuitionism.

CZF and choice axioms

The materials in the lectures could be formalized in

the constructive Zermelo-Fraenkel set theory (**CZF**)

without the powerset axiom and the full separation axiom, together with the following choice axioms.

- The axiom of countable choice (AC_0):

$$\forall n \exists y \in Y A(n, y) \rightarrow \exists f \in Y^{\mathbf{N}} \forall n A(n, f(n))$$

- The axiom of dependent choice (DC):

$$\begin{aligned} &\forall x \in X \exists y \in X A(x, y) \rightarrow \\ &\qquad \forall x \in X \exists f \in X^{\mathbf{N}} [f(0) = x \wedge \forall n A(f(n), f(n+1))] \end{aligned}$$

Number systems

- The set **Z** of integers is the set **N** × **N** with the equality

$$(n, m) =_{\mathbf{Z}} (n', m') \Leftrightarrow n + m' = n' + m.$$

  The arithmetical relations and operations are defined on **Z** in a straightforwad way; natural numbers are embedded into **Z** by the mapping $n \mapsto (n, 0)$.

- The set **Q** of rationals is the set **Z** × **N** with the equality

$$(a, m) =_{\mathbf{Q}} (b, n) \Leftrightarrow a \cdot (n + 1) =_{\mathbf{Z}} b \cdot (m + 1).$$

  The arithmetical relations and operations are defined on **Q** in a straightforwad way; integers are embedded into **Q** by the mapping $a \mapsto (a, 0)$.

Real numbers

Definition

A real number is a sequence $(p_n)_n$ of rationals such that

$$\forall mn \left(|p_m - p_n| < 2^{-m} + 2^{-n} \right) .$$

We shall write $\mathbf{R}$ for the set of real numbers as usual.

Remark

Rationals are embedded into $\mathbf{R}$ by the mapping $p \mapsto p^* = \lambda n.p$.

Ordering relation

Definition

Let $<$ be the ordering relation between real numbers $x = (p_n)_n$ and $y = (q_n)_n$ defined by

$$x < y \Leftrightarrow \exists n \left(2^{-n+2} < q_n - p_n\right) .$$

Proposition

Let $x, y, z \in \mathbf{R}$. *Then*

- $\neg(x < y \wedge y < x)$,
- $x < y \rightarrow x < z \vee z < y$.

Ordering relation

Proof.

Let $x = (p_n)_n$, $y = (q_n)_n$ and $z = (r_n)_n$, and suppose that $x < y$. Then there exists n such that $2^{-n+2} < q_n - p_n$. Setting $N = n + 3$, either $(p_n + q_n)/2 < r_N$ or $r_N \leq (p_n + q_n)/2$. In the former case, we have

$$\begin{aligned} 2^{-N+2} &< 2^{-n+1} - (2^{-(n+3)} + 2^{-n}) < \frac{q_n - p_n}{2} - (p_N - p_n) \\ &= \frac{p_n + q_n}{2} - p_N < r_N - p_N, \end{aligned}$$

and hence $x < z$. In the latter case, we have

$$\begin{aligned} 2^{-N+2} &< -(2^{-(n+3)} + 2^{-n}) + 2^{-n+1} < (q_N - q_n) + \frac{q_n - p_n}{2} \\ &= q_N - \frac{p_n + q_n}{2} \leq q_N - r_N, \end{aligned}$$

and hence $z < y$. □

Apartness and equality

Definition

We define the apartness $\#$, the equality $=$, and the ordering relation $\leq$ between real numbers x and y by

- $x \# y \Leftrightarrow (x < y \vee y < x)$,
- $x = y \Leftrightarrow \neg(x \# y)$,
- $x \leq y \Leftrightarrow \neg(y < x)$.

Lemma

Let $x, y, z \in \mathbf{R}$. Then

- $x \# y \leftrightarrow y \# x$,
- $x \# y \rightarrow x \# z \vee z \# y$.

Apartness and equality

Proposition

Let $x, y, z \in \mathbf{R}$. Then

- $x = x$,
- $x = y \to y = x$,
- $x = y \land y = z \to x = z$.

Proposition

Let $x, x', y, y' \in \mathbf{R}$. Then

- $x = x' \land y = y' \land x < y \to x' < y'$,
- $\neg\neg(x < y \lor x = y \lor y < x)$,
- $x < y \land y < z \to x < z$.

Apartness and equality

Corollary

Let $x, x', y, y', z \in \mathbf{R}$. *Then*

- $x = x' \wedge y = y' \wedge x \# y \to x' \# y'$,
- $x = x' \wedge y = y' \wedge x \leq y \to x' \leq y'$,
- $x \leq y \leftrightarrow \neg\neg(x < y \vee x = y)$,
- $\neg\neg(x \leq y \vee y \leq x)$,
- $x \leq y \wedge y \leq x \to x = y$,
- $x < y \wedge y \leq z \to x < z$,
- $x \leq y \wedge y < z \to x < z$,
- $x \leq y \wedge y \leq z \to x \leq z$.

Apartness and equality

Proposition

$\forall xy \in \mathbf{R}(x \# y \vee x = y) \Leftrightarrow \mathrm{LPO}$,

Proof.

($\Leftarrow$): Let $x = (p_n)_n$ and $y = (q_n)_n$, and define a binary sequence α by

$$\alpha(n) = 1 \Leftrightarrow 2^{-n+2} < |q_n - p_n|.$$

Then $\alpha \# \mathbf{0} \leftrightarrow x \# y$, and hence $x \# y \vee x = y$, by LPO.
($\Rightarrow$): Let α be a binary sequence α with at most one nonzero term, and define a sequence $(p_n)_n$ of rationals by

$$p_n = \sum_{k=0}^{n} \alpha(k) \cdot 2^{-k}.$$

Then $x = (p_n)_n \in \mathbf{R}$, and $x \# 0 \leftrightarrow \alpha \# \mathbf{0}$. Therefore $\alpha \# \mathbf{0} \vee \neg\alpha \# \mathbf{0}$, by $x \# 0 \vee x = 0$. □

Apartness and equality

Proposition

- $\forall xy \in \mathbf{R}(\neg x = y \vee x = y) \Leftrightarrow \mathrm{WLPO}$,
- $\forall xy \in \mathbf{R}(x \leq y \vee y \leq x) \Leftrightarrow \mathrm{LLPO}$,
- $\forall xy \in \mathbf{R}(\neg x = y \to x \# y) \Leftrightarrow \mathrm{MP}$,
- $\forall xyz \in \mathbf{R}(\neg x = y \to \neg x = z \vee \neg z = y) \Leftrightarrow \mathrm{MP}^{\vee}$,
- $\forall xy \in \mathbf{R}(\forall z \in \mathbf{R}(\neg x = z \vee \neg z = y) \to x \# y) \Leftrightarrow \mathrm{WMP}$.

Arithmetical operations

The arithmetical operations are defined on $\mathbf{R}$ in a straightforwad way.

For $x = (p_n), y = (q_n) \in \mathbf{R}$, define

- $x + y = (p_{n+1} + q_{n+1})$;
- $-x = (-p_n)$;
- $|x| = (|p_n|)$;
- $\max\{x, y\} = (\max\{p_n, q_n\})$;
- $\vdots$

Cauchy completeness

Definition

A sequence (x_n) of real numbers converges to $x \in \mathbf{R}$ if

$$\forall k \exists N_k \forall n \geq N_k [|x_n - x| < 2^{-k}].$$

Definition

A sequence (x_n) of real numbers is a Cauchy sequence if

$$\forall k \exists N_k \forall mn \geq N_k [|x_m - x_n| < 2^{-k}].$$

Theorem

A sequence of real numbers converges if and only if it is a Cauchy sequence.

Classical order completeness

Theorem

If S is an inhabited subset of $\mathbf{R}$ with an upper bound, then $\sup S$ exists.

Proposition

If every inhabited subset S of $\mathbf{R}$ with an upper bound has a supremum, then WLPO holds.

Proof.

Let α be a binary sequence. Then $S = \{\alpha(n) \mid n \in \mathbf{N}\}$ is an inhabited subset of $\mathbf{R}$ with an upper bound 2. If $\sup S$ exists, then either $0 < \sup S$ or $\sup S < 1$; in the former case, we have $\neg\neg\alpha \# \mathbf{0}$; in the latter case, we have $\neg\alpha \# \mathbf{0}$. □

Constructive order completeness

Theorem

Let S be an inhabited subset of $\mathbf{R}$ with an upper bound. If either $\exists s \in S(a < s)$ or $\forall s \in S(s < b)$ for each $a, b \in \mathbf{R}$ with $a < b$, then $\sup S$ exists.

Proof.

Let $s_0 \in S$ and u_0 be an upper bound of S with $s_0 < u_0$. Define sequences (s_n) and (u_n) of real numbers by

$$\begin{array}{ll} s_{n+1} = (2s_n + u_n)/3, u_{n+1} = u_n & \text{if } \exists s \in S[(2s_n + u_n)/3 < s]; \\ s_{n+1} = s_n, u_{n+1} = (s_n + 2u_n)/3 & \text{if } \forall s \in S[s < (s_n + 2u_n)/3]. \end{array}$$

Note that $s_n < u_n$, $\exists s \in S(s_n \leq s)$ and $\forall s \in S(s \leq u_n)$ for each n. Then (s_n) and (u_n) converge to the same limit which is a supremum of S. □

Constructive order completeness

Definition

A set S of real numbers is totally bounded if for each k there exist $s_0, \ldots, s_{n-1} \in S$ such that

$$\forall y \in S \exists m < n[|s_m - y| < 2^{-k}].$$

Constructive order completeness

Proposition

An inhabited totally bounded set S of real numbers has a supremum.

Proof.

Let $a, b \in \mathbf{R}$ with $a < b$, and let k be such that $2^{-k} < (b-a)/2$. Then there exists $s_0, \dots, s_{n-1} \in S$ such that

$$\forall y \in S \exists m < n[|s_m - y| < 2^{-k}].$$

Either $a < \max\{s_m \mid m < n\}$ or $\max\{s_m \mid m < n\} < (a+b)/2$. In the former case, there exists $s \in S$ such that $a < s$. In the latter case, for each $s \in S$ there exists m such that $|s - s_m| < 2^{-k}$, and hence

$$s < s_m + |s - s_m| < (a+b)/2 + (b-a)/2 = b.$$

□

Classical intermediate value theorem

Definition

A function f from $[0,1]$ into $\mathbf{R}$ is uniformly continuous if

$$\forall k \exists M_k \forall xy \in [0,1][|x-y| < 2^{-M_k} \rightarrow |f(x) - f(y)| < 2^{-k}].$$

Theorem

If f is a uniformly continuous function from $[0,1]$ into $\mathbf{R}$ with $f(0) \leq 0 \leq f(1)$, then there exists $x \in [0,1]$ such that $f(x) = 0$.

Classical intermediate value theorem

Proposition

The classical intermediate value theorem implies LLPO*.*

Proof.

Let $a \in \mathbf{R}$, and define a function f from $[0,1]$ into $\mathbf{R}$ by

$$f(x) = \min\{3(1+a)x - 1, 0\} + \max\{0, 3(1-a)x + (3a-2)\}.$$

Then f is uniformly continuous, and $f(0) = -1$ and $f(1) = 1$. If there exists $x \in [0,1]$ such that $f(x) = 0$, then either $1/3 < x$ or $x < 2/3$; in the former case, we have $a \leq 0$; in the latter case, we have $0 \leq a$. □

Constructive intermediate value theorem

Theorem

If f is a uniformly continuous function from $[0,1]$ into $\mathbf{R}$ with $f(0) \leq 0 \leq f(1)$, then for each k there exists $x \in [0,1]$ such that $|f(x)| < 2^{-k}$.

Constructive intermediate value theorem

Proof.

For given a k, let $l_0 = 0$ and $r_0 = 1$, and define sequences (l_n) and (r_n) by

$$\begin{array}{ll} l_{n+1} = (l_n + r_n)/2, r_{n+1} = r_n & \text{if } f((l_n + r_n)/2) < 0, \\ l_{n+1} = l_n, r_{n+1} = (l_n + r_n)/2 & \text{if } 0 < f((l_n + r_n)/2), \\ l_{n+1} = (l_n + r_n)/2, r_{n+1} = (l_n + r_n)/2 & \text{if } |f((l_n + r_n)/2)| < 2^{-(k+1)}. \end{array}$$

Note that $f(l_n) < 2^{-(k+1)}$ and $-2^{-(k+1)} < f(r_n)$ for each n. Then (l_n) and (r_n) converge to the same limit $x \in [0, 1]$. Either $2^{-(k+1)} < |f(x)|$ or $|f(x)| < 2^{-k}$. In the former case, if $2^{-(k+1)} < f(x)$, then $2^{-(k+1)} < f(l_n) < 2^{-(k+1)}$ for some n, a contradiction; if $f(x) < -2^{-(k+1)}$, then $-2^{-(k+1)} < f(r_n) < -2^{-(k+1)}$ for some n, a contradiction. Therefore the latter must be the case. □

References

- Peter Aczel and Michael Rathjen, *CST Book draft*, 2010, http://www1.maths.leeds.ac.uk/~rathjen/book.pdf.
- Errett Bishop, *Foundations of Constructive Analysis*, McGraw-Hill, New York, 1967.
- Errett Bishop and Douglas Bridges, *Constructive Analysis*, Springer-Verlag, Berlin, 1985.
- Douglas Bridges and Fred Richman, *Varieties of Constructive Mathematics*, Cambridge Univ. Press, London, 1987.
- Douglas Bridges and Luminiţa Vîţă, *Techniques of Constructive Analysis*, Springer, New York, 2006.
- D. van Dalen, *Logic and Structure*, 5th ed., Springer, London, 2013.
- A.S. Troelstra and D. van Dalen, *Constructivism in Mathematics, An Introduction*, Vol. I, North-Holland, Amsterdam, 1988.