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
The BHK interpretation
Natural deduction
Omniscience principles
Number systems
Real numbers
Ordering relation
Apartness and equality
Arithmetical operations
Cauchy competeness
Order completeness
The intermediate value theorem
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)
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

- **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 $\land, \lor, \rightarrow, \bot, \forall, \exists$.

We introduce the abbreviations

- $\neg A \equiv A \rightarrow \bot$;
- $A \leftrightarrow B \equiv (A \rightarrow B) \land (B \rightarrow A)$.
The BHK interpretation

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

- A proof of $A \land B$ is given by presenting a proof of $A$ and a proof of $B$.
- A proof of $A \lor B$ 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 $\bot$ 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 $A(t)$.
We shall use $\mathcal{D}$, possibly with a subscript, for arbitrary deduction. We write

$$\Gamma \vdash \mathcal{D}$$

$$\vdash \ A$$

to indicate that $\mathcal{D}$ is deduction with conclusion $A$ and assumptions $\Gamma$. 
For each formula $A$,

$A$

is a deduction with conclusion $A$ and assumptions \{A\}. 
Deduction (Induction step, →I)

If

\[
\begin{array}{c}
\Gamma \\
\mathcal{D} \\
B
\end{array}
\]

is a deduction, then

\[
\begin{array}{c}
\Gamma \\
\mathcal{D} \\
B
\end{array}
\]

\[B\]

\[
\frac{A \rightarrow B}{A \rightarrow B} \rightarrow I
\]

is a deduction with conclusion \(A \rightarrow B\) and assumptions \(\Gamma \setminus \{A\}\). We write

\[
\begin{array}{c}
[A] \\
\mathcal{D} \\
B
\end{array}
\]

\[B\]

\[
\frac{A \rightarrow B}{A \rightarrow B} \rightarrow I
\]
Deduction (Induction step, $\rightarrow E$)

If

\[
\begin{array}{c}
\Gamma_1 \\
D_1 \\
A \rightarrow B \\
\end{array}
\quad
\begin{array}{c}
\Gamma_2 \\
D_2 \\
A \\
\end{array}
\]

are deductions, then

\[
\begin{array}{c}
\Gamma_1 \\
D_1 \\
A \rightarrow B \\
\end{array}
\quad
\begin{array}{c}
\Gamma_2 \\
D_2 \\
A \\
\end{array}
\]

\[
\begin{array}{c}
B \\
E \\
\end{array}
\]

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

\[
\begin{align*}
\neg B & \quad \frac{[A \rightarrow B]}{B} \quad \frac{[A]}{\rightarrow E} \\
\neg (A \rightarrow B) & \quad \frac{\bot}{\rightarrow I} \quad \frac{\neg (A \rightarrow B)}{\rightarrow E} \\
A \rightarrow B & \quad \frac{\bot}{\rightarrow I} \quad \frac{\neg A}{\rightarrow E}
\end{align*}
\]
Minimal logic

\[
\begin{align*}
&\frac{\mathcal{D}}{B} \quad \frac{\mathcal{D}_2}{A \rightarrow B} \quad \rightarrow I \\
&\frac{\mathcal{D}_1}{A} \quad \frac{\mathcal{D}_2}{B} \quad \wedge I \\
&\frac{\mathcal{D}}{A} \quad \frac{\mathcal{D}_2}{A \wedge B} \quad \vee I_r \\
&\frac{\mathcal{D}_1}{A \vee B} \quad \frac{\mathcal{D}_2}{A \vee B} \quad \vee I_l
\end{align*}
\]

\[
\begin{align*}
&\frac{\mathcal{D}_1}{A \rightarrow B} \quad \frac{\mathcal{D}_2}{A} \quad \rightarrow E \\
&\frac{\mathcal{D}}{A \wedge B} \quad \wedge E_r \\
&\frac{\mathcal{D}}{A \wedge B} \quad \wedge E_l \\
&\frac{\mathcal{D}_1}{A \vee B} \quad \frac{\mathcal{D}_2}{C} \quad \frac{\mathcal{D}_3}{C} \quad \vee E
\end{align*}
\]
Minimal logic

\[
\begin{align*}
\frac{D}{A} & \quad \forall yA[x/y] \quad \forall I \\
\frac{\forall xA}{A[x/t]} & \quad \forall E \\
\frac{\exists xA}{A[x/t]} & \quad \exists I \\
\frac{\exists yA[x/y]}{D_2 \quad C} & \quad \exists E
\end{align*}
\]

- In \( \forall E \) and \( \exists I \), \( t \) must be free for \( x \) in \( A \).
- In \( \forall I \), \( D \) must not contain assumptions containing \( x \) free, and \( y \equiv x \) or \( y \not\in \text{FV}(A) \).
- In \( \exists E \), \( D_2 \) must not contain assumptions containing \( x \) free except \( A \), \( x \not\in \text{FV}(C) \), and \( y \equiv x \) or \( y \not\in \text{FV}(A) \).
Example

\[
\begin{align*}
((A \rightarrow B) \land (A \rightarrow C)) &\quad \land E_r \quad [A] \\
A \rightarrow B &\rightarrow E \quad B \\
B &\rightarrow E \\
B \land C &\quad \land I \quad C \\
A \rightarrow B \land C &\rightarrow I \\
(A \rightarrow B) \land (A \rightarrow C) \rightarrow (A \rightarrow B \land C) &\rightarrow I
\end{align*}
\]
Example

\[
\begin{align*}
[(A \to C) \land (B \to C)] & \\
\frac{A \to C}{A \lor B} & \\
\frac{C}{\frac{[(A \to C) \land (B \to C)]}{\rightarrow \text{E}}} & \\
\frac{[(A \to C) \land (B \to C)]}{\frac{B \to C}{\rightarrow \text{E}}} & \\
\frac{C}{\frac{\rightarrow \text{E}}{\lor \text{E}}} & \\
\frac{A \lor B \to C}{(A \to C) \land (B \to C) \rightarrow (A \lor B \rightarrow C)} & \\
\end{align*}
\]
Example

\[ \frac{[A \rightarrow \forall x B]}{\forall x B} \frac{[A]}{\forall E} \frac{\frac{B}{A \rightarrow B}}{\rightarrow I} \frac{\frac{\forall x (A \rightarrow B)}{\forall I}}{(A \rightarrow \forall x B) \rightarrow \forall x (A \rightarrow B)} \rightarrow I \]

where \( x \notin \text{FV}(A) \).
Example

\[
\begin{align*}
\exists x (A \rightarrow B) \quad &\quad [A 
\quad \rightarrow E \\
\exists x B \quad &\quad \exists E \\
A \rightarrow \exists x B \quad &\quad \rightarrow I \\
\exists x (A \rightarrow B) \rightarrow (A \rightarrow \exists x B) \quad &\quad \rightarrow I
\end{align*}
\]

where \( x \notin FV(A) \).
Intuitionistic logic is obtained from minimal logic by adding the intuitionistic absurdity rule (ex falso quodlibet).

If

$$\Gamma \quad \mathcal{D} \quad \bot$$

is a deduction, then

$$\Gamma \quad \mathcal{D} \quad \bot \quad \bot_i$$

is a deduction with conclusion $A$ and assumptions $\Gamma$. 
Example

\[
\frac{[\neg A]}{
\begin{array}{c}
\frac{[A]}{\perp} \\
\frac{[\neg (A \rightarrow B)]}{A \rightarrow B} \rightarrow I \\
\frac{\neg A}{\neg B} \rightarrow E
\end{array}
}{\rightarrow E}
\]

\[
\frac{[\neg (A \rightarrow B)]}{A \rightarrow B} \rightarrow I
\]

\[
\frac{[\neg B]}{\neg B} \rightarrow I
\]

\[
\frac{[\neg (A \rightarrow B)]}{A \rightarrow B} \rightarrow I
\]

\[
\frac{[\neg (A \rightarrow B)]}{A \rightarrow B} \rightarrow E
\]

\[
\frac{[\neg (A \rightarrow B)]}{A \rightarrow B} \rightarrow I
\]

\[
\frac{\neg (A \rightarrow B)}{(\neg A \rightarrow \neg B) \rightarrow \neg (A \rightarrow B)} \rightarrow I
\]
Example

\[
\begin{align*}
&\quad [\neg A] \quad [A] \quad \rightarrow \mathsf{E} \\
&\quad [A \lor B] \quad \bot \quad \bot \mathsf{i} \\
&\quad B \quad \mathsf{i} \\
&\quad \neg A \rightarrow B \quad \rightarrow \mathsf{I} \\
&\quad A \lor B \rightarrow (\neg A \rightarrow B) \quad \rightarrow \mathsf{I}
\end{align*}
\]
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

\[
\begin{array}{c}
\Gamma \\
\mathcal{D} \\
\bot \\
\bot_c
\end{array}
\]

is a deduction with conclusion \( A \) and assumption \( \Gamma \setminus \{\neg A\} \).
Example (classical logic)

The double negation elimination (DNE):

\[
\frac{[\neg\neg A] \quad [\neg A]}{\bot} \quad \text{\rightarrow E}
\]

\[
\frac{\bot}{A} \quad \bot_c
\]

\[
\frac{A}{\neg\neg A \rightarrow A} \quad \text{\rightarrow I}
\]
The principle of excluded middle (**PEM**):

\[
\frac{\neg(A \lor \neg A)}{A \lor \neg A} \quad \frac{[A]}{\neg I_r \rightarrow E}
\]

\[
\frac{\bot}{\neg A} \quad \frac{\neg I}{\rightarrow I} \quad \frac{A \lor \neg A}{A \lor \neg A} \quad \frac{\bot}{\rightarrow E}
\]

\[
\frac{\bot}{A \lor \neg A} \quad \frac{\bot}{\bot_c}
\]
De Morgan’s law (DML):

\[
\neg(A \land B) \quad \frac{[A], [B]}{A \land B} \quad \wedge I
\]

\[
\neg(A \lor \neg B) \quad \frac{[\neg A], [\neg B]}{A \lor \neg B} \quad \lor I_r
\]

\[
\neg(A \lor \neg B) \quad \frac{[\neg B]}{A \lor \neg B} \quad \lor I_l
\]

\[
\frac{[\neg(A \land B)]}{\neg(A \lor \neg B)} \quad \frac{[\neg(A \lor \neg B)]}{\neg(A \land B)} \quad \neg c
\]

\[
\neg(A \land B) \rightarrow \neg A \lor \neg B \quad \rightarrow I
\]
RAA vs →I

⊥_c: deriving A by deducing absurdity (⊥) from ¬A.

\[
\begin{array}{c}
[\neg A] \\
D \\
\bot \\
A \\
\bot_c
\end{array}
\]

→I: deriving ¬A by deducing absurdity (⊥) from A.

\[
\begin{array}{c}
[A] \\
D \\
\bot \\
\neg A \\
\rightarrow I
\end{array}
\]
Notations

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

- The limited principle of omniscience (LPO, $\Sigma_1^0$-PEM):
  \[ \forall \alpha [\alpha \neq 0 \lor \neg \alpha \neq 0] \]

- The weak limited principle of omniscience (WLPO, $\Pi_1^0$-PEM):
  \[ \forall \alpha [\neg \neg \alpha \neq 0 \lor \neg \alpha \neq 0] \]

- The lesser limited principle of omniscience (LLPO, $\Sigma_1^0$-DML):
  \[ \forall \alpha \beta [\neg (\alpha \neq 0 \land \beta \neq 0) \rightarrow \neg \alpha \neq 0 \lor \neg \beta \neq 0] \]
Markov’s principle

- Markov’s principle ($\textbf{MP}$, $\Sigma^0_1$-DNE):
  \[ \forall \alpha [\neg \neg \alpha \not\equiv 0 \rightarrow \alpha \not\equiv 0] \]

- Markov’s principle for disjunction ($\textbf{MP^\lor}$, $\Pi^0_1$-DML):
  \[ \forall \alpha \beta [\neg (\neg \alpha \not\equiv 0 \land \neg \beta \not\equiv 0) \rightarrow \neg \neg \alpha \not\equiv 0 \lor \neg \neg \beta \not\equiv 0] \]

- Weak Markov’s principle ($\textbf{WMP}$):
  \[ \forall \alpha [\forall \beta(\neg \neg \beta \not\equiv 0 \lor \neg \neg \beta \not\equiv \alpha) \rightarrow \alpha \not\equiv 0] \]
Remark

We may assume without loss of generality that $\alpha$ (and $\beta$) are ranging over

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

- $LPO \iff WLPO + MP$
- $MP \iff WMP + MP^\vee$
Remark

- MP (and hence WMP and $\text{MP}^\vee$) holds in constructive recursive 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 ($\text{AC}_0$):

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

- The axiom of dependent choice ($\text{DC}$):

$$\forall x \in X \exists y \in XA(x, y) \rightarrow$$

$$\forall x \in X \exists f \in X^N [f(0) = x \land \forall n A(f(n), f(n + 1))]$$
Number systems

The set $\mathbb{Z}$ of integers is the set $\mathbb{N} \times \mathbb{N}$ with the equality

$$(n, m) =_{\mathbb{Z}} (n', m') \iff n + m' = n' + m.$$  

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

The set $\mathbb{Q}$ of rationals is the set $\mathbb{Z} \times \mathbb{N}$ with the equality

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

The arithmetical relations and operations are defined on $\mathbb{Q}$ in a straightforward way; integers are embedded into $\mathbb{Q}$ by the mapping $a \mapsto (a, 0)$. 
Definition
A real number is a sequence \((p_n)_n\) of rationals such that

\[
\forall mn (|p_m - p_n| < 2^{-m} + 2^{-n}) .
\]

We shall write \(\mathbb{R}\) for the set of real numbers as usual.

Remark
Rationals are embedded into \(\mathbb{R}\) 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

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

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

- $\neg (x < y \land y < x)$,
- $x < y \rightarrow x < z \lor z < y$. 
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

\[
2^{-N+2} < 2^{-n+1} - (2^{-(n+3)} + 2^{-n}) < \frac{q_n - p_n}{2} - (p_N - p_n)
\]

\[
= \frac{p_n + q_n}{2} - p_n < r_N - p_N,
\]

and hence \( x < z \). In the latter case, we have

\[
2^{-N+2} < -(2^{-(n+3)} + 2^{-n}) + 2^{-n+1} < (q_N - q_n) + \frac{q_n - p_n}{2}
\]

\[
= q_N - \frac{p_n + q_n}{2} \leq q_N - r_N,
\]

and hence \( z < y \). \( \square \)
Apartness and equality

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

- $x \# y \iff (x < y \lor y < x)$,
- $x = y \iff \neg(x \# y)$,
- $x \leq y \iff \neg(y < x)$.

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

- $x \# y \iff y \# x$,
- $x \# y \rightarrow x \# z \lor z \# y$. 

Apartness and equality

Proposition

Let \( x, y, z \in \mathbb{R} \). Then

\[ ▶ \ x = x, \]
\[ ▶ \ x = y \rightarrow y = x, \]
\[ ▶ \ x = y \wedge y = z \rightarrow x = z. \]

Proposition

Let \( x, x', y, y' \in \mathbb{R} \). Then

\[ ▶ \ x = x' \wedge y = y' \wedge x < y \rightarrow x' < y', \]
\[ ▶ \neg \neg (x < y \vee x = y \vee y < x), \]
\[ ▶ \ x < y \wedge y < z \rightarrow x < z. \]
Apartness and equality

Corollary

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

- $x = x' \land y = y' \land x \neq y \rightarrow x' \neq y'$,
- $x = x' \land y = y' \land x \leq y \rightarrow x' \leq y'$,
- $x \leq y \leftrightarrow \neg \neg(x < y \lor x = y)$,
- $\neg \neg(x \leq y \lor y \leq x)$,
- $x \leq y \land y \leq x \rightarrow x = y$,
- $x < y \land y \leq z \rightarrow x < z$,
- $x \leq y \land y < z \rightarrow x < z$,
- $x \leq y \land y \leq z \rightarrow x \leq z$. 
Apartness and equality

Proposition
\[ \forall xy \in \mathbb{R} (x \neq y \lor x = y) \iff \text{LPO}, \]

Proof.
\((\Leftarrow)\): Let \( x = (p_n)_n \) and \( y = (q_n)_n \), and define a binary sequence \( \alpha \) by
\[ \alpha(n) = 1 \iff 2^{-n+2} < |q_n - p_n|. \]

Then \( \alpha \neq 0 \iff x \neq y \), and hence \( x \neq y \lor x = y \), by LPO.

\((\Rightarrow)\): Let \( \alpha \) be a binary sequence \( \alpha \) 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 \( x = (p_n)_n \in \mathbb{R} \), and \( x \neq 0 \iff \alpha \neq 0 \). Therefore \( \alpha \neq 0 \lor \neg \alpha \neq 0 \), by \( x \neq 0 \lor x = 0 \).
Apartness and equality

Proposition

- \( \forall xy \in \mathbb{R}(\neg x = y \lor x = y) \iff \text{WLPO}, \)
- \( \forall xy \in \mathbb{R}(x \leq y \lor y \leq x) \iff \text{LLPO}, \)
- \( \forall xy \in \mathbb{R}(\neg x = y \rightarrow x \# y) \iff \text{MP}, \)
- \( \forall xyz \in \mathbb{R}(\neg x = y \rightarrow \neg x = z \lor \neg z = y) \iff \text{MP}^\lor, \)
- \( \forall xy \in \mathbb{R}(\forall z \in \mathbb{R}(\neg x = z \lor \neg z = y) \rightarrow x \# y) \iff \text{WMP}. \)
Arithmetical operations

The arithmetical operations are defined on $\mathbb{R}$ in a straightforward way.

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

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

**Definition**
A sequence \((x_n)\) of real numbers converges to \(x \in \mathbb{R}\) if

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

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

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

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

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

Proposition

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

Proof.

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

**Theorem**

Let $S$ be an inhabited subset of $\mathbb{R}$ with an upper bound. If either

$\exists s \in S (a < s)$ or $\forall s \in S (s < b)$ for each $a, b \in \mathbb{R}$ 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

$$
s_{n+1} = \frac{(2s_n + u_n)}{3}, \quad u_{n+1} = u_n \quad \text{if } \exists s \in S \left(\frac{(2s_n + u_n)}{3} < s\right);
$$

$$
s_{n+1} = s_n, \quad u_{n+1} = \frac{(s_n + 2u_n)}{3} \quad \text{if } \forall s \in S \left[s < \frac{(s_n + 2u_n)}{3}\right].
$$

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 $S$. \qed
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 $a, b \in \mathbb{R}$ with $a < b$, and let $k$ be such that $2^{-k} < (b - a)/2$. Then there exists $s_0, \ldots, s_{n-1} \in S$ 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 \( \mathbb{R} \) is uniformly continuous if

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

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

The classical intermediate value theorem implies LLPO.

Proof.
Let \( a \in \mathbb{R} \), and define a function \( f \) from \([0, 1]\) into \( \mathbb{R} \) 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 \( 0 \leq a \). \( \square \)
Constructive intermediate value theorem

Theorem

If $f$ is a uniformly continuous function from $[0, 1]$ into $\mathbb{R}$ 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

\[
\begin{align*}
l_{n+1} &= (l_n + r_n)/2, \quad r_{n+1} = r_n & \quad \text{if } f((l_n + r_n)/2) < 0, \\
l_{n+1} &= l_n, \quad r_{n+1} = (l_n + r_n)/2 & \quad \text{if } 0 < f((l_n + r_n)/2), \\
l_{n+1} &= (l_n + r_n)/2, \quad r_{n+1} = (l_n + r_n)/2 & \quad \text{if } |f((l_n + r_n)/2)| < 2^{-(k+1)}.
\end{align*}
\]

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. \qed
References


