Constructive Analysis in Nuprl

Mark Bickford

Cornell University, Computer Science

September 29, 2017

Lecture 2

- Theorems derivable from continuity

Lecture 2

- Theorems derivable from continuity
  - Weak Markov Principle

Lecture 2

- Theorems derivable from continuity
  - Weak Markov Principle
  - Other derived continuity principles

Lecture 2

- Theorems derivable from continuity
    - Weak Markov Principle
    - Other derived continuity principles
    - Connectedness of $\mathbb{R}$

CONT :

$$\forall F:\mathbb{S} \to \mathbb{N}.\ \forall f:\mathbb{S}.\ \downharpoonleft \exists k:\mathbb{N}.\ \forall g:\mathbb{S}.\ (g = f \in \mathbb{S}_k) \Rightarrow F(g) = F(f)$$

CONT :

$$\forall F:\mathbb{S} \to \mathbb{N}.\ \forall f:\mathbb{S}.\ \downarrow \exists k:\mathbb{N}.\ \forall g:\mathbb{S}.\ (g = f \in \mathbb{S}_k) \Rightarrow F(g) = F(f)$$

What can we prove with this?

CONT :

$$\forall F{:}\mathbb{S} \to \mathbb{N}.\ \forall f{:}\mathbb{S}.\ \downharpoonleft \exists k{:}\mathbb{N}.\ \forall g{:}\mathbb{S}.\ (g = f \in \mathbb{S}_k) \Rightarrow F(g) = F(f)$$

What can we prove with this?
How do we deal with the $\downharpoonleft \exists k{:}\mathbb{N}$?

Product (Σ) type, Set type, Squash type

Product (Σ) type, Set type, Squash type

- Dependent product type $a : A \times B[a]$.

Product (Σ) type, Set type, Squash type

- Dependent product type $a{:}A \times B[a]$.
- $p = q \in a{:}A \times B[a]$ iff $p \mapsto \langle a_1, b_1 \rangle$ and $q \mapsto \langle a_2, b_2 \rangle$ and $a_1 = a_2 \in A$ and $b_1 = b_2 \in B[a_1]$.

Product (Σ) type, Set type, Squash type

- Dependent product type $a{:}A \times B[a]$.
- $p = q \in a{:}A \times B[a]$ iff $p \mapsto \langle a_1, b_1 \rangle$ and $q \mapsto \langle a_2, b_2 \rangle$ and $a_1 = a_2 \in A$ and $b_1 = b_2 \in B[a_1]$.
- Set type (aka refinement type) $\{a{:}A \mid B[a]\}$

Product (Σ) type, Set type, Squash type

- Dependent product type $a{:}A \times B[a]$.
- $p = q \in a{:}A \times B[a]$ iff $p \mapsto \langle a_1, b_1 \rangle$ and $q \mapsto \langle a_2, b_2 \rangle$ and $a_1 = a_2 \in A$ and $b_1 = b_2 \in B[a_1]$.
- Set type (aka refinement type) $\{a{:}A \mid B[a]\}$
- $a \in \{a{:}A \mid B[a]\}$ iff $a = \text{fst}(p)$ for some $p \in a{:}A \times B[a]$

Product (Σ) type, Set type, Squash type

- Dependent product type $a{:}A \times B[a]$.
- $p = q \in a{:}A \times B[a]$ iff $p \mapsto \langle a_1, b_1 \rangle$ and $q \mapsto \langle a_2, b_2 \rangle$ and $a_1 = a_2 \in A$ and $b_1 = b_2 \in B[a_1]$.
- Set type (aka refinement type) $\{a{:}A \mid B[a]\}$
- $a \in \{a{:}A \mid B[a]\}$ iff $a = \mathrm{fst}(p)$ for some $p \in a{:}A \times B[a]$
- Squash type $\downarrow T = \{x{:}\mathrm{Unit} \mid T\}$

Product (Σ) type, Set type, Squash type

- Dependent product type $a{:}A \times B[a]$.
- $p = q \in a{:}A \times B[a]$ iff $p \mapsto \langle a_1, b_1 \rangle$ and $q \mapsto \langle a_2, b_2 \rangle$ and $a_1 = a_2 \in A$ and $b_1 = b_2 \in B[a_1]$.
- Set type (aka refinement type) $\{a{:}A \mid B[a]\}$
- $a \in \{a{:}A \mid B[a]\}$ iff $a = \mathrm{fst}(p)$ for some $p \in a{:}A \times B[a]$
- Squash type $\downarrow T = \{x{:}\mathrm{Unit} \mid T\}$
- $T \Rightarrow (\downharpoonleft T) \Rightarrow (\downarrow T) \Rightarrow \neg\neg T$

Stable and Squash Stable Propositions

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$
- Markov's Principle (MP) says that for decidable $P(n)$, $\exists n\!:\!\mathbb{N}.\ P(n)$ is stable.

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$
- Markov's Principle (MP) says that for decidable $P(n)$, $\exists n\!:\!\mathbb{N}.\ P(n)$ is stable.
- Nuprl does not prove MP, but is consistent with MP.

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$
- Markov's Principle (MP) says that for decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is stable.
- Nuprl does not prove MP, but is consistent with MP.
- P is *squash stable* if $\downarrow P \Rightarrow P$

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$
- Markov's Principle (MP) says that for decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is stable.
- Nuprl does not prove MP, but is consistent with MP.
- P is *squash stable* if $\downarrow P \Rightarrow P$
- Any proposition expressed using only $\forall$, $\Rightarrow$, $\wedge$, $=$, or decidable things like $<$, $\leq$, is squash stable.

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$
- Markov's Principle (MP) says that for decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is stable.
- Nuprl does not prove MP, but is consistent with MP.
- P is *squash stable* if $\downarrow P \Rightarrow P$
- Any proposition expressed using only $\forall$, $\Rightarrow$, $\wedge$, $=$, or decidable things like $<$, $\leq$, is squash stable.
- For decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is squash stable, because if $\downarrow\exists n{:}\mathbb{N}.\ P(n)$ then $\mu n.\ P(n) \in \exists n{:}\mathbb{N}.\ P(n)$.

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$
- Markov's Principle (MP) says that for decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is stable.
- Nuprl does not prove MP, but is consistent with MP.
- P is *squash stable* if $\downarrow P \Rightarrow P$
- Any proposition expressed using only $\forall$, $\Rightarrow$, $\wedge$, $=$, or decidable things like $<$, $\leq$, is squash stable.
- For decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is squash stable, because if $\downarrow\exists n{:}\mathbb{N}.\ P(n)$ then $\mu n.\ P(n) \in \exists n{:}\mathbb{N}.\ P(n)$.
- If $P \Rightarrow Q$ then $\downarrow P \Rightarrow\downarrow Q$, so if Q is squash stable, $\downarrow P \Rightarrow Q$.

Stable and Squash Stable Propositions

- P is *stable* if $\neg\neg P \Rightarrow P$
- Markov's Principle (MP) says that for decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is stable.
- Nuprl does not prove MP, but is consistent with MP.
- P is *squash stable* if $\downarrow P \Rightarrow P$
- Any proposition expressed using only $\forall$, $\Rightarrow$, $\wedge$, $=$, or decidable things like $<$, $\leq$, is squash stable.
- For decidable $P(n)$, $\exists n{:}\mathbb{N}.\ P(n)$ is squash stable, because if $\downarrow\exists n{:}\mathbb{N}.\ P(n)$ then $\mu n.\ P(n) \in \exists n{:}\mathbb{N}.\ P(n)$.
- If $P \Rightarrow Q$ then $\downarrow P \Rightarrow \downarrow Q$, so if Q is squash stable, $\downarrow P \Rightarrow Q$.
- So we can use CONT to at least prove things that are squash stable.

Weak Markov's Principle

Theorem

(Weak Markov's Principle) For all $a, b \in \mathbb{S}$

$$(\forall c:\mathbb{S}.\ \neg(a = c) \vee \neg(b = c)) \Rightarrow \exists n:\mathbb{N}.\ \neg(a(n) = b(n))$$

Weak Markov's Principle

Theorem

(Weak Markov's Principle) For all $a, b \in \mathbb{S}$

$$(\forall c\!:\!\mathbb{S}.\ \neg(a = c) \lor \neg(b = c)) \Rightarrow \exists n\!:\!\mathbb{N}.\ \neg(a(n) = b(n))$$

Proof.

From the hypothesis we get a functional $F\!:\!\mathbb{S} \to \mathbb{N}$ such that $F(c) = 0 \Rightarrow \neg(a = c)$ and $F(c) > 0 \Rightarrow \neg(b = c)$. Since $b = b$, we must have $F(b) = 0$, and similarly $F(a) > 0$.

Weak Markov's Principle

Theorem

(Weak Markov's Principle) For all $a, b \in \mathbb{S}$

$$(\forall c\!:\!\mathbb{S}.\ \neg(a = c) \vee \neg(b = c)) \Rightarrow \exists n\!:\!\mathbb{N}.\ \neg(a(n) = b(n))$$

Proof.

From the hypothesis we get a functional $F\!:\!\mathbb{S} \rightarrow \mathbb{N}$ such that $F(c) = 0 \Rightarrow \neg(a = c)$ and $F(c) > 0 \Rightarrow \neg(b = c)$. Since $b = b$, we must have $F(b) = 0$, and similarly $F(a) > 0$. Using CONT for this F and with $f = b$, we have

$$\downarrow\exists k\!:\!\mathbb{N}.\ \forall g\!:\!\mathbb{S}.\ (g = b \in \mathbb{S}_k) \Rightarrow F(g) = 0$$

What we are proving is squash stable, so we may assume that we have a k for which $\forall g\!:\!\mathbb{S}.\ (g = b \in \mathbb{S}_k) \Rightarrow F(g) = 0$.

Weak Markov's Principle

Theorem

(Weak Markov's Principle) For all $a, b \in \mathbb{S}$

$$(\forall c{:}\mathbb{S}.\ \neg(a = c) \vee \neg(b = c)) \Rightarrow \exists n{:}\mathbb{N}.\ \neg(a(n) = b(n))$$

Proof.

From the hypothesis we get a functional $F{:}\mathbb{S} \to \mathbb{N}$ such that $F(c) = 0 \Rightarrow \neg(a = c)$ and $F(c) > 0 \Rightarrow \neg(b = c)$. Since $b = b$, we must have $F(b) = 0$, and similarly $F(a) > 0$. Using CONT for this F and with $f = b$, we have

$$\downarrow\exists k{:}\mathbb{N}.\ \forall g{:}\mathbb{S}.\ (g = b \in \mathbb{S}_k) \Rightarrow F(g) = 0$$

What we are proving is squash stable, so we may assume that we have a k for which $\forall g{:}\mathbb{S}.\ (g = b \in \mathbb{S}_k) \Rightarrow F(g) = 0$. Then we get $(a = b \in \mathbb{S}_k) \Rightarrow F(a) = 0$ so, because $F(a) > 0$, we have $\neg(a = b \in \mathbb{S}_k)$, and this implies $\exists n{:}\mathbb{N}_k.\ \neg(a(n) = b(n))$. □

Regularization

Lemma

For any $k \in \mathbb{N}^+$ *there is a map* $reg_k \in \mathbb{S} \rightarrow \mathbb{S}$ *such that* $reg_k(s)$ *is* k*-regular, and if* s *is* k*-regular, then* $reg_k(s) = s$.

Regularization

Lemma

For any $k \in \mathbb{N}^+$ there is a map $reg_k \in \mathbb{S} \to \mathbb{S}$ such that $reg_k(s)$ is k-regular, and if s is k-regular, then $reg_k(s) = s$.

Proof.

Let s be any sequence in $\mathbb{S}$. For any $j \in \mathbb{N}^+$ we can decide whether the k-regularity condition $|ns_m - ns_n| \leq 2k(n+m)$ holds for all $n, m \leq j$. If so, we let $\text{reg}_k(s)_j = s_j$. If not, we let j_0 be the first failure of regularity. There is a rational $q = a/b$ that is a member of all the intervals $\frac{s_n}{2kn} \pm \frac{1}{n}$ for $n < j_0$. Then, for $j \geq j_0$ we let $\text{reg}_k(s)_j = q_j$. Then $r = \text{reg}_k(s)$ is k-regular because q is in all the intervals $\frac{r_n}{2kn} \pm \frac{1}{n}$. □

Regularization

Lemma

For any $k \in \mathbb{N}^+$ there is a map $reg_k \in \mathbb{S} \to \mathbb{S}$ such that $reg_k(s)$ is k-regular, and if s is k-regular, then $reg_k(s) = s$.

Proof.

Let s be any sequence in $\mathbb{S}$. For any $j \in \mathbb{N}^+$ we can decide whether the k-regularity condition $|ns_m - ns_n| \leq 2k(n+m)$ holds for all $n, m \leq j$. If so, we let $\text{reg}_k(s)_j = s_j$. If not, we let j_0 be the first failure of regularity. There is a rational $q = a/b$ that is a member of all the intervals $\frac{s_n}{2kn} \pm \frac{1}{n}$ for $n < j_0$. Then, for $j \geq j_0$ we let $\text{reg}_k(s)_j = q_j$. Then $r = \text{reg}_k(s)$ is k-regular because q is in all the intervals $\frac{r_n}{2kn} \pm \frac{1}{n}$. □

Remark: The k-regular sequences form a *spread*.

Pseudo-positive real numbers

If $(0 < x)$ then $\forall y : \mathbb{R}.\ (0 < y) \vee (y < x)$.

Pseudo-positive real numbers

If $(0 < x)$ then $\forall y : \mathbb{R}.\ (0 < y) \lor (y < x)$. A real number x is *pseudo-positive* if $\forall y : \mathbb{R}.\ \neg\neg(0 < y) \lor \neg\neg(y < x)$.

Pseudo-positive real numbers

If $(0 < x)$ then $\forall y : \mathbb{R}.\ (0 < y) \vee (y < x)$. A real number x is *pseudo-positive* if $\forall y : \mathbb{R}.\ \neg\neg(0 < y) \vee \neg\neg(y < x)$. A negative real number $x < 0$ is not pseudo-positive because for $y = x$, both cases of $\neg\neg(0 < x) \vee \neg\neg(x < x)$ are false.

Pseudo-positive real numbers

If $(0 < x)$ then $\forall y : \mathbb{R}.\ (0 < y) \vee (y < x)$. A real number x is *pseudo-positive* if $\forall y : \mathbb{R}.\ \neg\neg(0 < y) \vee \neg\neg(y < x)$. A negative real number $x < 0$ is not pseudo-positive because for $y = x$, both cases of $\neg\neg(0 < x) \vee \neg\neg(x < x)$ are false.

Lemma

For $x \geq 0$, if $\forall y : \mathbb{R}.\ \neg(y = x) \vee \neg(y = 0)$ then x is pseudo-positive.

Pseudo-positive real numbers

If $(0 < x)$ then $\forall y\!:\!\mathbb{R}.\ (0 < y) \vee (y < x)$. A real number x is *pseudo-positive* if $\forall y\!:\!\mathbb{R}.\ \neg\neg(0 < y) \vee \neg\neg(y < x)$. A negative real number $x < 0$ is not pseudo-positive because for $y = x$, both cases of $\neg\neg(0 < x) \vee \neg\neg(x < x)$ are false.

Lemma

For $x \geq 0$, if $\forall y\!:\!\mathbb{R}.\ \neg(y = x) \vee \neg(y = 0)$ then x is pseudo-positive.

Proof.

Let $P(y)$ be $\neg\neg(0 < y) \vee \neg\neg(y < x)$. For y in the interval $[0, x]$ the assumption implies $P(y)$. For y in the interval $(-\infty, x]$, $\max(0, y) \in [0, x]$ so $P(\max(0, y))$ and this implies $P(y)$. For y in $(-\infty, \infty)$, $\min(y, x) \in (-\infty, x]$ so $P(\min(y, x))$ and this implies $P(y)$. □

Pseudo-positive $\Rightarrow$ positive

Lemma

For all $x \in \mathbb{R}$ *if* x *is pseudo-positive then* $x > 0$.

Pseudo-positive ⇒ positive

Lemma

For all $x \in \mathbb{R}$ if x is pseudo-positive then $x > 0$.

Proof.

Let $d(i) =$ if $|x_i| > 4$ then $|x_i|$ else 0. Since x is a 1-regular sequence, it is not hard to check that d is a 3-regular sequence. If we prove $(\forall c{:}\mathbb{S}.\ \neg(\bar{0} = c) \vee \neg(d = c))$ then by WMP there is an $n \in \mathbb{N}$ such that $\neg(\bar{0}(n) = d(n))$. This gives $|x_n| > 4$ so $|x| > 0$. Since a pseudo-positive x can not be negative, we have $x > 0$.

Pseudo-positive $\Rightarrow$ positive

Lemma

For all $x \in \mathbb{R}$ if x is pseudo-positive then $x > 0$.

Proof.

Let $d(i) = \text{if } |x_i| > 4 \text{ then } |x_i| \text{ else } 0$. Since x is a 1-regular sequence, it is not hard to check that d is a 3-regular sequence. If we prove $(\forall c\!:\!\mathbb{S}.\ \neg(\bar{0} = c) \vee \neg(d = c))$ then by WMP there is an $n \in \mathbb{N}$ such that $\neg(\bar{0}(n) = d(n))$. This gives $|x_n| > 4$ so $|x| > 0$. Since a pseudo-positive x can not be negative, we have $x > 0$.
Let $c \in \mathbb{S}$. Then $r = \text{accel}(3, \text{reg}_3(c)) \in \mathbb{R}$. Since x is pseudo-positive, we have $\neg\neg(0 < r) \vee \neg\neg(r < x)$.

Pseudo-positive $\Rightarrow$ positive

Lemma

For all $x \in \mathbb{R}$ if x is pseudo-positive then $x > 0$.

Proof.

Let $d(i) = \text{if } |x_i| > 4 \text{ then } |x_i| \text{ else } 0$. Since x is a 1-regular sequence, it is not hard to check that d is a 3-regular sequence. If we prove $(\forall c\!:\!\mathbb{S}.\ \neg(\overline{0} = c) \vee \neg(d = c))$ then by WMP there is an $n \in \mathbb{N}$ such that $\neg(\overline{0}(n) = d(n))$. This gives $|x_n| > 4$ so $|x| > 0$. Since a pseudo-positive x can not be negative, we have $x > 0$.
Let $c \in \mathbb{S}$. Then $r = \text{accel}(3, \text{reg}_3(c)) \in \mathbb{R}$. Since x is pseudo-positive, we have $\neg\neg(0 < r) \vee \neg\neg(r < x)$. If $\neg\neg(0 < r)$ then $\neg(c = \overline{0})$ because $c = \overline{0}$ implies that $r = \text{accel}(3, 0) \equiv 0$.

Pseudo-positive $\Rightarrow$ positive

Lemma

For all $x \in \mathbb{R}$ if x is pseudo-positive then $x > 0$.

Proof.

Let $d(i) = \text{if } |x_i| > 4 \text{ then } |x_i| \text{ else } 0$. Since x is a 1-regular sequence, it is not hard to check that d is a 3-regular sequence. If we prove $(\forall c{:}\mathbb{S}.\ \neg(\overline{0} = c) \vee \neg(d = c))$ then by WMP there is an $n \in \mathbb{N}$ such that $\neg(\overline{0}(n) = d(n))$. This gives $|x_n| > 4$ so $|x| > 0$. Since a pseudo-positive x can not be negative, we have $x > 0$.
Let $c \in \mathbb{S}$. Then $r = \text{accel}(3, \text{reg}_3(c)) \in \mathbb{R}$. Since x is pseudo-positive, we have $\neg\neg(0 < r) \vee \neg\neg(r < x)$. If $\neg\neg(0 < r)$ then $\neg(c = \overline{0})$ because $c = \overline{0}$ implies that $r = \text{accel}(3, 0) \equiv 0$. If $\neg\neg(r < x)$ then $\neg(c = d)$ because if $c = d$ then $\text{reg}_3(c) = d$ and $r = \text{accel}(3, d)$. Then, $\text{bnddiff}(\text{accel}(3, d), d)$ and $\text{bnddiff}(d, |x|)$ so $r \equiv |x|$, but $\neg(|x| < x)$. □

Weak Markov for $\mathbb{R}$. (Ishihara)

Theorem

(Weak Markov's Principle for $\mathbb{R}$) For all $a, b \in \mathbb{R}$

$$(\forall c\!:\!\mathbb{R}.\ \neg(a \equiv c) \vee \neg(b \equiv c)) \Rightarrow (a \# b)$$

Weak Markov for $\mathbb{R}$. (Ishihara)

Theorem

(Weak Markov's Principle for $\mathbb{R}$) For all $a, b \in \mathbb{R}$

$$(\forall c\!:\!\mathbb{R}.\ \neg(a \equiv c) \vee \neg(b \equiv c)) \Rightarrow (a \# b)$$

Proof.

By assumption, for any $y \in \mathbb{R}$, $\neg(a \equiv y + b) \vee \neg(b \equiv y + b)$ and also $\neg(a \equiv y + a) \vee \neg(b \equiv y + a)$.

Weak Markov for $\mathbb{R}$. (Ishihara)

Theorem

(Weak Markov's Principle for $\mathbb{R}$) *For all* $a, b \in \mathbb{R}$

$$(\forall c : \mathbb{R}.\ \neg(a \equiv c) \vee \neg(b \equiv c)) \Rightarrow (a \# b)$$

Proof.

By assumption, for any $y \in \mathbb{R}$, $\neg(a \equiv y + b) \vee \neg(b \equiv y + b)$ and also $\neg(a \equiv y + a) \vee \neg(b \equiv y + a)$. If either $\neg(a \equiv y + a)$ or $\neg(b \equiv y + b)$ then $\neg(y = 0)$.

Weak Markov for $\mathbb{R}$. (Ishihara)

Theorem

(Weak Markov's Principle for $\mathbb{R}$) For all $a, b \in \mathbb{R}$

$$(\forall c : \mathbb{R}.\ \neg(a \equiv c) \vee \neg(b \equiv c)) \Rightarrow (a \# b)$$

Proof.

By assumption, for any $y \in \mathbb{R}$, $\neg(a \equiv y + b) \vee \neg(b \equiv y + b)$ and also $\neg(a \equiv y + a) \vee \neg(b \equiv y + a)$. If either $\neg(a \equiv y + a)$ or $\neg(b \equiv y + b)$ then $\neg(y = 0)$. If both $\neg(a \equiv y + b)$ and $\neg(b \equiv y + a)$ then $\neg(y = |a - b|)$.

Weak Markov for $\mathbb{R}$. (Ishihara)

Theorem

(Weak Markov's Principle for $\mathbb{R}$) For all $a, b \in \mathbb{R}$

$$(\forall c{:}\mathbb{R}.\ \neg(a \equiv c) \vee \neg(b \equiv c)) \Rightarrow (a \# b)$$

Proof.

By assumption, for any $y \in \mathbb{R}$, $\neg(a \equiv y + b) \vee \neg(b \equiv y + b)$ and also $\neg(a \equiv y + a) \vee \neg(b \equiv y + a)$. If either $\neg(a \equiv y + a)$ or $\neg(b \equiv y + b)$ then $\neg(y = 0)$. If both $\neg(a \equiv y + b)$ and $\neg(b \equiv y + a)$ then $\neg(y = |a - b|)$. Thus, $\forall y{:}\mathbb{R}.\ \neg(y = |a - b|) \vee \neg(y = 0)$ so, by the penultimate lemma, $|a - b|$ is pseudo-positive. By the last lemma, $|a - b| > 0$ so $a \# b$. □

An *interval* is one of $(-\infty, \infty), (-\infty, a), (-\infty, a], [b, \infty), (b, \infty), (a, b), [a, b), (a, b)$,or $[a, b]$.

Extensional and Strongly Extensional Real Functions

An *interval* is one of $(-\infty, \infty), (-\infty, a), (-\infty, a], [b, \infty), (b, \infty), (a, b), [a, b), (a, b)$,or $[a, b]$.

If I is an interval and $f \in I \to \mathbb{R}$ then Bishop calls f an *operation* defined on I but reserves the word *function* for f that satisfies

$$\text{FUN}(f, I): \quad \forall x, y : I.\ x \equiv y \Rightarrow f(x) \equiv f(y)$$

Extensional and Strongly Extensional Real Functions

An *interval* is one of
$(-\infty, \infty), (-\infty, a), (-\infty, a], [b, \infty), (b, \infty), (a, b), [a, b), (a, b)$,or $[a, b]$.
If I is an interval and $f \in I \to \mathbb{R}$ then Bishop calls f an *operation* defined on I but reserves the word *function* for f that satisfies

$$\mathrm{FUN}(f, I): \quad \forall x, y : I.\ x \equiv y \Rightarrow f(x) \equiv f(y)$$

A seemingly stronger condition on f, called *strongly extensional* is

$$\mathrm{SFUN}(f, I): \quad \forall x, y : I.\ f(x) \# f(y) \Rightarrow x \# y$$

FUN ⇒ SFUN

Theorem

For any interval I and any $f \in I \to \mathbb{R}$,

$$FUN(f, I) \Rightarrow SFUN(f, I)$$

FUN $\Rightarrow$ SFUN

Theorem

For any interval I *and any* $f \in I \to \mathbb{R}$,

$$FUN(f, I) \Rightarrow SFUN(f, I)$$

Proof.

Suppose $x, y \in I$ and $f(x)\#f(y)$. We must prove $x\#y$. By WMP it is enough to prove that for any $z \in \mathbb{R}$, $\neg(z \equiv x) \vee \neg(z \equiv y)$. We first prove this for all $z \in I$. For such a z, $f(z)$ is a real number, and either $f(z)\#f(x)$ in which case, because FUN(f, I), $\neg(z \equiv x)$, or $f(z)\#f(y)$ in which case $\neg(z \equiv y)$.

FUN $\Rightarrow$ SFUN

Theorem

For any interval I and any $f \in I \to \mathbb{R}$,

$$FUN(f, I) \Rightarrow SFUN(f, I)$$

Proof.

Suppose $x, y \in I$ and $f(x)\#f(y)$. We must prove $x\#y$. By WMP it is enough to prove that for any $z \in \mathbb{R}$, $\neg(z \equiv x) \vee \neg(z \equiv y)$. We first prove this for all $z \in I$. For such a z, $f(z)$ is a real number, and either $f(z)\#f(x)$ in which case, because FUN(f, I), $\neg(z \equiv x)$, or $f(z)\#f(y)$ in which case $\neg(z \equiv y)$. We then let $a = \min(x, y)$ and $b = \max(x, y)$ then $[a, b]$ is a sub-interval of I and for an arbitrary real number z we have $z' = \min(b, \max(a, z)) \in [a, b]$. So, either $\neg(z' \equiv x)$ or $\neg(z' \equiv y)$. But $z \equiv x \Rightarrow z' \equiv x$ and $z \equiv y \Rightarrow z' \equiv y$, so we also have $\neg(z \equiv x) \vee \neg(z \equiv y)$. □

Weak Continuity

Here is a continuity principle that does not mention squash.

Weak Continuity

Here is a continuity principle that does not mention squash.

Lemma

(Weak Continuity) For any $F \in \mathbb{S} \to \mathbb{N}$ *and any* $f \in \mathbb{S}$*,*

$$\forall G : k : \mathbb{N} \to \{g : \mathbb{S} \mid g = f \in \mathbb{S}_k\}.\ \exists k : \mathbb{N}.\ F(G(k)) = F(f)$$

Here is a continuity principle that does not mention squash.

Lemma

(Weak Continuity) For any $F \in \mathbb{S} \to \mathbb{N}$ and any $f \in \mathbb{S}$,

$$\forall G : k : \mathbb{N} \to \{g : \mathbb{S} \mid g = f \in \mathbb{S}_k\}.\ \exists k : \mathbb{N}.\ F(G(k)) = F(f)$$

Proof.

From CONT we have
$\downarrow \exists k : \mathbb{N}.\ \forall g : \mathbb{S}.\ (g = f \in \mathbb{S}_k) \Rightarrow F(g) = F(f).$

Weak Continuity

Here is a continuity principle that does not mention squash.

Lemma

(Weak Continuity) For any $F \in \mathbb{S} \to \mathbb{N}$ *and any* $f \in \mathbb{S}$,

$$\forall G{:}k{:}\mathbb{N} \to \{g{:}\mathbb{S} \mid g = f \in \mathbb{S}_k\}.\ \exists k{:}\mathbb{N}.\ F(G(k)) = F(f)$$

Proof.

From CONT we have $\downarrow\exists k{:}\mathbb{N}.\ \forall g{:}\mathbb{S}.\ (g = f \in \mathbb{S}_k) \Rightarrow F(g) = F(f)$. And from this we get $\downarrow\exists k{:}\mathbb{N}.\ F(G(k)) = F(f)$.

Weak Continuity

Here is a continuity principle that does not mention squash.

Lemma

(Weak Continuity) For any $F \in \mathbb{S} \to \mathbb{N}$ *and any* $f \in \mathbb{S}$*,*

$$\forall G{:}k{:}\mathbb{N} \to \{g{:}\mathbb{S} \mid g = f \in \mathbb{S}_k\}.\ \exists k{:}\mathbb{N}.\ F(G(k)) = F(f)$$

Proof.

From CONT we have $\downarrow\exists k{:}\mathbb{N}.\ \forall g{:}\mathbb{S}.\ (g = f \in \mathbb{S}_k) \Rightarrow F(g) = F(f)$. And from this we get $\downarrow\exists k{:}\mathbb{N}.\ F(G(k)) = F(f)$. But this is squash stable, so $\exists k{:}\mathbb{N}.\ F(G(k)) = F(f)$. □

Weak Continuity for $\mathbb{R}$

Lemma

For any $F \in \mathbb{R} \to \mathbb{N}$ *and any* $x \in \mathbb{R}$

$$\forall G : k : \mathbb{N} \to \{y : \mathbb{R} \mid y = x \in \mathbb{S}_k\}.\ \exists k : \mathbb{N}.\ F(G(k)) = F(x)$$

Weak Continuity for $\mathbb{R}$

Lemma

For any $F \in \mathbb{R} \to \mathbb{N}$ and any $x \in \mathbb{R}$

$$\forall G : k : \mathbb{N} \to \{y : \mathbb{R} \mid y = x \in \mathbb{S}_k\}. \ \exists k : \mathbb{N}. \ F(G(k)) = F(x)$$

Proof.

Apply Weak Continuity to $\lambda s. \ F(\text{reg}_1(s))$, x, and G to get k for which $F(\text{reg}_1(G(k))) = F(\text{reg}_1(x))$. But since $G(k)$ and x are regular, $\text{reg}_1(G(k)) = G(k)$ and $\text{reg}_1(x) = x$. So $F(G(k)) = F(x)$. □

Better Continuity for $\mathbb{R}$

Lemma

For all $x \in \mathbb{R}$ *there exists* $x' \in \mathbb{R}$ *such that* $x' \equiv x$ *and for any sequence* g_n *converging to* x *and any operation* $F \in \mathbb{R} \to \mathbb{N}$, *there exist* $n \in \mathbb{N}$ *and* $z \in \mathbb{R}$ *such that* $z \equiv g_n$ *and* $F(z) = F(x')$.

Better Continuity for $\mathbb{R}$

Lemma

For all $x \in \mathbb{R}$ there exists $x' \in \mathbb{R}$ such that $x' \equiv x$ and for any sequence g_n converging to x and any operation $F \in \mathbb{R} \to \mathbb{N}$, there exist $n \in \mathbb{N}$ and $z \in \mathbb{R}$ such that $z \equiv g_n$ and $F(z) = F(x')$.

We are given $x \in \mathbb{R}$, $F \in \mathbb{R} \to \mathbb{N}$, and a sequence of reals g_n converging to x.

Better Continuity for $\mathbb{R}$

Lemma

For all $x \in \mathbb{R}$ there exists $x' \in \mathbb{R}$ such that $x' \equiv x$ and for any sequence g_n converging to x and any operation $F \in \mathbb{R} \to \mathbb{N}$, there exist $n \in \mathbb{N}$ and $z \in \mathbb{R}$ such that $z \equiv g_n$ and $F(z) = F(x')$.

We are given $x \in \mathbb{R}$, $F \in \mathbb{R} \to \mathbb{N}$, and a sequence of reals g_n converging to x. To use Weak Continuity for $\mathbb{R}$ we need a family of reals $G(k)$ such that $G(k)$ agrees exactly with x up to k and is equivalent to some g_n.

Better Continuity for $\mathbb{R}$

Lemma

For all $x \in \mathbb{R}$ there exists $x' \in \mathbb{R}$ such that $x' \equiv x$ and for any sequence g_n converging to x and any operation $F \in \mathbb{R} \to \mathbb{N}$, there exist $n \in \mathbb{N}$ and $z \in \mathbb{R}$ such that $z \equiv g_n$ and $F(z) = F(x')$.

We are given $x \in \mathbb{R}$, $F \in \mathbb{R} \to \mathbb{N}$, and a sequence of reals g_n converging to x. To use Weak Continuity for $\mathbb{R}$ we need a family of reals $G(k)$ such that $G(k)$ agrees exactly with x up to k and is equivalent to some g_n. To get a real number that is equivalent to g_n and agrees exactly with x up to k we need to “blend” x and g_n.

Blending reals

Definition

$$\text{blend}(k, x, y) = \lambda n.\ \text{if } n < k \text{ then } x_n \text{ else } y_n$$

Lemma

If $k \in \mathbb{N}^+$, $x, y \in \mathbb{R}$ *and* $|x - y| \leq 1/6k$ *then* $\mathit{blend}(6k, x, y)$ *is a 3-regular sequence,* $z = \mathit{accel}(3, \mathit{blend}(6k, x, y))$ *is a real number,* $z \equiv y$, *and* $z = \mathit{accel}(3, x) \in \mathbb{S}_k$.

Proof.

See the notes. □

Proof of Better Continuity for $\mathbb{R}$

For any $x \in \mathbb{R}$, and any sequence g_n converging to x we can find a function c such that for all $k \in \mathbb{N}^+$, $|x - g_{c(k)}| \leq 1/6k$

Proof of Better Continuity for $\mathbb{R}$

For any $x \in \mathbb{R}$, and any sequence g_n converging to x we can find a function c such that for all $k \in \mathbb{N}^+$, $|x - g_{c(k)}| \leq 1/6k$
We define G by

$$G(k) = \text{accel}(3, \text{blend}(6k, x, g_{c(k)}))$$

By the blending lemma, $G : k : \mathbb{N}^+ \to \{y : \mathbb{R} \mid y = \text{accel}(3, x) \in \mathbb{S}_k\}$, and for all $k \in \mathbb{N}^+$, $G(k) \equiv g_{c(k)}$.
Let $x' = \text{accel}(3, x)$. Then $x' \equiv x$ and by Weak Continuity for $\mathbb{R}$, for any $P \in \mathbb{R} \to \mathbb{B}$ there is a $k \in \mathbb{N}^+$ such that

$$P(G(k)) = P(x')$$

Proof of Better Continuity for $\mathbb{R}$

For any $x \in \mathbb{R}$, and any sequence g_n converging to x we can find a function c such that for all $k \in \mathbb{N}^+$, $|x - g_{c(k)}| \leq 1/6k$
We define G by

$$G(k) = \text{accel}(3, \text{blend}(6k, x, g_{c(k)}))$$

By the blending lemma, $G : k : \mathbb{N}^+ \to \{y : \mathbb{R} \mid y = \text{accel}(3, x) \in \mathbb{S}_k\}$, and for all $k \in \mathbb{N}^+$, $G(k) \equiv g_{c(k)}$.
Let $x' = \text{accel}(3, x)$. Then $x' \equiv x$ and by Weak Continuity for $\mathbb{R}$, for any $P \in \mathbb{R} \to \mathbb{B}$ there is a $k \in \mathbb{N}^+$ such that

$$P(G(k)) = P(x')$$

Then for $z = G(k)$ and $n = c(k)$ we have $P(z) = P(x')$, and $z \equiv g_n$. QED.

Connectedness of $\mathbb{R}$

Bishop reserves the word *set* (of real numbers) to mean a proposition that respects the equivalence relation.

Definition

$P \in \mathbb{R} \rightarrow \mathbb{P}$ is a *set* of reals (and we write Set(P)) if $\forall x{:}\mathbb{R}.\ \forall y{:}\{\mathbb{R}|\ x \equiv y\}.\ P(x) \Rightarrow P(y)$

Connectedness of $\mathbb{R}$

Bishop reserves the word *set* (of real numbers) to mean a proposition that respects the equivalence relation.

Definition

$P \in \mathbb{R} \to \mathbb{P}$ is a *set* of reals (and we write Set(P)) if $\forall x{:}\mathbb{R}.\ \forall y{:}\{\mathbb{R}|\ x \equiv y\}.\ P(x) \Rightarrow P(y)$

Brouwer proved that the intuitionistic continuum is *indecomposable*: If A and B are sets of reals and $\mathbb{R} = A \cup B$ and $A \cap B = \emptyset$ then $A = \mathbb{R}$ or $A = \emptyset$.

Connectedness of $\mathbb{R}$

Bishop reserves the word *set* (of real numbers) to mean a proposition that respects the equivalence relation.

Definition

$P \in \mathbb{R} \to \mathbb{P}$ is a *set* of reals (and we write Set(P)) if $\forall x:\mathbb{R}.\ \forall y:\{\mathbb{R}|\ x \equiv y\}.\ P(x) \Rightarrow P(y)$

Brouwer proved that the intuitionistic continuum is *indecomposable*: If A and B are sets of reals and $\mathbb{R} = A \cup B$ and $A \cap B = \emptyset$ then $A = \mathbb{R}$ or $A = \emptyset$. We can now prove a stronger theorem.

Connectedness of $\mathbb{R}$

Bishop reserves the word *set* (of real numbers) to mean a proposition that respects the equivalence relation.

Definition

$P \in \mathbb{R} \rightarrow \mathbb{P}$ is a *set* of reals (and we write Set(P)) if $\forall x\!:\!\mathbb{R}.\ \forall y\!:\!\{\mathbb{R}|\ x \equiv y\}.\ P(x) \Rightarrow P(y)$

Brouwer proved that the intuitionistic continuum is *indecomposable*: If A and B are sets of reals and $\mathbb{R} = A \cup B$ and $A \cap B = \emptyset$ then $A = \mathbb{R}$ or $A = \emptyset$. We can now prove a stronger theorem.

Theorem

(Connectedness of $\mathbb{R}$) For all $A, B : \mathbb{R} \rightarrow \mathbb{P}$, if $Set(A)$ and $Set(B)$ and $\exists a\!:\!\mathbb{R}.\ A(a)$ and $\exists b\!:\!\mathbb{R}.\ B(b)$ then

$$(\forall r\!:\!\mathbb{R}.\ A(r) \vee B(r)) \Rightarrow (\exists r\!:\!\mathbb{R}.\ A(r) \wedge B(r))$$

Proof of connectedness of $\mathbb{R}$

Let a_0 and b_0 be reals such that $A(a_0)$ and $B(b_0)$.
The assumption $\forall r : \mathbb{R}.\ A(r) \vee B(r)$ gives us a *operation* $d \in \mathbb{R} \rightarrow \mathbb{N}$ such that

$$\begin{aligned} (d(r) = 0) &\Rightarrow A(r) \\ (d(r) > 0) &\Rightarrow B(r) \end{aligned}$$

Proof of connectedness of $\mathbb{R}$

Let a_0 and b_0 be reals such that $A(a_0)$ and $B(b_0)$.
The assumption $\forall r:\mathbb{R}.\ A(r) \vee B(r)$ gives us a *operation* $d \in \mathbb{R} \to \mathbb{N}$ such that

$$\begin{aligned}(d(r) = 0) &\Rightarrow A(r)\\ (d(r) > 0) &\Rightarrow B(r)\end{aligned}$$

We may assume $d(a_0) = 0$ and $d(b_0) > 0$. Note that d is an *operation* and not a *function* in Bishop's sense.

Proof of connectedness of $\mathbb{R}$

Let a_0 and b_0 be reals such that $A(a_0)$ and $B(b_0)$.
The assumption $\forall r{:}\mathbb{R}.\ A(r) \vee B(r)$ gives us a *operation* $d \in \mathbb{R} \to \mathbb{N}$ such that

$$\begin{array}{rcl} (d(r) = 0) & \Rightarrow & A(r) \\ (d(r) > 0) & \Rightarrow & B(r) \end{array}$$

We may assume $d(a_0) = 0$ and $d(b_0) > 0$. Note that d is an *operation* and not a *function* in Bishop's sense. Now we define by primitive recursion a sequence of pairs $\langle a_n, b_n \rangle$ starting with our given $\langle a_0, b_0 \rangle$.

Proof of connectedness of $\mathbb{R}$

Let a_0 and b_0 be reals such that $A(a_0)$ and $B(b_0)$.
The assumption $\forall r:\mathbb{R}.\ A(r) \vee B(r)$ gives us a *operation* $d \in \mathbb{R} \to \mathbb{N}$ such that

$$\begin{aligned} (d(r) = 0) &\Rightarrow A(r) \\ (d(r) > 0) &\Rightarrow B(r) \end{aligned}$$

We may assume $d(a_0) = 0$ and $d(b_0) > 0$. Note that d is an *operation* and not a *function* in Bishop's sense. Now we define by primitive recursion a sequence of pairs $\langle a_n, b_n \rangle$ starting with our given $\langle a_0, b_0 \rangle$. To define $\langle a_{n+1}, b_{n+1} \rangle$ we let $m_n = (a_n + b_n)/2$ and

$$\langle a_{n+1}, b_{n+1} \rangle = \text{if } d(m_n) = 0 \text{ then} \langle m_n, b_n \rangle \text{ else } \langle a_n, m_n \rangle$$

Proof of connectedness of $\mathbb{R}$

Let a_0 and b_0 be reals such that $A(a_0)$ and $B(b_0)$.
The assumption $\forall r:\mathbb{R}.\ A(r) \vee B(r)$ gives us a *operation* $d \in \mathbb{R} \to \mathbb{N}$ such that

$$\begin{array}{lcl} (d(r) = 0) & \Rightarrow & A(r) \\ (d(r) > 0) & \Rightarrow & B(r) \end{array}$$

We may assume $d(a_0) = 0$ and $d(b_0) > 0$. Note that d is an *operation* and not a *function* in Bishop's sense. Now we define by primitive recursion a sequence of pairs $\langle a_n, b_n \rangle$ starting with our given $\langle a_0, b_0 \rangle$. To define $\langle a_{n+1}, b_{n+1} \rangle$ we let $m_n = (a_n + b_n)/2$ and

$$\langle a_{n+1}, b_{n+1} \rangle = \text{if } d(m_n) = 0 \text{ then} \langle m_n, b_n \rangle \text{ else } \langle a_n, m_n \rangle$$

The sequences a_n and b_n are Cauchy sequences and they converge to the same real number x.

Connectedness proof concluded

Use Better Continuity for $\mathbb{R}$ with real x the common limit of sequences a_n and b_n to get a real $x' \equiv x$, numbers n and m and reals z and w such that $z \equiv a_n$ and $w \equiv b_m$ and $d(z) = d(x') = d(w)$.

Connectedness proof concleded

Use Better Continuity for $\mathbb{R}$ with real x the common limit of sequences a_n and b_n to get a real $x' \equiv x$, numbers n and m and reals z and w such that $z \equiv a_n$ and $w \equiv b_m$ and
$d(z) = d(x') = d(w)$.
If $d(x') = 0$ then $d(w) = 0$ and $w \equiv b_m$. Therefore $A(w)$ is true and, because Set(A), also $A(b_m)$. But $B(b_m)$ because $d(b_m) > 0$, so b_m is in both sets A and B and we are done in this case.

Connectedness proof concluded

Use Better Continuity for $\mathbb{R}$ with real x the common limit of sequences a_n and b_n to get a real $x' \equiv x$, numbers n and m and reals z and w such that $z \equiv a_n$ and $w \equiv b_m$ and $d(z) = d(x') = d(w)$.

If $d(x') = 0$ then $d(w) = 0$ and $w \equiv b_m$. Therefore $A(w)$ is true and, because $\text{Set}(A)$, also $A(b_m)$. But $B(b_m)$ because $d(b_m) > 0$, so b_m is in both sets A and B and we are done in this case.

If $d(x') > 0$ then $d(z) > 0$ and $z \equiv a_n$. Then $B(z)$ and hence $B(a_n)$, because $\text{Set}(B)$. But also, $A(a_n)$, because $d(a_n) = 0$, so a_n is in both sets A and B.

Connectedness proof concluded

Use Better Continuity for $\mathbb{R}$ with real x the common limit of sequences a_n and b_n to get a real $x' \equiv x$, numbers n and m and reals z and w such that $z \equiv a_n$ and $w \equiv b_m$ and $d(z) = d(x') = d(w)$.

If $d(x') = 0$ then $d(w) = 0$ and $w \equiv b_m$. Therefore $A(w)$ is true and, because $\text{Set}(A)$, also $A(b_m)$. But $B(b_m)$ because $d(b_m) > 0$, so b_m is in both sets A and B and we are done in this case.

If $d(x') > 0$ then $d(z) > 0$ and $z \equiv a_n$. Then $B(z)$ and hence $B(a_n)$, because $\text{Set}(B)$. But also, $A(a_n)$, because $d(a_n) = 0$, so a_n is in both sets A and B. QED.

Indecomposability of $\mathbb{R}$

Corollary

If $Set(A)$ *and* $Set(B)$ *and* $A \cap B = \emptyset$ *and* $A \cup B = \mathbb{R}$ *then* $(A = \mathbb{R}) \vee (A = \emptyset)$

Indecomposability of $\mathbb{R}$

Corollary

If Set(A) *and Set*(B) *and* $A \cap B = \emptyset$ *and* $A \cup B = \mathbb{R}$ *then* $(A = \mathbb{R}) \vee (A = \emptyset)$

Proof.

From $A \cup B = \mathbb{R}$ we have $A(x) \vee B(x)$ for any $x \in \mathbb{R}$, so $A(0) \vee B(0)$. If $A(0)$ then $(A = \mathbb{R}) \wedge (B = \emptyset)$ because if $B(x)$ for any x then, by connectedness, $A \cap B \neq \emptyset$. Similarly, if $B(0)$ then $(B = \mathbb{R}) \wedge (A = \emptyset)$. □

Lecture 3

- Bar Induction
  - Statement of BID, Realizer for BID (bar recursion)
  - Fan Theorem
  - Kleene's singular tree
  - Soundness of Bar Induction
- Brouwer's uniform continuity theorem
  - Uniform continuity from Fan
  - Uniform continuity for real functions
- Consequences of Brouwer's theorem
  - Simplification of formal theory
  - Two functional equations