Constructivism in Mathematics

Kit L (u2111082@warwick.ac.uk)

Introduction

“Concrete” Mathematics

Up to the 19th Century, mathematics was primarily concerned with “concrete objects”, which could be explicitly constructed:

- Every integer is either even or odd;
- There are infinitely many primes;
- Every natural number can be written as the sum of four squares;
- Every continuous function is integrable;
- Every non-constant polynomial over $\mathbb{C}$ has a root.

“Concrete” Mathematics

- Every integer is either even or odd;
- There are infinitely many primes;
- Every natural number can be written as the sum of four squares;
- Every continuous function is integrable;
- Every non-constant polynomial over $\mathbb{C}$ has a root.

Proofs of these results yield *effective algorithms*:

- We can *decide* whether any given integer is even or odd;
- We can *find* the next prime number;
- We can *find* four squares which sum to that number;
- We can *compute* the integral up to *any desired accuracy*;
- We can *compute* roots up to *any desired accuracy*.

“Ideal” Mathematics

In the 19th Century, however, mathematicians became increasingly interested in reasoning about *non-constructible* objects:

- For every function $f : \mathbb{N} \to \mathbb{N}$, there exists n such that $f(n) \leq f(m)$ for all m;
- Every bounded above non-empty set of real numbers has a least upper bound;
- Every field has an algebraic closure;
- Every ring has a maximal ideal;
- Every vector space has a basis.

“Ideal” Mathematics

In the 19th Century, however, mathematicians became increasingly interested in reasoning about *non-constructible* objects:

- For every function $f : \mathbb{N} \to \mathbb{N}$, there exists n such that $f(n) \leq f(m)$ for all m;
- Every bounded above non-empty set of real numbers has a least upper bound;
- Every field has an algebraic closure;
- Every ring has a maximal ideal;
- Every vector space has a basis.

These *existence results* do not yield effective algorithms.

“Ideal” Mathematics

In the 19th Century, however, mathematicians became increasingly interested in reasoning about *non-constructible* objects:

- For every function $f : \mathbb{N} \to \mathbb{N}$, there exists n such that $f(n) \leq f(m)$ for all m;
- Every bounded above non-empty set of real numbers has a least upper bound;
- Every field has an algebraic closure;
- Every ring has a maximal ideal;
- Every vector space has a basis.

These *existence results* do not yield effective algorithms.

Question. Do ideal objects really “exist”?

The Foundational Crisis

Example (Russell's Paradox).

Define the set

$$R := \{x : x \notin x\}$$

Is $R \in R$?

- If $R \in R$, then by definition, $R \notin R$.
- But if $R \notin R$, then we must have $R \in R$.

Contradiction.

The Foundational Crisis

Example (Russell's Paradox).

Define the set

$$R := \{x : x \notin x\}$$

Is $R \in R$?

- If $R \in R$, then by definition, $R \notin R$.
- But if $R \notin R$, then we must have $R \in R$.

Contradiction.

Corollary.

Frege's foundations of arithmetic are inconsistent.

The Foundational Crisis

Can we construct solid formal foundations for mathematics?

- Can we ensure they are *consistent*?
- Can we ensure they are *complete*?
- Can we ensure they are *decidable*?
- Can we ensure they are *finitarily conservative*?

The Foundational Crisis

Can we construct solid formal foundations for mathematics?

- Can we ensure they are *consistent*?
- Can we ensure they are *complete*?
- Can we ensure they are *decidable*?
- Can we ensure they are *finitarily conservative*?

This led to a resurgence of fundamental philosophical questions.

- What *is* a mathematical proof?
- Can arithmetic/mathematics be reduced to *pure logic*?
- Do mathematical objects *exist*, or are they just *symbols*?

Formalism, Intuitionism

Two main schools of thought emerged from the foundational crisis:

Intuitionism (Brouwer)

- Based on semantics;
- Mathematics is about *mental construction*;
- Infinite sets, maximal ideals, etc. do not exist unless explicitly constructed.

Formalism (Hilbert)

- Based on syntax;
- Mathematics is a game of manipulating strings;
- Infinite sets, maximal ideals, etc. are all fine, as long as our underlying logical calculus can be trusted.

Constructivity

Axiom (Choice). For any non-empty family of sets X, there is a choice function f defined on X.

$$\forall X \left[\varnothing \notin X \implies \exists f\colon X \to \bigcup_{A \in X} A \quad \forall A \in X\, (f(A) \in A) \right]$$

Axiom (LEM)**.** For every proposition p, either p or not p.

$$\vdash p \vee \neg p$$

Axiom (LEM). For every proposition p, either p or not p.

$$\vdash p \vee \neg p$$

$p =$ “there exist 1,000 consecutive 0s in the decimal expansion of $\boldsymbol{\pi}$”

Axiom (LEM). For every proposition p, either p or not p.

$$\vdash p \vee \neg p$$

$p =$ “there exist 1,000 consecutive 0s in the decimal expansion of $\boldsymbol{\pi}$”

We might never know whether p is true or not... but by LEM, one of the two possibilities must hold.

Proposition. There exist irrational a, b such that a^b is rational.

Proposition. There exist irrational a and b such that a^b is rational.

Proof. We know that $\sqrt{2}$ is irrational. What about $\sqrt{2}^{\sqrt{2}}$? We have two cases.

- If $\sqrt{2}^{\sqrt{2}}$ is rational, then we are done, with $a = b = \sqrt{2}$.
- Otherwise, $\sqrt{2}^{\sqrt{2}}$ is irrational, in which case,

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^{2} = 2 \in \mathbb{Q}$$

so taking $a = \sqrt{2}^{\sqrt{2}}$and $b = \sqrt{2}$ suffices.

Proposition. There exist irrational a and b such that a^b is rational.

Proof. We know that $\sqrt{2}$ is irrational. What about $\sqrt{2}^{\sqrt{2}}$? We have two cases.

- If $\sqrt{2}^{\sqrt{2}}$ is rational, then we are done, with $a = b = \sqrt{2}$.
- Otherwise, $\sqrt{2}^{\sqrt{2}}$ is irrational, in which case,

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^{2} = 2 \in \mathbb{Q}$$

so taking $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ suffices.

Question. Is $\sqrt{2}^{\sqrt{2}}$ rational or irrational?!

Constructive Mathematics

Constructive mathematics

- Mathematics without LEM

Constructive mathematics

- Mathematics without LEM

Constructivism

- Constructive mathematics is useful.
- Or, in more extreme cases, that non-constructive mathematics is “wrong”.

Constructive mathematics

- Mathematics without LEM

Constructivism

- Constructive mathematics is useful.
- Or, in more extreme cases, that non-constructive mathematics is “wrong”.

Constructive mathematics

- Mathematics without LEM

Constructivism

- Constructive mathematics is useful.
- Or, in more extreme cases, that non-constructive mathematics is "wrong".

Varieties of Constructivism

Intuitionism

Intuitionism

- The objects of mathematics are mental construction, grasped only in the mind of the (idealised) mathematician.

Intuitionism

- The objects of mathematics are mental construction, grasped only in the mind of the (idealised) mathematician.
- Mathematics is a matter of creation, not discovery. Mathematicians do not mentally reconstruct or discover preexisting mathematical objects existing independently of our thoughts.

Intuitionism

- The objects of mathematics are mental construction, grasped only in the mind of the (idealised) mathematician.
- Mathematics is a matter of creation, not discovery. Mathematicians do not mentally reconstruct or discover preexisting mathematical objects existing independently of our thoughts.
- It does not make sense to ask the truth or falsity of a mathematical statement independently from our knowledge concerning the statement.

Intuitionism

- The objects of mathematics are mental construction, grasped only in the mind of the (idealised) mathematician.
- Mathematics is a matter of creation, not discovery. Mathematicians do not mentally reconstruct or discover preexisting mathematical objects existing independently of our thoughts.
- It does not make sense to ask the truth or falsity of a mathematical statement independently from our knowledge concerning the statement.

Markov’s Constructive Recursive Mathematics (CRM)

CRM

- The objects of mathematics are *algorithms*, in the precise sense of strings formed from a formal grammar called a Markov-algorithm.
- The abstraction of potential realisability is permissible, but not the abstraction of actual infinity
- (Markov's Principle) If it is impossible that an algorithmic computation does not terminate, then for some input, it does terminate.

Bishop’s Constructive Mathematics (BCM)

BCM

Mathematical statements should have numerical meaning.

In particular, existential quantifiers and disjunctions must, in principle, be capable of being made explicit. Furthermore, one can only show that an object exists by giving a finite routine for finding it.

BCM

Mathematical statements should have numerical meaning.

In particular, existential quantifiers and disjunctions must, in principle, be capable of being made explicit. Furthermore, one can only show that an object exists by giving a finite routine for finding it.

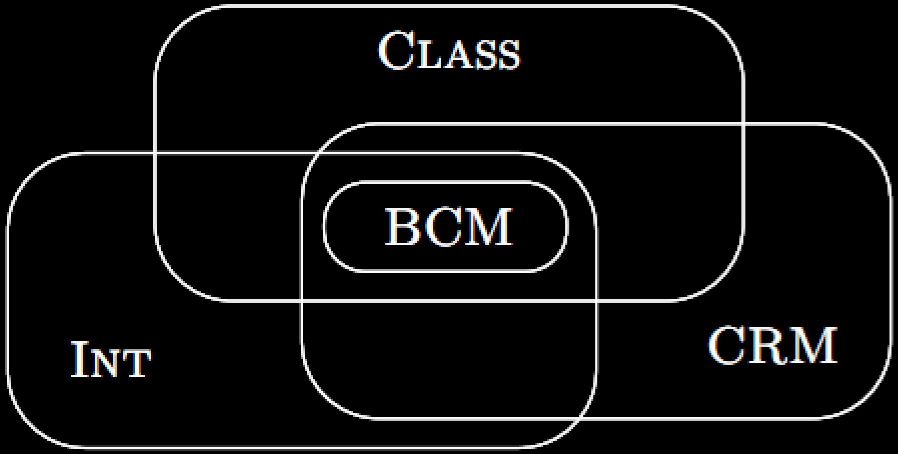
> The movement [Brouwer] had founded has long been dead, killed [...] chiefly by the failure of Brouwer and his followers to convince the mathematical public that abandonment of the idealistic viewpoint would not sterilize or cripple the development of mathematics. Brouwer and other constructivists were much more successful in their criticisms of classical mathematics than in their efforts to replace it with something better.
>
> - Errett Bishop

BCM

- Avoid defining irrelevant concepts; if several definitions are classically equivalent but constructively distinct, use only the ones that yield useful results.
- Avoid pseudo-generality; if an extra assumption simplifies the theory and the examples that one is interested in satisfy the assumption, then the assumption should be made.

BCM

- Avoid defining irrelevant concepts; if several definitions are classically equivalent but constructively distinct, use only the ones that yield useful results.
- Avoid pseudo-generality; if an extra assumption simplifies the theory and the examples that one is interested in satisfy the assumption, then the assumption should be made.



The Brouwer-Heyting-Kolmogorov Interpretation

1) The number a is the greatest prime such that $a - 1$ is also prime, or 0 if such a number does not exist.

2) The number b is the greatest prime such that $b - 2$ is also prime, or 0 if such a number does not exist.

Proposition. There exist irrational a, b such that a^b is rational.

$$p : a = \sqrt{2}, b = \sqrt{2}$$

$$q : a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$$

Lemma (Kőnig). Let G be connected locally finite graph. Then, G contains a ray. That is, an infinite simple path.

Proof. We can "construct" the ray as follows. Select some vertex v_0. As G is connected, each of the infinitely-many vertices of G can be reached by a simple path that starts from v_0.

However, G is locally finite, so v_0 only has finitely many neighbours. By the pigeonhole principle, there is at least one neighbours through which infinitely-many of these paths route through. So connect the path through this neighbour and repeat.

$$\neg\forall x P(x) \quad\iff\quad \exists x \neg P(x)$$

BHK Interpretation

- A proof of $A \wedge B$ consists of a proof of A and a proof of B.
- A proof of $A \vee B$ consists of a proof of A or a proof of B, along with information about which is the case.
- A proof of $A \rightarrow B$ consists of an algorithm that transforms a proof of p into a proof of q.
- A proof of $\forall x\, A(x)$ consists of an algorithm that transforms a proof that t is an element of the intended domain D into a proof of $A(t)$.
- A proof of $\exists x\, A(x)$ consists of an element $t \in D$ and a proof of $A(t)$.
- $\perp$ is not provable; a proof of $\neg A$ is a proof that A is not provable; or equivalently, an algorithm that derives a supposed proof of $\perp$ from a proof of A; that is, $A \rightarrow \perp$.

BHK Interpretation

- A proof of $A \wedge B$ consists of a proof of A and a proof of B.
- A proof of $A \vee B$ consists of a proof of A or a proof of B, along with information about which is the case.
- A proof of $A \to B$ consists of an algorithm that transforms a proof of p into a proof of q.
- A proof of $\forall x\, A(x)$ consists of an algorithm that transforms a proof that t is an element of the intended domain D into a proof of $A(t)$.
- A proof of $\exists x\, A(x)$ consists of an element $t \in D$ and a proof of $A(t)$.
- $\bot$ is not provable; a proof of $\neg A$ is a proof that A is not provable; or equivalently, an algorithm that derives a supposed proof of $\bot$ from a proof of A; that is, $A \to \bot$.

Example.

The statement $p \to p$ is constructively valid for any p: we just take the identity function $\lambda x.x$ as our algorithm transforming a proof of p into a proof of p.

BHK Interpretation

- A proof of $A \wedge B$ consists of a proof of A and a proof of B.
- A proof of $A \vee B$ consists of a proof of A or a proof of B, along with information about which is the case.
- A proof of $A \to B$ consists of an algorithm that transforms a proof of p into a proof of q.
- A proof of $\forall x\, A(x)$ consists of an algorithm that transforms a proof that t is an element of the intended domain D into a proof of $A(t)$.
- A proof of $\exists x\, A(x)$ consists of an element $t \in D$ and a proof of $A(t)$.
- $\bot$ is not provable; a proof of $\neg A$ is a proof that A is not provable; or equivalently, an algorithm that derives a supposed proof of $\bot$ from a proof of A; that is, $A \to \bot$.

Example.

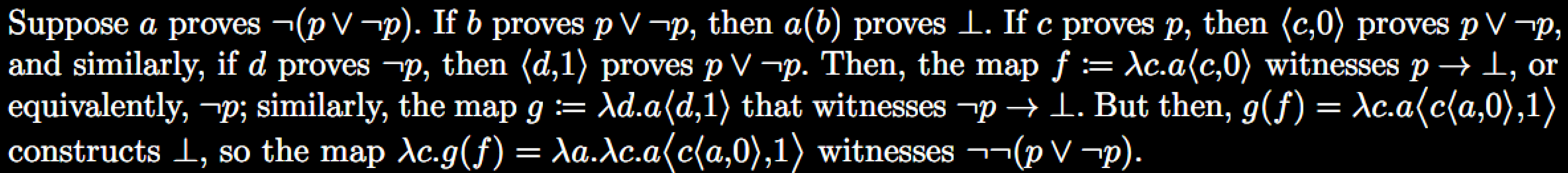
Consider the statement $A \to (B \to A)$ for arbitrary propositions A and B. A proof of this statement is an algorithm that transforms a proof of A into an algorithm that transforms a proof of B into a proof of A. Under this reading, we can see that the proof of B is extraneous, so the second algorithm should just be the function that returns the proof of A given by the first.

BHK Interpretation

- A proof of $A \wedge B$ consists of a proof of A and a proof of B.
- A proof of $A \vee B$ consists of a proof of A or a proof of B, along with information about which is the case.
- A proof of $A \to B$ consists of an algorithm that transforms a proof of p into a proof of q.
- A proof of $\forall x\, A(x)$ consists of an algorithm that transforms a proof that t is an element of the intended domain D into a proof of $A(t)$.
- A proof of $\exists x\, A(x)$ consists of an element $t \in D$ and a proof of $A(t)$.
- $\bot$ is not provable; a proof of $\neg A$ is a proof that A is not provable; or equivalently, an algorithm that derives a supposed proof of $\bot$ from a proof of A; that is, $A \to \bot$.

We cannot refute any instance of LEM. That is, we cannot prove $\neg(p \vee \neg p)$ for any proposition p.

This is because $\neg\neg(p \vee \neg p)$ holds constructively:



Suppose a proves $\neg(p \vee \neg p)$. If b proves $p \vee \neg p$, then $a(b)$ proves $\perp$. If c proves p, then $\langle c{,}0\rangle$ proves $p \vee \neg p$, and similarly, if d proves $\neg p$, then $\langle d{,}1\rangle$ proves $p \vee \neg p$. Then, the map $f \coloneqq \lambda c.a\langle c{,}0\rangle$ witnesses $p \to \perp$, or equivalently, $\neg p$; similarly, the map $g \coloneqq \lambda d.a\langle d{,}1\rangle$ that witnesses $\neg p \to \perp$. But then, $g(f) = \lambda c.a\big\langle c\langle a{,}0\rangle{,}1\big\rangle$ constructs $\perp$, so the map $\lambda c.g(f) = \lambda a.\lambda c.a\big\langle c\langle a{,}0\rangle{,}1\big\rangle$ witnesses $\neg\neg(p \vee \neg p)$.

All Functions are Continuous

Taking the principle of excluded middle from the mathematician would be the same, say, as proscribing the telescope to the astronomer or to the boxer the use of his fists. To prohibit existence statements and the principle of excluded middle is tantamount to relinquishing the science of mathematics altogether. For compared with the immense expanse of modern mathematics, what would the wretched remnants mean, the few isolated results, incomplete and unrelated, that the intuitionists have obtained without the use of logical ϵ-axiom?

– David Hilbert

Theorem (Brouwer). Every function $f : \mathbb{R} \to \mathbb{R}$ is continuous.

Choice Sequences

A *choice sequence* is an unfinished and indefinitely ongoing process of selecting values one by one, by the ideal mathematician.

At any particular step, the ideal mathematician has determined only finitely many values, and for the next step, they are constrained by a collection of restrictions on future choices that define the choice sequence.

A *spread* M consists of a *spread law* Λ_M and a *complementary law* Γ_M.

A *spread* M consists of a *spread law* Λ_M and a *complementary law* Γ_M.

The spread law is a function that divides the space of finite sequences of natural numbers into the *admissible* and *inadmissible*, such that:

- Λ_M is decidable. That is, we should be able to determine in finite time whether any given sequence is admissible or not.
- If a sequence a is admissible, every initial segment of a must be admissible.
- If a sequence $\langle a_0, \dots, a_n \rangle$ is admissible, then Λ_M decides for each natural number k whether $\langle a_0, \dots, a_n, k \rangle$ is admissible. Moreover, there must exist at least one k such that this extension is admissible.

Real Number Generators

A *Real Number Generator* (RNG) is a sequence $\langle a_n \rangle$ of rationals such that for every natural number k, there exists a natural number $n = n(k)$ such that

$$|a_{n+p} - a_n| < \frac{1}{k}$$

for every natural number p.

Two RNGs a and b *coincide* if for every k, there exists a natural number $n = n(k)$ such that

$$|a_{n+p} - b_{n+p}| < \frac{1}{k}$$

for every natural number p, and we write $a = b$ to denote this relation.

A *real number* is an “equivalence class” of RNGs, modulo coincidence.

The *closed interval* $[a,b]$ is the “set” of real numbers x such that $x>a$ and $x>b$ are impossible, and $x<a$ and $x<b$ are impossible.

$$\neg(x > a \wedge x > b) \wedge \neg(x < a \wedge x < b)$$

A *canonical number generator* (CNG) is an RNG of the form $\langle x_n 2^{-n} \rangle$, where each x_n is an integer, satisfying

$$|x_n 2^{-n} - x_{n+1} 2^{-n-1}| \leq 2^{-n-1}$$

A *canonical number generator* (CNG) is an RNG of the form $\langle x_n 2^{-n} \rangle$, where each x_n is an integer, satisfying

$$|x_n 2^{-n} - x_{n+1} 2^{-n-1}| \leq 2^{-n-1}$$

Theorem. Every real number x coincides with a CNG $\langle x_n 2^{-n} \rangle$ with

$$|x - x_n 2^{-n}| < \frac{5}{8} n^{-n}$$

Weak Continuity for Numbers

$$\Phi : \omega^\omega \to \mathbb{N}$$

$$\Phi : \omega^\omega \to \mathbb{N}$$

$$\forall\alpha\exists m\forall\beta\big(\bar{\beta}_m = \bar{\alpha}_m \to \Phi(\beta) = \Phi(\alpha)\big)$$

$$\forall\alpha\exists m\forall\beta \sqsupseteq \bar{\alpha}_m\big(\Phi(\beta) = \Phi(\alpha)\big)$$

$$\Phi : \omega^\omega \to \mathbb{N}$$

$$\forall \alpha \exists m \forall \beta \big(\bar{\beta}_m = \bar{\alpha}_m \to \Phi(\beta) = \Phi(\alpha) \big)$$

$$\forall \alpha \exists m \forall \beta \sqsupseteq \bar{\alpha}_m \big(\Phi(\beta) = \Phi(\alpha) \big)$$

$$\forall \alpha \exists n \big(\varphi(\alpha, n) \big) \to \exists (\Phi \in \omega^\omega \to \mathbb{N}) \forall \alpha : \varphi\big(\alpha, \Phi(\alpha)\big)$$

Axiom (WC-$\mathbb{N}$). *For any formula $\varphi(\alpha,n)$ depending on sequences α and naturals n,*

$$\forall\alpha\exists n\big(\varphi(\alpha,n)\big) \to \forall\alpha\exists m\exists n\forall\beta \sqsupseteq \alpha_m\big(\varphi(\beta,n)\big)$$

Axiom (WC-$\mathbb{N}$). *For any formula $\varphi(\alpha,n)$ depending on sequences α and naturals n,*

$$\forall\alpha\exists n\big(\varphi(\alpha,n)\big) \to \forall\alpha\exists m\exists n\forall\beta \sqsupseteq \alpha_m\big(\varphi(\beta,n)\big)$$

Theorem. WC-$\mathbb{N}$ refutes LEM.

Bars and Fans

Let M be a spread, and F be the set of Λ_M-admissible sequences. Then, a subset B of F is a *bar* on M if every choice sequence in M has an initial segment in B:

$$\forall\alpha \in M \exists n(\bar{\alpha}_n \in B)$$

Given a finite sequence a, we say that B *bars* a (in M) if every choice sequence α in M extending a, there is an initial segment of α that is in B.

A set S of finite sequences in M is *inductive* if whenever every Λ_M-admissible immediate descendent of a is in S, then a is also in S.

Theorem 8.2 (Bar Induction)**.** *Let* P *be a decidable bar on* S *and let* Q *be an inductive subspecies of* F *containing* P*. Then* Q *is a bar.*

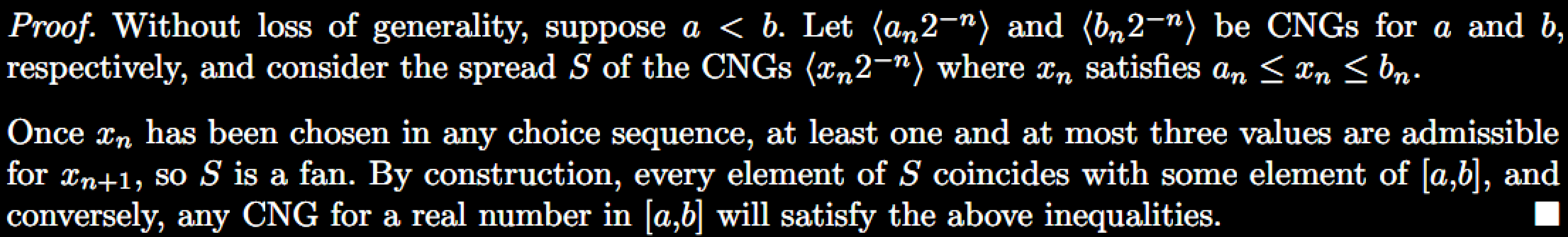
A *fan* is a locally-finite spread.

Example. The spread defining the Cantor space is a fan, because every node a has precisely two immediate descendants: namely its concatenation with 0, and its concatenation with 1.

A *fan* is a locally-finite spread.

Example. The spread defining the Cantor space is a fan, because every node a has precisely two immediate descendants: namely its concatenation with 0, and its concatenation with 1.

Lemma. Every closed interval $[a,b]$ of the continuum coincides with a fan.



Proof. Without loss of generality, suppose $a < b$. Let $\langle a_n 2^{-n} \rangle$ and $\langle b_n 2^{-n} \rangle$ be CNGs for a and b, respectively, and consider the spread S of the CNGs $\langle x_n 2^{-n} \rangle$ where x_n satisfies $a_n \leq x_n \leq b_n$.

Once x_n has been chosen in any choice sequence, at least one and at most three values are admissible for x_{n+1}, so S is a fan. By construction, every element of S coincides with some element of $[a,b]$, and conversely, any CNG for a real number in $[a,b]$ will satisfy the above inequalities. ■

Theorem (Fan Theorem). Let S be a fan, and Φ be a natural-valued function defined on every element δ of S. Then,

$$\exists m \forall \alpha{,}\beta\big(\bar{\alpha}_m = \bar{\beta}_m \to \Phi(\alpha) = \Phi(\beta)\big)$$

Theorem. Every function $f : [a,b] \to \mathbb{R}$ is uniformly continuous.

Proof. The interval $[a,b]$ coincides with a fan, S. To every element ξ of S, we can associate a real number $y := f(\xi)$. Now, let $\eta = \langle \eta_n 2^{-n} \rangle$ be a CNG for y. Then, for any fixed n, we can associate η_n to ξ , thus defining a natural-valued function ϕ_n on S. By the fan theorem, there is a uniform bound $m = m(n)$ such that for each $\xi \in S$, $\phi_n(\xi) = \eta_n$ is determined entirely by the initial segment $\bar{\xi}_m$.

Now, let x_1 and x_2 be real numbers in $[a,b]$ such that $|x_1 - x_2| < 2^{-m-2}$. Then, x_1 and x_2 have CNGs ξ_1 and ξ_2, respectively, whose initial segments up to m are equal. It follows that η_n is the same for both, and hence $\left| f(\xi_1) - f(\xi_2) \right| < \frac{5}{4} 2^{-n}$. That is, f is uniformly continuous.