4

Constructive Mathematics

It is distinguished from its traditional counterpart, classical mathematics, by strict interpr$^=$ of the phase "there exists" and "we can construct".

Before mathematicians assert something (other than an axioms), they are supposed to have proved it true

eg: $P \vee Q$, where P, Q are syntactically correct statem$^=$; in some formal/informal language

can be asserted only if one proof of P or one of Q can be produced

We run into a problem, in the case where Q is the negation $\neg P$ of P.
To assert $\neg P$, is to show that P implies a contrad$^=$
But it is often possible that mathematicians have no proof, of neither P or $\neg P$.

<u>Goldbach Conjecture</u>

Every integer > 2, can be written as a sum of two primes

This has neither been proved or disproved.
We are thus forced to conclude, that under the very natural decidability interpretation of $P \vee Q$, only a stubborn optimist can retain a belif in the law of excluded middle.

Law of Excluded Middle:

For every statement P, either P or $\neg P$ holds,

Classical logic widens the interpretation of disjunction:

$$P \vee Q \text{ is seen as, } \underbrace{\neg(\neg P \wedge \neg Q)}$$

it is contradictory that both P and Q be false

This leads to an idealistic interpr^n of existance, in which,

$$\exists x\, P(x), \text{ means } \underbrace{\neg \forall x\, \neg P(x)}$$

it is contradictory that P(x) be false for all x

Classical Mathematics is built on this interpret^n of logic.

This wider def^n however comes at cost, when we pass from our initial natural interpr^n of $P \vee Q$, to unrestricted use of the idealistic one, $\neg(\neg P \wedge \neg Q)$

↳ The resulted model can not be generated by computational models, such as recursive function theory.

This is illustrated here,

There exists a real number such that a, b are irrational but a^b is rational.

<u>Proof</u>:

We know $(\sqrt{2})$ is irrational. Consider $(\sqrt{2})^{\sqrt{2}}$.

Either $(\sqrt{2})^{\sqrt{2}}$ is rational, or if it is irr, $\left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}}$ is rat.

We have proved the existance of (a, b) without actually knowing what a and b are.

There is a school of mathematics, that rejects such proofs. It makes a stronger demand from proofs.

to show the existance of a mathematical object, with property P, we should construct it

Constructive Interpretation of Logic

Clearly, a computational development of mathematics disallows idealistic interps of disjunction. Thus we need to return to natural constructs.

Important in CS, due to its algorithmic nature:

BHK Interpretations (Brouwer, Heyting and Kolmogorov)

$\vee$ (or)

to prove $P \vee Q$, we must either have a proof of P, or a proof of Q.

$\wedge$ (and)

to prove $P \wedge Q$, we must either have a proof of P, and a proof of Q.

$\Rightarrow$ (implies)

a proof of $P \to Q$, is an algorithm, that converts any proof of P, into a proof of Q.

$\neg$ (not)

to prove, $\neg P$, we show P implies $0 = 1$

$\exists$ (there exists)

to prove, $\exists x\, P(x)$ we must construct an object x, and prove that $P(x)$ holds

$\forall$ (for all)

a proof of $\forall x \in S\, P(x)$, is an algorithm that, applied to any object x, and to data proving $x \in S$, proves that $P(x)$ holds.

> Atomic Propositions.
$p : A$, is a primitive / given notation

> $A \equiv A_1 \vee A_2$
- $inl(A_1) : A$, where $t : A_1$
- $inr(A_2) : A$, where $t : A_2$

> $A \equiv A_1 \wedge A_2$
- $\langle t_1, t_2 \rangle$, where $t_1 : A_1$
$t_2 : A$

> $A \equiv A_1 \rightarrow A_2$
- $t : A$, where t is a fn st. for any input $c : A_1$, $t(c_1) : A_2$

> There is no construction for $\perp$.

BHK Interpretation

In constructive maths, a proof is a (semantically meaningful) construction.

BHK interpretation for propositions

$$C : A \quad (C \text{ is a construction for } A)$$

by induction on A

1. $\boxed{\text{If } A \text{ is atomic then } C : A \text{ is primitive or given}}$

2. $A \equiv A_1 \wedge A_2$

   $C : A_1 \wedge A_2$

   if $C \equiv \langle C_1, C_2 \rangle$ s.t. $C_1 : A_1$ & $C_2 : A_2$.

3. $A \equiv A_1 \rightarrow A_2$

   $C : A$ where C is a construction that converts any construction of A_1 to a construction of A_2

4. $A \equiv A_1 \vee A_2$

$C : A_1 \vee A_2$

then $C \equiv \langle 0, c_1 \rangle$ where $c_1 : A_1$

or $C \equiv \langle n, c_2 \rangle$ where $c_2 : A_2$, $n \neq 0$.

5. $A \equiv \perp$

there is no $C : \perp$.

<u>Examples</u>

1. $A \rightarrow A \vee B$

$C : A \rightarrow A \vee B$

$C(a) = \langle 0, a \rangle$

2. $A \rightarrow \neg\neg A$

$C : A \rightarrow (\neg A \rightarrow \perp)$

$[C(a)](b) : \perp$

(where $a : A$, $b : A \rightarrow \perp$)

$[C(a)](b) = b(a)$

$C \equiv \lambda a . \lambda b . b(a)$

why was the proof of our lemma not constructive?

$(\sqrt{2})^{\sqrt{2}}$ is rational or

$((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}}$ is irrational.

$$\frac{\underbrace{A \vee \neg A}_{\text{law of excluded middle led to non-constructive}} \qquad A \vdash \ldots \qquad \neg A \vdash \ldots}{}$$

Constructive reasoning rejects law of excluded middle.

(consequently also, the "proof by contradiction principle")

Exercises

1 Try to give a construction for $\neg\neg A \to A$ $(\equiv (\neg A \to \bot) \to A)$

or $A \vee \neg A$ and see why it fails.