# My 10 Years of Computer Verified Mathematics

or How I Learned to Stop Worrying and Love Constructive Mathematics

Russell O’Connor
(Google Canada)

2013-09-12
Humboldt-Kolleg: Proof

# The Logic Gap

- Conventional Wisdom:
  - Constructive Mathematics is less powerful that Classical Mathematics
    - Constructive Mathematics is a subset of Classical Mathematics
  - Computer Science is a sub-discipline of Mathematics.

# The Logic Gap

- A Truth:
  - Constructive Mathematics is more powerful than Classical Mathematics.
    - Constructive Mathematics is an extension of Classical Mathematics.
  - Classical Mathematics is a sub-discipline of Computer Science.

# Abridged CV

- B. Math in Computer Science and Pure Mathematics
- PhD
  - Formal proof of Gödel-Rosser 1st incompleteness theorem in Coq
  - Developments in Constructive Analysis in Coq
- Post-Doc
  - Primitive Element Theorem in Coq
  - Fundamental Theorem of Galois Theory in Coq

# Classic Deduction Theorem

- $\Gamma \cup \{\varphi\} \supseteq F \vdash \forall x.\phi$ and $x \notin FV(F)$
  - Case: $\varphi \in F$
    - $x \notin FV(\varphi)$
    - ...
    - $\Gamma \supseteq F' \vdash \varphi \Rightarrow \forall x.\phi$
  - Case: $\varphi \notin F$
    - $\Gamma \supseteq F \vdash \varphi \Rightarrow \forall x.\phi$

# Constructive Deduction Theorem

- Observation:
  - $\varphi \notin F$ is only used to conclude that $\Gamma \supseteq F$
  - Suffices to prove $\Gamma \cup \{\varphi\} \supseteq F \Rightarrow \Gamma \supseteq F + \varphi \in F$
    - Easy by induction on $F$.

# Constructive Deduction Theorem

- $\Gamma \cup \{\varphi\} \supseteq F \vdash \forall x.\phi$ and $x \notin FV(F)$
  - Case: $\varphi \in F$
    - $x \notin FV(\varphi)$
    - ...
    - $\Gamma \supseteq F' \vdash \varphi \Rightarrow \forall x.\phi$
  - Case: $\Gamma \supseteq F$
    - $\Gamma \supseteq F \vdash \varphi \Rightarrow \forall x.\phi$

# Constructive Arithmetic

- If a classical $\prod_2$ proposition is provable, then the corresponding constructive $\prod_2$ proposition is also provable.
- This answers the question:
  - “What would happen if you could classically prove that a theorem is provable, but not constructively?”

# An Alternative Philosophy

1. Constructive Logic is an extension of Classical Logic.
2. Constructive Mathematics is (mostly) an extension of Classical Mathematics.
3. The Classical Fragment is usable in Constructive Mathematics.
4. The Classical Fragment is useful in Constructive Mathematics.
5. Constructive Mathematics is more expressive than Classical Mathematics

# Classical Logic

- Take $\forall$, $\Rightarrow$, $\wedge$, $\top$, $\bot$ as primitives
  - with their natural deduction rules.
- Define $\exists$, $\vee$, $\neg$ by their classical definitions.
- $A \vee \neg A$ is easy to prove.

# Classical Arithmetic

- Add $\mathbb{N}$ and induction
  - with some functions, e.g. primitive recursive
- Add $=_{\mathbb{N}}$
  - We can prove equality is Double Negation Stable (DNS) by induction.
- Every sentence is DNS by induction on formulas.
  - Because every connective (so far) preserves DNS.

# Constructive “Logic”

- Add connectives Σ, +
  - with their natural deduction rules.
  - These connectives do not preserve DNS.
- It is important to use distinct symbols for the classical and constructive existential quantifier and disjunction.
- Define a classical proposition / predicate to be one that is DNS.

# Classical Mathematics

- Add function types.
  - Hint: Just use existing implication type.
- To support subsets and quotients work with classical PERs
  - A classical PER is a carrier type, a classical binary relation, and laws for symmetry and transitivity bundled into a dependent record.

# Classical Mathematics

- The usual definition of a classical function is a special kind of binary relation.
- Currying this definition leads to the notion of a Classical Value
  - A classical value is a classical predicate on a type which has at most one value and is classically inhabited.
    - Also can define a classical partial value.
- You now should have all you need to be able to define classical real numbers and do classical analysis and much of classical mathematics.
  - All within constructive dependent type theory.

# Classical Choice

- The Classical Axiom of Choice states
  - For every well-defined classical binary relation, R, on classical PERs X and Y, if for every $x \in X$ there exists a $y \in Y$ such that R x y, then there classically exists an $f \in X \to Y$, where $X \to Y$ is the classical PER classical function space, such that for every $x \in X$, R x (f x) holds.
  - We do not expect this to be provable.
    - This could be safely added to Observational Type Theory.

# Classical Choice

- Maxim:
  - Whenever you want to apply a theorem that depends on the axiom of choice, a choice function is available.
- Shoenfield's absoluteness theorem implies:
  - Every $\Pi^1_3$ proposition provable with choice is provable without choice.
    - I am not certain how much this applies outside ZF.

# On Radical Constructivism

- A constructivist cannot deny classical reasoning any more than a Euclidean Geometer can deny Non-Euclidean Geometry.
- One can only argue about the value of classical theorems.

# Classical Mathematics is Usable

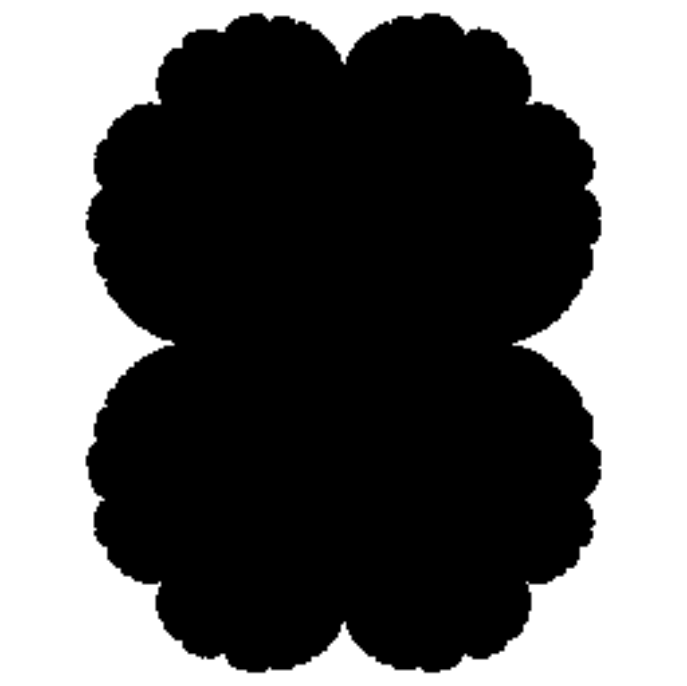
- Whenever you are trying to prove a goal which is DNS in any context, you can use classical reasoning.
  - You can split classical disjunctions.
  - You can extract classical witnesses.
- Achtung: The following statistics are made up.
  - 80% of theorems in constructive mathematics are classical (i.e. DNS).
    - e.g. anything concluding with real number equality.
  - 95% of the time you are trying to prove a goal which is DNS.

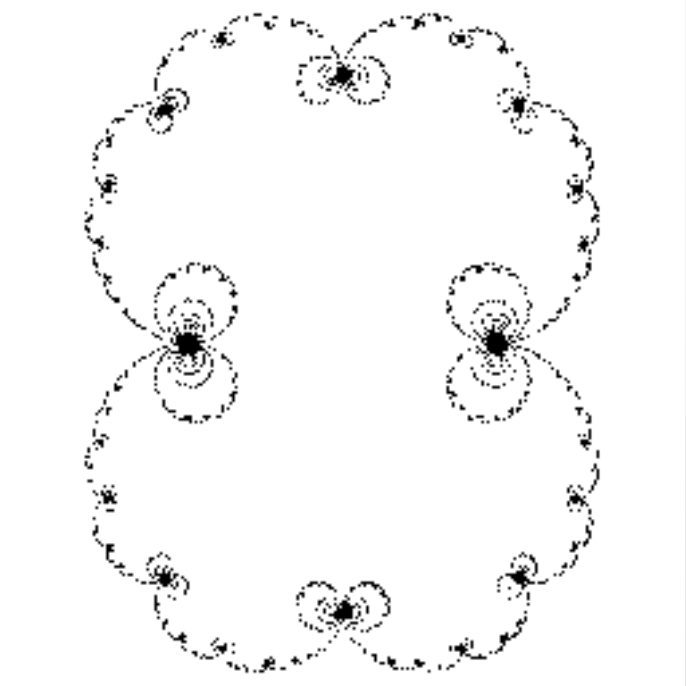
# Classical Mathematics is Useful

- The characteristic of a constructive field is a classical value.
- The degree of a constructive real-valued polynomial is a classical value.
- The Hausdorff metric predicate requires classical existence.
  - We do not want to know which points in a finite sets witness the Hausdorff distance.
  - Classical Infinite Pigeon Hole Principle used in the theory.

# Constructive Math is Expressive

- Mark Braverman showed classically that every quadratic Julia set is computable.
- There is a nice computable *c* such the Julia set is either:





# Constructive Math is Expressive

- Constructive mathematics says:
  - $\forall c:\mathbb{C}$. ($p_c$ has an attracting orbit +
    $p_c$ has a parabolic orbit +
    $p_c$ has a Siegel orbit +
    $p_c$ has a Cremer orbit +
    all orbits of $p_c$ are repelling) ⇒
    $K_c$ is Bishop compact.
- The exact knowledge needed to do the computation is clearly stated.
  - No need to mess with “uniformly computable”.

# Mathematics is Computer Science

- Types define both data structures and logical structures
- We define propositions to be types whose inhabitants are all extensionally equal.
  - Propositions-are-Types
  - Proofs are values that belong to propositions.
  - By definition, proofs are irrelevant.
- In this sense Mathematics, and in particular Classical Mathematics are just “non-informative” programs.
  - Hence Mathematics is a sub-disciple of Programming.

# Mathematics is Computer Science

- The constructive “logical” connectives Σ, + do not form propositions except under unusual inputs.
  - These are data structures.
- Constructive Mathematics is Programming.
  - Programs are not extracted from proofs
  - “Constructive proofs” were actually programs to begin with.

# 21st Century Phil. of Mathematics

- Fully formalized mathematics is not only practical, but it is currently practiced.
- The Four Colour Theorem's proof is more reliable than most mathematical results
- The details of the proof need not be "surveyed" any more than a software developer need survey her programs by executing them by hand.
  - It suffices that there exists a program that does the case analysis and there is a proof that the program performs correctly.

# 21st Century Phil. of Mathematics

- Do mathematical values “exist”?

# 21st Century Phil. of Mathematics

- Do mathematical values “exist”?
- Same answer as: Does software exist?

# 21st Century Phil. of Mathematics

- Do mathematical values “exist”?
- Same answer as: Does software exist?
- The answer is: Yes.

# The Future to Come

My ~~prediction~~ of the future.

# The Future to Come

My vision of the future.

# The Future to Come

- Formalized constructive mathematics is the most common form of mathematical reasoning.
- Dependently typed programming is the dominant software paradigm.
  - Dependently typed languages are accessible by many software developers today.
  - Software developers desperately want to enforce invariants of their software.
- There are more programmers than mathematicians.

# Not your mother's mathematics

- Your typical computer science curriculum includes:
  - Your favourite dependently typed language.
  - Monoids, Semirings, Dioids, Kleene Algebras.
  - Monads, Comonads, Algebras, Coalgebras, Applicative Functors, Traversable Functors.
  - Scott Topology.
    - Typically not Hausdorff.

# Classical Mathematicians

- Most Mathematicians won’t be converted to Constructivism.
- Instead they will simply be replaced by young Constructivists.

# Personal Example

- Recently I have been working on Functional References.

# Personal Example

- Recently I have been working on Functional References.
- I solved an open problem to demonstrate that every traversable functor is a finitary container.

# Personal Example

- Recently I have been working on Functional References.
- I solved an open problem to demonstrate that every traversable functor is a finitary container.
- What does a formalist do when he solves an open problem?

# Personal Example

- Recently I have been working on Functional References.
- I solved an open problem to demonstrate that every traversable functor is a finitary container.
- What does a formalist do when he solves an open problem?
- I proved the result in Coq.
  - It only took about two weekends.