# The weird and wonderful world of constructive mathematics

Anti

Mathcamp 2017

# 1. Down the rabbit hole

# A puzzle

### Question

Does there exist a computer program that is guaranteed to terminate in a finite amount of time, and will print “Yes” if there is intelligent life elsewhere in the universe and “No” if there is not?

# A puzzle

### Question

Does there exist a computer program that is guaranteed to terminate in a finite amount of time, and will print “Yes” if there is intelligent life elsewhere in the universe and “No” if there is not?

### Answer

Yes, there is.

- If there is intelligent life elsewhere in the universe, then the program is

  ```
  print "Yes".
  ```

- If not, the program is

  ```
  print "No".
  ```

# Two responses

1. Haha, that’s clever.

# Two responses

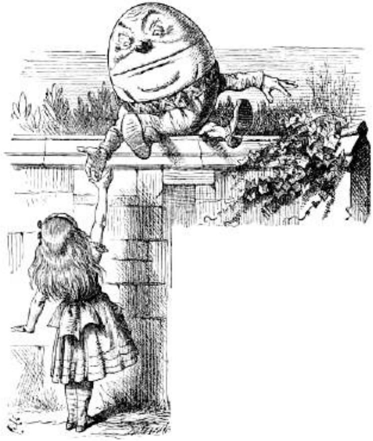
1. Haha, that’s clever.
2. NO! That’s WRONG!

# More of the same

## A joke

The math department at USD, where I work, is on the ground floor of Serra Hall, which is laid out as “a maze of twisty little passages, all alike.” One day a lost visitor poked his head into an office and said “Excuse me, is there a way out of this maze?” The math professor in the office looked up and replied “Yes.”

# Does it have to be that way?



"When *I* use a word," Humpty Dumpty said, in rather a scornful tone, "it means just what I choose it to mean—neither more nor less."

"The question is," said Alice, "whether you can make words mean so many different things."

"The question is," said Humpty Dumpty, "which is to be master—that's all."

In mathematics, *we make the rules!* In particular, we decide what words mean. If we don't like something, we can define it away.

# Constructive proofs

## The anathema

- If there is intelligent life elsewhere in the universe, then the program is

  ```
  print "Yes".
  ```

- If not, the program is

  ```
  print "No".
  ```

We will change logic so that this no longer counts as a proof.

# Constructive proofs

### The anathema

- If there is intelligent life elsewhere in the universe, then the program is

  ```
  print "Yes".
  ```

- If not, the program is

  ```
  print "No".
  ```

We will change logic so that this no longer counts as a proof.

### “Definition”

- A constructive proof of existence is one that actually tells you how to find the object being claimed to exist.
- A non-constructive proof is one that doesn’t.

# Non-constructive proofs

Non-constructivity comes from. . .

1. The axiom of choice.
   So if you know what that is, pretend you don't.
2. More importantly: the law of excluded middle:

   *Every statement is either true or false.*

   This was our problem; we silently assumed that

   *Either there is intelligent life somewhere*
   *else in the universe, or there isn't.*

# Non-constructive proofs

Non-constructivity comes from. . .

1. The axiom of choice.
   So if you know what that is, pretend you don't.
2. More importantly: the law of excluded middle:

   *Every statement is either true or false.*

   This was our problem; we silently assumed that

   *Either there is intelligent life somewhere*
   *else in the universe, or there isn't.*

**Mathcamp T-shirt slogan, 1993–2002**

A mathematician is cautious in the presence of the obvious.

# On freedom

## Mathcamp T-shirt slogan, 2003

"In mathematics, existence is freedom from contradiction."

– David Hilbert

# On freedom

### Mathcamp T-shirt slogan, 2003

"In mathematics, existence is freedom from contradiction."

– David Hilbert

### On the other hand

"None are more hopelessly enslaved than
those who falsely believe they are free."

– Johann Wolfgang von Goethe

# Moving forward

**Mathcamp T-shirt slogan, 2004–present**

Out of nothing I have constructed a strange new universe.

– János Bolyai

# Moving forward

### Mathcamp T-shirt slogan, 2004–present

Out of nothing I have constructed a strange new universe.

– János Bolyai

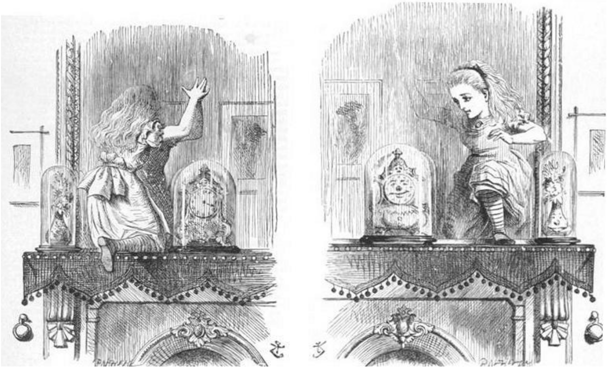
### In our case

We have to learn to do mathematics entirely without the law of excluded middle!

# What

You must unlearn what you have learned!

# 2. Looking-glass logic



# What is a proof?

What is a “proof” anyway?

### “Definition”

“I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description, and perhaps I could never succeed in intelligibly doing so. But I know it when I see it.”

– Supreme Court Justice Potter Stewart, *Jacobellis v. Ohio*

# What is a proof?

Put differently:

**“Definition”**

A proof is an argument that convinces other mathematicians.

Pros:

- Describes the way proofs are used in practice.
- Doesn’t require us to do any work.

Cons:

- Doesn’t help us teach a computer what a proof is.
- Doesn’t help us invent a new “notion of proof”.

# What is a proof? Take 2

**Definition**

A proof is a deduction from hypotheses to conclusion in which each step is justified by one of a finite list of rules of inference.

Pros:

- Can program the rules of inference into a computer.
- To describe a new notion of proof, just specify the rules of inference.

Cons:

- Most “real-world” proofs are at a much higher level than the rules of inference. (This is an “assembly language” description of proofs.)

Humans use the rules of inference as a guide to learn what kinds of arguments are valid.

# Rules of inference

Most rules of inference fall into two groups:

1. A way to prove a statement of a particular form.
2. A way to use a known statement of a particular form.

For example:

- To prove “if P then Q”, assume P and prove Q under that hypothetical assumption.
- If we know “if P then Q”, and we also know P, then we can conclude Q.
- To prove “P and Q”, prove P and also prove Q.
- If we know that “P and Q”, then we know P and we also know Q.

“Proof by induction” is another kind of rule of inference.

# Rules of constructive logic

Most of the rules of constructive logic are familiar. The important ones are those involving "or":

### Rules for "or"

- To prove "P or Q", it suffices to prove P.
- To prove "P or Q", it suffices to prove Q.
- If we know that "P or Q", then we can divide any proof into "Case 1: Assume P" and "Case 2: Assume Q".

# Rules of constructive logic

Most of the rules of constructive logic are familiar. The important ones are those involving “or”:

## Rules for “or”

- To prove “P or Q”, it suffices to prove P.
- To prove “P or Q”, it suffices to prove Q.
- If we know that “P or Q”, then we can divide any proof into “Case 1: Assume P” and “Case 2: Assume Q”.

In “classical” (non-constructive) mathematics, there is an additional “excluded middle” rule

- For any P, we can conclude “P or not P”.

To get constructive mathematics, we just leave this out.
In particular, every constructive proof is also a classical proof.

# Some theorems can be made constructive

## Theorem

*There exist irrational numbers $\alpha, \beta$ such that $\alpha^\beta$ is rational.*

## Non-constructive proof.

The number $\sqrt{2}^{\sqrt{2}}$ must be either irrational or rational.
(N.B. “irrational” means “not rational”.)

- If $\sqrt{2}^{\sqrt{2}}$ is rational, take $\alpha = \beta = \sqrt{2}$.
- If $\sqrt{2}^{\sqrt{2}}$ is irrational, take $\alpha = \sqrt{2}^{\sqrt{2}}$ and $\beta = \sqrt{2}$.

$$\alpha^\beta = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2.$$

□

# Some theorems can be made constructive

## Theorem

*There exist irrational numbers $\alpha, \beta$ such that $\alpha^\beta$ is rational.*

## Non-constructive proof.

The number $\sqrt{2}^{\sqrt{2}}$ must be ~~either irrational or rational.~~
(N.B. “irrational” means “not rational”.)

- If $\sqrt{2}^{\sqrt{2}}$ is rational, take $\alpha = \beta = \sqrt{2}$.
- If $\sqrt{2}^{\sqrt{2}}$ is irrational, take $\alpha = \sqrt{2}^{\sqrt{2}}$ and $\beta = \sqrt{2}$.

$$\alpha^\beta = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2.$$

□

# Some theorems can be made constructive

## Theorem

*There exist irrational numbers $\alpha, \beta$ such that $\alpha^\beta$ is rational.*

## Constructive proof.

Let $\alpha = \sqrt{3}$ and $\beta = \log_3(4)$. Then

$$\alpha^\beta = \sqrt{3}^{\log_3(4)} = 3^{\frac{1}{2}\log_3(4)} = 3^{\log_3(2)} = 2.$$

It is easy to show that $\alpha$ and $\beta$ are both irrational. □

# Excluded middle is sometimes fine

We can sometimes use excluded middle; we just can't assume it without proving it.

**Theorem**

*Every natural number is either equal to zero or not equal to zero.*

**Constructive proof.**

By induction.

- If $n = 0$, then $n = 0$.
- Assume inductively that either $n = 0$ or $n \neq 0$.
  In either case, $n + 1 \neq 0$.

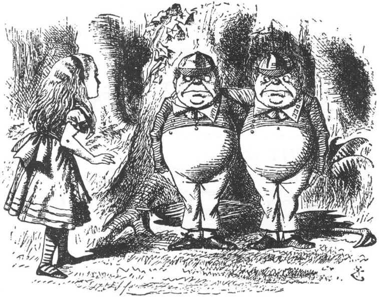
Thus, by induction, for all natural numbers $n$, either $n = 0$ or $n \neq 0$. □

# Arithmetic and algebra are familiar

Other facts we can prove constructively by induction:

1. Any two integers are either equal or not equal.
2. Any integer is either odd or even.
3. Any two rational numbers are either equal or not equal.
4. For rational numbers $x, y$, either $x < y$ or $x = y$ or $x > y$.
5. For any two integers $a, b$, either $a$ divides $b$ or not.
6. Any integer $n \geq 2$ is either prime or composite.

# What about proof by contradiction?



"Contrariwise," continued Tweedledee, "if it was so, it might be; and if it were so, it would be; but as it isn't, it ain't. That's logic."

"*Reductio ad absurdum*, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game."

# What is proof by contradiction anyway?

Proof by contradiction is informally used to refer to two different rules of inference:

- To prove P, it suffices to assume “not P” and derive a contradiction.
- To prove “not P”, it suffices to assume P and derive a contradiction.

# What is proof by contradiction anyway?

Proof by contradiction is informally used to refer to two different rules of inference:

- ~~To prove P, it suffices to assume “not P” and derive a contradiction.~~

  This one is equivalent to excluded middle.

- To prove “not P”, it suffices to assume P and derive a contradiction.

  This one is fine constructively! It’s the basic “prove” rule associated to “not” statements.

Classically, “P is true” is the same as “not-P is false”. Constructively, claims of falsity have a qualitatively different status from claims of truth.

# Proof of negation by contradiction

## Theorem

5 is prime.

## Constructive proof.

Suppose that $5 = ab$ where $0 < a < 5$ and $0 < b < 5$ are integers. Then $a = 1, 2, 3$, or 4.

- If $a = 1$, then $b = 5$, which is not $< 5$, a contradiction.
- If $a = 2$, then $b = \frac{5}{2}$, which is not an integer, a contradiction.
- If $a = 3$, then $b = \frac{5}{3}$, which is not an integer, a contradiction.
- If $a = 4$, then $b = \frac{5}{4}$, which is not an integer, a contradiction.

Thus, 5 can not be written as the product of two smaller positive integers. Hence, by definition, 5 is prime. □

# Some proofs by contradiction aren't really

## Theorem

*Every integer $n \geq 2$ can be written as a product of primes.*

## Non-constructive proof.

Suppose for contradiction that there is an $n \geq 2$ that cannot be so written. Without loss of generality, let $n$ be the smallest such counterexample.

- If $n$ is prime, then $n = n$ is a product of one prime, a contradiction.
- If $n$ is composite, then $n = ab$ with $a, b < n$, so they can be written as products of primes. Hence $n = ab$ is also a product of primes, a contradiction.

□

# Some proofs by contradiction aren't really

### Theorem

*Every integer $n \geq 2$ can be written as a product of primes.*

### Non-constructive proof.

~~Suppose for contradiction~~ that there is an $n \geq 2$ that cannot be so written. Without loss of generality, let $n$ be the smallest such counterexample.

- If $n$ is prime, then $n = n$ is a product of one prime, a contradiction.
- If $n$ is composite, then $n = ab$ with $a, b < n$, so they can be written as products of primes. Hence $n = ab$ is also a product of primes, a contradiction.

□

# Some proofs by contradiction aren't really

**Theorem**

*Every integer $n \geq 2$ can be written as a product of primes.*

**Constructive proof.**

By strong induction, we may assume that for any $2 \leq k < n$ we can write $k$ as a product of primes.

- If $n$ is prime, then $n = n$ is a product of one prime.
- If $n$ is composite, then $n = ab$ with $a, b < n$, so they can be written as products of primes. Hence $n = ab$ is also a product of primes.

□

Constructive logic encourages better "proof hygiene".

# Some proofs by contradiction really are

## “Theorem”

*For any real numbers $x, y$, either $x < y$ or $x = y$ or $x > y$.*

## Non-constructive proof.

Suppose not, so that $x \not< y$ and $x \neq y$ and $x \not> y$. Starting at the left, compare the decimal expansions[†] of $x$ and $y$ digit-by-digit until they differ (if ever).

- Since $x \not< y$, at the first point of difference, the digit of $x$ is not smaller.
- Since $x \not> y$, at the first point of difference, the digit of $x$ is not bigger.
- Since of two *different* digits one must be bigger, there can be no first point of difference. Hence $x = y$, contradicting our assumption that $x \neq y$.

[†] Technically we have to use Cauchy sequences. □

# Some proofs by contradiction really are

### “Theorem”

*For any real numbers $x, y$, either $x < y$ or $x = y$ or $x > y$.*

### Non-constructive proof.

~~Suppose not,~~ so that $x \not< y$ and $x \neq y$ and $x \not> y$. Starting at the left, compare the decimal expansions[†] of $x$ and $y$ digit-by-digit until they differ (if ever).

- Since $x \not< y$, at the first point of difference, the digit of $x$ is not smaller.
- Since $x \not> y$, at the first point of difference, the digit of $x$ is not bigger.
- Since of two *different* digits one must be bigger, there can be no first point of difference. Hence $x = y$, contradicting our assumption that $x \neq y$.

[†] Technically we have to use Cauchy sequences.

□

# Some proofs by contradiction really are

**“Theorem”**

*For any real numbers $x, y$, either $x < y$ or $x = y$ or $x > y$.*

This theorem has no constructive proof!

# A weak counterexample

$$z_n = \begin{cases} 1 & \text{if a string of one billion nines in the decimal expansion of } \pi \text{ starts at the } n^{\mathrm{th}} \text{ place.} \\ 0 & \text{otherwise.} \end{cases}$$

$$z = \sum_{n=0}^{\infty} (-1)^n \frac{z_n}{2^n}.$$

This is well-defined constructively, since we can compute it to arbitrary precision.

- $z = 0$ iff there is no string of one billion nines in $\pi$,
- $z > 0$ iff the first such string starts at an even place,
- $z < 0$ iff the first such string starts at an odd place.

So if we could prove "either $z < 0$ or $z = 0$ or $z > 0$" constructively, we could decide whether the first string of one billion nines in $\pi$ starts at an even or an odd place.

I have a feeling we're not in Kansas anymore.

# What is truth?

There are (at least) two ways to wrap your head around this.

1. Continue to believe that every real number "really" is either positive, negative, or zero. We just can't give a *constructive* proof of this because we have no method to tell which is the case in general.
2. Start to believe that in the "world of constructive mathematics" it really *isn't* true that every real number is either positive, negative, or zero.

The first is the easiest. But (as we will see) the more constructive math you do, the harder it is to avoid the second.

# Plus, it's not that big a deal

### Theorem

*For any real numbers $x, y$, if $x \not< y$ and $x \not> y$, then $x = y$.*

### Constructive proof.

Suppose $x \not< y$ and $x \not> y$, and compare the decimal expansions[†] of $x$ and $y$ digit-by-digit until they differ (if ever).

- Since $x \not< y$, at the first point of difference, the digit of $x$ is not smaller.
- Since $x \not> y$, at the first point of difference, the digit of $x$ is not bigger.
- Since of two different digits one must be bigger, there can be no first point of difference. Hence $x = y$.

□

# It's not that big a deal, part 2

### Theorem

*For any real numbers $x, y$ and positive integer $n$, either $x < y + \frac{1}{n}$ or $x > y - \frac{1}{n}$.*

### Constructive proof.

Let $k$ be such that $10^k > n$, and let $x_k$ and $y_k$ be the decimal expansions$^\dagger$ of $x$ and $y$ out to the $k^{\text{th}}$ decimal place. These are *rational* numbers, so either $x_k < y_k$ or $x_k = y_k$ or $x_k > y_k$.

- If $x_k < y_k$, then $x < y + \frac{1}{n}$.
- If $x_k = y_k$, then both $x < y + \frac{1}{n}$ and $x > y - \frac{1}{n}$.
- If $x_k > y_k$, then $x > y - \frac{1}{n}$.

□

# Calculus is a little weird

Other classical theorems that we can't prove constructively:

- For any real numbers $x, y$, either $x = y$ or $x \neq y$.
- If $x \neq y$, then $x < y$ or $x > y$.
- For any real numbers $x, y$, either $x \leq y$ or $x \geq y$.
- If $x \neq 0$, then $1/x$ exists.
- If $x \neq y$ is false, then $x = y$.
- The Intermediate Value Theorem (IVT).
- The Extreme Value Theorem (EVT).

# Calculus is a little weird

Other classical theorems that we can't prove constructively:

- For any real numbers $x, y$, either $x = y$ or $x \neq y$.
- If $x \neq y$, then $x < y$ or $x > y$.
- For any real numbers $x, y$, either $x \leq y$ or $x \geq y$.
- If $x \neq 0$, then $1/x$ exists.
- If $x \neq y$ is false, then $x = y$.
- The Intermediate Value Theorem (IVT).
- The Extreme Value Theorem (EVT).

But we can prove that

- If $x > 0$ or $x < 0$, then $1/x$ exists.
- IVT holds for any differentiable function whose derivative is bounded away from 0.
- IVT holds "approximately" for any continuous function.

With sufficient care, we can develop all of calculus constructively.

# Set theory is very weird

Let $P$ be any statement, and consider the set

$$A = \{\, 0 \mid P \text{ is true} \,\}.$$

### Theorem

*If $A$ is finite, then $P$ is either true or false.*

### Proof.

If $A$ is finite, then its cardinality is a natural number $|A|$.

- If $|A| = 0$, then $A = \emptyset$, hence $0 \notin A$ and so $P$ is false.
- if $|A| \neq 0$, we must have $0 \in A$ and so $P$ is true.

□

# Set theory is very weird

Let $P$ be any statement, and consider the set

$$A = \{\, 0 \mid P \text{ is true} \,\}.$$

**Theorem**

*If $A$ is finite, then $P$ is either true or false.*

- Thus, we cannot prove constructively that $A$ is always finite for any $P$.
- Note that $A$ is a subset of the finite set $\{0\}$. Thus, we cannot prove that every subset of a finite set is finite!

# Set theory is very weird

Let $P$ be any statement, and consider the set

$$A = \{\, 0 \mid P \text{ is true} \,\}.$$

But. . .

## Theorem

*$A$ is not infinite.*

## Proof.

Suppose $A$ were infinite, i.e. not finite. Then $|A| \neq 1$, so $P$ is not true, i.e. $P$ is false. But also $|A| \neq 0$, so $P$ is not false either. Since $P$ can't be both false and not false, this is a contradiction. □

# 3. Impossible things

"I can't believe *that*!" said Alice.

"Can't you?" the Queen said in a pitying tone. "Try again: draw a long breath, and shut your eyes."

Alice laughed. "There's no use trying," she said "one can't believe impossible things."

"I daresay you haven't had much practice," said the Queen. "When I was your age, I always did it for half-an-hour a day. Why, sometimes I've believed as many as six impossible things before breakfast."

# Calculus can be very weird too

**Fact**

In constructive mathematics, every function is continuous!

The usual example of a discontinuous function

$$f(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases}$$

is not well-defined everywhere: we can't say that every real number is either $\geq 0$ or $< 0$.

# Wait a minute

Every constructive proof is also a classical proof! So

“Every function is continuous”

is not a constructive theorem — even though every *particular* function we can *define* constructively *is* continuous.

# Wait a minute

Every constructive proof is also a classical proof! So

“Every function is continuous”

is not a constructive theorem — even though every *particular* function we can *define* constructively *is* continuous.

But because of this, in constructive mathematics we can *consistently* take

“Every function is continuous”

as an axiom!

# Computability

### Another fact

In constructive mathematics, every function is computable!

- In other words, anything we can *define* can be *computed* by an algorithm.
- This has to be understood in the same way as continuity: it's not a theorem, but can consistently be taken as an axiom.
- This is reassuring: it means our "constructive proofs" really are constructive in the intuitive sense.
- Exercise: if you know an example of a noncomputable function, look and see where it uses excluded middle.

# Infinitesimal calculus

“And what are these [infinitesimals]? The Velocities of evanescent Increments? And what are these same evanescent Increments? They are neither finite Quantities nor Quantities infinitely small, nor yet nothing. May we not call them the ghosts of departed quantities?”

– Berkeley, *The Analyst: a discourse addressed to an infidel mathematician*

# Infinitesimal calculus

- In constructive mathematics, there can also be numbers[†] $d$ such that $d^2 = 0$ but not necessarily $d = 0$.
- Any such $d$ will necessarily be not unequal to 0.
- We can't divide by them, but we can consistently assume

  If $a \cdot d = b \cdot d$ for *all* $d$ such that $d^2 = 0$, then $a = b$.
- Now we can define $f'(x)$ to be the unique number such that

  $$f(x+d) = f(x) + f'(x) \cdot d$$

  for all $d$ such that $d^2 = 0$.

For example, if $f(x) = x^2$, then

$$\begin{aligned} f(x+d) &= (x+d)^2 \\ &= x^2 + 2x \cdot d + d^2 \qquad \Longrightarrow \qquad f'(x) = 2x. \\ &= x^2 + 2x \cdot d \end{aligned}$$

[†] Well, not *real* numbers.

# What is truth? Take 2

## Conclusion

Using constructive logic not only ensures our proofs are constructive; it gives us axiomatic freedom: we can assume powerful axioms that would classically be inconsistent.

- This places us firmly on the side of viewing constructive logic as a "strange new universe", rather than just a refined notion of proof for ordinary mathematics.
- This can be made precise by constructing *models* of constructive logic, with new nonclassical axioms, inside classical logic.

# Congratulations

You've taken your first step into a larger world.