COMP 761: Lecture 4 – Contradiction

David Rolnick

September 11, 2020

Problem

An infinite set of numbers is said to be *countable* if you can list them all. For example, the positive integers are countable:

$$1, 2, 3, 4, \ldots$$

So are all the integers:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

Are the real numbers countable? Why or why not?

Course Announcements

Problem sets - what math can you use?

Course Announcements

Problem sets - what math can you use?

- Any method of proof is fine

Course Announcements

Problem sets - what math can you use?

- Any method of proof is fine
- Don’t cite existing theorems if they make the problem really easy

Course Announcements

Problem sets - what math can you use?

- Any method of proof is fine
- Don't cite existing theorems if they make the problem really easy
- If you aren't certain, ask me or just reprove the theorem

Course Announcements

Problem sets - what math can you use?

- Any method of proof is fine
- Don't cite existing theorems if they make the problem really easy
- If you aren't certain, ask me or just reprove the theorem
- Problem Set 1 shouldn't require any previous results more than just intuition

Course Announcements

Problem sets - what math can you use?

- Any method of proof is fine
- Don't cite existing theorems if they make the problem really easy
- If you aren't certain, ask me or just reprove the theorem
- Problem Set 1 shouldn't require any previous results more than just intuition
- If you get stuck, talk to your classmates (on Slack)!

Course Announcements

Problem sets - what math can you use?

- Any method of proof is fine
- Don't cite existing theorems if they make the problem really easy
- If you aren't certain, ask me or just reprove the theorem
- Problem Set 1 shouldn't require any previous results more than just intuition
- If you get stuck, talk to your classmates (on Slack)!
- Also, office hours (mine are Mon 5pm and Fri 10am, Vincent's are Thu 10:30)

Proof by contradiction

Proof by contradiction

- Suppose that what you want to prove is not true.

Proof by contradiction

- Suppose that what you want to prove is not true.
- Show that this would result in something wrong.

Proof by contradiction

- Suppose that what you want to prove is not true.
- Show that this would result in something wrong.
- Conclude that the thing you want is actually true.

Intro problem

Prove that there are infinitely many prime numbers.

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.
- We want to show that there is some prime that isn't in our list.

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.
- We want to show that there is some prime that isn't in our list.
- One way to do that: look at the product $p_1 p_2 \cdots p_n$.

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.
- We want to show that there is some prime that isn't in our list.
- One way to do that: look at the product $p_1 p_2 \cdots p_n$.
- We know it's divisible by all the primes.

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.
- We want to show that there is some prime that isn't in our list.
- One way to do that: look at the product $p_1 p_2 \cdots p_n$.
- We know it's divisible by all the primes.
- That means

$$p_1 p_2 \cdots p_n + 1$$

  is not divisible by any of them.

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.
- We want to show that there is some prime that isn't in our list.
- One way to do that: look at the product $p_1 p_2 \cdots p_n$.
- We know it's divisible by all the primes.
- That means

$$p_1 p_2 \cdots p_n + 1$$

  is not divisible by any of them.
- So what?

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.
- We want to show that there is some prime that isn't in our list.
- One way to do that: look at the product $p_1 p_2 \cdots p_n$.
- We know it's divisible by all the primes.
- That means

$$p_1 p_2 \cdots p_n + 1$$

  is not divisible by any of them.
- So what?
- So it's divisible by some prime that is not on our list (it might be prime itself).

Intro problem

Prove that there are infinitely many prime numbers.

- What if there were only finitely many prime numbers?
- Then we could list them all: $p_1, p_2, \ldots, p_n$.
- We want to show that there is some prime that isn't in our list.
- One way to do that: look at the product $p_1 p_2 \cdots p_n$.
- We know it's divisible by all the primes.
- That means

$$p_1 p_2 \cdots p_n + 1$$

  is not divisible by any of them.
- So what?
- So it's divisible by some prime that is not on our list (it might be prime itself).
- Contradiction!

Formal proof

Formal proof

Suppose towards contradiction that there are only finitely many primes.

Formal proof

Suppose towards contradiction that there are only finitely many primes. Let them be denoted $p_1, p_2, \ldots, p_n$.

Formal proof

Suppose towards contradiction that there are only finitely many primes. Let them be denoted $p_1, p_2, \ldots, p_n$. Then, let

$$x = p_1 p_2 \cdots p_n + 1.$$

Formal proof

Suppose towards contradiction that there are only finitely many primes. Let them be denoted $p_1, p_2, \ldots, p_n$. Then, let

$$x = p_1 p_2 \cdots p_n + 1.$$

Since $x - 1$ is divisible by every prime in our list, x cannot be divisible by any of them.

Formal proof

Suppose towards contradiction that there are only finitely many primes. Let them be denoted $p_1, p_2, \ldots, p_n$. Then, let

$$x = p_1 p_2 \cdots p_n + 1.$$

Since $x - 1$ is divisible by every prime in our list, x cannot be divisible by any of them. Therefore, x must be divisible by some prime that isn't in our list.

Formal proof

Suppose towards contradiction that there are only finitely many primes. Let them be denoted $p_1, p_2, \ldots, p_n$. Then, let

$$x = p_1 p_2 \cdots p_n + 1.$$

Since $x - 1$ is divisible by every prime in our list, x cannot be divisible by any of them. Therefore, x must be divisible by some prime that isn't in our list.

This is a contradiction, and we conclude that there are infinitely many primes. ■

When is this useful?

In general, useful when there would be some particular interesting object to consider if the claim were false.

When is this useful?

In general, useful when there would be some particular interesting object to consider if the claim were false.

- Proving that something doesn't exist (e.g. a largest prime number).

When is this useful?

In general, useful when there would be some particular interesting object to consider if the claim were false.

- Proving that something doesn't exist (e.g. a largest prime number).
- Proving that some property always holds.

When is this useful?

In general, useful when there would be some particular interesting object to consider if the claim were false.

- Proving that something doesn't exist (e.g. a largest prime number).
- Proving that some property always holds.
- A lot of other situations...

Preamble: Countability

An infinite set of numbers is said to be *countable* if you can list them all. For example, the set $\mathbb{Z}^+$ of positive integers is countable:

$$1, 2, 3, 4, \ldots$$

So is the set $\mathbb{Z}$ of all integers:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

Preamble: Countability

An infinite set of numbers is said to be *countable* if you can list them all. For example, the set $\mathbb{Z}^+$ of positive integers is countable:

$$1, 2, 3, 4, \ldots$$

So is the set $\mathbb{Z}$ of all integers:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

Warmup: Are the positive even integers countable?

Preamble: Countability

An infinite set of numbers is said to be *countable* if you can list them all. For example, the set $\mathbb{Z}^+$ of positive integers is countable:

$$1, 2, 3, 4, \ldots$$

So is the set $\mathbb{Z}$ of all integers:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

Warmup: Are the positive even integers countable?

- Yes:

$$2, 4, 6, \ldots$$

Preamble: Countability

An infinite set of numbers is said to be *countable* if you can list them all. For example, the set $\mathbb{Z}^+$ of positive integers is countable:

$$1, 2, 3, 4, \ldots$$

So is the set $\mathbb{Z}$ of all integers:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

Warmup: Are the positive even integers countable?

- Yes:

$$2, 4, 6, \ldots$$

- Note that a countable set can contain another countable set.

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

- Let's try counting them out:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

- Let's try counting them out:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

- Wait, that's just integers, where does $1/2$ go?

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

- Let's try counting them out:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

- Wait, that's just integers, where does $1/2$ go?
- It can't go after, since there is no way to be after infinitely many :)

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

- Let's try counting them out:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

- Wait, that's just integers, where does $1/2$ go?
- It can't go after, since there is no way to be after infinitely many :)
- Maybe in the middle?

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, 3, -3, \ldots$$

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

- Let's try counting them out:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

- Wait, that's just integers, where does $1/2$ go?
- It can't go after, since there is no way to be after infinitely many :)
- Maybe in the middle?

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, 3, -3, \ldots$$

- But what about $1/3$?

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{3}, 2, -2, 3, -3, \ldots$$

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

- Let's try counting them out:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

- Wait, that's just integers, where does $1/2$ go?
- It can't go after, since there is no way to be after infinitely many :)
- Maybe in the middle?

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, 3, -3, \ldots$$

- But what about $1/3$?

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{3}, 2, -2, 3, -3, \ldots$$

- Oops, then we are going to need $1/n$ for every n before 2.

The rational numbers

A *rational number* is a number that can be written as the quotient m/n of two integers m and n. Is the set $\mathbb{Q}$ of rational numbers countable?

- Let's try counting them out:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

- Wait, that's just integers, where does $1/2$ go?
- It can't go after, since there is no way to be after infinitely many :)
- Maybe in the middle?

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, 3, -3, \ldots$$

- But what about $1/3$?

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{3}, 2, -2, 3, -3, \ldots$$

- Oops, then we are going to need $1/n$ for every n before 2.
- Better way? Or does it not work?

The rational numbers

The rational numbers

- Let's just look at the positive rationals for the moment

The rational numbers

- Let's just look at the positive rationals for the moment
- Here is a way to visualize them:

$$\begin{array}{ccccccc} 1/1 & 1/2 & 1/3 & 1/4 & 1/5 & \cdots \\ 2/1 & 2/2 & 2/3 & 2/4 & 2/5 & \cdots \\ 3/1 & 3/2 & 3/3 & 3/4 & 3/5 & \cdots \\ 4/1 & 4/2 & 4/3 & 4/4 & 4/5 & \cdots \\ 5/1 & 5/2 & 5/3 & 5/4 & 5/5 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

- Is this helpful?

The rational numbers

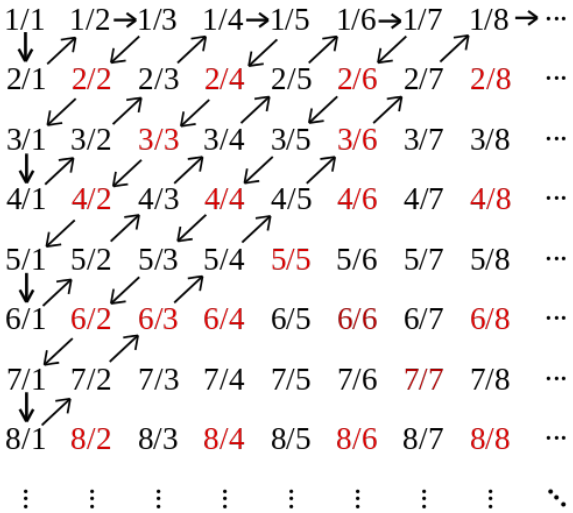
- Let's just look at the positive rationals for the moment
- Here is a way to visualize them:

$$\begin{array}{ccccccc} 1/1 & 1/2 & 1/3 & 1/4 & 1/5 & \cdots \\ 2/1 & 2/2 & 2/3 & 2/4 & 2/5 & \cdots \\ 3/1 & 3/2 & 3/3 & 3/4 & 3/5 & \cdots \\ 4/1 & 4/2 & 4/3 & 4/4 & 4/5 & \cdots \\ 5/1 & 5/2 & 5/3 & 5/4 & 5/5 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

- Is this helpful?
- We can count them all with a sort of zigzagging path

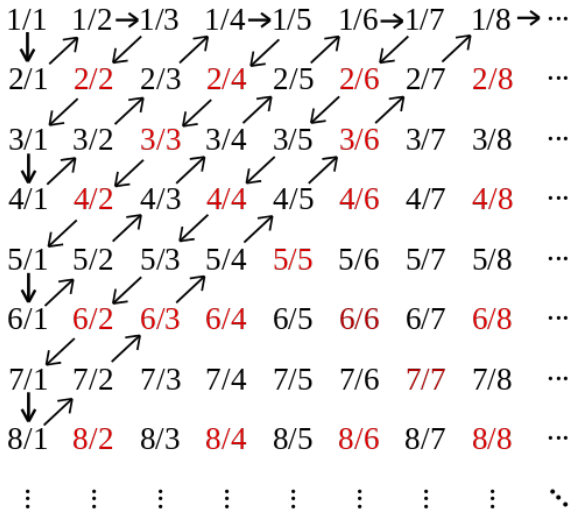
The rational numbers

- We can count them all with a sort of zigzagging path



The rational numbers

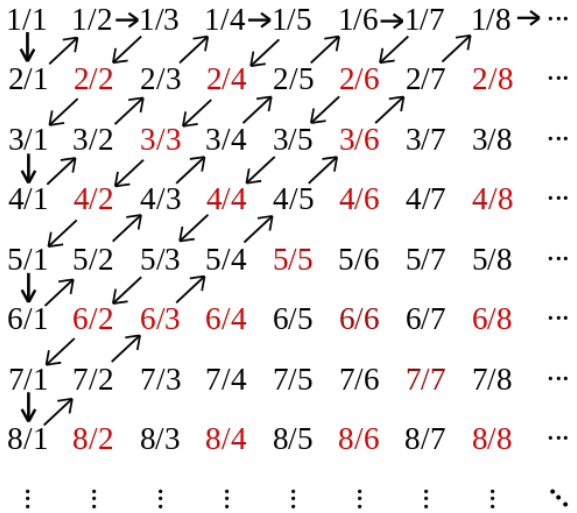
- We can count them all with a sort of zigzagging path



- Red numbers are repeats (e.g. $2/2 = 1/1$). What to do with them?

The rational numbers

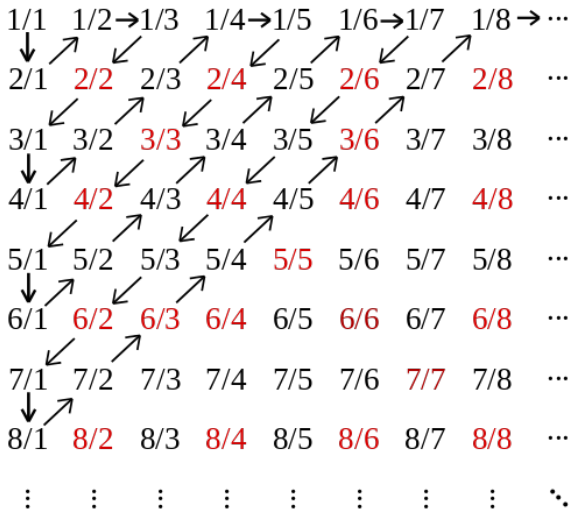
- We can count them all with a sort of zigzagging path



- Red numbers are repeats (e.g. $2/2 = 1/1$). What to do with them?
- Just skip them...

The rational numbers

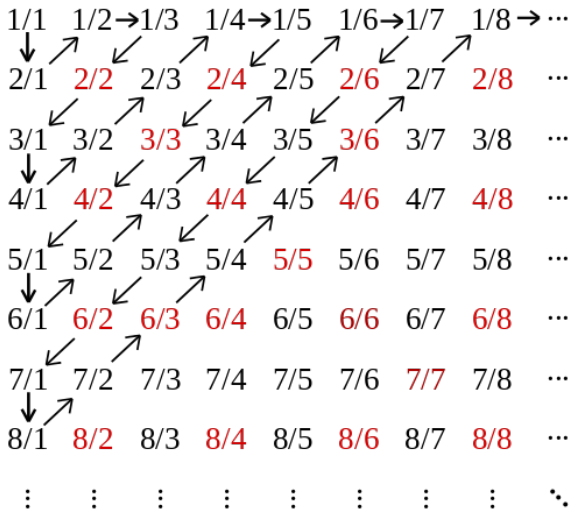
- We can count them all with a sort of zigzagging path



- Red numbers are repeats (e.g. $2/2 = 1/1$). What to do with them?
- Just skip them...
- How to do the negative rationals?

The rational numbers

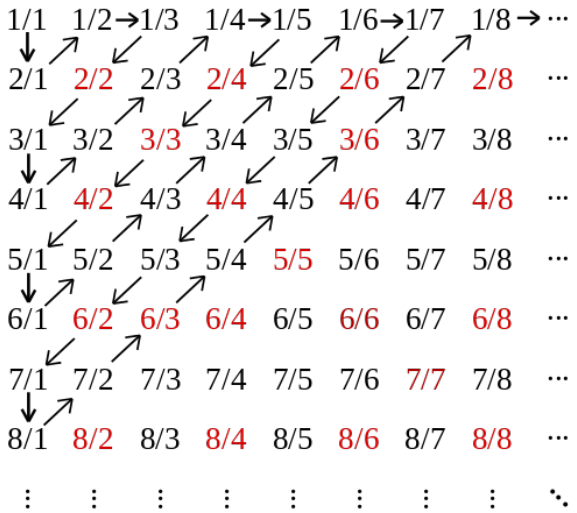
- We can count them all with a sort of zigzagging path



- Red numbers are repeats (e.g. $2/2 = 1/1$). What to do with them?
- Just skip them...
- How to do the negative rationals?
- We can alternate between positive and negative to get both

The rational numbers

- We can count them all with a sort of zigzagging path



- Red numbers are repeats (e.g. $2/2 = 1/1$). What to do with them?
- Just skip them...
- How to do the negative rationals?
- We can alternate between positive and negative to get both
- So $\mathbb{Q}$ is countable! (not a formal proof)

The real numbers

Is the set of real numbers $\mathbb{R}$ countable?

The real numbers

Is the set of real numbers $\mathbb{R}$ countable?

- This includes numbers like

$$0.185601757\ldots$$

with infinite non-repeating digits.

The real numbers

Is the set of real numbers $\mathbb{R}$ countable?

- This includes numbers like

$$0.185601757\ldots$$

  with infinite non-repeating digits.
- Thoughts?

The real numbers

Is the set of real numbers $\mathbb{R}$ countable?

- This includes numbers like

$$0.185601757\ldots$$

  with infinite non-repeating digits.
- Thoughts?
- I'm hearing a lot of "not countable"

The real numbers

Is the set of real numbers $\mathbb{R}$ countable?

- This includes numbers like

$$0.185601757\ldots$$

  with infinite non-repeating digits.
- Thoughts?
- I'm hearing a lot of "not countable"
- Let's try to prove it isn't countable – how?

The real numbers

Is the set of real numbers $\mathbb{R}$ countable?

- This includes numbers like

$$0.185601757\ldots$$

  with infinite non-repeating digits.
- Thoughts?
- I'm hearing a lot of "not countable"
- Let's try to prove it isn't countable – how?
- Well, this class is on contradiction...

The real numbers

Is the set of real numbers $\mathbb{R}$ countable?

- This includes numbers like

$$0.185601757\ldots$$

  with infinite non-repeating digits.
- Thoughts?
- I'm hearing a lot of "not countable"
- Let's try to prove it isn't countable – how?
- Well, this class is on contradiction...
- Let's actually prove something stronger, that the set $[0, 1]$ of real numbers between 0 and 1 is uncountable.

The real numbers

The real numbers

- Suppose that $[0, 1]$ is countable.

The real numbers

- Suppose that $[0, 1]$ is countable.
- That means there is a sequence $x_1, x_2, \ldots$ including all of $[0, 1]$.

The real numbers

- Suppose that $[0, 1]$ is countable.
- That means there is a sequence $x_1, x_2, \ldots$ including all of $[0, 1]$.
- We need to prove some $y \in [0, 1]$ isn't in that sequence

The real numbers

- Suppose that $[0, 1]$ is countable.
- That means there is a sequence $x_1, x_2, \ldots$ including all of $[0, 1]$.
- We need to prove some $y \in [0, 1]$ isn't in that sequence
- Since we know real numbers have infinite representations, let's write that out:

$$
\begin{aligned}
x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\cdots \\
x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\cdots \\
x_3 &= 0.x_{31}x_{32}x_{33}x_{34}\cdots \\
&\vdots
\end{aligned}
$$

(those x_{ij} are digits)

The real numbers

- Suppose that $[0, 1]$ is countable.
- That means there is a sequence $x_1, x_2, \ldots$ including all of $[0, 1]$.
- We need to prove some $y \in [0, 1]$ isn't in that sequence
- Since we know real numbers have infinite representations, let's write that out:

$$
\begin{aligned}
x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\cdots \\
x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\cdots \\
x_3 &= 0.x_{31}x_{32}x_{33}x_{34}\cdots \\
&\vdots
\end{aligned}
$$

  (those x_{ij} are digits)
- How can we define y?

Cantor's diagonal argument

Cantor's diagonal argument

- We can look at the diagonal here:

$$
\begin{aligned}
x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\cdots \\
x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\cdots \\
x_3 &= 0.x_{31}x_{32}x_{33}x_{34}\cdots \\
&\vdots
\end{aligned}
$$

Cantor's diagonal argument

- We can look at the diagonal here:

$$
\begin{aligned}
x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\cdots \\
x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\cdots \\
x_3 &= 0.x_{31}x_{32}x_{33}x_{34}\cdots \\
&\vdots
\end{aligned}
$$

- For each x_{nn}, let y_n be a digit that is *different* from x_{nn} (if we're working in binary, just flip the bit).

Cantor's diagonal argument

- We can look at the diagonal here:

$$\begin{aligned} x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\cdots \\ x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\cdots \\ x_3 &= 0.x_{31}x_{32}x_{33}x_{34}\cdots \\ &\vdots \end{aligned}$$

- For each x_{nn}, let y_n be a digit that is *different* from x_{nn} (if we're working in binary, just flip the bit).
- What do we know about

$$y = 0.y_1y_2y_3y_4\cdots?$$

Cantor's diagonal argument

- We can look at the diagonal here:

$$\begin{aligned} x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\cdots \\ x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\cdots \\ x_3 &= 0.x_{31}x_{32}x_{33}x_{34}\cdots \\ &\vdots \end{aligned}$$

- For each x_{nn}, let y_n be a digit that is *different* from x_{nn} (if we're working in binary, just flip the bit).
- What do we know about

$$y = 0.y_1y_2y_3y_4\cdots?$$

- It's different from every x_n in the nth digit!

Cantor's diagonal argument

- We can look at the diagonal here:

$$\begin{aligned} x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\cdots \\ x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\cdots \\ x_3 &= 0.x_{31}x_{32}x_{33}x_{34}\cdots \\ &\vdots \end{aligned}$$

- For each x_{nn}, let y_n be a digit that is *different* from x_{nn} (if we're working in binary, just flip the bit).
- What do we know about

$$y = 0.y_1y_2y_3y_4\cdots?$$

- It's different from every x_n in the nth digit!
- So it has to be a number that isn't in our list - contradiction.

Another problem

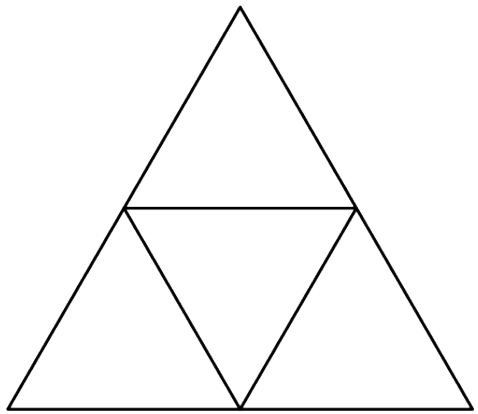
There are 5 points inside an equilateral triangle of side length 1. Prove that some two of them are at distance at most $1/2$ from each other.

What's bad about this proof?

What's bad about this proof?

Suppose towards contradiction that this claim is not true. Then, every two points are at distance more than $1/2$.

Consider subdividing the triangle into 4 smaller equilateral triangles, each with side length $1/2$, as shown in the figure. By the Pigeonhole Principle, at least 2 out of the 5 points must lie in the same subtriangle. However, for each subtriangle, the maximum distance between points is $1/2$ – giving us a contradiction. We conclude that the result holds. ■



What's bad about this proof?

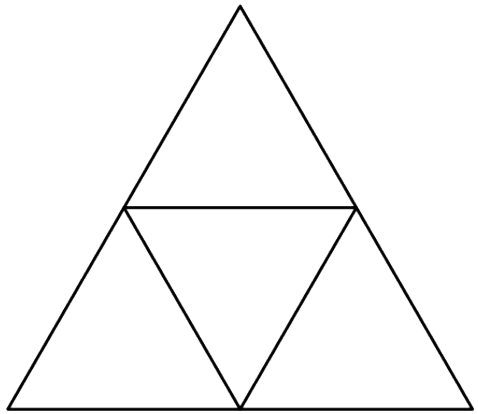
What's bad about this proof?

That proof is correct, but there is no need for the contradiction! We can rewrite it:

What's bad about this proof?

That proof is correct, but there is no need for the contradiction! We can rewrite it:

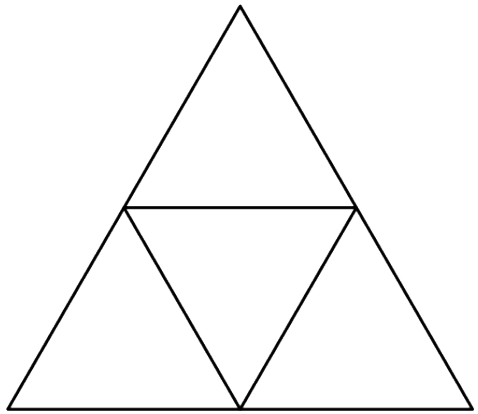
Consider subdividing the triangle into 4 smaller equilateral triangles, each with side length $1/2$, as shown in the figure. By the Pigeonhole Principle, at least 2 out of the 5 points must lie in the same subtriangle. Since, for each subtriangle, the maximum distance between points is $1/2$, we are done. ■



What's bad about this proof?

That proof is correct, but there is no need for the contradiction! We can rewrite it:

Consider subdividing the triangle into 4 smaller equilateral triangles, each with side length $1/2$, as shown in the figure. By the Pigeonhole Principle, at least 2 out of the 5 points must lie in the same subtriangle. Since, for each subtriangle, the maximum distance between points is $1/2$, we are done. ■



Try not to write proofs where you assume the claim is false, but never use that fact. (It's not wrong, but it's unnecessary and can be confusing to the reader.)

Preamble: Turing machines

Warning: the next few slides compress a large chunk of a Theory of Computation course into a few minutes. I'm not expecting you to get it all.

Preamble: Turing machines

Warning: the next few slides compress a large chunk of a Theory of Computation course into a few minutes. I'm not expecting you to get it all.

- You won't actually need to know what a Turing machine is, but...

Preamble: Turing machines

Warning: the next few slides compress a large chunk of a Theory of Computation course into a few minutes. I'm not expecting you to get it all.

- You won't actually need to know what a Turing machine is, but...
- A *Turing machine* is a machine that transitions between a finite number of states based upon (i) the state where it currently is, (ii) the part of memory it is reading from at the moment.

Preamble: Turing machines

Warning: the next few slides compress a large chunk of a Theory of Computation course into a few minutes. I'm not expecting you to get it all.

- You won't actually need to know what a Turing machine is, but...
- A *Turing machine* is a machine that transitions between a finite number of states based upon (i) the state where it currently is, (ii) the part of memory it is reading from at the moment.
- A *state* can include directions to write to memory or move to a different part of memory.

Preamble: Turing machines

Preamble: Turing machines

- Basically, a Turing machine is a formalization of a computer – it's able to compute any function that is computable by an algorithm.

Preamble: Turing machines

- Basically, a Turing machine is a formalization of a computer – it's able to compute any function that is computable by an algorithm.
- (This is proven in something called the *Church-Turing thesis*.)

Preamble: Turing machines

- Basically, a Turing machine is a formalization of a computer – it's able to compute any function that is computable by an algorithm.
- (This is proven in something called the *Church-Turing thesis*.)
- You'd probably never want to describe exactly how a Turing machine executes any normal algorithm – it would be complicated.

Preamble: Turing machines

- Basically, a Turing machine is a formalization of a computer – it's able to compute any function that is computable by an algorithm.
- (This is proven in something called the *Church-Turing thesis*.)
- You'd probably never want to describe exactly how a Turing machine executes any normal algorithm – it would be complicated.
- When we talk about Turing machines, it's about things a computer *can* compute, not how fast or efficiently. Turing machines are a mathematical abstraction – they are used in working out whether something can be computed or not, not the best way of doing it.

Preamble: Turing machines

- Basically, a Turing machine is a formalization of a computer – it's able to compute any function that is computable by an algorithm.
- (This is proven in something called the *Church-Turing thesis*.)
- You'd probably never want to describe exactly how a Turing machine executes any normal algorithm – it would be complicated.
- When we talk about Turing machines, it's about things a computer *can* compute, not how fast or efficiently. Turing machines are a mathematical abstraction – they are used in working out whether something can be computed or not, not the best way of doing it.
- **All you need to know:** Given an input, a Turing machine can do one of three things: **accept** (output yes), **reject** (output no), or **loop** forever.

Problem

Prove there is no Turing machine that can do the following: Given M and w, where M is a Turing machine, **accept** (M, w) if M accepts w and **reject** (M, w) if M rejects w or if M loops forever.

Problem

Prove there is no Turing machine that can do the following: Given M and w, where M is a Turing machine, **accept** (M, w) if M accepts w and **reject** (M, w) if M rejects w or if M loops forever.

- Basically, we want a Turing machine that simulates another Turing machine it's given as input.

Problem

Prove there is no Turing machine that can do the following: Given M and w, where M is a Turing machine, **accept** (M, w) if M accepts w and **reject** (M, w) if M rejects w or if M loops forever.

- Basically, we want a Turing machine that simulates another Turing machine it's given as input.
- But we want this simulator to be better – it should never loop.

Problem

Prove there is no Turing machine that can do the following: Given M and w, where M is a Turing machine, **accept** (M, w) if M accepts w and **reject** (M, w) if M rejects w or if M loops forever.

- Basically, we want a Turing machine that simulates another Turing machine it's given as input.
- But we want this simulator to be better – it should never loop.
- Let's try to prove this using contradiction – suppose there is this magic Turing machine. Let's call it H.

Problem

Prove there is no Turing machine that can do the following: Given M and w, where M is a Turing machine, **accept** (M, w) if M accepts w and **reject** (M, w) if M rejects w or if M loops forever.

- Basically, we want a Turing machine that simulates another Turing machine it's given as input.
- But we want this simulator to be better – it should never loop.
- Let's try to prove this using contradiction – suppose there is this magic Turing machine. Let's call it H.
- Since we have the magic simulator H, we know how any Turing machine acts for input w.

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.
- In particular, we know the output of M when given its own description as input.

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.
- In particular, we know the output of M when given its own description as input.
- Define a new Turing machine A:

  A takes input M and outputs whatever M outputs when given its own description M as input.

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.
- In particular, we know the output of M when given its own description as input.
- Define a new Turing machine A:

  A takes input M and outputs whatever M outputs when given its own description M as input.

- Now define B that does the opposite:

  B rejects whenever A accepts, and vice versa.

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.
- In particular, we know the output of M when given its own description as input.
- Define a new Turing machine A:

  A takes input M and outputs whatever M outputs when given its own description M as input.
- Now define B that does the opposite:

  B rejects whenever A accepts, and vice versa.
- Here is the punchline: **What does B do when applied to itself**?

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.
- In particular, we know the output of M when given its own description as input.
- Define a new Turing machine A:

  A takes input M and outputs whatever M outputs when given its own description M as input.
- Now define B that does the opposite:

  B rejects whenever A accepts, and vice versa.
- Here is the punchline: **What does B do when applied to itself**?
- It has to do the **opposite** of A, so what does A do.

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.
- In particular, we know the output of M when given its own description as input.
- Define a new Turing machine A:

  A takes input M and outputs whatever M outputs when given its own description M as input.
- Now define B that does the opposite:

  B rejects whenever A accepts, and vice versa.
- Here is the punchline: **What does B do when applied to itself**?
- It has to do the **opposite** of A, so what does A do.
- A would do **whatever its input B does when applied to itself**.

Problem

- Since we have the magic simulator H, we know what any Turing machine M outputs for input w.
- In particular, we know the output of M when given its own description as input.
- Define a new Turing machine A:

  A takes input M and outputs whatever M outputs when given its own description M as input.

- Now define B that does the opposite:

  B rejects whenever A accepts, and vice versa.

- Here is the punchline: **What does B do when applied to itself**?
- It has to do the **opposite** of A, so what does A do.
- A would do **whatever its input B does when applied to itself**.
- So B has to do the opposite of what it does! Contradiction.

The Halting Problem

As a corollary, we can prove the famous Halting Problem, which says it's impossible to determine in general whether a Turing machine will loop forever or "halt" (i.e., accept or reject).

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

- Suppose towards contradiction that such a machine H did exist.

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

- Suppose towards contradiction that such a machine H did exist.
- Then, we could use it to solve the previous problem!

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

- Suppose towards contradiction that such a machine H did exist.
- Then, we could use it to solve the previous problem!
- Reminder – previous problem was to simulate M but reject if it loops.
- If H outputs **accept** for (M, w), then we know M doesn't loop.

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

- Suppose towards contradiction that such a machine H did exist.
- Then, we could use it to solve the previous problem!
- Reminder – previous problem was to simulate M but reject if it loops.
- If H outputs **accept** for (M, w), then we know M doesn't loop.
- We then simulate M and output whatever it outputs.

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

- Suppose towards contradiction that such a machine H did exist.
- Then, we could use it to solve the previous problem!
- Reminder – previous problem was to simulate M but reject if it loops.
- If H outputs **accept** for (M, w), then we know M doesn't loop.
- We then simulate M and output whatever it outputs.
- If H outputs **reject** for (M, w), then we know M loops.

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

- Suppose towards contradiction that such a machine H did exist.
- Then, we could use it to solve the previous problem!
- Reminder – previous problem was to simulate M but reject if it loops.
- If H outputs **accept** for (M, w), then we know M doesn't loop.
- We then simulate M and output whatever it outputs.
- If H outputs **reject** for (M, w), then we know M loops.
- We just reject it.

The Halting Problem

Theorem. There is no Turing machine that, given input (M, w), outputs **accept** when M halts on input w and **reject** when M loops forever.

- Suppose towards contradiction that such a machine H did exist.
- Then, we could use it to solve the previous problem!
- Reminder – previous problem was to simulate M but reject if it loops.
- If H outputs **accept** for (M, w), then we know M doesn't loop.
- We then simulate M and output whatever it outputs.
- If H outputs **reject** for (M, w), then we know M loops.
- We just reject it.
- Since we knew the previous problem *couldn't be solved*, we get a contradiction.

Next time!

Other proof techniques
(invariants, monovariants, inequalities)