# Introduction to Proofs - Cantor's Theorem

Prof Mike Pawliuk

UTM

August 6, 2020

Slides available at: mikepawliuk.ca

# Learning Objectives (for this video)

By the end of this video, participants should be able to:

1. Construct functions between sets and power sets, and compute subsets from definitions relating to those functions.
2. Construct arbitrarily large (in cardinality) sets.

# Motivation

## Motivation

Power sets can be used to create larger and larger infinite sets; this is called Cantor's theorem.

The standard proof of Cantor's theorem involves a self-reference idea that is used in many deep ways in math and computer science.

# 1. Finite Cantor's theorem

**Finite Cantor's Theorem**

Let $A$ be a <u>finte</u> set, and $\mathcal{P}(A)$ be its power set. Then

$$|A| < |\mathcal{P}(A)|.$$

# 1. Finite Cantor's theorem

**Finite Cantor's Theorem**

Let $A$ be a finte set, and $\mathcal{P}(A)$ be its power set. Then

$$|A| < |\mathcal{P}(A)|.$$

**Proof.**

It is enough to recall that $|\mathcal{P}(A)| = 2^{|A|}$. □

# 1. Finite Cantor's theorem

## Finite Cantor's Theorem

Let $A$ be a finte set, and $\mathcal{P}(A)$ be its power set. Then

$$|A| < |\mathcal{P}(A)|.$$

## Proof.

It is enough to recall that $|\mathcal{P}(A)| = 2^{|A|}$. □

The above proof only works when $A$ is finite. How can we prove that there is never a surjection $f : A \to \mathcal{P}(A)$?

# 2. Functions $f : A \to \mathcal{P}(A)$.

Let $A = \{1, 2, 3\}$, so
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

1. Write down any function $f : A \to \mathcal{P}(A)$.
2. Can you choose one that is an injection?
3. Can you choose one that is a surjection? (Proof?)
4. For your function $f$, compute $D = \{a \in A : a \notin f(a)\}$.
5. For your function, $f$, is there any $y \in A$ such that $f(y) = D$?

# 2. Functions $f : A \to \mathcal{P}(A)$.

Let $A = \{1, 2, 3\}$, so
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

1. Write down any function $f : A \to \mathcal{P}(A)$.
   $f(1) = \{1, 2\}, f(2) = \{1, 3\}, f(3) = \emptyset$
2. Can you choose one that is an injection?
3. Can you choose one that is a surjection? (Proof?)
4. For your function $f$, compute $D = \{a \in A : a \notin f(a)\}$.
5. For your function, $f$, is there any $y \in A$ such that $f(y) = D$?

# 2. Functions $f : A \to \mathcal{P}(A)$.

Let $A = \{1, 2, 3\}$, so
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

1. Write down any function $f : A \to \mathcal{P}(A)$.
   $f(1) = \{1, 2\}, f(2) = \{1, 3\}, f(3) = \emptyset$
2. Can you choose one that is an injection? Yes, $f(x) = \{x\}$ also works.
3. Can you choose one that is a surjection? (Proof?)
4. For your function $f$, compute $D = \{a \in A : a \notin f(a)\}$.
5. For your function, $f$, is there any $y \in A$ such that $f(y) = D$?

# 2. Functions $f : A \to \mathcal{P}(A)$.

Let $A = \{1, 2, 3\}$, so
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

1. Write down any function $f : A \to \mathcal{P}(A)$.
   $f(1) = \{1, 2\}, f(2) = \{1, 3\}, f(3) = \emptyset$
2. Can you choose one that is an injection? Yes, $f(x) = \{x\}$ also works.
3. Can you choose one that is a surjection? (Proof?) No, this is impossible.
4. For your function $f$, compute $D = \{a \in A : a \notin f(a)\}$.
5. For your function, $f$, is there any $y \in A$ such that $f(y) = D$?

# 2. Functions $f : A \to \mathcal{P}(A)$.

Let $A = \{1, 2, 3\}$, so
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

1. Write down any function $f : A \to \mathcal{P}(A)$.
   $f(1) = \{1, 2\}, f(2) = \{1, 3\}, f(3) = \emptyset$
2. Can you choose one that is an injection? Yes, $f(x) = \{x\}$ also works.
3. Can you choose one that is a surjection? (Proof?) No, this is impossible.
4. For your function $f$, compute $D = \{a \in A : a \notin f(a)\}$. $D = \{2, 3\}$
5. For your function, $f$, is there any $y \in A$ such that $f(y) = D$?

# 2. Functions $f : A \to \mathcal{P}(A)$.

Let $A = \{1, 2, 3\}$, so
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

1. Write down any function $f : A \to \mathcal{P}(A)$.
   $f(1) = \{1, 2\}, f(2) = \{1, 3\}, f(3) = \emptyset$
2. Can you choose one that is an injection? Yes, $f(x) = \{x\}$ also works.
3. Can you choose one that is a surjection? (Proof?) No, this is impossible.
4. For your function $f$, compute $D = \{a \in A : a \notin f(a)\}$. $D = \{2, 3\}$
5. For your function, $f$, is there any $y \in A$ such that $f(y) = D$? No, $f(1) \neq D, f(2) \neq D, f(3) \neq D$.

# 3. Cantor's theorem

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Proof.

We see that $|A| \leq |\mathcal{P}(A)|$ by the injection $f(x) = \{x\}$.

# 3. Cantor's theorem

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Proof.

We see that $|A| \leq |\mathcal{P}(A)|$ by the injection $f(x) = \{x\}$.
For the sake of contradiction, let $f : A \to \mathcal{P}(A)$ be a bijection (we only need surjection). Define

$$D = \{a \in A : a \notin f(a)\} \subseteq A.$$

# 3. Cantor's theorem

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Proof.

We see that $|A| \leq |\mathcal{P}(A)|$ by the injection $f(x) = \{x\}$.
For the sake of contradiction, let $f : A \to \mathcal{P}(A)$ be a bijection (we only need surjection). Define

$$D = \{a \in A : a \notin f(a)\} \subseteq A.$$

Since $f$ is a surjection, there is a $y \in A$ with $f(y) = D$.

# 3. Cantor's theorem

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Proof.

We see that $|A| \leq |\mathcal{P}(A)|$ by the injection $f(x) = \{x\}$.
For the sake of contradiction, let $f : A \to \mathcal{P}(A)$ be a bijection (we only need surjection). Define

$$D = \{a \in A : a \notin f(a)\} \subseteq A.$$

Since $f$ is a surjection, there is a $y \in A$ with $f(y) = D$.
**Is $y \in D$?**

# 3. Cantor's theorem

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Proof.

We see that $|A| \leq |\mathcal{P}(A)|$ by the injection $f(x) = \{x\}$.
For the sake of contradiction, let $f : A \to \mathcal{P}(A)$ be a bijection (we only need surjection). Define

$$D = \{a \in A : a \notin f(a)\} \subseteq A.$$

Since $f$ is a surjection, there is a $y \in A$ with $f(y) = D$.
**Is** $y \in D$**?**

1. $\boxed{\text{If no}}$, then by definition of $D$, $y \in f(y) = D$.

# 3. Cantor's theorem

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Proof.

We see that $|A| \leq |\mathcal{P}(A)|$ by the injection $f(x) = \{x\}$.
For the sake of contradiction, let $f : A \to \mathcal{P}(A)$ be a bijection (we only need surjection). Define

$$D = \{a \in A : a \notin f(a)\} \subseteq A.$$

Since $f$ is a surjection, there is a $y \in A$ with $f(y) = D$.
**Is $y \in D$?**

1. If no, then by definition of $D$, $y \in f(y) = D$.
2. If yes, then $y \notin f(y) = D$.

# 3. Cantor's theorem

## Cantor's Theorem

Let $A$ be a set. Then $|A| < |\mathcal{P}(A)|$.

## Proof.

We see that $|A| \leq |\mathcal{P}(A)|$ by the injection $f(x) = \{x\}$.
For the sake of contradiction, let $f : A \to \mathcal{P}(A)$ be a bijection (we only need surjection). Define

$$D = \{a \in A : a \notin f(a)\} \subseteq A.$$

Since $f$ is a surjection, there is a $y \in A$ with $f(y) = D$.
**Is $y \in D$?**

1. If no, then by definition of $D$, $y \in f(y) = D$.
2. If yes, then $y \notin f(y) = D$.

This is a contradiction or paradox.

□

# 4. Corollaries

**Theorem**

1. $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$
2. $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \dots$

# 4. Corollaries

**Theorem**

1. $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$
2. $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \dots$

In words: There are infinitely many sizes of infinity.

# 4. Corollaries

**Theorem**

1. $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$
2. $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \dots$

In words: There are infinitely many sizes of infinity.

**Theorem**

$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

This is a very challenging exercise.

# Reflection

- Do all uncountable sets have the same cardinality?
- Is there a largest size of infinity?
- How is this proof of Cantor's theorem like the Barber paradox?