Unit 4

Infinity

Albert Sung

Outline of Unit 4

- 4.1 Indirect Proofs
- 4.2 Cardinalities of Infinite Sets
- 4.3 The Infinite Prisoner Hat Riddle

Unit 4.1

Indirect Proofs

AmazingZip

AmazingZip can compress any data file without information loss, provided that its size is greater than B bits.

Do you believe?

Indirect Proofs (two types)

Proof by Contradiction

- Also called reductio ad absurdum
  - (i.e., Reduction to the Absurd)

Proof by Contraposition

- Based on the logical equivalence between a conditional and its contrapositive.

$$\boxed{p \to q \equiv \sim q \to \sim p}$$

- "If p then q" is logically equivalent to "If not q, then not p."

Proof by Contradiction

To prove that p is true:

1. Assume that p is false.
2. With the above assumption, show that there is a contradiction.
3. Conclude that p is true.

Contradiction rule:

$$\frac{\sim p \rightarrow \mathbf{c}}{p}$$

where **c** is a contradiction.

Example (Proof by Contradiction)

Theorem: There is no greatest integer.

Proof *(by contradiction)**:***

Suppose there were a greatest integer N, i.e.,

$$N \geq k \text{ for all integer } k.$$

Let $M = N + 1$. Now M is an integer and $M > N$.

Therefore, N is not greatest, which is a contradiction.

Hence, the statement is true.

Q.E.D.

Proof by Contraposition

- This method is based on

$$\boxed{p \to q \equiv {\sim}q \to {\sim}p}$$

To prove that $p \to q$ is true:

1. Assume ${\sim}q$ is true.
2. Show that ${\sim}p$ is true.
3. Conclude that $p \to q$.

This shows that ${\sim}q \to {\sim}p$ is true.

Example (Proof by Contraposition)

Theorem: For all integer n, if n^2 is even, then n is even.

Proof:

Suppose n is not even, i.e., $n = 2k + 1$ for some integer k.

Then,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

We can write it as $n^2 = 2t + 1$, where $t = 2k^2 + 2k$ is an integer. (This step is obvious, which may be skipped.)

Therefore, n^2 is odd (i.e., not even).

Hence, the statement is proved.

Q.E.D.

The Pigeonhole Principle

- Suppose that you have n pigeonholes.
- Suppose that you have m pigeons, where $m > n$.
- If you put the m pigeons into the n pigeonholes, some pigeonhole will have more than one pigeon in it.

- $n = 9$ pigeonholes
- $m = 10$ pigeons
- Some pigeonhole has more than one pigeon.

Is it true?

Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains more than one object.

Proof:

Assume that every bin contains no more than one object.

We want to prove $m \leq n$. (proof by contraposition)

Let x_i be the number of objects in bin i.

By assumption, $x_i \leq 1$.

Since m is the number of objects, we have

$$m = \sum_{i=1}^{n} x_i \leq \sum_{i=1}^{n} 1 = n.$$

Hence, $m \leq n$, as required.

Q.E.D.

AmazingZip cannot exist

Proof: Suppose AmazingZip exists. It can compress any file of size $B+1$ bits to a file of size B bits or less.

To ensure that the original file can be recovered, the compression function must be an injection.

- Otherwise, two different files can be compressed into the same zip file. You can't tell which one is the original file.

There are $M = 2^{B+1}$ distinct files having size $B+1$ bits.

There are N distinct files having size B bits or less, where

$$N = 1 + 2 + 2^2 + \cdots + 2^B = 2^{B+1} - 1.$$

By the Pigeonhole Principle, there must be more than one file being compressed into the same zip file.

The compression is not an injection.

A contradiction. *Q.E.D.*

Unit 4.2

Cardinality of Infinite Sets

Countable Sets

- Recall from Unit 2:
  - A countable set is either a finite set or a countably infinite set.
  - A set S is countably infinite if there exists a bijection between S and $\mathbb{N}$.
  - $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are all countably infinite sets.
  - The union of two countable sets is countable.
- In this section, we will talk about uncountable sets.

The (0,1) Interval is Uncountable

Show that the set of real numbers in the interval (0, 1) is uncountable.

Solution: We prove by contradiction.

Suppose they are *countable* then we can create a list like

1	$\leftrightarrow$	$x_1 = 0.256173\ldots$
2	$\leftrightarrow$	$x_2 = 0.654321\ldots$
3	$\leftrightarrow$	$x_3 = 0.876241\ldots$
4	$\leftrightarrow$	$x_4 = 0.600002\ldots$
5	$\leftrightarrow$	$x_5 = 0.676783\ldots$
6	$\leftrightarrow$	$x_6 = 0.387514\ldots$
.	.	. .
.	.	. .
n	$\leftrightarrow$	$x_n = 0.a_1a_2a_3a_4a_5 \ldots a_n \ldots$
.	.	. .
.	.	. .

1	$\leftrightarrow$	$x_1 = 0.256173\ldots$	Construct the number
2	$\leftrightarrow$	$x_2 = 0.654321\ldots$	$b = 0.b_1b_2b_3b_4b_5\ \ldots$
3	$\leftrightarrow$	$x_3 = 0.876241\ldots$	
4	$\leftrightarrow$	$x_4 = 0.600002\ldots$	Choose
5	$\leftrightarrow$	$x_5 = 0.676783\ldots$	b_1 not equal to 2 say is 4
6	$\leftrightarrow$	$x_6 = 0.387514\ldots$	b_2 not equal to 5 say is 7
.	.	. .	b_3 not equal to 6 say is 8
.	.	. .	b_4 not equal to 0 say is 3
n	$\leftrightarrow$	$x_n = 0.a_1a_2a_3a_4a_5\ \ldots a_n$	b_5 not equal to 8 say is 7
…			
.	.	. .	b_n not equal to a_n
.	.	. .	

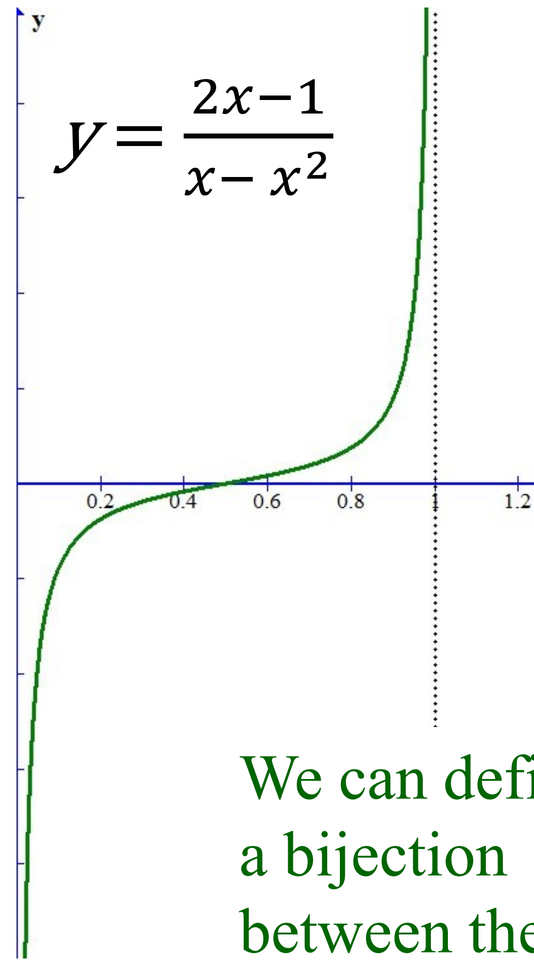
Then $b = 0.b_1b_2b_3b_4b_5\ \ldots = 0.47837\ldots$ is NOT in the list.

The set of real numbers is uncountable! *Q.E.D.*

$\mathbb{R}$ is Uncountable

- The set of real numbers has the same cardinality as the set of real numbers in $(0, 1)$. *Why?*

- The cardinality is often denoted by c.
  - i.e., the continuum of real numbers.



We can define a bijection between them.

Irrational Numbers are Uncountable

- There is no generally used convention for the set of irrationals.
- Often it is just denoted by $\mathbb{R} \backslash \mathbb{Q}$, the set of reals minus the set of rationals.
- Note that $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \backslash \mathbb{Q})$.
- ***Proof by contradiction***:

  Suppose $\mathbb{R} \backslash \mathbb{Q}$ is countable.

  We have proved that $\mathbb{Q}$ is countable.

  Their union should be countable, which contradicts with the fact that $\mathbb{R}$ is uncountable.

Q.E.D.

Equality of Cardinalities

For any two sets S and T,
$|S| = |T|$ iff there is a bijection between S and T.

- It is easy to verify that equality of cardinality is an equivalence relation:
  - Reflexivity: $|S| = |S|$;
  - Symmetry: If $|S| = |T|$, then $|T| = |S|$;
  - Transitivity: If $|S| = |T| = |R|$, then $|S| = |R|$.

Summary: Cardinality of Some Sets

Set	Description	Cardinality
Natural numbers	1, 2, 3, 4, 5, …	$\aleph_0$
Integers	…, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, …	$\aleph_0$
Rational numbers	All the fractions (i.e., decimals which terminate or repeat)	$\aleph_0$
Irrational numbers	All the decimals which do not terminate or repeat	c
Real numbers	All decimals	c
Complex numbers	All ordered pairs (x, y) of real numbers	c

Is there any cardinality between $\aleph_0$ and c?

A Hierarchy of Infinities (8 min video)

https://www.youtube.com/watch?v=i7c2qz7sO0I

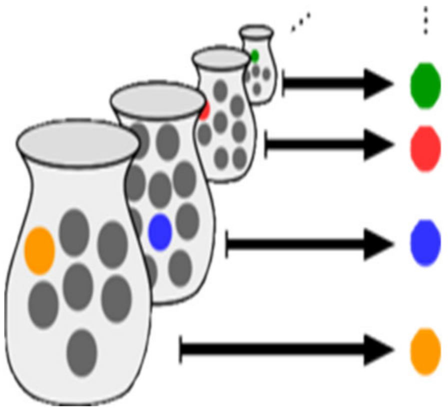
Unit 4.3

The Infinite Prisoner Hat Riddle

Axiom of Choice

- The Axiom of Choice is an axiom in set theory.

Given any (possibly infinite) collection of non-empty bins, it is possible to select exactly one object from each bin.



The Infinite Prisoner Hat Riddle

- There is a line of infinite prisoners, $P_1, P_2, P_3, \ldots$
- Each wears a white or a black hat randomly.
- Each one can see the hats of the prisoners in front of him, but cannot see his own hat (or the hat of anyone behind him).
- Everyone has to guess and call out the color of his own hat at the same time.
- Prisoners who call out incorrectly will be shot.
- **Problem:** Find a strategy that would guarantee that *at most finitely many prisoners* are shot.

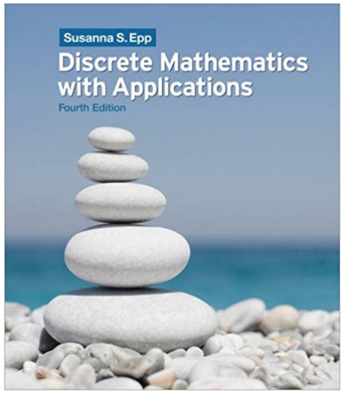
Classwork: Infinite Binary Sequences

- Let $\mathbb{B}^\infty$ be the set of all infinite binary sequences.
- Define the relation R on $\mathbb{B}^\infty$, where xRy iff x and y *differ in only finitely many positions*.
  - $x = 000010101010101\ldots$ (repeating 01…)
  - $y = 111010101010101\ldots$ (repeating 01…)
  - xRy because they differ only in the first three positions.
- Is R an equivalence relation?
  a) reflexive?
  b) symmetric?
  c) transitive?
- Two sequences belonging to the same equivalence class are said to be close.

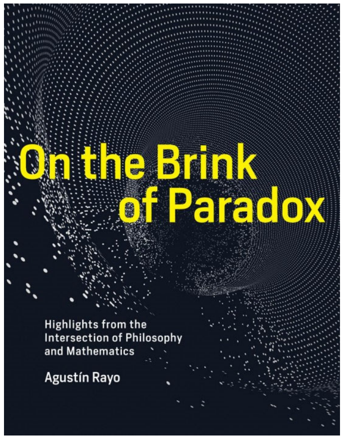
Infinite Prisoner Hat Riddle

- (first 6 min) https://www.youtube.com/watch?v=aDOP0XynAzA

Recommended Reading



- Chapter 4, Sections 5.4 and 7.4, S. S. Epp, *Discrete Mathematics with Applications*, 4th ed., Brooks Cole, 2010.



- Chapter 1, A. Rayo, *On the Brink of Paradox*, The MIT Press, 2019.