Theory of Automata and Languages

Preliminaries

Fall 2024

Sharif University of Technology

Mehran Moeini Jam

Overview

- Naïve Set Theory
- Principle of Extensionality
- Subsets and Power Sets
- Pairs, Tuples, Cartesian Product
- Russell's Paradox and Axiomatic Set Theory
- Relation as Sets
- Special Properties of Relations

Overview

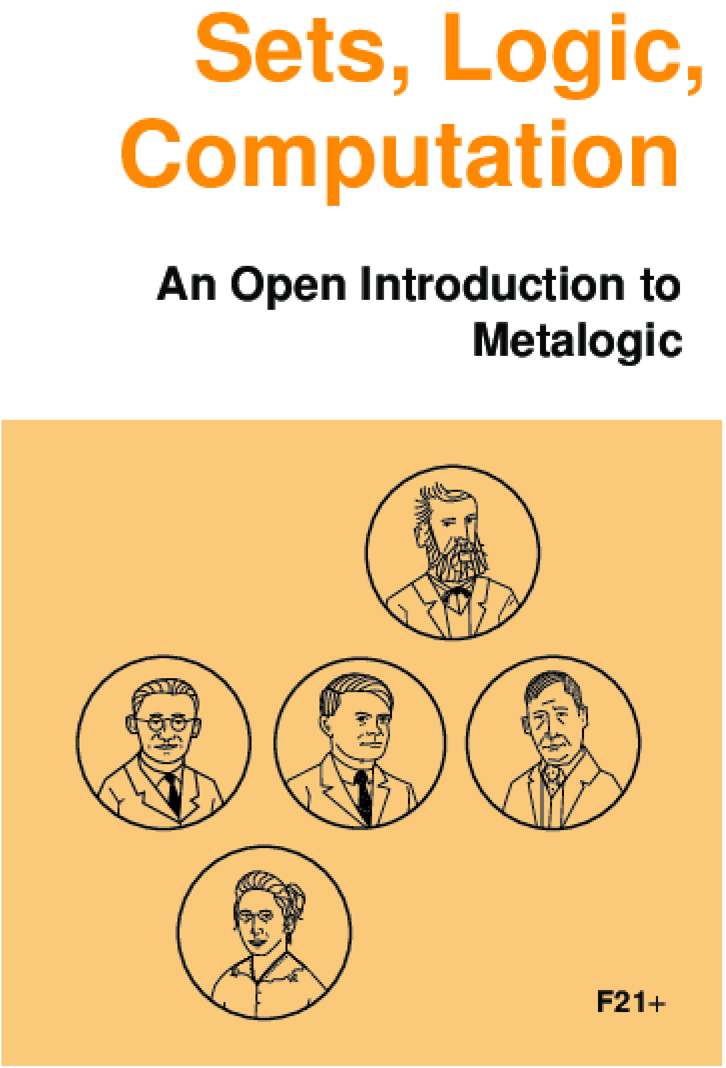
- Equivalence Relations
- Order Relations
- Functions
- Kinds of Functions
- Functions as Relations
- The size of Sets
- Enumerable Sets

Overview

- Cantor’s Zig-Zag Method
- Non-enumerable Sets
- Cantor’s Diagonal Method
- Equinumerosity
- The Schröder–Bernstein Theorem
- Some Other Important Theorems

Reference

This lecture draws from the book "Sets, Logic, Computation" which introduces the foundational concepts essential for our upcoming sections. It's an open-source and evolving project, available for free at openlogicproject.org, so keep in mind that the content may vary slightly depending on your version. The material presented here is based on the September 2021 edition.



Naïve Set Theory

- The Naïve theory of sets is a branch of mathematics that studies sets simply as collection of objects. The objects making up the set are called elements or members of the set.

- If x is an element of a set A, we write $x \in A$; and if not, we write $x \notin A$.

  The set which has no elements is called the empty set and denoted “$\emptyset$”.

The Principle of Extensionality

- It does not matter how we specify the set, or how we order its elements, or indeed how many times we count its elements. All that matters are what its elements are.

- If A and B are sets, then A = B iff every element of A is also an element of B, and vice versa. We call this The Principle of Extensionality.

Specifying Sets using Shared Properties

- Frequently we'll specify a set by some property that its elements share. We'll use the shorthand notation $\{x : \varphi(x)\}$ for that, where the $\varphi(x)$ stands for the property that x has to have in order to be counted among the elements of the set.

- Extensionality guarantees that there is always only one set of x's such that $\varphi(x)$.

  So, extensionality justifies calling $\{x : \varphi(x)\}$ the set of x's such that $\varphi(x)$.

Subsets and Power Sets

- If every element of a set A is also an element of B, then we say that A is a subset of B, and write $A \subseteq B$. If A is not a subset of B we write $A \nsubseteq B$.

  If $A \subseteq B$ but $A \neq B$, we write $A \subsetneq B$ and say that A is a proper subset of B.

- Every set is a subset of itself, and $\emptyset$ is a subset of every set

Subsets and Power Sets

- The set consisting of all subsets of a set A is called the power set of A, written $\wp(A)$ or 2^A. We can also define it based on shared properties, as follows:

$$\wp(A) = \{B : B \subseteq A\}$$

- The power set of a set A consist of both A and the empty set $\emptyset$.

Some Important Sets

- The set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- The set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- The set of rationals $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z} \text{ and } n \neq 0\}$
- The set of real numbers $\mathbb{R} = (-\infty, \infty)$

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

One More Important Class of Sets

- One more important class of sets is the class of sets of finite strings over a finite alphabet Σ. Consider a finite alphabet set Σ. We (for now) define Σ^* to be the set of all finite strings over the alphabet Σ. We will come back to this set later.

- Example: Consider the set of English alphabet $\Sigma_{Eng} = \{a, A, b, B, \ldots, z, Z\}$, then the set Σ_{Eng}^* consists of all English words, meaningful or not. For instance, "automata", "Language", "inFiniTe", "asdjsafasfh", "oafsuasFnasf", … are all members of Σ_{Eng}^*

One More Important Class of Sets

- Consider the set B = {0, 1}. Based on the previous definition, we define B^* as the set of all finite strings of 0's and 1's. We also include a special string "ε", representing the empty string, which doesn't include any member of B.

$$B^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 101, \dots\}$$

- We can also define the set B^ω, representing all infinite strings over alphabet B. An infinite sequence $b_1 b_2 b_3 b_4 \dots$ consists of a one-way infinite list of objects, each one of which is an element of B.

Unions and Intersections

- if A and B are sets, the set $\{x : x \in A \vee x \in B\}$ consists of all those objects which are elements of either A or B. This is called the Union of two sets, written $A \cup B$.

$$A \cup B = \{x : x \in A \vee x \in B\}$$

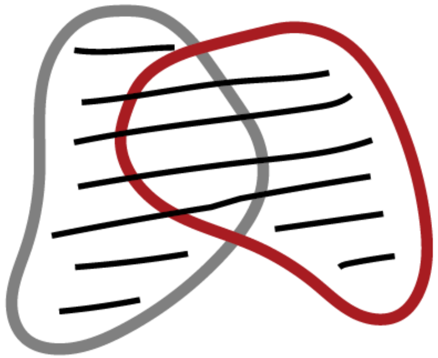
- In a similar way, the intersection of two sets A and B, written $A \cap B$, is the set of all things which are elements of both A and B.

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

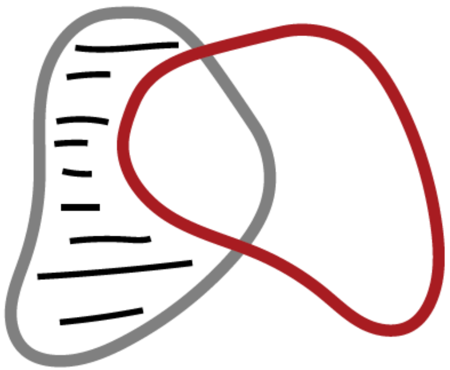
- Two sets are called disjoint if their intersection is equal to the empty set $\emptyset$.

Difference and Complement

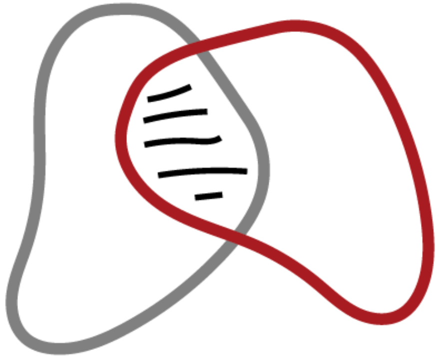
$A \cup B = \{x : x \in A \vee x \in B\}$



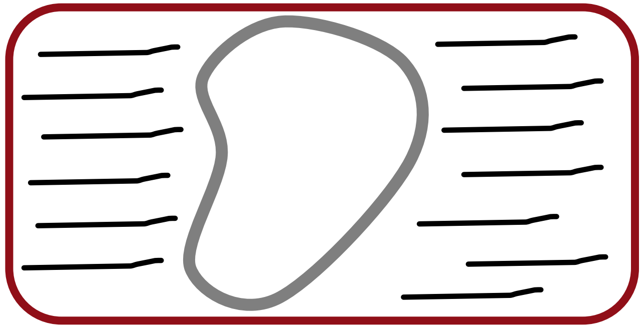
$A \setminus B = \{x : x \in A \text{ and } x \notin B\}$



$A \cap B = \{x : x \in A \wedge x \in B\}$



$A^C = \{x : x \notin A\}$



Under Specific Contexts and a Fixed “Universal” Set

Pairs, Tuples, Cartesian Products

- It follows from extensionality that sets have no order to their elements. So if we want to represent order, we use ordered pairs $\langle x, y \rangle$.

- In an unordered pair $\{x, y\}$, the order does not matter: $\{x, y\} = \{y, x\}$. In an ordered pair, it does: if $x \neq y$, then $\langle x, y \rangle \neq \langle y, x \rangle$.

- But, how should we think about ordered pairs in set theory?

Pairs, Tuples, Cartesian Products

- We define an ordered pair $\langle a, b\rangle$ as $\{ \{a\}, \{a, b\} \}$. Now that we have fixed a definition of an ordered pair, we can use it to define further sets. For example, sometimes we also want ordered sequences of more than two objects, e.g., triples (or 3-tuple) $\langle x, y, z\rangle$, quadruples (or 4-tuple) $\langle x, y, z, u\rangle$, and so on.

- Given sets A and B, their Cartesian product (cross product) $A \times B$ is defined by:

$$A \times B = \{\langle x, y\rangle : x \in A \text{ and } y \in B\}$$

The Non-self-membered Set

- Extensionality licenses the notation $\{x : \varphi(x)\}$, for the set of x's such that $\varphi(x)$. We know that sets may be elements of other sets — for instance, the power set of a set A is made up of sets. And so it makes sense to ask or investigate whether a set is an element of another set.
- Now one important question arises: Can a set be a member of itself?

  Consider the following set:

$$R = \{x : x \notin x\}$$

Russell's Paradox

- Russell's Paradox: There is no set $R = \{x : x \notin x\}$.
- Proof: If $R = \{x : x \notin x\}$ exists, then $R \in R$ iff $R \notin R$, which is a contradiction.
- How do we set up a set theory which avoids falling into Russell's Paradox? We would need to lay down axioms which give us very precise conditions for stating when sets exist (and when they don't). This branch is called Axiomatic Set Theory. We won't further pursue this, as naïve set theory is enough for our purposes.

Relation as Sets

- Recall the notion of a Cartesian product: if A and B are sets, then we can form $A \times B$, the set of all pairs $\langle x, y \rangle$ with $x \in A$ and $y \in B$.

  In particular, $A^2 = A \times A$ is the set of all ordered pairs from A.

- A binary relation *on a set A* is a subset of A^2. If $R \subseteq A^2$ is a binary relation on A and $x, y \in A$, we sometimes write xRy (or Rxy) for $\langle x, y \rangle \in R$.

Relation as Sets

- Example: Consider the $<$ — relation on the set $\mathbb{N}$ of natural numbers.

  Without any loss of information, we can consider the following set R to be the

  $<$ — relation on $\mathbb{N}$:

$$R = \{\langle n,m \rangle : n,m \in N \text{ and } n < m\}$$

$$R = \{\langle 0,1 \rangle, \langle 0,2 \rangle, \langle 1,2 \rangle, \langle 0,3 \rangle, \langle 1,3 \rangle, \langle 2,3 \rangle, \dots \}$$

Special Properties of Relations

- Some kinds of relations turn out to be so common that they have been given special names. The following are the most important ones.

- A relation $R \subseteq A^2$ is reflexive iff, for every $x \in A$, xRx.
- A relation $R \subseteq A^2$ is transitive iff, whenever xRy and yRz, then also xRz.
- A relation $R \subseteq A^2$ is symmetric iff, whenever xRy, then also yRx.
- A relation $R \subseteq A^2$ is anti-symmetric iff, whenever both xRy and yRx, then $x = y$

Special Properties of Relations

- A relation $R \subseteq A^2$ is reflexive iff, for every $x \in A$, xRx.
- A relation $R \subseteq A^2$ is irreflexive iff, for all $x \in A$, not xRx.
- A relation $R \subseteq A^2$ is transitive iff, whenever xRy and yRz, then also xRz.
- A relation $R \subseteq A^2$ is symmetric iff, whenever xRy, then also yRx.
- A relation $R \subseteq A^2$ is anti-symmetric iff, whenever both xRy and yRx, then $x = y$
- A relation $R \subseteq A^2$ is connected iff, for all $x, y \in A$, if $x \neq y$, then either xRy or yRx.

Equivalent Relations

- A relation $R \subseteq A^2$ that is reflexive, symmetric, and transitive is called an equivalence relation. Elements x and y of A are said to be R-equivalent when xRy.

- Let $R \subseteq A^2$ be an equivalence relation. For every $x \in A$, the equivalence class of x in A is the set $[x]_R = \{y \in A : xRy\}$.

- If $R \subseteq A^2$ is an equivalence relation, then xRy iff $[x]_R = [y]_R$. In other words, each equivalence relations partitions the set to disjoint equivalent classes.

Orders

- A relation which is both reflexive and transitive is called a preorder.

- A preorder which is also anti-symmetric is called a partial order.

- A partial order which is also connected is called a total order or linear order.

Functions

- A function $f : A \to B$ is a mapping of each element of A to an element of B.

- We call A the domain of f and B the codomain of f. The elements of A are called inputs or arguments of f , and the element of B that is paired with an argument x by f is called the value of f for argument x, written f(x).
- The range ran(f) of f is the subset of the codomain consisting of the values of f for some argument; $\text{ran}(f) = \{ f(x) : x \in A \}$

Functions as Relations

- Let $f : A \to B$ be a function. The graph of f is the relation $R_f \subseteq A \times B$ defined by

$$R_f = \{ \langle x, y \rangle : f(x) = y \}$$

- Let $R \subseteq A \times B$ be such that:

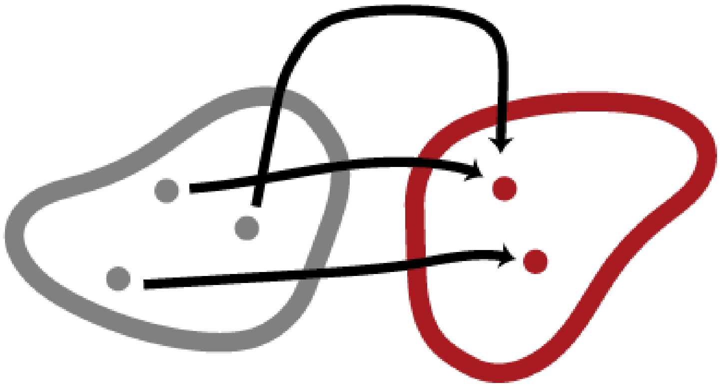
1. If xRy and xRz then $y = z$; and
2. for every $x \in A$ there is some $y \in B$ such that $\langle x, y \rangle \in R$.

Then R is functional, i.e. it's the graph of the function f

Kinds of Functions

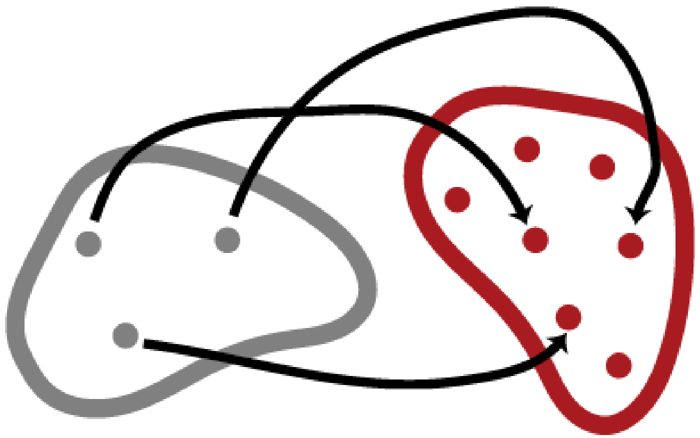
- A function $f : A \to B$ is surjective iff B is also the range of f , i.e., for every $y \in B$ there is at least one $x \in A$ such that $f(x) = y$, or in symbols:

$$(\forall y \in B)(\exists x \in A)\ f(x) = y$$



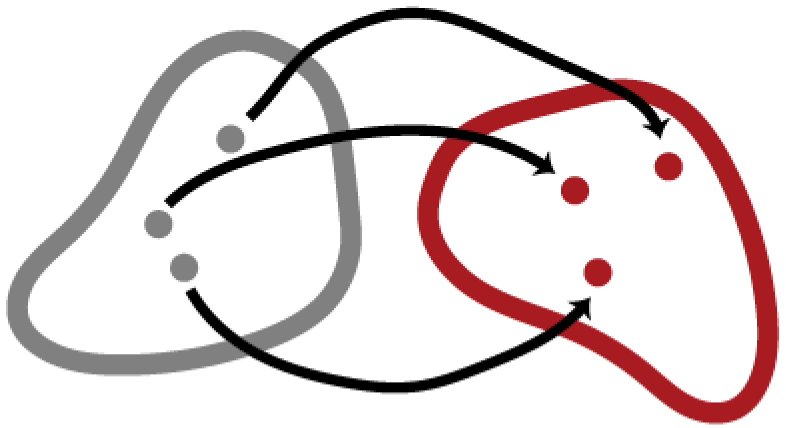
Kinds of Functions

- A function $f : A \rightarrow B$ is injective iff for each $y \in B$ there is at most one $x \in A$ such that $f(x) = y$. We call such a function an injection from A to B.



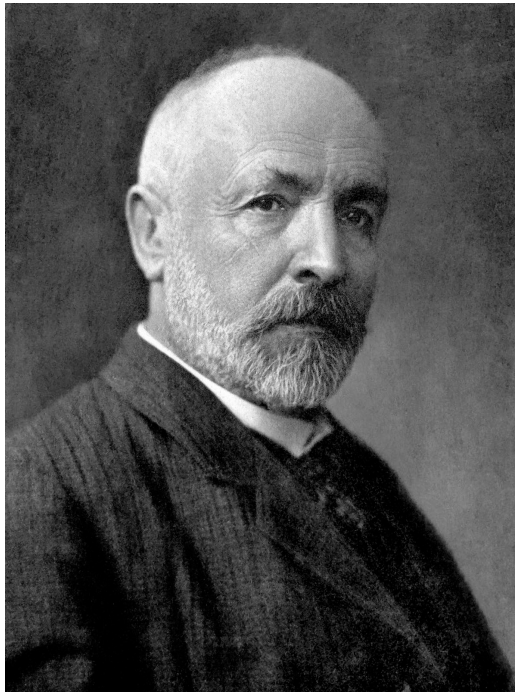
Kinds of Functions

- A function $f : A \to B$ is bijective iff it is both surjective and injective. We call such a function a bijection from A to B (or between A and B).



The size of Sets

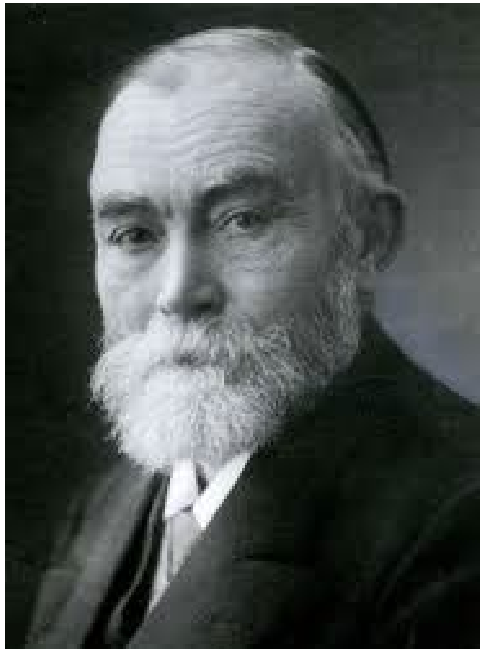
- When Georg Cantor developed set theory in the 1870s, one of his aims was to make palatable the idea of an infinite collection.



- A key part of this was his treatment of the size of different sets. If a, b and c are all distinct, then the set {a, b, c} is intuitively larger than {a, b}. But what about infinite sets? Are they all as large as each other? It turns out that they are not.

The size of Sets

- If a waiter wants to be sure that he has laid exactly as many knives as plates on the table, he does not need to count either of them, if he simply lays a knife to the right of each plate, so that every knife on the table lies to the right of some plate. The plates and knives are thus uniquely correlated to each other, and indeed through that same spatial relationship.



Gotleb Frege

Enumeration

- The first important idea here is that of an enumeration. We can list every finite set by listing all its elements. For some infinite sets, we can also list all their elements if we allow the list itself to be infinite. Such sets are called enumerable or countable.

- Cantor's surprising result, which we will fully understand by the end of this lecture, was that some infinite sets are not enumerable.

Enumerable Sets

- We can specify what a finite set is by simply enumerating its elements. We do this when we define a set like so

$$A = \{a_1, a_2, \ldots, a_n\}$$

- Assuming that the elements $a_1, \ldots, a_n$ are all distinct, this gives us a bijection between A and the first n natural numbers $0, \ldots, n - 1$.

- We can extend this to some certain kinds of infinite sets, too.

Enumeration (Definition)

- An enumeration of a set A is a bijection whose range is A and whose domain is either an initial set of natural numbers {0, 1, . . . , n} or the entire set of natural numbers $\mathbb{N}$.

- There is an intuitive underpinning to this use of the word enumeration. To say that we have enumerated a set A is to say that there is a bijection f which allows us to count out the elements of the set A. The 0_{th} element is f(0), the 1_{st} is f(1), ...

Cantor's Zig-Zag Method

- Consider the set of pairs of natural numbers $\mathbb{N}^2$ defined by:

$$\mathbb{N} \times \mathbb{N} = \{ \langle n, m \rangle : n, m \in \mathbb{N} \}$$

- We can organize these ordered pairs into an array, like so :

	0	**1**	**2**	**3**	...
0	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$	$\langle 0,2 \rangle$	$\langle 0,3 \rangle$	...
1	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$	$\langle 1,2 \rangle$	$\langle 1,3 \rangle$	...
2	$\langle 2,0 \rangle$	$\langle 2,1 \rangle$	$\langle 2,2 \rangle$	$\langle 2,3 \rangle$	...
3	$\langle 3,0 \rangle$	$\langle 3,1 \rangle$	$\langle 3,2 \rangle$	$\langle 3,3 \rangle$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Cantor's Zig-Zag Method

- Clearly, every ordered pair in $\mathbb{N} \times \mathbb{N}$ will appear exactly once in the array.

  In particular, $\langle n, m \rangle$ will appear in the *n*th row and *m*th column.

	0	1	2	3	...
0	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$	$\langle 0,2 \rangle$	$\langle 0,3 \rangle$	...
1	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$	$\langle 1,2 \rangle$	$\langle 1,3 \rangle$	...
2	$\langle 2,0 \rangle$	$\langle 2,1 \rangle$	$\langle 2,2 \rangle$	$\langle 2,3 \rangle$	...
3	$\langle 3,0 \rangle$	$\langle 3,1 \rangle$	$\langle 3,2 \rangle$	$\langle 3,3 \rangle$	...
⋮	⋮	⋮	⋮	⋮	⋱

	0	1	2	3	4	...
0	0	1	3	6	10	...
1	2	4	7	11	...	...
2	5	8	12	...	...	...
3	9	13	...	...	...	...
4	14	...	...	...	...	...
⋮	⋮	⋮	⋮	⋮	...	⋱

- This is called Cantor's zig-zag method, and forms a bijection f as an enumeration.

Non-enumerable Sets

- The set $\mathbb{N}$ of natural numbers is infinite. It is also trivially enumerable. But the remarkable fact is that there are non-enumerable sets, i.e., sets which are not enumerable.
- This might be surprising. After all, to say that A is non-enumerable is to say that there is no bijection $f : \mathbb{N} \to A$; that is, no function mapping the infinitely many elements of N to A exhausts all of A. So if A is non-enumerable, there are “more” elements of A than there are natural numbers!

Non-enumerable Sets

- To prove that a set is non-enumerable, the best way is to show that every attempt to enumerate elements of A must leave at least one element out; this shows that no function f : $\mathbb{N} \longrightarrow$ A is surjective.

- One general strategy for establishing this is to use the Cantor's diagonal method.

Cantor's Diagonal Method (Diagonalization)

- Consider any (hypothetical) enumeration of a subset of B^ω

  So we have some list $s_0, s_1, s_2, \ldots$ where every s_n is an infinite string of 0's and 1's

- Let $s_n(m)$ be the *m*th digit of the *n*th string in this list. So we can now think of our list as an array, where $s_n(m)$ is placed at the *n*th row and *m*th column:

	0	1	2	3	…
0	$\mathbf{s_0(0)}$	$s_0(1)$	$s_0(2)$	$s_0(3)$	…
1	$s_1(0)$	$\mathbf{s_1(1)}$	$s_1(2)$	$s_1(3)$	…
2	$s_2(0)$	$s_2(1)$	$\mathbf{s_2(2)}$	$s_2(3)$	…
3	$s_3(0)$	$s_3(1)$	$s_3(2)$	$\mathbf{s_3(3)}$	…
⋮	⋮	⋮	⋮	⋮	⋱

Cantor's Diagonal Method (Diagonalization)

- Now we construct an infinite sequence, d, of 0's and 1's which cannot possibly
- be on this list. To define s, we specify what all its elements are, i.e., we specify d(n) for all $n \in \mathbb{N}$.

$$d(n) = \begin{cases} 1 & \text{if} \quad s_n(n) = 0 \\ 0 & \text{if} \quad s_n(n) = 1 \end{cases}$$

- Clearly $d \in B^\omega$, since it is an infinite string of 0's and 1's. But because d differs from each s_n in the nth entry, $d \neq s_n$ for any $n \in \mathbb{N}$.
- So d cannot be on the list $s_0, s_1, s_2, \ldots$.

	0	1	2	3	...
0	$\mathbf{s_0(0)}$	$s_0(1)$	$s_0(2)$	$s_0(3)$	...
1	$s_1(0)$	$\mathbf{s_1(1)}$	$s_1(2)$	$s_1(3)$	...
2	$s_2(0)$	$s_2(1)$	$\mathbf{s_2(2)}$	$s_2(3)$	...
3	$s_3(0)$	$s_3(1)$	$s_3(2)$	$\mathbf{s_3(3)}$	...
⋮	⋮	⋮	⋮	⋮	⋱

Comparing Size of Sets

- A is equinumerous with B (have the same size or cardinality as B), written $A \approx B$, iff there is a bijection $f : A \longrightarrow B$. Equinumerosity is an equivalence relation (Prove!).

- For any two sets A and B, we say that A is no larger than B, written $A \preceq B$, iff there is an injection function $f : A \longrightarrow B$.
- A is smaller than B, written $A \prec B$, iff there is an injection $f : A \longrightarrow B$ but no bijection $g : A \longrightarrow B$; in other words : $A \preceq B$ and $A \not\approx B$

The Schröder–Bernstein Theorem

- For any two sets A and B, If $A \preceq B$ and $B \preceq A$, then $A \approx B$. In other words, if there is an injection from A to B, and an injection from B to A, then there is a bijection from A to B.
- It can be difficult to think of a bijection between two equinumerous sets. The Theorem allows us to break the comparison down into two cases.
- This result, is really difficult to prove. Indeed, although Cantor stated the result, others proved it.

Prove These!

- **Theorem**: $\mathbb{N} \prec \mathbb{R}$
- **Theorem**: A $\prec \wp$(A), for any set A.
- **Theorem**: Every subset of an enumerable set is enumerable.
- **Theorem**: Enumerable (countable) union of enumerable sets is enumerable.
- **Theorem**: If B is any enumerable subset of a non-enumerable set A,

  then A $\setminus$ B is non-enumerable.