Classifying Relations Based on its Graph

function: if it has [$\leq$ 1 arrow **out**] property

total: if it has [$\geq$ 1 arrow **out**] property

surjective: if it has [$\geq$ 1 arrow **in**] property

injective: if it has [$\leq$ 1 arrow **in**] property

bijective: if it has *all of the above properties*
i.e., it has [$=$ 1 arrow **out**] and [$=$ 1 arrow **in**].

Using Injection and Surjection to Relate Set Cardinalities

A surj B iff there is a *surjective* function from A to B

A inj B iff there is a *injective, total* function from A to B

A bij B iff there is a *bijection* from A to B

Using Injection and Surjection to Relate Set Cardinalities

A surj B iff there is a *surjective* function from A to B

A inj B iff there is a *injective, total* function from A to B

A bij B iff there is a *bijection* from A to B

For *finite* sets

- $|A| \geq |B|$ iff A *surj* B
- $|A| \leq |B|$ iff A *inj* B
- $|A| = |B|$ iff A *bij* B

Counting Using Bijections: Power Set Size Revisited

Counting Infinite Sets (Textbook §7.1)

Can we use the same ideas as finite sets?

- $|A| \geq |B|$ iff A *surj* B
- $|A| \leq |B|$ iff A *inj* B
- $|A| = |B|$ iff A *bij* B

Counting Infinite Sets (Textbook §7.1)

Can we use the same ideas as finite sets?

- $|A| \geq |B|$ iff A *surj* B
- $|A| \leq |B|$ iff A *inj* B
- $|A| = |B|$ iff A *bij* B

Basically. But:

- There are some unintuitive things about the "size" of infinite sets
- We don't know how to say one set is stricly larger
- We don't know how to measure the size of an infinite set.

We will ignore the third problem, and just talk about comparing sizes.

Infinite Sets are Different ...

For finite sets, adding an element strictly increases its size

- i.e., if A is finite, and $b \notin A$, there is no bijection from A to $A \cup \{b\}$

Infinite Sets are Different ...

For finite sets, adding an element strictly increases its size

- i.e., if A is finite, and $b \notin A$, there is no bijection from A to $A \cup \{b\}$

This is not true for infinite sets

Infinite Sets are Different ...

For finite sets, adding an element strictly increases its size

- i.e., if A is finite, and $b \notin A$, there is no bijection from A to $A \cup \{b\}$

This is not true for infinite sets In fact:

A set A is infinite iff there is a bijection from A to $A \cup \{b\}$

Countable and Infinite Sets

Countability of set A

- A is countable if its elements can be listed in some order $c_0, c_1, c_2, \ldots$ such that *every element will eventually appear in the list.*
- Equivalently, there is a surjection from $\mathbb{N}$ to A.

Countable and Infinite Sets

Countability of set A

- A is countable if its elements can be listed in some order $c_0, c_1, c_2, \ldots$ such that *every element will eventually appear in the list.*
- Equivalently, there is a surjection from $\mathbb{N}$ to A.

Countably infinite: Infinite and countable.

- In other words, there is a bijection from $\mathbb{N}$ to A.

Countable: Finite or countably infinite

Proving Countability of Sets

Strategy 1

- Identify an enumeration order for the set
- Show that every element will eventually occur in that order.

Example: The set $\mathbb{Z}$

Properties of Countable Sets

Countable sets are closed under union, intersection and set product

If A and B are countable, then the following sets are countable as well:

- $A \cup B$
- $A \cap B$
- $A \times B$

Proving Countability of Sets

Strategy 2

- Use closure properties.

Examples: The set $\mathbb{Q}$

Proving Countability of Sets

Strategy 2

- Use closure properties.

Examples: The set of complex rational numbers of the form $p + qi$ where p and q are rational

Proving Countability of Sets

Strategy 1

- Identify an enumeration order for the set
- Show that every element will eventually occur in that order.

Example: The set of all finite-length strings over a finite alphabet

Proving Countability of Sets

Strategy 1

- Identify an enumeration order for the set
- Show that every element will eventually occur in that order.

Example: The set of all finite-length strings over a countably infinite alphabet

Strict Inequality on Infinite Set Cardinality

$$\boxed{A \text{ strict } B \text{ iff } \neg(A \text{ surj } B)}$$

- On finite sets, “strict” obviously means strictly smaller. But what about infinite sets?

Strict Inequality on Infinite Set Cardinality

$$\boxed{A \text{ strict } B \text{ iff } \neg(A \text{ surj } B)}$$

- On finite sets, "strict" obviously means strictly smaller. But what about infinite sets? We will take it as a given that it holds for infinite sets as well.

Power Sets are Strictly Larger

Theorem [Cantor]

A strict $\wp(A)$

- So far, our proofs involved constructing a surjective or bijective mapping
- But now, we need to show no such mapping is possible. How in the world can we do that?

Power Sets are Strictly Larger

Theorem [Cantor]

$A \text{ strict } \wp(A)$

- So far, our proofs involved constructing a surjective or bijective mapping
- But now, we need to show no such mapping is possible. How in the world can we do that?

Answer: We need new proof techniques

Power Sets are Strictly Larger

Theorem [Cantor]

A strict $\wp(A)$

- So far, our proofs involved constructing a surjective or bijective mapping
- But now, we need to show no such mapping is possible. How in the world can we do that?

Answer: We need new proof techniques

We use *Diagonalization*, a particular form of proof by contradiction.

Diagonalization: Uncountability of infinite strings over {0,1}

$$
\begin{array}{ll}
s_1 & = \color{red}{0}\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \ldots \\
s_2 & = 1\ \color{red}{1}\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \ldots \\
s_3 & = 0\ 1\ \color{red}{0}\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ \ldots \\
s_4 & = 1\ 0\ 1\ \color{red}{0}\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \ldots \\
s_5 & = 1\ 1\ 0\ 1\ \color{red}{0}\ 1\ 1\ 0\ 1\ 0\ 1\ \ldots \\
s_6 & = 0\ 0\ 1\ 1\ 0\ \color{red}{1}\ 1\ 0\ 1\ 1\ 0\ \ldots \\
s_7 & = 1\ 0\ 0\ 0\ 1\ 0\ \color{red}{0}\ 0\ 1\ 0\ 0\ \ldots \\
s_8 & = 0\ 0\ 1\ 1\ 0\ 0\ 1\ \color{red}{1}\ 0\ 0\ 1\ \ldots \\
s_9 & = 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ \color{red}{1}\ 1\ 0\ \ldots \\
s_{10} & = 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ \color{red}{0}\ 1\ \ldots \\
s_{11} & = 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ \color{red}{0}\ \ldots \\
\vdots & \quad \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \ddots
\end{array}
$$

$$
s = \color{blue}{1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1}\ \ldots
$$

Diagonalization: Uncountability of infinite strings over {0,1}

s_1	=	**0**	0	0	0	0	0	0	0	0	0	0	...
s_2	=	1	**1**	1	1	1	1	1	1	1	1	1	...
s_3	=	0	1	**0**	1	0	1	0	1	0	1	0	...
s_4	=	1	0	1	**0**	1	0	1	0	1	0	1	...
s_5	=	1	1	0	1	**0**	1	1	0	1	0	1	...
s_6	=	0	0	1	1	0	**1**	1	0	1	1	0	...
s_7	=	1	0	0	0	1	0	**0**	0	1	0	0	...
s_8	=	0	0	1	1	0	0	1	**1**	0	0	1	...
s_9	=	1	1	0	0	1	1	0	0	**1**	1	0	...
s_{10}	=	1	1	0	1	1	1	0	0	1	**0**	1	...
s_{11}	=	1	1	0	1	0	1	0	0	1	0	**0**	...
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

s	=	1	0	1	1	1	0	1	0	0	1	1	...

Can prove uncountability of real numbers using this

- Focus on real numbers over $[0, 1)$
  - We can define a bijection from $\mathbb{R}$ to real numbers of $[0, 1)$, so they contain the same number of elements.
- Each real number over $[0, 1)$ can be expressed as a binary number $0.d_1 d_2 d_3 \cdots$ where each d_i is a 0 or 1.

Diagonalization: Proving that $\wp(\mathbb{N})$ is uncountable

Idea

- List $\wp(\mathbb{N})$ in some order $S_1, S_2, \ldots$
- Construct S by drawing at least one element in $n_i \in \mathbb{N}$ that is not included in S_i
  - n_i is a *witness* to verify $S \neq S_i$
- $S \subseteq \mathbb{N}$ but will never appear in the enumeration – a contradiction.. ■

Diagonalization: Proving that $\wp(\mathbb{N})$ is uncountable

Idea

- List $\wp(\mathbb{N})$ in some order $S_1, S_2, \ldots$
- Construct S by drawing at least one element in $n_i \in \mathbb{N}$ that is not included in S_i
  - n_i is a *witness* to verify $S \neq S_i$
- $S \subseteq \mathbb{N}$ but will never appear in the enumeration – a contradiction.. ∎

Unfortunately, this is not a correct proof.

- What if some set includes every element?

Proving that $\wp(\mathbb{N})$ is uncountable: 2nd Attempt

- Why not apply our idea of a bijection between subsets and bitstrings that we used for counting $\wp(A)$?

Proving that $\wp(\mathbb{N})$ is uncountable: 2nd Attempt

- Why not apply our idea of a bijection between subsets and bitstrings that we used for counting $\wp(A)$?
- Because the subsets are countably infinite, the string lengths will be countably infinite.

Proving that $\wp(\mathbb{N})$ is uncountable: 2nd Attempt

- Why not apply our idea of a bijection between subsets and bitstrings that we used for counting $\wp(A)$?
- Because the subsets are countably infinite, the string lengths will be countably infinite.

s_1	=	0	0	0	0	0	0	0	0	0	0	0	...
s_2	=	1	1	1	1	1	1	1	1	1	1	1	...
s_3	=	0	1	0	1	0	1	0	1	0	1	0	...
s_4	=	1	0	1	0	1	0	1	0	1	0	1	...
s_5	=	1	1	0	1	0	1	1	0	1	0	1	...
s_6	=	0	0	1	1	0	1	1	0	1	1	0	...
s_7	=	1	0	0	0	1	0	0	0	1	0	0	...
s_8	=	0	0	1	1	0	0	1	1	0	0	1	...
s_9	=	1	1	0	0	1	1	0	0	1	1	0	...
s_{10}	=	1	1	0	1	1	1	0	0	1	0	1	...
s_{11}	=	1	1	0	1	0	1	0	0	1	0	0	...
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

s	=	1	0	1	1	1	0	1	0	0	1	1	...

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- We can't use the proof from slide because it relies on A being enumerable.
  - The bit strings we use contain countably infinite digits
- Instead, we need to think directly in terms of surjections:
  - *Assume, contrary to the theorem, there is a surjection* $g\colon A \longrightarrow \wp(A)$

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- We can't use the proof from slide because it relies on A being enumerable.
  - The bit strings we use contain countably infinite digits
- Instead, we need to think directly in terms of surjections:
  - *Assume, contrary to the theorem, there is a surjection* $g\colon A \longrightarrow \wp(A)$
- The witness idea is still the key:
  - Specifically, define $S = \{a \in A | a \notin g(a)\}$
  - i.e., such a's don't point to a set containing themselves

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- We can't use the proof from slide because it relies on A being enumerable.
  - The bit strings we use contain countably infinite digits
- Instead, we need to think directly in terms of surjections:
  - *Assume, contrary to the theorem, there is a surjection* $g\colon A \longrightarrow \wp(A)$
- The witness idea is still the key:
  - Specifically, define $S = \{a \in A | a \notin g(a)\}$
  - i.e., such a's don't point to a set containing themselves
- "S is the set of elements that don't point to themselves"

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- We can't use the proof from slide because it relies on A being enumerable.
  - The bit strings we use contain countably infinite digits
- Instead, we need to think directly in terms of surjections:
  - *Assume, contrary to the theorem, there is a surjection $g\colon A \longrightarrow \wp(A)$*
- The witness idea is still the key:
  - Specifically, define $S = \{a \in A | a \notin g(a)\}$
  - i.e., such a's don't point to a set containing themselves
- "S is the set of elements that don't point to themselves"
- *Now, who will point to S?*

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- *Who will point to S?*
  - Since g is a surjection and $S \subseteq A$, *there must be* an $x \in A$ such that $g(x) = S$.
  - i.e., "x points to the elements of S"

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- *Who will point to S?*
  - Since g is a surjection and $S \subseteq A$, *there must be* an $x \in A$ such that $g(x) = S$.
  - i.e., "x points to the elements of S"
- Now, do a case-split on whether x itself is in S:

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- *Who will point to S?*
  - Since g is a surjection and $S \subseteq A$, *there must be* an $x \in A$ such that $g(x) = S$.
  - i.e., "x points to the elements of S"
- Now, do a case-split on whether x itself is in S:

  $x \in S$: Then, x is "pointing to itself"
    - by definition, S leaves out such x, so this case is impossible

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- *Who will point to S?*
  - Since g is a surjection and $S \subseteq A$, *there must be* an $x \in A$ such that $g(x) = S$.
  - i.e., "x points to the elements of S"
- Now, do a case-split on whether x itself is in S:

  $x \in S$: Then, x is "pointing to itself"
    - by definition, S leaves out such x, so this case is impossible

  $x \notin S$: Then, "x is not pointing to itself"
    - By definition, S includes such x, so this case is impossible as well.

Diagonalization: Proof of Cantor's Theorem (A strict $\wp(A)$)

- *Who will point to S?*
  - Since g is a surjection and $S \subseteq A$, *there must be* an $x \in A$ such that $g(x) = S$.
  - i.e., "x points to the elements of S"
- Now, do a case-split on whether x itself is in S:

  $x \in S$: Then, x is "pointing to itself"
  - by definition, S leaves out such x, so this case is impossible

  $x \notin S$: Then, "x is not pointing to itself"
  - By definition, S includes such x, so this case is impossible as well.

As we have reached a contradiction in all cases, our original assumption about the existence of g must be false.

- No surjective function from A to $\wp(A)$ is possible. ■