CSE 215: Foundations of Computer Science

(Functions)

Pramod Ganapathil
Department of Computer Science
State University of New York at Stony Brook

January 11, 2020
## Contents

- One-to-One, Onto, One-to-One Correspondences, Inverse Functions
- Composition of Functions
- Infinite Sets
One-to-One, Onto, One-to-One Correspondences, Inverse Functions
One-to-one functions

- What is the difference between the two marriage functions?

Every female is a wife of at most one male.

One-to-one function

There is a female who is a wife of at least two males.

Not a one-to-one function
One-to-one functions

- What is the difference between the two marriage functions?

- Every female is a wife of at most one male
  - One-to-one function

- There is a female who is a wife of at least two males
  - Not a one-to-one function
### One-to-one functions

**Definition**

- A function $F : X \to Y$ is **one-to-one** (or injective) if and only if for all elements $x_1$ and $x_2$ in $X$,

  
  - if $F(x_1) = F(x_2)$, then $x_1 = x_2$, or
  
  - if $x_1 \neq x_2$, then $F(x_1) \neq F(x_2)$.

- A function $F : X \to Y$ is **one-to-one** $\iff$

  $\forall x_1, x_2 \in X$, if $F(x_1) = F(x_2)$ then $x_1 = x_2$.

- A function $F : X \to Y$ is **not one-to-one** $\iff$

  $\exists x_1, x_2 \in X$, if $F(x_1) = F(x_2)$ then $x_1 \neq x_2$. 

Problem

- Prove that a function $f$ is one-to-one.

Proof

Direct proof.

Suppose $x_1$ and $x_2$ are elements of $X$ such that $f(x_1) = f(x_2)$.

Show that $x_1 = x_2$.

Proof

Counterexample.

Find elements $x_1$ and $x_2$ in $X$ so that $f(x_1) = f(x_2)$ but $x_1 \neq x_2$. 
Problem

• Prove that a function $f$ is one-to-one.

Proof

Direct proof.

• Suppose $x_1$ and $x_2$ are elements of $X$ such that $f(x_1) = f(x_2)$.
• Show that $x_1 = x_2$. 
<table>
<thead>
<tr>
<th>Problem</th>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that a function $f$ is one-to-one.</td>
<td>Direct proof.</td>
</tr>
<tr>
<td></td>
<td>• Suppose $x_1$ and $x_2$ are elements of $X$ such that $f(x_1) = f(x_2)$.</td>
</tr>
<tr>
<td></td>
<td>• Show that $x_1 = x_2$.</td>
</tr>
<tr>
<td>Problem</td>
<td></td>
</tr>
<tr>
<td>• Prove that a function $f$ is not one-to-one.</td>
<td></td>
</tr>
</tbody>
</table>
One-to-one functions: Proof technique

Problem
• Prove that a function \( f \) is one-to-one.

Proof

Direct proof.
• Suppose \( x_1 \) and \( x_2 \) are elements of \( X \) such that \( f(x_1) = f(x_2) \).
• Show that \( x_1 = x_2 \).

Problem
• Prove that a function \( f \) is not one-to-one.

Proof

Counterexample.
• Find elements \( x_1 \) and \( x_2 \) in \( X \) so that \( f(x_1) = f(x_2) \) but \( x_1 \neq x_2 \).
Problem

• Define $f : \mathbb{R} \to \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Is $f$ one-to-one? Prove or give a counterexample.
## One-to-one functions: Example 1

**Problem**

- Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Is $f$ one-to-one? Prove or give a counterexample.

**Proof**

**Direct proof.**

- Suppose $x_1$ and $x_2$ are elements of $X$ such that $f(x_1) = f(x_2)$.

  $\implies 4x_1 - 1 = 4x_2 - 1$ (∵ Defn. of $f$)

  $\implies 4x_1 = 4x_2$ (∵ Add 1 on both sides)

  $\implies x_1 = x_2$ (∵ Divide by 4 on both sides)

- Hence, $f$ is one-to-one.
Problem

- Define $g : \mathbb{Z} \rightarrow \mathbb{Z}$ by the rule $g(n) = n^2$ for all $n \in \mathbb{Z}$. Is $g$ one-to-one? Prove or give a counterexample.
Problem

- Define \( g : \mathbb{Z} \rightarrow \mathbb{Z} \) by the rule \( g(n) = n^2 \) for all \( n \in \mathbb{Z} \). Is \( g \) one-to-one? Prove or give a counterexample.

Proof

Direct proof.

- Suppose \( n_1 \) and \( n_2 \) are elements of \( X \) such that \( g(n_1) = g(n_2) \).
  
  \[ \implies n_1^2 = n_2^2 \quad (\because \text{Defn. of } g) \]
  
  \[ \implies n_1 = n_2 \quad (\because \text{Taking square root on both sides}) \]

- Hence, \( g \) is one-to-one.
<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Define $g : \mathbb{Z} \rightarrow \mathbb{Z}$ by the rule $g(n) = n^2$ for all $n \in \mathbb{Z}$. Is $g$ one-to-one? Prove or give a counterexample.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Direct proof.</strong></td>
</tr>
<tr>
<td>• Suppose $n_1$ and $n_2$ are elements of $X$ such that $g(n_1) = g(n_2)$.</td>
</tr>
<tr>
<td>$\implies n_1^2 = n_2^2$ (\because Defn. of $g$)</td>
</tr>
<tr>
<td>$\implies n_1 = n_2$ (\because Taking square root on both sides)</td>
</tr>
<tr>
<td>• Hence, $g$ is one-to-one.</td>
</tr>
</tbody>
</table>

• **Incorrect! What's wrong?**
One-to-one functions: Example 2

Problem

- Define \( g : \mathbb{Z} \to \mathbb{Z} \) by the rule \( g(n) = n^2 \) for all \( n \in \mathbb{Z} \). Is \( g \) one-to-one? Prove or give a counterexample.

Proof

Counterexample.

- Let \( n_1 = -1 \) and \( n_2 = 1 \).
  \[ g(n_1) = (-1)^2 = 1 \] and \( g(n_2) = 1^2 = 1 \)
  \[ \implies g(n_1) = g(n_2) \text{ but, } n_1 \neq n_2 \]
- Hence, \( g \) is not one-to-one.
Onto functions

What is the difference between the two marriage functions?

Every female is a wife

Not an onto function
What is the difference between the two marriage functions?

- Every female is a wife
- Onto function

- There is a female who is not a wife
- Not an onto function
Onto functions

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A function $F : X \to Y$ is <strong>onto</strong> (or surjective) if and only if given any element $y$ in $Y$, it is possible to find an element $x$ in $X$ with the property that $y = F(x)$.</td>
</tr>
</tbody>
</table>
| • A function $F : X \to Y$ is **onto** $\iff$ $
\forall y \in Y, \exists x \in X \text{ such that } F(x) = y.$
A function $F : X \to Y$ is **not onto** $\iff$
$\exists y \in Y, \forall x \in X \text{ such that } F(x) \neq y.$ |
Problem

• Prove that a function $f$ is onto.
## Onto functions: Proof technique

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Prove that a function $f$ is onto.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Direct proof.</strong></td>
</tr>
<tr>
<td>● <strong>Suppose</strong> that $y$ is any element of $Y$</td>
</tr>
<tr>
<td>● <strong>Show</strong> that there is an element $x$ of $X$ with $F(x) = y$</td>
</tr>
</tbody>
</table>
## Onto functions: Proof technique

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that a function $f$ is onto.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Direct proof.</strong></td>
</tr>
<tr>
<td>• <strong>Suppose</strong> that $y$ is any element of $Y$</td>
</tr>
<tr>
<td>• <strong>Show</strong> that there is an element $x$ of $X$ with $F(x) = y$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that a function $f$ is not onto.</td>
</tr>
</tbody>
</table>
### Onto functions: Proof technique

<table>
<thead>
<tr>
<th>Problem</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that a function $f$ is onto.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct proof.</td>
<td></td>
</tr>
<tr>
<td>• Suppose that $y$ is any element of $Y$</td>
<td></td>
</tr>
<tr>
<td>• Show that there is an element $x$ of $X$ with $F(x) = y$</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that a function $f$ is not onto.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterexample.</td>
<td></td>
</tr>
<tr>
<td>• Find an element $y$ of $Y$ such that $y \neq F(x)$ for any $x$ in $X$.</td>
<td></td>
</tr>
</tbody>
</table>
Problem

- Define \( f : \mathbb{R} \rightarrow \mathbb{R} \) by the rule \( f(x) = 4x - 1 \) for all \( x \in \mathbb{R} \). Is \( f \) onto? Prove or give a counterexample.

Proof

Direct proof. Let \( y \in \mathbb{R} \). We need to show that \( \exists x \) such that \( f(x) = y \).

Let \( x = \frac{y + 1}{4} \). Then \( f \left( \frac{y + 1}{4} \right) = 4 \left( \frac{y + 1}{4} \right) - 1 = y \) (∵ Defn. of \( f \)).

Hence, \( f \) is onto.
Problem

• Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Is $f$ onto? Prove or give a counterexample.

Proof

Direct proof.

• Let $y \in \mathbb{R}$. We need to show that $\exists x$ such that $f(x) = y$.
  
  Let $x = \frac{y+1}{4}$. Then
  
  $f \left( \frac{y+1}{4} \right) = 4 \left( \frac{y+1}{4} \right) - 1$ \hspace{1cm} (\because \text{Defn. of } f)
  
  $= y$ \hspace{1cm} (\because \text{Simplify})

• Hence, $f$ is onto.
Problem

- Define $g : \mathbb{Z} \rightarrow \mathbb{Z}$ by the rule $g(n) = 4n - 1$ for all $n \in \mathbb{Z}$. Is $g$ onto? Prove or give a counterexample.
Onto functions: Example 2

Problem

- Define $g : \mathbb{Z} \rightarrow \mathbb{Z}$ by the rule $g(n) = 4n - 1$ for all $n \in \mathbb{Z}$. Is $g$ onto? Prove or give a counterexample.

Proof

Direct proof.

- Let $m \in \mathbb{Z}$. We need to show that $\exists n$ such that $g(n) = m$.
  - Let $n = \frac{m+1}{4}$. Then
  - $g \left( \frac{m+1}{4} \right) = 4 \left( \frac{m+1}{4} \right) - 1 \quad (\because \text{Defn. of } g)$
  - $= m \quad (\because \text{Simplify})$
- Hence, $g$ is onto.
Problem

- Define $g : \mathbb{Z} \rightarrow \mathbb{Z}$ by the rule $g(n) = 4n - 1$ for all $n \in \mathbb{Z}$. Is $g$ onto? Prove or give a counterexample.

Proof

Direct proof.

- Let $m \in \mathbb{Z}$. We need to show that $\exists n$ such that $g(n) = m$.
  - Let $n = \frac{m+1}{4}$. Then
    
    
    
    
    $g \left( \frac{m+1}{4} \right) = 4 \left( \frac{m+1}{4} \right) - 1 \quad (\because \text{Defn. of } g)$
    
    
    
    
    $= m \quad (\because \text{Simplify})$
  
  - Hence, $g$ is onto.

- Incorrect! What's wrong?
Onto functions: Example 2

Problem
- Define \( g : \mathbb{Z} \rightarrow \mathbb{Z} \) by the rule \( g(n) = 4n - 1 \) for all \( n \in \mathbb{Z} \). Is \( g \) onto? Prove or give a counterexample.

Proof

Counterexample.
- We know that \( 0 \in \mathbb{Z} \).
- Let \( g(n) = 0 \) for some integer \( n \).
  \[ \implies 4n - 1 = 0 \quad (\because \text{Defn. of } g) \]
  \[ \implies n = \frac{1}{4} \quad (\because \text{Simplify}) \]
  But \( \frac{1}{4} \notin \mathbb{Z} \).
  So, \( g(n) \neq 0 \) for any integer \( n \).
- Hence, \( g \) is not onto.
What is the difference between the three marriage functions?
What is the difference between the three marriage functions?

- Every female is a wife of at most one male
- **One-to-one**
- **Not onto**

- Every female is a wife of exactly one male
- **Onto**
- **Not one-to-one**

- Every female is a wife of especially one male
- **One-to-one**
- **Onto**
One-to-one correspondences

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A <strong>one-to-one correspondence</strong> (or bijection) from a set $X$ to a set $Y$ is a function $F : X \rightarrow Y$ that is both one-to-one and onto.</td>
</tr>
<tr>
<td>• <strong>Intuition:</strong> One-to-one correspondence $= \text{One-to-one} + \text{Onto}$</td>
</tr>
</tbody>
</table>
## One-to-one correspondences: Example 1

<table>
<thead>
<tr>
<th>Subset of ( {a, b, c, d} )</th>
<th>4-tuple of ( {0, 1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>{}</td>
<td>( (0, 0, 0, 0) )</td>
</tr>
<tr>
<td>{a}</td>
<td>( (1, 0, 0, 0) )</td>
</tr>
<tr>
<td>{b}</td>
<td>( (0, 1, 0, 0) )</td>
</tr>
<tr>
<td>{c}</td>
<td>( (0, 0, 1, 0) )</td>
</tr>
<tr>
<td>{d}</td>
<td>( (0, 0, 0, 1) )</td>
</tr>
<tr>
<td>{a, b}</td>
<td>( (1, 1, 0, 0) )</td>
</tr>
<tr>
<td>{a, c}</td>
<td>( (1, 0, 1, 0) )</td>
</tr>
<tr>
<td>{a, d}</td>
<td>( (1, 0, 0, 1) )</td>
</tr>
<tr>
<td>{b, c}</td>
<td>( (0, 1, 1, 0) )</td>
</tr>
<tr>
<td>{b, d}</td>
<td>( (0, 1, 0, 1) )</td>
</tr>
<tr>
<td>{c, d}</td>
<td>( (0, 0, 1, 1) )</td>
</tr>
<tr>
<td>{a, b, c}</td>
<td>( (1, 1, 1, 0) )</td>
</tr>
<tr>
<td>{a, b, d}</td>
<td>( (1, 1, 0, 1) )</td>
</tr>
<tr>
<td>{a, c, d}</td>
<td>( (1, 0, 1, 1) )</td>
</tr>
<tr>
<td>{b, c, d}</td>
<td>( (0, 1, 1, 1) )</td>
</tr>
<tr>
<td>{a, b, c, d}</td>
<td>( (1, 1, 1, 1) )</td>
</tr>
</tbody>
</table>
Problem

- Define $F : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ by the rule $F(x, y) = (x + y, x - y)$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is $F$ a one-to-one correspondence? Prove or give a counterexample.
## Problem

- Define $F : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by the rule $F(x, y) = (x + y, x - y)$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is $F$ a one-to-one correspondence? Prove or give a counterexample.

## Proof

To show that $F$ is a one-to-one correspondence, we need to show that:

1. $F$ is one-to-one.
2. $F$ is onto.
Proof (continued)

- **Proof that** \( F \) **is one-to-one.**

  Suppose that \((x_1, y_1)\) and \((x_2, y_2)\) are any ordered pairs in \( \mathbb{R} \times \mathbb{R} \) such that \( F(x_1, y_1) = F(x_2, y_2) \).

  \[
  \implies (x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2)
  \]

  \((\because \text{Defn. of } F)\)

  \[
  \implies x_1 + y_1 = x_2 + y_2 \text{ and } x_1 - y_1 = x_2 - y_2
  \]

  \((\because \text{Defn. of equality of ordered pairs})\)

  \[
  \implies x_1 = x_2 \text{ and } y_1 = y_2
  \]

  \((\because \text{Solve the two simultaneous equations})\)

  \[
  \implies (x_1, y_1) = (x_2, y_2)
  \]

  \((\because \text{Defn. of equality of ordered pairs})\)

  Hence, \( F \) is one-to-one.
Proof (continued)

- Proof that $F$ is onto.
  
  Suppose $(u, v)$ is any ordered pair in the co-domain of $F$. We will show that there is an ordered pair in the domain of $F$ that is sent to $(u, v)$ by $F$.
  
  Let $r = \frac{u+v}{2}$ and $s = \frac{u-v}{2}$. The ordered pair $(r, s)$ belongs to $\mathbb{R} \times \mathbb{R}$. Also,
  
  $$F(r, s) = F\left(\frac{u+v}{2}, \frac{u-v}{2}\right) \quad (\because \text{Defn. of } F)$$
  
  $$= \left(\frac{u+v}{2} + \frac{u-v}{2}, \frac{u+v}{2} - \frac{u-v}{2}\right) \quad (\because \text{Substitution})$$
  
  $$= (u, v) \quad (\because \text{Simplify})$$
  
  Hence, $F$ is onto.
Inverse functions

- What is the difference between the two marriage functions?

```plaintext
```
Inverse functions

What is the difference between the two marriage functions?

- $F$

- $F^{-1}$
### Definition

- Suppose $F : X \to Y$ is a one-to-one correspondence. Then, the **inverse function** $F^{-1} : Y \to X$ is defined as follows:

  Given any element $y$ in $Y$,
  
  $F^{-1}(y) =$ that unique element $x$ in $X$ such that $F(x) = y$.

- $F^{-1}(y) = x \iff y = F(x)$.
Inverse functions: Example 1

Subset of \{a, b, c, d\}  
{a}  
{b}  
{c}  
{d}  
{a, b}  
{a, c}  
{a, d}  
{b, c}  
{b, d}  
{c, d}  
{a, b, c}  
{a, b, d}  
{a, c, d}  
{b, c, d}  
{a, b, c, d}  

4-tuple of \{0, 1\}  
(0, 0, 0, 0)  
(1, 0, 0, 0)  
(0, 1, 0, 0)  
(0, 0, 1, 0)  
(0, 0, 0, 1)  
(1, 1, 0, 0)  
(1, 0, 1, 0)  
(1, 0, 0, 1)  
(0, 1, 1, 0)  
(0, 1, 0, 1)  
(0, 0, 1, 1)  
(1, 1, 1, 0)  
(1, 1, 0, 1)  
(1, 0, 1, 1)  
(0, 1, 1, 1)  
(1, 1, 1, 1)
Inverse functions: Example 2

Problem

- Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Find its inverse function.
Problem

• Define $f : \mathbb{R} \to \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Find its inverse function.

Proof

For any $y$ in $\mathbb{R}$, by definition of $f^{-1}$

• $f^{-1} = \text{unique number } x \text{ such that } f(x) = y$

Consider $f(x) = y$

$\implies 4x - 1 = y$ (\because \text{Defn. of } f)

$\implies x = \frac{y+1}{4}$ (\because \text{Simplify})

• Hence, $f^{-1}(y) = \frac{y+1}{4}$ is the inverse function.
# Inverse functions

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If $X$ and $Y$ are sets and $F : X \rightarrow Y$ is a one-to-one correspondence, then $F^{-1} : Y \rightarrow X$ is also a one-to-one correspondence.</td>
</tr>
</tbody>
</table>
## Inverse functions

### Theorem

If $X$ and $Y$ are sets and $F : X \to Y$ is a one-to-one correspondence, then $F^{-1} : Y \to X$ is also a one-to-one correspondence.

### Proof

- **$F^{-1}$ is one-to-one.**
  
  Suppose $F^{-1}(y_1) = F^{-1}(y_2)$ for some $y_1, y_2 \in Y$.
  
  We must show that $y_1 = y_2$.
  
  Let $F^{-1}(y_1) = F^{-1}(y_2) = x \in X$. Then
  
  $y_1 = F(x)$ since $F^{-1}(y_1) = x$ and
  
  $y_2 = F(x)$ since $F^{-1}(y_2) = x$.
  
  So, $y_1 = y_2$.

- **$F^{-1}$ is onto.**
  
  We must show that for any $x \in X$, there exists an element $y$ in $Y$ such that $F^{-1}(y) = x$.
  
  For any $x \in X$, we consider $y = F(x)$.
  
  We see that $y \in Y$ and $F^{-1}(y) = x$. 
Composition of Functions
Composition of functions

successor function

n

n + 1

squaring function

(n + 1)^2
Composition of functions
Definition

- Let \( f : X \rightarrow Y \) and \( g : Y \rightarrow Z \). Let the range of \( f \) is a subset of the domain of \( g \).
- Define a new composition function \( g \circ f : X \rightarrow Z \) as follows:

\[
(g \circ f)(x) = g(f(x)) \text{ for all } x \in X,
\]

where \( g \circ f \) is read “\( g \) circle \( f \)” and \( g(f(x)) \) is read “\( g \) of \( f \) of \( x \).”
Problem

- Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be the successor function and let $g : \mathbb{Z} \rightarrow \mathbb{Z}$ be the squaring function. Then $f(n) = n + 1$ for all $n \in \mathbb{Z}$ and $g(n) = n^2$ for all $n \in \mathbb{Z}$. Find $g \circ f$. Find $f \circ g$. Is $g \circ f = f \circ g$?
## Composition of functions: Example 1

**Problem**

- Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be the successor function and let $g : \mathbb{Z} \rightarrow \mathbb{Z}$ be the squaring function. Then $f(n) = n + 1$ for all $n \in \mathbb{Z}$ and $g(n) = n^2$ for all $n \in \mathbb{Z}$. Find $g \circ f$. Find $f \circ g$. Is $g \circ f = f \circ g$?

**Solution**

- $g \circ f$.
  
  $(g \circ f)(n) = g(f(n)) = g(n + 1) = (n + 1)^2$ for all $n \in \mathbb{Z}$.

- $f \circ g$.
  
  $(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1$ for all $n \in \mathbb{Z}$.

- $g \circ f \neq f \circ g$.
  
  E.g. $(g \circ f)(1) = 4$ and $(f \circ g)(1) = 2$
Problem

- Draw the arrow diagram for $g \circ f$. What is the range of $g \circ f$?

\[ \text{Range of } g \circ f = \{y, z\} \]
Composition of functions: Example 2

Problem

- Draw the arrow diagram for $g \circ f$. What is the range of $g \circ f$?

Solution

- Range of $g \circ f = \{y, z\}$. 
Composition of functions: Example 3

Problem

- Find $f \circ I_X$ and $I_Y \circ f$.

```
Problem

- Find $f \circ I_X$ and $I_Y \circ f$.

```

```
Solution

$$f \circ I_X = f.$$  
$$(f \circ I_X)(a) = f(I_X(a)) = f(a) = u.$$  
$$(f \circ I_X)(b) = f(I_X(b)) = f(b) = v.$$  
$$(f \circ I_X)(c) = f(I_X(c)) = f(c) = v.$$  
$$(f \circ I_X)(d) = f(I_X(d)) = f(d) = u.$$
```
**Problem**

- Find $f \circ I_X$ and $I_Y \circ f$.

**Solution**

- $f \circ I_X = f$.
  
- $(f \circ I_X)(a) = f(I_X(a)) = f(a) = u$
- $(f \circ I_X)(b) = f(I_X(b)) = f(b) = v$
- $(f \circ I_X)(c) = f(I_X(c)) = f(c) = v$
- $(f \circ I_X)(d) = f(I_X(d)) = f(d) = u$
Problem

- Find $f \circ I_X$ and $I_Y \circ f$.

Solution

- $I_Y \circ f = f$.

- $(I_Y \circ f)(a) = I_Y(f(a))$
  $= I_Y(u) = u$
- $(I_Y \circ f)(b) = I_Y(f(b))$
  $= I_Y(v) = v$
- $(I_Y \circ f)(c) = I_Y(f(c))$
  $= I_Y(v) = v$
- $(I_Y \circ f)(d) = I_Y(f(d))$
  $= I_Y(u) = u$
Composition of functions

**Theorem**

- If $f$ is a function from a set $X$ to a set $Y$, and $I_X$ is the identity function on $X$, and $I_Y$ is the identity function on $Y$, then $f \circ I_X = f$ and $I_Y \circ f = f$.

**Proof**

- $f \circ I_X = f$.
  \[(f \circ I_X)(x) = f(I_X(x)) = f(x).\]
- $I_Y \circ f = f$.
  \[(I_Y \circ f)(x) = I_Y(f(x)) = f(x).\]
Composition of functions: Example 4

Problem

- Find \( f^{-1} \circ f \) and \( f \circ f^{-1} \).

\[
\begin{align*}
X & \quad f \quad Y \\
\bullet a & \rightarrow \bullet x \\
\bullet b & \rightarrow \bullet y \\
\bullet c & \rightarrow \bullet z
\end{align*}
\]

\[
\begin{align*}
Y & \quad f^{-1} \quad X \\
\bullet x & \rightarrow \bullet a \\
\bullet y & \rightarrow \bullet b \\
\bullet z & \rightarrow \bullet c
\end{align*}
\]
Composition of functions: Example 4

Problem
• Find $f^{-1} \circ f$ and $f \circ f^{-1}$.

Solution
• $f^{-1} \circ f = I_X$.
  
  $$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(z) = a = I_X(a)$$
  $$(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(x) = b = I_X(b)$$
  $$(f^{-1} \circ f)(c) = f^{-1}(f(c)) = f^{-1}(y) = c = I_X(c).$$
Composition of functions: Example 4

Problem

- Find \( f^{-1} \circ f \) and \( f \circ f^{-1} \).

![Diagram]

Solution

- \( f \circ f^{-1} = I_Y \).
  
  \[
  (f \circ f^{-1})(x) = f(f^{-1}(x)) = f(b) = x = \mathcal{I}_Y(x) \\
  (f \circ f^{-1})(y) = f(f^{-1}(y)) = f(c) = y = \mathcal{I}_Y(y) \\
  (f \circ f^{-1})(z) = f(f^{-1}(z)) = f(a) = z = \mathcal{I}_Y(z).
  \]
## Composition of functions

**Theorem**

- If $f : X \to Y$ is a one-to-one and onto function with inverse function $f^{-1} : Y \to X$, then $f^{-1} \circ f = I_X$ and $f \circ f^{-1} = I_Y$.

**Proof**

- $f^{-1} \circ f = I_X$.

  To show that $f^{-1} \circ f = I_X$, we must show that for all $x \in X$, $(f^{-1} \circ f)(x) = x$. Let $x \in X$. Then
  
  $(f^{-1} \circ f)(x) = f^{-1}(f(x))$.

  Suppose $f^{-1}(f(x)) = x'$.

  $\implies f(x') = f(x)$ ($\because$ Defn. of inverse function)

  $\implies x' = x$ ($\because f$ is one-to-one)

  $\implies (f^{-1} \circ f)(x) = x$

  Hence, $f^{-1} \circ f = I_X$. 
Composition of functions

Theorem

- If \( f : X \to Y \) is a one-to-one and onto function with inverse function \( f^{-1} : Y \to X \), then \( f^{-1} \circ f = I_X \) and \( f \circ f^{-1} = I_Y \).

Proof (continued)

- \( f \circ f^{-1} = I_Y \).

  To show that \( f \circ f^{-1} = I_Y \), we must show that for all \( y \in Y \), \((f \circ f^{-1})(y) = y\). Let \( y \in Y \). Then
  \[
  (f \circ f^{-1})(x) = f(f^{-1}(y)).
  \]

  Suppose \( f(f^{-1}(y)) = y' \).
  \[
  \implies f^{-1}(y') = f^{-1}(y) \quad (\because \text{Defn. of inverse function})
  \]
  \[
  \implies y' = y \quad (\because f^{-1} \text{ is one-to-one, too})
  \]
  \[
  \implies (f \circ f^{-1})(y) = y
  \]

  Hence, \( f \circ f^{-1} = I_Y \).
Composition of one-to-one functions

$f$ is one-to-one and $g$ is one-to-one
Composition of one-to-one functions

$f$ is one-to-one and $g$ is one-to-one

$g \circ f$ is one-to-one
Composition of one-to-one functions

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are both one-to-one functions, then $g \circ f$ is one-to-one.</td>
</tr>
</tbody>
</table>
Composition of one-to-one functions

Problem

- If \( f : X \rightarrow Y \) and \( g : Y \rightarrow Z \) are both one-to-one functions, then \( g \circ f \) is one-to-one.

Proof

Direct proof.

- Suppose \( x_1 \) and \( x_2 \) are elements of \( X \). To prove that \( g \circ f \) is one-to-one we must show that:
  
  “If \( (g \circ f)(x_1) = (g \circ f)(x_2) \), then \( x_1 = x_2 \).”

Suppose \( (g \circ f)(x_1) = (g \circ f)(x_2) \).

\[
\begin{align*}
\Rightarrow & \quad g(f(x_1)) = g(f(x_2)) \quad (\because \text{Defn. of composition}) \\
\Rightarrow & \quad f(x_1) = f(x_2) \quad (\because g \text{ is one-to-one}) \\
\Rightarrow & \quad x_1 = x_2 \quad (\because f \text{ is one-to-one})
\end{align*}
\]

- Hence, \( g \circ f \) is one-to-one.
Composition of onto functions

$f$ is onto and $g$ is onto
Composition of onto functions

\[ f \text{ is onto and } g \text{ is onto} \]

\[ g \circ f \text{ is onto} \]
Composition of onto functions

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>If $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are both onto functions, then $g \circ f$ is onto.</td>
</tr>
</tbody>
</table>
Composition of onto functions

Problem

- If $f : X \to Y$ and $g : Y \to Z$ are both onto functions, then $g \circ f$ is onto.

Proof (Core idea)
Composition of onto functions

Problem

- If \( f : X \rightarrow Y \) and \( g : Y \rightarrow Z \) are both onto functions, then \( g \circ f \) is onto.

Proof

Direct proof.
- Let \( z \) be an element of \( Z \). To prove that \( g \circ f \) is onto we must show the existence of an element \( x \) in \( X \) such that \((g \circ f)(x) = z\).

There is an element \( y \) in \( Y \) such that \( g(y) = z \), because \( g \) is onto. Similarly, there is an element \( x \) in \( X \) such that \( f(x) = y \). Hence there exists an element \( x \) in \( X \) such that \((g \circ f)(x) = g(f(x)) = g(y) = z\).
- Hence, \( g \circ f \) is onto.
Infinite Sets
Finite sets

• Two finite sets are of the same size if there is a one-to-one correspondence between the two sets.
Finite sets

Two finite sets are not of the same size if there is no one-to-one correspondence between the two sets.

- Two finite sets are **not of the same size** if there is no one-to-one correspondence between the two sets.
Definition

- A finite set is one that has no elements at all or that can be put into one-to-one correspondence with a set of the form \( \{1, 2, \ldots, n\} \) for some positive integer \( n \).
Infinite sets

Definition

- An **infinite set** is a nonempty set that cannot be put into one-to-one correspondence with \( \{1, 2, \ldots, n\} \) for any positive integer \( n \).
Definition

- Let $A$ and $B$ be any sets. $A$ has the same cardinality as $B$ if, and only if, there is a one-to-one correspondence from $A$ to $B$.
- $A$ has the same cardinality as $B$ if, and only if, there is a function $f$ from $A$ to $B$ that is both one-to-one and onto.
Properties of infinite sets

Properties

For all sets $A$, $B$, and $C$:

- **Reflexive property.**
  $A$ has the same cardinality as $A$.

- **Symmetric property.**
  If $A$ has the same cardinality as $B$, then $B$ has the same cardinality as $A$.

- **Transitive property.**
  If $A$ has the same cardinality as $B$ and $B$ has the same cardinality as $C$, then $A$ has the same cardinality as $C$. 
Same cardinality

Definition

- *A* and *B* have the same cardinality if, and only if, *A* has the same cardinality as *B* or *B* has the same cardinality as *A*.
Integers and even numbers are not of the same size

There is no one-to-one correspondence between the two sets

Cardinality of integers and even numbers are different

i.e., $|\mathbb{Z}| \neq |\mathbb{Z}_{\text{even}}|$

Incorrect! What's wrong?
Integers and even numbers are not of the same size

<table>
<thead>
<tr>
<th>$\mathbb{Z}$</th>
<th>$\mathbb{Z}_{\text{even}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$-4$</td>
<td>$-4$</td>
</tr>
<tr>
<td>$-3$</td>
<td>$-2$</td>
</tr>
<tr>
<td>$-2$</td>
<td>$-2$</td>
</tr>
<tr>
<td>$-1$</td>
<td>$0$</td>
</tr>
<tr>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$1$</td>
<td>$2$</td>
</tr>
<tr>
<td>$2$</td>
<td>$2$</td>
</tr>
<tr>
<td>$3$</td>
<td>$4$</td>
</tr>
<tr>
<td>$4$</td>
<td>$4$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

- There is no one-to-one correspondence between the two sets
- Cardinality of integers and even numbers are different
  i.e., $|\mathbb{Z}| \neq |\mathbb{Z}_{\text{even}}|$
Integers and even numbers are not of the same size

<table>
<thead>
<tr>
<th>( \mathbb{Z} )</th>
<th>( \mathbb{Z}_{\text{even}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>(-4)</td>
<td>(-4)</td>
</tr>
<tr>
<td>(-3)</td>
<td>(-2)</td>
</tr>
<tr>
<td>(-2)</td>
<td>(\rightarrow)</td>
</tr>
<tr>
<td>(-1)</td>
<td>(0)</td>
</tr>
<tr>
<td>(0)</td>
<td>(\rightarrow)</td>
</tr>
<tr>
<td>(1)</td>
<td>(2)</td>
</tr>
<tr>
<td>(2)</td>
<td>(\rightarrow)</td>
</tr>
<tr>
<td>(3)</td>
<td>(4)</td>
</tr>
<tr>
<td>(4)</td>
<td>(\rightarrow)</td>
</tr>
<tr>
<td>(\vdots)</td>
<td>(\vdots)</td>
</tr>
</tbody>
</table>

- There is no one-to-one correspondence between the two sets
- Cardinality of integers and even numbers are different
  i.e., \( |\mathbb{Z}| \neq |\mathbb{Z}_{\text{even}}| \)
- Incorrect! What's wrong?
Integers and even numbers are of the same size

<table>
<thead>
<tr>
<th>( \mathbb{Z} )</th>
<th>( \mathbb{Z} \text{even} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>(-4)</td>
<td>(-8)</td>
</tr>
<tr>
<td>(-3)</td>
<td>(-6)</td>
</tr>
<tr>
<td>(-2)</td>
<td>(-4)</td>
</tr>
<tr>
<td>(-1)</td>
<td>(-2)</td>
</tr>
<tr>
<td>(0)</td>
<td>(0)</td>
</tr>
<tr>
<td>(1)</td>
<td>(2)</td>
</tr>
<tr>
<td>(2)</td>
<td>(4)</td>
</tr>
<tr>
<td>(3)</td>
<td>(6)</td>
</tr>
<tr>
<td>(4)</td>
<td>(8)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

- Take-home lesson: If we fail to identify a one-to-one correspondence, it does not mean that there is no one-to-one correspondence
Integers and even numbers are of the same size

<table>
<thead>
<tr>
<th>( \mathbb{Z} )</th>
<th>( \mathbb{Z}^{\text{even}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( -4 )</td>
<td>( -8 )</td>
</tr>
<tr>
<td>( -3 )</td>
<td>( -6 )</td>
</tr>
<tr>
<td>( -2 )</td>
<td>( -4 )</td>
</tr>
<tr>
<td>( -1 )</td>
<td>( -2 )</td>
</tr>
<tr>
<td>( 0 )</td>
<td>( 0 )</td>
</tr>
<tr>
<td>( 1 )</td>
<td>( 2 )</td>
</tr>
<tr>
<td>( 2 )</td>
<td>( 4 )</td>
</tr>
<tr>
<td>( 3 )</td>
<td>( 6 )</td>
</tr>
<tr>
<td>( 4 )</td>
<td>( 8 )</td>
</tr>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
</tbody>
</table>

- Take-home lesson: If we fail to identify a one-to-one correspondence, it does not mean that there is no one-to-one correspondence.
- There is a one-to-one correspondence between the two sets.
- Cardinality of integers and even numbers are the same.
  
i.e., \( |\mathbb{Z}| = |\mathbb{Z}^{\text{even}}| \)
## Problem

- Prove that the cardinality of integers and even numbers are the same.
<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that the cardinality of integers and even numbers are the same.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To prove that (</td>
</tr>
<tr>
<td>• Prove that ( f ) is one-to-one.</td>
</tr>
</tbody>
</table>
| Suppose \( f(n_1) = f(n_2) \).  
\[ \implies 2n_1 = 2n_2 \quad (\because \text{Defn. of } f) \]
\[ \implies n_1 = n_2 \quad (\because \text{Simplify}) \]
| • Prove that \( f \) is onto. |
| Suppose \( m \in \mathbb{Z}^{\text{even}} \).  
\[ \implies m \text{ is even} \quad (\because \text{Defn. of } \mathbb{Z}^{\text{even}}) \]
\[ \implies m = 2k \text{ for } k \in \mathbb{Z} \quad (\because \text{Defn. of even}) \]
\[ \implies f(k) = m \quad (\because \text{Defn. of } f) \]
An infinite set and its proper subset can have the same size!
**Defined Sets**

<table>
<thead>
<tr>
<th>$\mathbb{N}$</th>
<th>$A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>“First” element of $A$</td>
</tr>
<tr>
<td>$2$</td>
<td>“Second” element of $A$</td>
</tr>
<tr>
<td>$3$</td>
<td>“Third” element of $A$</td>
</tr>
<tr>
<td>$4$</td>
<td>“Fourth” element of $A$</td>
</tr>
<tr>
<td>$5$</td>
<td>“Fifth” element of $A$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

**Definition**

- A set is called **countably infinite** if, and only if, it has the same cardinality as the set of positive integers.
- A set is called **countable** if, and only if, it is finite or countably infinite. A set that is not countable is called **uncountable**.
### Integers are countable

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that the set of integers is countably infinite.</td>
</tr>
</tbody>
</table>
Integers are countable

**Problem**

- Prove that the set of integers is countably infinite.

**Solution**

\[
\begin{array}{cccccccccccc}
\cdots & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & \cdots \\
11 & 9 & 7 & 5 & 3 & 1 & 2 & 4 & 6 & 8 & 10 & & \\
\end{array}
\]
Define a function $f(n) : \mathbb{N} \rightarrow \mathbb{Z}$ such that

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is an even natural number,} \\ -\left(\frac{n-1}{2}\right) & \text{if } n \text{ is an odd natural number.} \end{cases}$$

As $f$ is a one-to-one correspondence between $\mathbb{N}$ and $\mathbb{Z}$, the set of integers is countably infinite.
Consequences of same cardinality

Suppose $A$ and $B$ be two sets such that $|A| = |B|$.
Let $f : A \rightarrow B$ be the mapping function between the two sets.

- $A$ and $B$ are finite.
  - $f$ is one-to-one $\iff f$ is onto
- $A$ and $B$ are infinite.
  - $f$ is one-to-one $\niff f$ is onto
Set of positive rationals is uncountable

<table>
<thead>
<tr>
<th>$\mathbb{N}$</th>
<th>$\mathbb{Q}^+$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

There is no one-to-one correspondence between the two sets $\mathbb{N}$ and $\mathbb{Q}^+$.

Cardinality of natural numbers and positive rationals are different, i.e., $|\mathbb{N}| \neq |\mathbb{Q}^+|$. Incorrect! What's wrong?
Set of positive rationals is uncountable

<table>
<thead>
<tr>
<th>$\mathbb{N}$</th>
<th>$\mathbb{Q}^+$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\frac{1}{1}$</td>
</tr>
<tr>
<td>2</td>
<td>$\frac{2}{1}$</td>
</tr>
<tr>
<td>3</td>
<td>$\frac{3}{1}$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

- There is no one-to-one correspondence between the two sets.
- Cardinality of natural numbers and positive rationals are different.
  i.e., $|\mathbb{N}| \neq |\mathbb{Q}^+|$
Set of positive rationals is uncountable

There is no one-to-one correspondence between the two sets
Cardinality of natural numbers and positive rationals are different
i.e., $|\mathbb{N}| \neq |\mathbb{Q}^+|$

Incorrect! What’s wrong?
Set of positive rationals is uncountable

<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>...</td>
</tr>
</tbody>
</table>

Take-home lesson: If we fail to identify a one-to-one correspondence, it does not mean that there is no one-to-one correspondence.
Set of positive rationals is countable

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that the set of positive rational numbers are countable.</td>
</tr>
</tbody>
</table>
Set of positive rationals is countable

Problem

- Prove that the set of positive rational numbers are countable.

Solution

\[ \begin{array}{cccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 & 5 & 6 & \ldots \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & \ldots \\
1 & 2 & 3 & 4 & 5 & 6 & \ldots \\
3 & 3 & 3 & 3 & 3 & 3 & 3 & \ldots \\
1 & 2 & 3 & 4 & 5 & 6 & \ldots \\
4 & 4 & 4 & 4 & 4 & 4 & 4 & \ldots \\
1 & 2 & 3 & 4 & 5 & 6 & \ldots \\
5 & 5 & 5 & 5 & 5 & 5 & 5 & \ldots \\
1 & 2 & 3 & 4 & 5 & 6 & \ldots \\
6 & 6 & 6 & 6 & 6 & 6 & 6 & \ldots \\
1 & 2 & 3 & 4 & 5 & 6 & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\end{array} \]

\[ \begin{array}{cccc}
\mathbb{N} & \mathbb{Q}^+ \\
1 & 1/1 \\
2 & 1/2 \\
3 & 2/1 \\
4 & 3/1 \\
5 & 1/3 \\
6 & 1/4 \\
7 & 2/3 \\
8 & 3/2 \\
9 & 4/1 \\
10 & 5/1 \\
\vdots & \vdots \\
\end{array} \]
**Problem**

- Prove that the set of positive rational numbers are countable.

**Solution (continued)**

- To prove that $|\mathbb{N}| = |\mathbb{Q}^+|$, we need to prove that there is a one-to-one correspondence, say $f$, between $\mathbb{N}$ and $\mathbb{Q}^+$.
- **Prove that $f$ is onto.**
  Every positive rational number appears somewhere in the grid. Every point in the grid is reached eventually.
- **Prove that $f$ is one-to-one.**
  Skipping numbers that have already been counted ensures that no number is counted twice.
Problem

- Prove that the set of all real numbers between 0 and 1 is uncountable.
### Problem

- Prove that the set of all real numbers between 0 and 1 is uncountable.

### Solution

- To prove that $|\mathbb{N}| \neq |[0..1]|$, we need to prove that there is no one-to-one correspondence between $\mathbb{N}$ and $[0..1]$.
- A powerful approach to prove the theorem is: **proof by contradiction.**
Problem

- Prove that the set of all real numbers between 0 and 1 is uncountable.

Solution

Proof by contradiction.

- Suppose $[0..1]$ is countable.
- We will derive a contradiction by showing that there is a number in $[0..1]$ that does not appear on this list.

<table>
<thead>
<tr>
<th>$\mathbb{N}$</th>
<th>$[0..1]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 $\rightarrow$</td>
<td>$0.a_{11}a_{12}a_{13} \ldots a_{1n} \ldots$</td>
</tr>
<tr>
<td>2 $\rightarrow$</td>
<td>$0.a_{21}a_{22}a_{23} \ldots a_{2n} \ldots$</td>
</tr>
<tr>
<td>3 $\rightarrow$</td>
<td>$0.a_{31}a_{32}a_{33} \ldots a_{3n} \ldots$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$n$ $\rightarrow$</td>
<td>$0.a_{n1}a_{n2}a_{n3} \ldots a_{nn} \ldots$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>
Set of real numbers in $[0, 1]$ is uncountable

### Solution (continued)

- **Suppose the list of reals starts out as follows:**

<table>
<thead>
<tr>
<th></th>
<th>0. 9 0 1 4 8 ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>0. 1 1 6 6 6 ...</td>
<td></td>
</tr>
<tr>
<td>0. 0 3 3 5 3 ...</td>
<td></td>
</tr>
<tr>
<td>0. 9 6 7 2 6 ...</td>
<td></td>
</tr>
<tr>
<td>0. 0 0 0 3 1 ...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>... ... ... ...</td>
</tr>
</tbody>
</table>

- **Construct a new number $d = 0.d_1d_2d_3\ldots d_n\ldots$ as follows:**

  $d_n = \begin{cases} 
  1 & a_{nn} \neq 1, \\
  2 & a_{nn} = 1. 
  \end{cases}$

- **We have $d = 0.12112\ldots$, i.e.,**

<table>
<thead>
<tr>
<th></th>
<th>0. 1 2 1 1 2 ...</th>
</tr>
</thead>
</table>

Observation:

For each natural number $n$, the constructed real number $d$ differs in the $n$th decimal position from the $n$th number on the list.

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This implies that $d$ is not on the list. But, $d \in [0, 1]$.

Contradiction! So, our supposition is false.

Set of real numbers in $[0, 1]$ is uncountable.
There are different types of $\infty$!
<table>
<thead>
<tr>
<th>Theorems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A subset of a countable set is countable.</td>
</tr>
<tr>
<td>• A set with an uncountable subset is uncountable.</td>
</tr>
</tbody>
</table>
\textbf{Problem}

- Prove that the set of all real numbers has the same cardinality as the set of real numbers between 0 and 1.
Prove that the set of all real numbers has the same cardinality as the set of real numbers between 0 and 1.

Let $S = \{ x \in \mathbb{R} \mid 0 < x < 1 \}$

Bend $S$ to create a circle as shown in the diagram.

Define $F : S \to \mathbb{R}$ as follows.

$F(x)$ is called the projection of $x$ onto the number line.
We show that $S$ and $\mathbb{R}$ have the same cardinality by showing that $F$ is a one-to-one correspondence.

- **$F$ is one-to-one.** Distinct points on the circle go to distinct points on the number line.
- **$F$ is onto.** Given any point $y$ on the number line, a line can be drawn through $y$ and the circle’s topmost point. This line must intersect the circle at some point $x$, and, by definition, $y = F(x)$.
Set of bit strings is countable

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that the set of all bit strings (strings of 0’s and 1’s) is countable.</td>
</tr>
</tbody>
</table>
### Problem

- Prove that the set of all bit strings (strings of 0's and 1's) is countable.

### Solution

- Define a function \( f(n) : \mathbb{N} \rightarrow \mathbb{B} \) such that

\[
f(n) = \begin{cases} 
\epsilon & \text{if } n = 1, \\
\text{k-bit binary repr. of } n - 2^k & \text{if } n > 1 \& \lfloor \log n \rfloor = k.
\end{cases}
\]
Set of bit strings is countable

Solution (continued)

<table>
<thead>
<tr>
<th>$\mathbb{N}$</th>
<th>$\mathbb{B}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\epsilon$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>00</td>
</tr>
<tr>
<td>5</td>
<td>01</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$n$</td>
<td>$f(n)$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

As $f$ is a one-to-one correspondence between $\mathbb{N}$ and $\mathbb{B}$, the set of bit strings is countably infinite.

- Generalizing, the set of strings from an alphabet consisting of a finite number of symbols is countably infinite.
Problem

- Prove that the set of all computer programs in a given computer language is countable.
Set of computer programs is countable

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that the set of all computer programs in a given computer language is countable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Let $\mathbb{P}$ denote the set of all computer programs in the given computer language.</td>
</tr>
<tr>
<td>• Any computer program in any computer language is a finite set of symbols from a finite alphabet.</td>
</tr>
<tr>
<td>• [Encoding] Translate the symbols of each program to binary string using the ASCII code.</td>
</tr>
<tr>
<td>• Sort the strings by length.</td>
</tr>
<tr>
<td>• Sort the strings of a particular length in ascending order.</td>
</tr>
<tr>
<td>• Define a function $f(n) : \mathbb{N} \rightarrow \mathbb{P}$ such that $f(n) = n$th program in $\mathbb{P}$</td>
</tr>
</tbody>
</table>
Set of computer programs is countable

<table>
<thead>
<tr>
<th>(\mathbb{N})</th>
<th>(\mathbb{P})</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(01)</td>
</tr>
<tr>
<td>2</td>
<td>(11)</td>
</tr>
<tr>
<td>3</td>
<td>(0010)</td>
</tr>
<tr>
<td>4</td>
<td>(1010)</td>
</tr>
<tr>
<td>5</td>
<td>(1011)</td>
</tr>
<tr>
<td>6</td>
<td>(00010)</td>
</tr>
<tr>
<td>7</td>
<td>(00100)</td>
</tr>
<tr>
<td>8</td>
<td>(10111)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>(n)</td>
<td>(f(n))</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

- Suppose the following are all programs in \(\mathbb{P}\) that translate to bit strings of length less than or equal to 5.

- As \(f\) is a one-to-one correspondence between \(\mathbb{N}\) and \(\mathbb{P}\), the set of bit strings is countably infinite.
Problem

• Prove that the set of all functions \( \mathbb{N} \rightarrow \{0, 1\} \) is uncountable
Problem

- Prove that the set of all functions \( \mathbb{N} \rightarrow \{0, 1\} \) is uncountable

Solution

- Let \( \mathcal{S} \) be the set of all real numbers in \([0, 1]\) represented in the form \(0.a_1a_2a_3\ldots a_n\ldots\), where \(a_i \in \{0, 1\}\).
- This representation is unique if the bit sequences that end with all 1’s are omitted. \(\quad\) △ Why?
- Let \( \mathbb{L} \) be the set of all functions \( \mathbb{N} \rightarrow \{0, 1\} \)
- We will show a 1-to-1 correspondence between \( \mathcal{S} \) and a subset of \( \mathbb{L} \) by showing we can map an element of \( \mathcal{S} \) to a unique element of \( \mathbb{L} \).
Set of all functions $\mathbb{N} \rightarrow \{0, 1\}$ is uncountable

Solution (continued)

- As $f$ is a one-to-one correspondence between $S$ and a subset of $L$, the set of functions $\mathbb{N} \rightarrow \{0, 1\}$ is uncountably infinite.
- Using this result, we can show that the set of languages (or decision problems or computable functions) is uncountable.
There is an infinite sequence of larger and larger infinities!