Discrete Mathematics

(Functions)

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

January 24, 2021

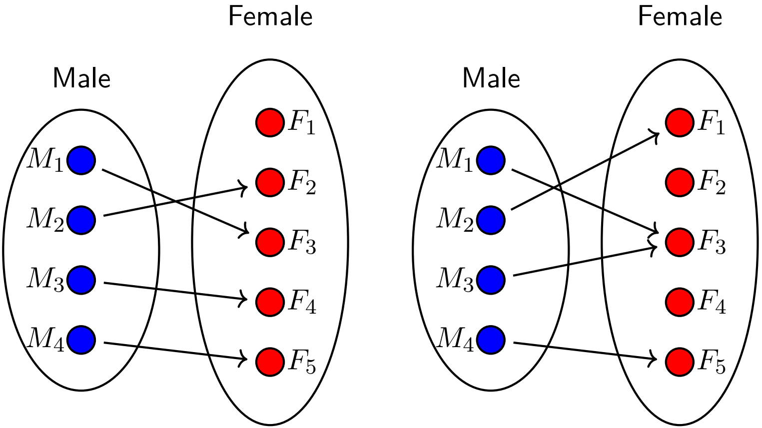
Contents

Contents

One-to-One, Onto, One-to-One Correspondences, Inverse Functions

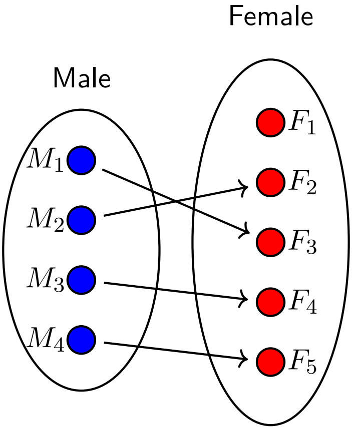
One-to-one functions

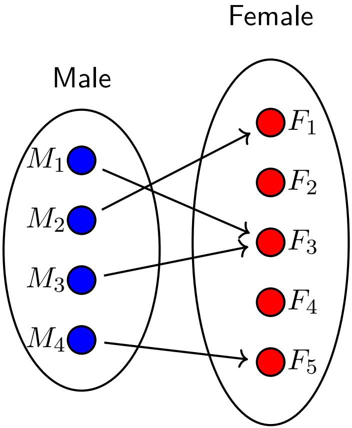
- What is the difference between the two marriage functions?



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

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,

$$\text{if } F(x_1) = F(x_2), \text{ then } x_1 = x_2, \text{ or}$$
$$\text{if } x_1 \neq x_2, \text{ then } F(x_1) \neq F(x_2).$$

- A function $F : X \to Y$ is one-to-one $\Leftrightarrow$
  $\forall x_1, x_2 \in X$, if $F(x_1) = F(x_2)$ then $x_1 = x_2$.
  A function $F : X \to Y$ is not one-to-one $\Leftrightarrow$
  $\exists x_1, x_2 \in X$, if $F(x_1) = F(x_2)$ then $x_1 \neq x_2$.

One-to-one functions: Proof technique

Problem

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

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 $x_1 = x_2$.

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.

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 $x_1 \neq x_2$.

One-to-one functions: Example 1

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

Proof

Direct proof.

- Suppose x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$.
  $\implies 4x_1 - 1 = 4x_2 - 1$ ($\because$ Defn. of f)
  $\implies 4x_1 = 4x_2$ ($\because$ Add 1 on both sides)
  $\implies x_1 = x_2$ ($\because$ Divide by 4 on both sides)
- Hence, f is one-to-one.

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.

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

Direct proof.

- Suppose n_1 and n_2 are elements of X such that $g(n_1) = g(n_2)$.
  $\implies n_1^2 = n_2^2$ $\quad$ ($\because$ Defn. of g)
  $\implies n_1 = n_2$ $\quad$ ($\because$ Taking square root on both sides)
- Hence, g is one-to-one.

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

Direct proof.

- Suppose n_1 and n_2 are elements of X such that $g(n_1) = g(n_2)$.

  $\implies n_1^2 = n_2^2 \qquad (\because$ Defn. of $g)$

  $\implies n_1 = n_2 \qquad (\because$ Taking square root on both sides$)$
- Hence, g is one-to-one.

- 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.

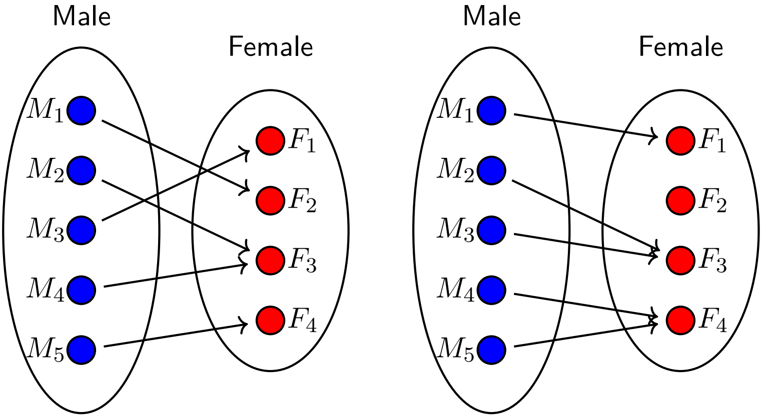
Proof

Counterexample.

- Let $n_1 = -1$ and $n_2 = 1$.
  $\implies g(n_1) = (-1)^2 = 1$ and $g(n_2) = 1^2 = 1$
  $\implies g(n_1) = g(n_2)$ but, $n_1 \neq n_2$
- Hence, g is not one-to-one.

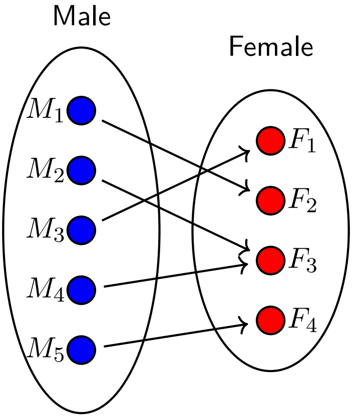
Onto functions

- What is the difference between the two marriage functions?

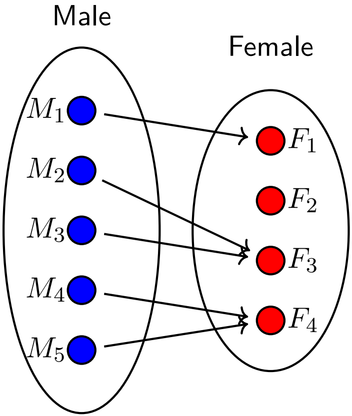


Onto functions

- 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

Definition

- A function $F : X \to Y$ is onto (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 $y = F(x)$.
- A function $F : X \to Y$ is onto $\Leftrightarrow$
  $\forall y \in Y, \exists x \in X$ such that $F(x) = y$.
  A function $F : X \to Y$ is not onto $\Leftrightarrow$
  $\exists y \in Y, \forall x \in X$ such that $F(x) \neq y$.

Onto functions: Proof technique

Problem

- Prove that a function f is onto.

Onto functions: Proof technique

Problem

- Prove that a function f is onto.

Proof

Direct proof.

- Suppose that y is any element of Y
- Show that there is an element x of X with $F(x) = y$

Onto functions: Proof technique

Problem

- Prove that a function f is onto.

Proof

Direct proof.

- Suppose that y is any element of Y
- Show that there is an element x of X with $F(x) = y$

Problem

- Prove that a function f is not onto.

Onto functions: Proof technique

Problem

- Prove that a function f is onto.

Proof

Direct proof.

- Suppose that y is any element of Y
- Show that there is an element x of X with $F(x) = y$

Problem

- Prove that a function f is not onto.

Proof

Counterexample.

- Find an element y of Y such that $y \neq F(x)$ for any x in X.

Onto functions: Example 1

Problem

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

Onto functions: Example 1

Problem

- Define $f : \mathbb{R} \to \mathbb{R}$ 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
  $f\left(\frac{y+1}{4}\right) = 4\left(\frac{y+1}{4}\right) - 1 \qquad (\because \text{Defn. of } f)$
  $= y \qquad (\because \text{Simplify})$
- Hence, f is onto.

Onto functions: Example 2

Problem

- Define $g : \mathbb{Z} \to \mathbb{Z}$ 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 $g : \mathbb{Z} \to \mathbb{Z}$ 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
  $g\left(\frac{m+1}{4}\right) = 4\left(\frac{m+1}{4}\right) - 1 \qquad (\because \text{Defn. of } g)$
  $= m \qquad (\because \text{Simplify})$
- Hence, g is onto.

Onto functions: Example 2

Problem

- Define $g : \mathbb{Z} \to \mathbb{Z}$ 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
  $g\left(\frac{m+1}{4}\right) = 4\left(\frac{m+1}{4}\right) - 1 \qquad (\because \text{Defn. of } g)$
  $= m \qquad (\because \text{Simplify})$
- Hence, g is onto.

- Incorrect! What's wrong?

Onto functions: Example 2

Problem

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

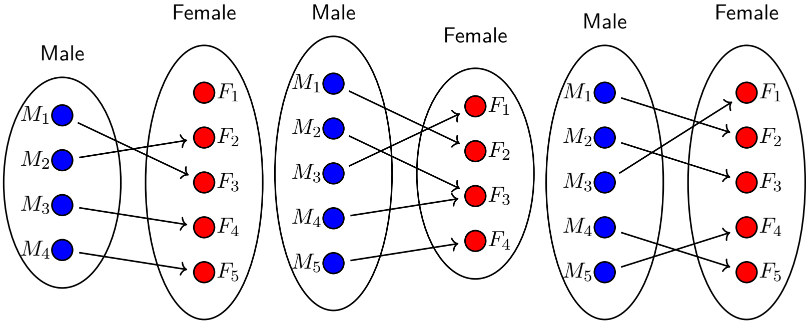
Proof

Counterexample.

- We know that $0 \in \mathbb{Z}$.
- Let $g(n) = 0$ for some integer n.
  $\Longrightarrow\ 4n - 1 = 0 \qquad (\because$ Defn. of $g)$
  $\Longrightarrow\ n = \frac{1}{4} \qquad (\because$ Simplify$)$
  But $\frac{1}{4} \notin \mathbb{Z}$.
  So, $g(n) \neq 0$ for any integer n.
- Hence, g is not onto.

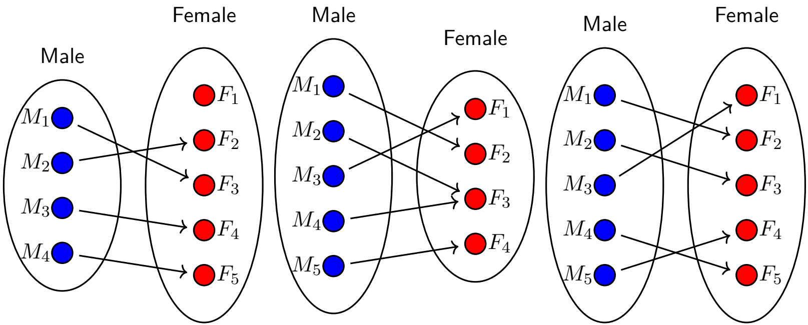
One-to-one correspondences

- What is the difference between the three marriage functions?



One-to-one correspondences

- 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
- Onto
- Not one-to-one

- Every female is a wife of exactly one male
- One-to-one
- Onto

One-to-one correspondences

Definition

- A one-to-one correspondence (or bijection) from a set X to a set Y is a function $F : X \to Y$ that is both one-to-one and onto.
- Intuition:
  One-to-one correspondence $=$ One-to-one $+$ Onto

One-to-one correspondences: Example 1

Subset of $\{a,b,c,d\}$		4-tuple of $\{0,1\}$
$\{\}$	$\longrightarrow$	$(0,0,0,0)$
$\{a\}$	$\longrightarrow$	$(1,0,0,0)$
$\{b\}$	$\longrightarrow$	$(0,1,0,0)$
$\{c\}$	$\longrightarrow$	$(0,0,1,0)$
$\{d\}$	$\longrightarrow$	$(0,0,0,1)$
$\{a,b\}$	$\longrightarrow$	$(1,1,0,0)$
$\{a,c\}$	$\longrightarrow$	$(1,0,1,0)$
$\{a,d\}$	$\longrightarrow$	$(1,0,0,1)$
$\{b,c\}$	$\longrightarrow$	$(0,1,1,0)$
$\{b,d\}$	$\longrightarrow$	$(0,1,0,1)$
$\{c,d\}$	$\longrightarrow$	$(0,0,1,1)$
$\{a,b,c\}$	$\longrightarrow$	$(1,1,1,0)$
$\{a,b,d\}$	$\longrightarrow$	$(1,1,0,1)$
$\{a,c,d\}$	$\longrightarrow$	$(1,0,1,1)$
$\{b,c,d\}$	$\longrightarrow$	$(0,1,1,1)$
$\{a,b,c,d\}$	$\longrightarrow$	$(1,1,1,1)$

One-to-one correspondences: Example 2

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.

One-to-one correspondences: Example 2

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.

One-to-one correspondences: Example 2

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 $F(x_1, y_1) = F(x_2, y_2)$.

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

  ($\because$ Defn. of F)

  $\implies x_1 + y_1 = x_2 + y_2$ and $x_1 - y_1 = x_2 - y_2$

  ($\because$ Defn. of equality of ordered pairs)

  $\implies x_1 = x_2$ and $y_1 = y_2$

  ($\because$ Solve the two simultaneous equations)

  $\implies (x_1, y_1) = (x_2, y_2)$

  ($\because$ Defn. of equality of ordered pairs)

  Hence, F is one-to-one.

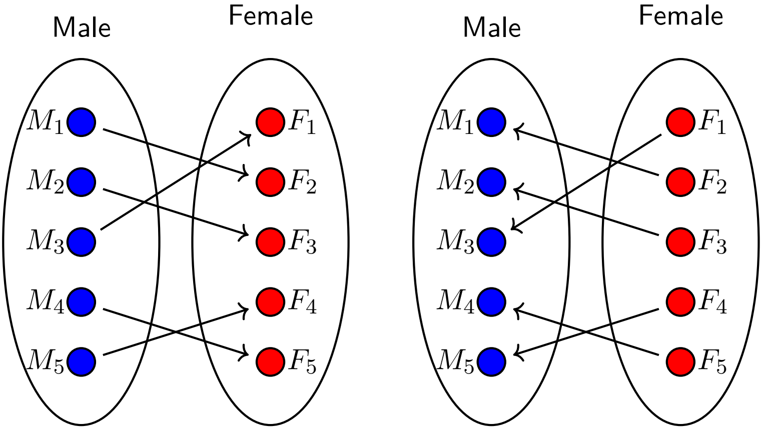
One-to-one correspondences: Example 2

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,
  $F(r, s)$
  $= F(\frac{u+v}{2}, \frac{u-v}{2}) \qquad (\because$ Defn. of $F)$
  $= (\frac{u+v}{2} + \frac{u-v}{2}, \frac{u+v}{2} - \frac{u-v}{2}) \qquad (\because$ Substitution$)$
  $= (u, v) \qquad (\because$ Simplify$)$
  Hence, F is onto.

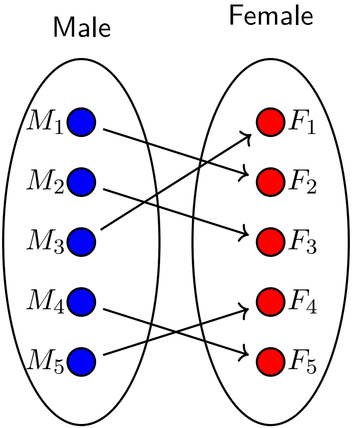
Inverse functions

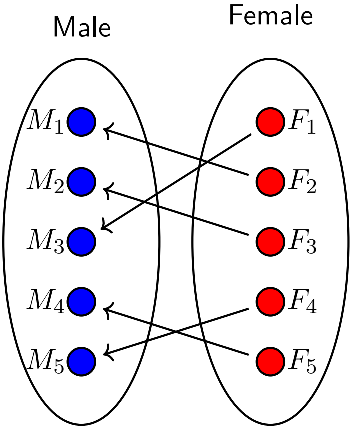
- What is the difference between the two marriage functions?



Inverse functions

- What is the difference between the two marriage functions?





- Input: male. Output: female.
- F

- Input: female. Output: male.
- F^{-1}

Inverse functions

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 $F(x) = y$.
- $F^{-1}(y) = x \Leftrightarrow y = F(x)$.

Inverse functions: Example 1

Subset of $\{a, b, c, d\}$		4-tuple of $\{0, 1\}$
$\{\}$	$\longleftarrow$	$(0, 0, 0, 0)$
$\{a\}$	$\longleftarrow$	$(1, 0, 0, 0)$
$\{b\}$	$\longleftarrow$	$(0, 1, 0, 0)$
$\{c\}$	$\longleftarrow$	$(0, 0, 1, 0)$
$\{d\}$	$\longleftarrow$	$(0, 0, 0, 1)$
$\{a, b\}$	$\longleftarrow$	$(1, 1, 0, 0)$
$\{a, c\}$	$\longleftarrow$	$(1, 0, 1, 0)$
$\{a, d\}$	$\longleftarrow$	$(1, 0, 0, 1)$
$\{b, c\}$	$\longleftarrow$	$(0, 1, 1, 0)$
$\{b, d\}$	$\longleftarrow$	$(0, 1, 0, 1)$
$\{c, d\}$	$\longleftarrow$	$(0, 0, 1, 1)$
$\{a, b, c\}$	$\longleftarrow$	$(1, 1, 1, 0)$
$\{a, b, d\}$	$\longleftarrow$	$(1, 1, 0, 1)$
$\{a, c, d\}$	$\longleftarrow$	$(1, 0, 1, 1)$
$\{b, c, d\}$	$\longleftarrow$	$(0, 1, 1, 1)$
$\{a, b, c, d\}$	$\longleftarrow$	$(1, 1, 1, 1)$

Inverse functions: Example 2

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.

Inverse functions: Example 2

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 R, by definition of f^{-1}

- $f^{-1} =$ unique number x such that $f(x) = y$
  Consider $f(x) = y$
  $\implies 4x - 1 = y \qquad (\because \text{Defn. of } f)$
  $\implies x = \frac{y+1}{4} \qquad (\because \text{Simplify})$
- Hence, $f^{-1}(y) = \frac{y+1}{4}$ is the inverse function.

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.

Inverse functions

Theorem

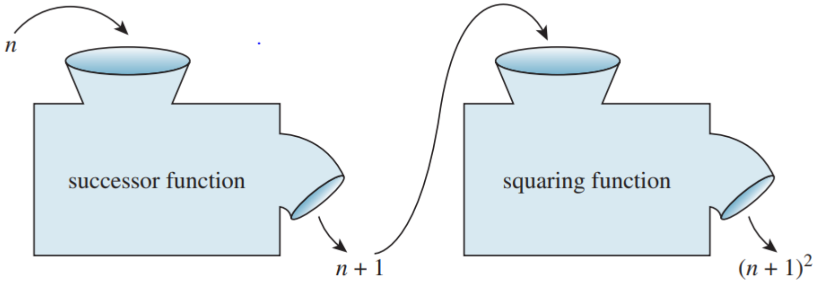
- If X and Y are sets and $F : X \to Y$ is a one-to-one correspondence, then $F^{-1} : Y \to X$ is also a one-to-one correspondence.

Proof

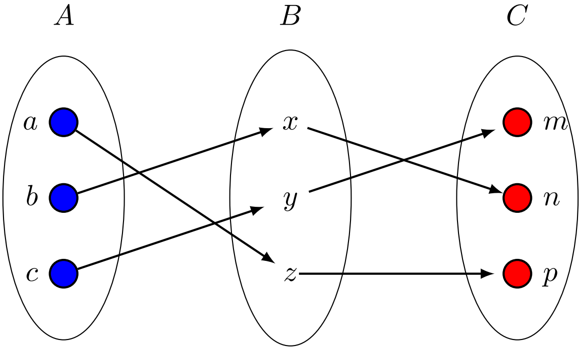
- F^{-1} is one-to-one.
  Suppose $F^{-1}(y_1) = F^{-1}(y_2)$ for some $y_1, y_2 \in Y$.
  We must show that $y_1 = y_2$.
  Let $F^{-1}(y_1) = F^{-1}(y_2) = x \in X$. Then
  $y_1 = F(x)$ since $F^{-1}(y_1) = x$ and
  $y_2 = F(x)$ since $F^{-1}(y_2) = x$.
  So, $y_1 = y_2$.
- F^{-1} is onto.
  We must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



Composition of functions



Composition of functions

Definition

- Let $f : X \to Y$ and $g : Y \to Z$. Let the range of f is a subset of the domain of g.
- Define a new composition function $g \circ f : X \to Z$ 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."

Composition of functions: Example 1

Problem

- Let $f : \mathbb{Z} \to \mathbb{Z}$ be the successor function and let $g : \mathbb{Z} \to \mathbb{Z}$ 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 $f : \mathbb{Z} \to \mathbb{Z}$ be the successor function and let $g : \mathbb{Z} \to \mathbb{Z}$ 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 $g \circ f = f \circ g$?

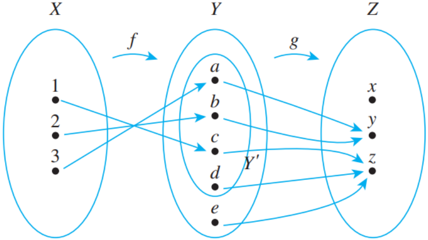
Solution

- $g \circ f$.
  $(g \circ f)(n) = g(f(n)) = g(n + 1) = (n + 1)^2$ 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 $(f \circ g)(1) = 2$

Composition of functions: Example 2

Problem

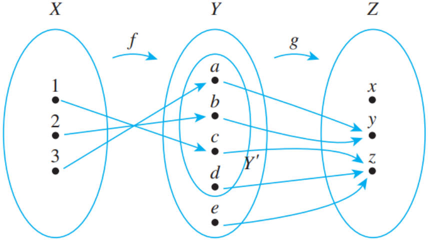
- Draw the arrow diagram for $g \circ f$. What is the range of $g \circ f$?



Composition of functions: Example 2

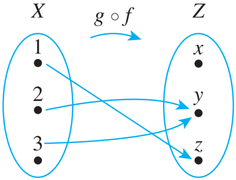
Problem

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



Solution

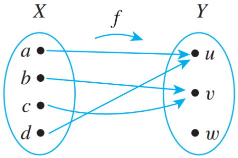
- Range of $g \circ f = \{y, z\}$.



Composition of functions: Example 3

Problem

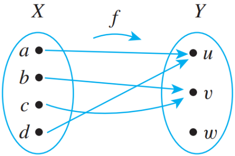
- Find $f \circ I_X$ and $I_Y \circ f$.



Composition of functions: Example 3

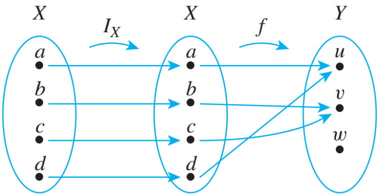
Problem

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



Solution

- $f \circ I_X = f$.

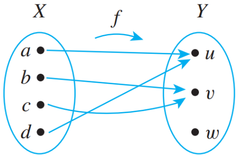


- $(f \circ I_X)(a) = f(I_X(a))$
  $= f(a) = u$
- $(f \circ I_X)(b) = f(I_X(b))$
  $= f(b) = v$
- $(f \circ I_X)(c) = f(I_X(c))$
  $= f(c) = v$
- $(f \circ I_X)(d) = f(I_X(d))$
  $= f(d) = u$

Composition of functions: Example 3

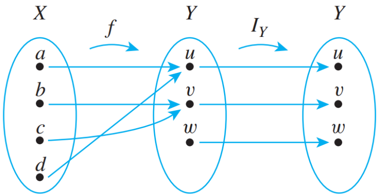
Problem

- 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 $I_Y \circ f = f$.

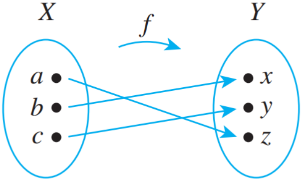
Proof

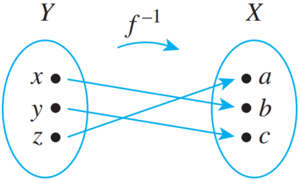
- $f \circ I_X = f$.
  $(f \circ I_X)(x) = f(I_X(x)) = f(x)$.
- $I_Y \circ f = f$.
  $(I_Y \circ f)(x) = I_Y(f(x)) = f(x)$.

Composition of functions: Example 4

Problem

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

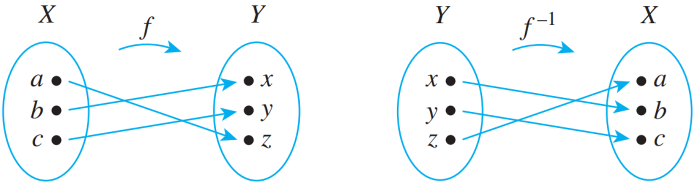




Composition of functions: Example 4

Problem

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



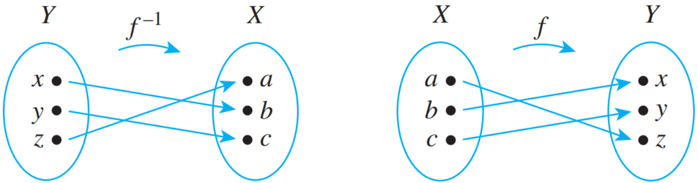
Solution

- $f^{-1} \circ f = I_X$.
  $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(z) = a = I_X(a)$
  $(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(x) = b = I_X(b)$
  $(f^{-1} \circ f)(c) = f^{-1}(f(c)) = f^{-1}(y) = c = I_X(c)$.

Composition of functions: Example 4

Problem

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



Solution

- $f \circ f^{-1} = I_Y$.
$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(b) = x = I_Y(x)$
$(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(c) = y = I_Y(y)$
$(f \circ f^{-1})(z) = f(f^{-1}(z)) = f(a) = z = I_Y(z)$.

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 $f^{-1}(f(x)) = x'$.
  $\implies f(x') = f(x)$ $\quad$ ($\because$ Defn. of inverse function)
  $\implies x' = x$ $\quad$ ($\because$ 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 $f \circ f^{-1} = I_Y$.

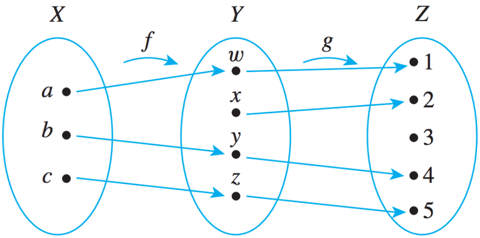
Proof (continued)

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

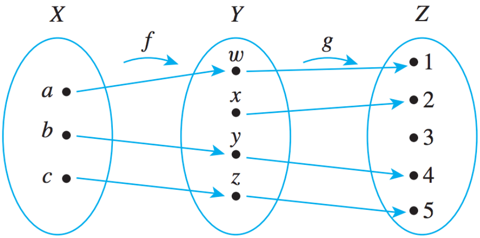
  Hence, $f \circ f^{-1} = I_Y$.

Composition of one-to-one functions

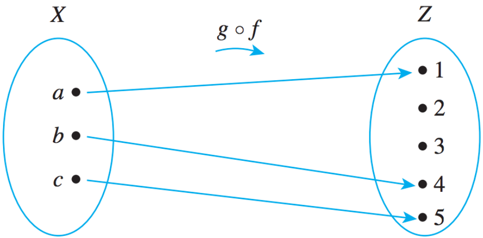


f is one-to-one and g is one-to-one

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

Problem

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

Composition of one-to-one functions

Problem

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

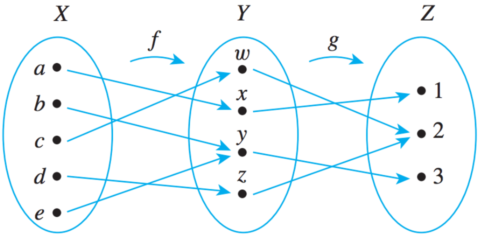
Proof

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 $x_1 = x_2$."

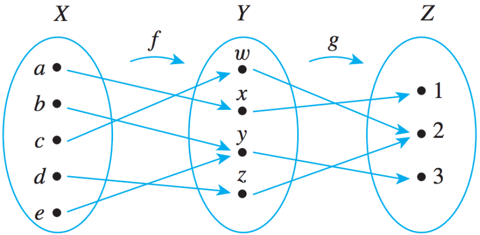
  Suppose $(g \circ f)(x_1) = (g \circ f)(x_2)$.
  $\Longrightarrow\ g(f(x_1)) = g(f(x_2))$ $\quad$ ($\because$ Defn. of composition)
  $\Longrightarrow\ f(x_1) = f(x_2)$ $\quad$ ($\because$ g is one-to-one)
  $\Longrightarrow\ x_1 = x_2$ $\quad$ ($\because$ f is one-toone)
- Hence, $g \circ f$ is one-to-one.

Composition of onto functions

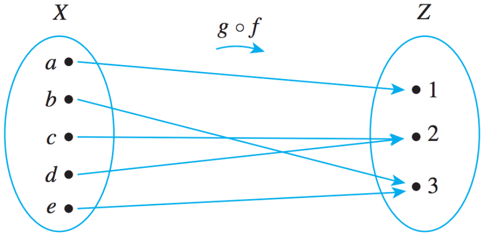


f is onto and g is onto

Composition of onto functions



f is onto and g is onto



$g \circ f$ is onto

Composition of onto functions

Problem

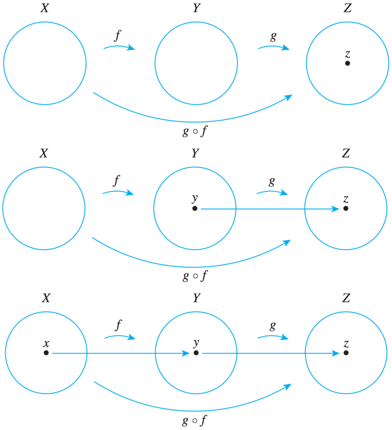
- If $f : X \to Y$ and $g : Y \to Z$ are both onto functions, then $g \circ f$ is onto.

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

Proof

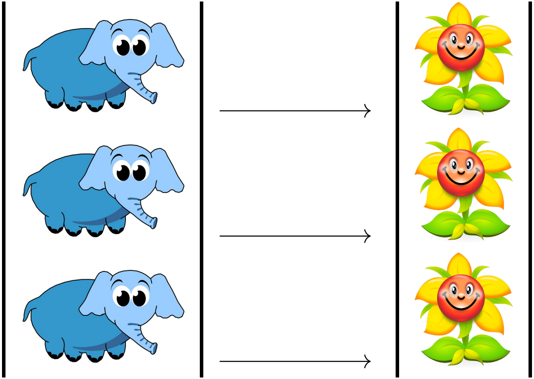
Direct proof.

- 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.

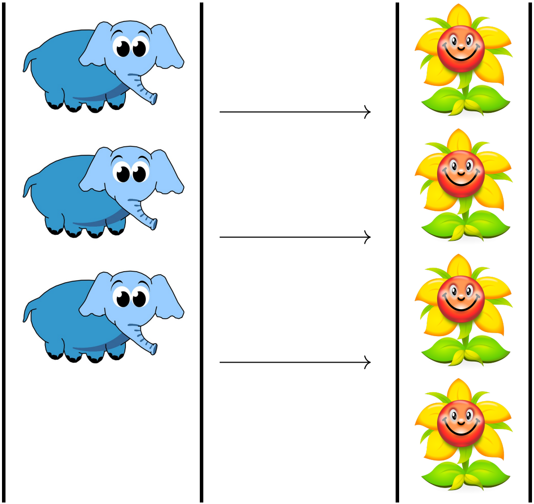
Infinite Sets

Finite sets



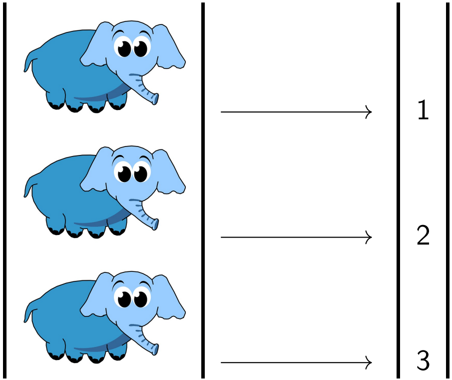
- Two finite sets are of the same size if there is a one-to-one correspondence between the two sets

Finite sets



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

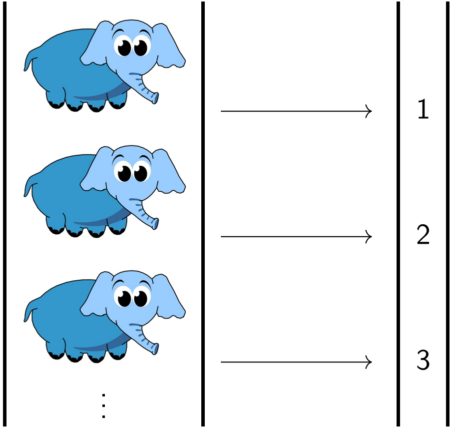
Finite sets



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.

Same cardinality

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

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{Z}} & & \boxed{\mathbb{Z}^{\mathsf{even}}} \\
\vdots & & \vdots \\
-4 & \longrightarrow & -4 \\
-3 & & \\
-2 & \longrightarrow & -2 \\
-1 & & \\
0 & \longrightarrow & 0 \\
1 & & \\
2 & \longrightarrow & 2 \\
3 & & \\
4 & \longrightarrow & 4 \\
\vdots & & \vdots
\end{array}
$$

Integers and even numbers are not of the same size

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{Z}} & & \boxed{\mathbb{Z}^{\textsf{even}}} \\
\vdots & & \vdots \\
-4 & \longrightarrow & -4 \\
-3 & & \\
-2 & \longrightarrow & -2 \\
-1 & & \\
0 & \longrightarrow & 0 \\
1 & & \\
2 & \longrightarrow & 2 \\
3 & & \\
4 & \longrightarrow & 4 \\
\vdots & & \vdots
\end{array}
$$

- There is no one-to-one correspondence between the two sets
- Cardinality of integers and even numbers are different
  i.e., $|\mathbb{Z}| \neq |\mathbb{Z}^{\textsf{even}}|$

Integers and even numbers are not of the same size

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{Z}} & & \boxed{\mathbb{Z}^{\text{even}}} \\
\vdots & & \vdots \\
-4 & \longrightarrow & -4 \\
-3 & & \\
-2 & \longrightarrow & -2 \\
-1 & & \\
0 & \longrightarrow & 0 \\
1 & & \\
2 & \longrightarrow & 2 \\
3 & & \\
4 & \longrightarrow & 4 \\
\vdots & & \vdots
\end{array}
$$

- 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

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{Z}} & & \boxed{\mathbb{Z}^{\text{even}}} \\
\vdots & & \vdots \\
-4 & \longrightarrow & -8 \\
-3 & \longrightarrow & -6 \\
-2 & \longrightarrow & -4 \\
-1 & \longrightarrow & -2 \\
0 & \longrightarrow & 0 \\
1 & \longrightarrow & 2 \\
2 & \longrightarrow & 4 \\
3 & \longrightarrow & 6 \\
4 & \longrightarrow & 8 \\
\vdots & & \vdots
\end{array}
$$

- 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

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{Z}} & & \boxed{\mathbb{Z}^{\text{even}}} \\
\vdots & & \vdots \\
-4 & \longrightarrow & -8 \\
-3 & \longrightarrow & -6 \\
-2 & \longrightarrow & -4 \\
-1 & \longrightarrow & -2 \\
0 & \longrightarrow & 0 \\
1 & \longrightarrow & 2 \\
2 & \longrightarrow & 4 \\
3 & \longrightarrow & 6 \\
4 & \longrightarrow & 8 \\
\vdots & & \vdots
\end{array}
$$

- 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., $|\mathbb{Z}| = |\mathbb{Z}^{\text{even}}|$

Integers and even numbers are of the same size

Problem

- Prove that the cardinality of integers and even numbers are the same.

Integers and even numbers are of the same size

Problem

- Prove that the cardinality of integers and even numbers are the same.

Solution

- To prove that $|\mathbb{Z}| = |\mathbb{Z}^{\text{even}}|$, we need to prove that there is a one-to-one correspondence, say f, between $\mathbb{Z}$ and $\mathbb{Z}^{\text{even}}$. Suppose $f = 2n$ for all integers $n \in \mathbb{Z}$.
- Prove that f is one-to-one.
  Suppose $f(n_1) = f(n_2)$.
  $\Longrightarrow \; 2n_1 = 2n_2 \qquad (\because \text{Defn. of } f)$
  $\Longrightarrow \; n_1 = n_2 \qquad (\because \text{Simplify})$
- Prove that f is onto.
  Suppose $m \in \mathbb{Z}^{\text{even}}$.
  $\Longrightarrow \; m \text{ is even} \qquad (\because \text{Defn. of } \mathbb{Z}^{\text{even}})$
  $\Longrightarrow \; m = 2k \text{ for } k \in \mathbb{Z} \qquad (\because \text{Defn. of even})$
  $\Longrightarrow \; f(k) = m \qquad (\because \text{Defn. of } f)$

An infinite set and its proper subset can have the same size!

Countable sets

$\boxed{\mathbb{N}}$		$\boxed{A}$
1	$\longrightarrow$	"First" element of A
2	$\longrightarrow$	"Second" element of A
3	$\longrightarrow$	"Third" element of A
4	$\longrightarrow$	"Fourth" element of A
5	$\longrightarrow$	"Fifth" element of A
$\vdots$		$\vdots$

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

Problem

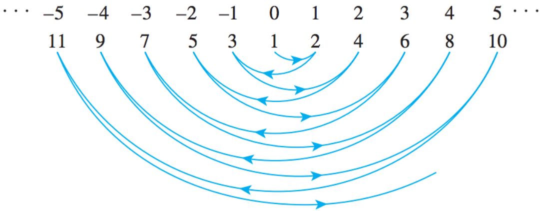
- Prove that the set of integers is countably infinite.

Integers are countable

Problem

- Prove that the set of integers is countably infinite.

Solution



Integers are countable

Solution (continued)

$\boxed{\mathbb{N}}$		$\boxed{\mathbb{Z}}$
1	$\longrightarrow$	0
2	$\longrightarrow$	1
3	$\longrightarrow$	-1
4	$\longrightarrow$	2
5	$\longrightarrow$	-2
$\vdots$		$\vdots$
n	$\longrightarrow$	$f(n)$
$\vdots$		$\vdots$

- Define a function $f(n) : \mathbb{N} \to \mathbb{Z}$ 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

Consequences

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

- A and B are finite.
  f is one-to-one $\Leftrightarrow$ f is onto
- A and B are infinite.
  f is one-to-one $\not\Leftrightarrow$ f is onto

Set of positive rationals is uncountable

$$
\begin{array}{|c|ccc|c|}
\boxed{\mathbb{N}} & & & & \boxed{\mathbb{Q}^{+}} \\
 & & & & \vdots \\
1 & & \longrightarrow & & \frac{1}{1} \\
 & & & & \vdots \\
2 & & \longrightarrow & & \frac{2}{1} \\
 & & & & \vdots \\
3 & & \longrightarrow & & \frac{3}{1} \\
\vdots & & & & \vdots
\end{array}
$$

Set of positive rationals is uncountable

$$
\begin{array}{|c|ccc|c|}
\boxed{\mathbb{N}} & & & & \boxed{\mathbb{Q}^+} \\
 & & & & \vdots \\
1 & & \longrightarrow & & \frac{1}{1} \\
 & & & & \vdots \\
2 & & \longrightarrow & & \frac{2}{1} \\
 & & & & \vdots \\
3 & & \longrightarrow & & \frac{3}{1} \\
\vdots & & & & \vdots
\end{array}
$$

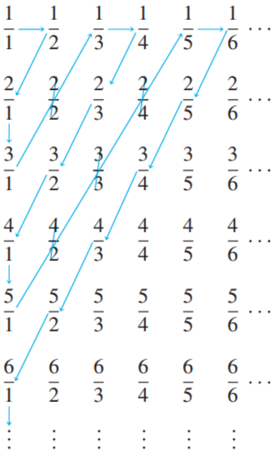
- There is no one-to-one correspondence between the two sets
- Cardinality of natural numbers and positive rationals are different i.e., $|\mathbb{N}| \neq |\mathbb{Q}^+|$

Set of positive rationals is uncountable

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{N}} & & \boxed{\mathbb{Q}^+} \\
 & & \vdots \\
1 & \longrightarrow & \frac{1}{1} \\
 & & \vdots \\
2 & \longrightarrow & \frac{2}{1} \\
 & & \vdots \\
3 & \longrightarrow & \frac{3}{1} \\
\vdots & & \vdots
\end{array}
$$

- 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



- 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

Problem

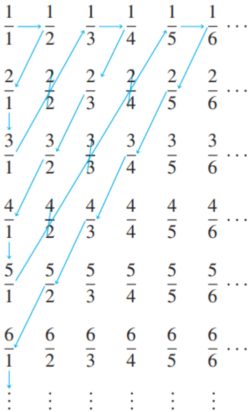
- Prove that the set of positive rational numbers are countable.

Set of positive rationals is countable

Problem

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

Solution



$\mathbb{N}$		$\mathbb{Q}^+$
1	$\longrightarrow$	$1/1$
2	$\longrightarrow$	$1/2$
3	$\longrightarrow$	$2/1$
4	$\longrightarrow$	$3/1$
5	$\longrightarrow$	$1/3$
6	$\longrightarrow$	$1/4$
7	$\longrightarrow$	$2/3$
8	$\longrightarrow$	$3/2$
9	$\longrightarrow$	$4/1$
10	$\longrightarrow$	$5/1$
$\vdots$		$\vdots$

Set of positive rational numbers is countable

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.

Set of real numbers in $[0, 1]$ is uncountable

Problem

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

Set of real numbers in $[0, 1]$ 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.

Set of real numbers in $[0,1]$ is uncountable

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.

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{N}} & & \boxed{[0..1]} \\
1 & \longrightarrow & 0.a_{11}a_{12}a_{13}\ldots a_{1n}\ldots \\
2 & \longrightarrow & 0.a_{21}a_{22}a_{23}\ldots a_{2n}\ldots \\
3 & \longrightarrow & 0.a_{31}a_{32}a_{33}\ldots a_{3n}\ldots \\
\vdots & \vdots & \vdots \\
n & \longrightarrow & 0.a_{n1}a_{n2}a_{n3}\ldots a_{nn}\ldots \\
\vdots & \vdots & \vdots
\end{array}
$$

Set of real numbers in $[0, 1]$ is uncountable

Solution (continued)

- Suppose the list of reals starts out as follows:

$$\begin{array}{ccccccc} 0. & \boxed{9} & 0 & 1 & 4 & 8 & \ldots \\ 0. & 1 & \boxed{1} & 6 & 6 & 6 & \ldots \\ 0. & 0 & 3 & \boxed{3} & 5 & 3 & \ldots \\ 0. & 9 & 6 & 7 & \boxed{2} & 6 & \ldots \\ 0. & 0 & 0 & 0 & 3 & \boxed{1} & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

- Construct a new number $d = 0.d_1 d_2 d_3 \ldots d_n \ldots$ 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.,

$$\begin{array}{ccccccc} 0. & \boxed{1} & \boxed{2} & \boxed{1} & \boxed{1} & \boxed{2} & \ldots \end{array}$$

Set of real numbers in $[0, 1]$ is uncountable

Solution (continued)

- Observation:
  For each natural number n, the constructed real number d differs in the nth decimal position from the nth number on the list.

$$
\begin{array}{cccccccccc}
1 & \longrightarrow & 0. & \boxed{9} & 0 & 1 & 4 & 8 & \ldots \\
2 & \longrightarrow & 0. & 1 & \boxed{1} & 6 & 6 & 6 & \ldots \\
3 & \longrightarrow & 0. & 0 & 3 & \boxed{3} & 5 & 3 & \ldots \\
4 & \longrightarrow & 0. & 9 & 6 & 7 & \boxed{2} & 6 & \ldots \\
5 & \longrightarrow & 0. & 0 & 0 & 0 & 3 & \boxed{1} & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\
\hline
d & \longrightarrow & 0. & \boxed{1} & \boxed{2} & \boxed{1} & \boxed{1} & \boxed{2} & \ldots \\
\hline
\end{array}
$$

- 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 ∞!

More theorems

Theorems

- A subset of a countable set is countable.
- A set with an uncountable subset is uncountable.

$\mathbb{R}$ and $[0, 1]$ have the same size

Problem

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

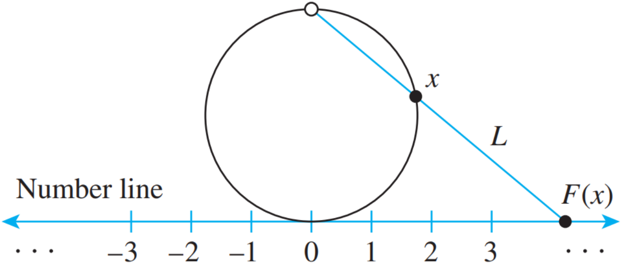
$\mathbb{R}$ and $[0,1]$ have the same size

Problem

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

Solution

- 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.

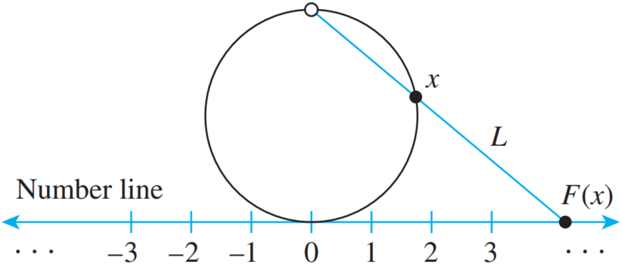


$\mathbb{R}$ and $[0, 1]$ have the same size

Solution (continued)

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

Problem

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

Set of bit strings is countable

Problem

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

Solution

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

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

Set of bit strings is countable

Solution (continued)

$\boxed{\mathbb{N}}$		$\boxed{\mathbb{B}}$
1	$\longrightarrow$	ϵ
2	$\longrightarrow$	0
3	$\longrightarrow$	1
4	$\longrightarrow$	00
5	$\longrightarrow$	01
6	$\longrightarrow$	10
7	$\longrightarrow$	11
$\vdots$		$\vdots$
n	$\longrightarrow$	$f(n)$
$\vdots$		$\vdots$

- 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.

Set of computer programs is countable

Problem

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

Set of computer programs is countable

Problem

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

Solution

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

Set of computer programs is countable

Solution (continued)

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

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{N}} & & \boxed{\mathbb{P}} \\
1 & \longrightarrow & 01 \\
2 & \longrightarrow & 11 \\
3 & \longrightarrow & 0010 \\
4 & \longrightarrow & 1010 \\
5 & \longrightarrow & 1011 \\
6 & \longrightarrow & 00010 \\
7 & \longrightarrow & 00100 \\
8 & \longrightarrow & 10111 \\
\vdots & & \vdots \\
n & \longrightarrow & f(n) \\
\vdots & & \vdots
\end{array}
$$

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

Set of all functions $\mathbb{N} \to \{0, 1\}$ is uncountable

Problem

- Prove that the set of all functions $\mathbb{N} \to \{0, 1\}$ is uncountable

Set of all functions $\mathbb{N} \to \{0, 1\}$ is uncountable

Problem

- Prove that the set of all functions $\mathbb{N} \to \{0, 1\}$ is uncountable

Solution

- Let $\mathbb{S}$ 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. $\triangleright$ Why?
- Let $\mathbb{L}$ be the set of all functions $\mathbb{N} \to \{0, 1\}$
- We will show a 1-to-1 correspondence between $\mathbb{S}$ and a subset of $\mathbb{L}$ by showing we can map an element of $\mathbb{S}$ to a unique element of $\mathbb{L}$.

Set of all functions $\mathbb{N} \to \{0,1\}$ is uncountable

Solution (continued)

$$
\begin{array}{|c|c|c|}
\boxed{\mathbb{S}} & & \text{Subset of } \boxed{\mathbb{L}} \\
& & \begin{array}{|c|c|c|}
\boxed{\mathbb{N}} & & \boxed{\{0,1\}} \\
1 & \longrightarrow & a_1 \\
2 & \longrightarrow & a_2 \\
3 & \longrightarrow & a_3 \\
\vdots & & \vdots \\
n & \longrightarrow & a_n \\
\vdots & & \vdots
\end{array} \\
0.a_1a_2a_3\ldots a_n\ldots & \longrightarrow &
\end{array}
$$

- As f is a one-to-one correspondence between $\mathbb{S}$ and a subset of $\mathbb{L}$, the set of functions $\mathbb{N} \to \{0,1\}$ 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!