Functions

CSE 215, Foundations of Computer Science

Stony Brook University

http://www.cs.stonybrook.edu/liu/~cse215

Functions defined on general sets

- A function f from a set X to a set Y

$$f : X \rightarrow Y$$

X is the domain, Y is the co-domain

(1) every element in X is related to some element in Y

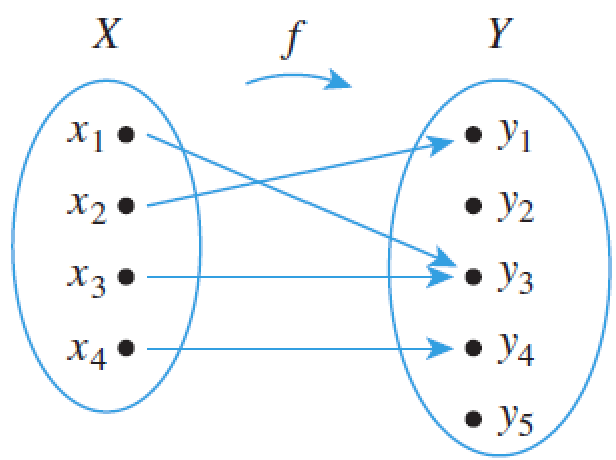
(2) no element in X is related to more than one element in Y

- Thus, **for any** element $x \in X$, there is a **unique** element $y \in Y$ such that $f(x)=y$

- range of f = image of X under f $= \{y \in Y \mid y = f(x), x \in X\}$
- inverse image of $y = \{x \in X \mid f(x) = y\}$

Arrow diagrams

- An arrow diagram, with elements in X and Y, and an arrow from each x in X to corresponding y in Y.



- It defines a function because:

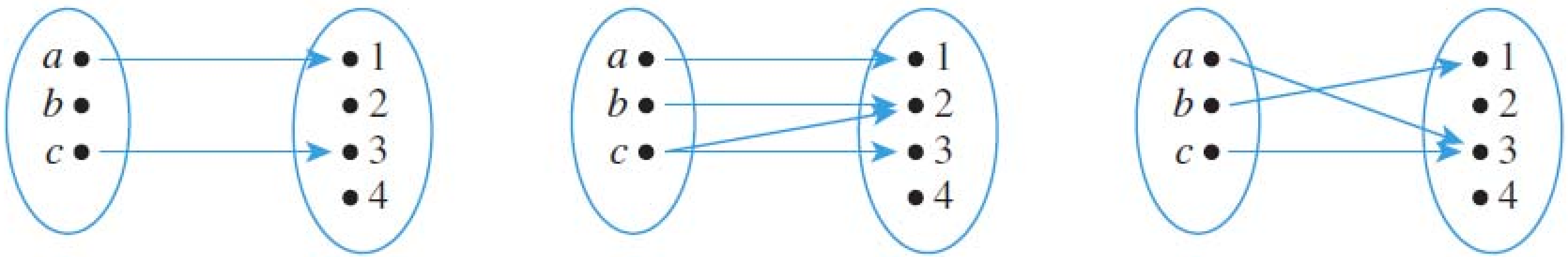
(1) Every element of X has an arrow coming out of it

(2) No element of X has two arrows coming out of it that point to two different elements of Y

Arrow diagrams: example 1

- $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$

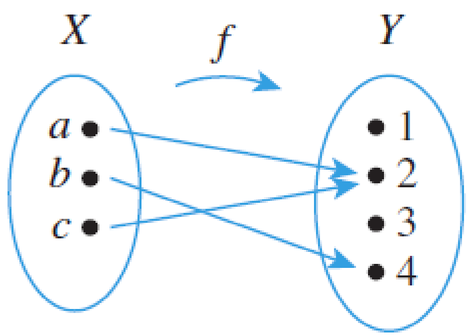
Which one defines a function?



This one!

Arrow diagrams: example 2

- $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$



f (a) = 2
f (b) = 4
f (c) = 2

- domain of $f = \{a, b, c\}$, co-domain of $f = \{1, 2, 3, 4\}$
- range of $f = \{2, 4\}$
- inverse image of $2 = \{a, c\}$
- inverse image of $4 = \{b\}$
- inverse image of $1 = \emptyset$
- function representation as a set of pairs: $\{(a,2), (b,4), (c,2)\}$

Function equality

Note the set notation for a function: $F(x) = y \Leftrightarrow (x,y) \in F$

- If $F: X \to Y$ and $G: X \to Y$ are functions, then $F = G$ if, and only if, $F(x) = G(x)$ for all $x \in X$.

Proof:

$F \subseteq X \times Y$ $\qquad$ $G \subseteq X \times Y$

$F(x) = y \Leftrightarrow (x, y) \in F$ $\qquad$ $G(x) = y \Leftrightarrow (x, y) \in G$

($\Rightarrow$) Suppose $F = G$. Then for all $x \in X$,

$$y = F(x) \Leftrightarrow (x, y) \in F \Leftrightarrow (x, y) \in G \Leftrightarrow y = G(x)$$

$$F(x) = y = G(x)$$

($\Leftarrow$) Suppose $F(x) = G(x)$ for all $x \in X$. Then for any $x \in X$:

$$(x, y) \in F \Leftrightarrow y = F(x) \Leftrightarrow y = G(x) \Leftrightarrow (x, y) \in G$$

F and G consist of exactly the same elements, hence $F = G$.

Function equality: example 1

- $J_3 = \{0, 1, 2\}$

$f : J_3 \to J_3$

$f(x) = (x^2 + x + 1) \bmod 3$

$g : J_3 \to J_3$

$g(x) = (x + 2)^2 \bmod 3$

x	$x^2 + x + 1$	$f(x) = (x^2 + x + 1)$ *mod* 3	$(x + 2)^2$	$g(x) = (x + 2)^2$ *mod* 3
0	1	1 *mod* 3 = 1	4	4 *mod* 3 = 1
1	3	3 *mod* 3 = 0	9	9 *mod* 3 = 0
2	7	7 *mod* 3 = 1	16	16 *mod* 3 = 1

$f(0) = g(0) = 1$

$f(1) = g(1) = 0$

$f(2) = g(2) = 1$

Hence, $f = g$

Function equality: example 2

- F: $\mathbf{R} \to \mathbf{R}$ and G: $\mathbf{R} \to \mathbf{R}$

  F + G: $\mathbf{R} \to \mathbf{R}$ and G + F: $\mathbf{R} \to \mathbf{R}$

  $(F + G)(x) = F(x) + G(x)$

  $(G + F)(x) = G(x) + F(x)$, for all $x \in \mathbf{R}$

For all real numbers x:

$(F + G)(x) = F(x) + G(x)$ by definition of F + G

$= G(x) + F(x)$ by commutative law for addition of real numbers

$= (G + F)(x)$ by definition of G + F

Hence, $F + G = G + F$ ■

Example functions (I)

- **Identity function on a set:**

  Given a set X, define identity function $I_X: X \to X$ by

  $$I_X(x) = x, \text{ for all } x \in X$$

- **Function for a sequence:**

  $1, -1/2, 1/3, -1/4, 1/5, \ldots, (-1)^n/(n+1), \ldots$

  $0 \to 1, \quad 1 \to -1/2, \quad 2 \to 1/3, \quad 3 \to -1/4, \quad 4 \to 1/5$

  $$n \to (-1)^n/(n+1)$$

  $f : \mathbf{N} \to \mathbf{R}$, for each integer $n \geq 0$, $f(n) = (-1)^n/(n+1)$

  where ($\mathbf{N} = \mathbf{Z}^{\mathbf{nonneg}}$) OR

  $g : \mathbf{Z}^+ \to \mathbf{R}$, for each integer $n \geq 1$, $g(n) = (-1)^{n+1}/n$

  where ($\mathbf{Z}^+ = \mathbf{Z}^{\mathbf{nonneg}} - \{\mathbf{0}\}$)

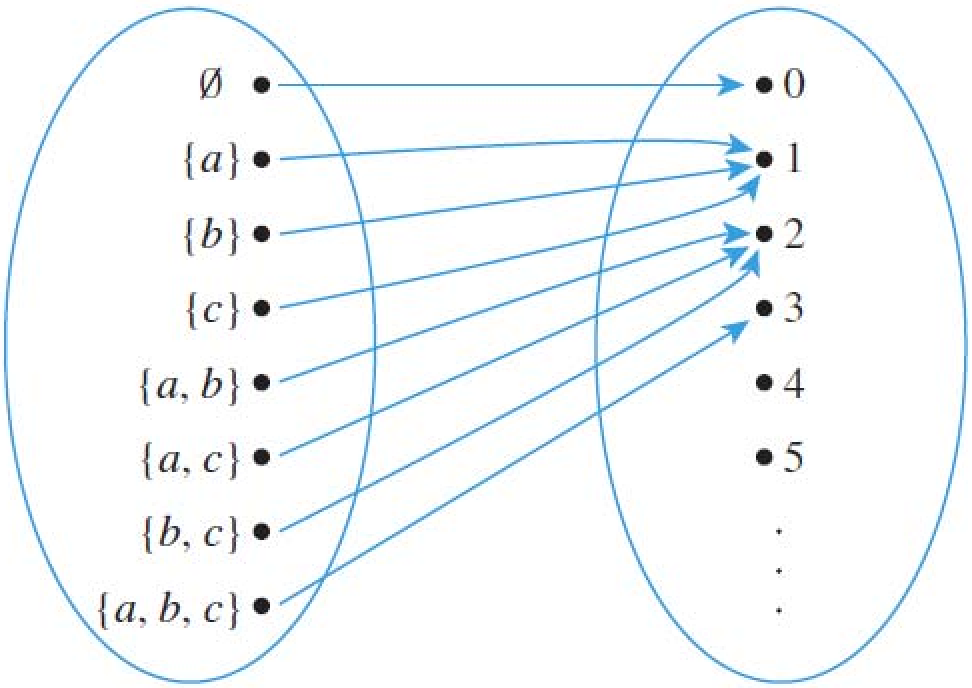
Example functions (II)

- **Function defined on a power set:**

$$F : P(\{a, b, c\}) \to \mathbf{Z}^{\mathbf{nonneg}}$$

For each $X \in P(\{a, b, c\})$,

F(X) = the number of elements in X (i.e., the cardinality of X)



Example functions (III)

- **Functions defined on a Cartesian product:**

$$M : \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \qquad \text{and} \qquad R : \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \times \mathbf{R}$$

The multiplication function: $M(a, b) = a * b$

We omit parenthesis for tuples: $M((a, b))=M(a,b)$

$$M(1, 1) = 1, \quad M(2, 2) = 4$$

The reflection function: $R(a, b) = (-a, b)$

R sends each point in the plane that corresponds to a pair of real numbers to the mirror image of the point across the vertical axis

$$R(1, 1) = (-1, 1), \quad R(2, 5) = (-2, 5), \quad R(-2, 5) = (2, 5)$$

Example functions (IV)

- **Logarithms and logarithmic functions:**
  - The base of a logarithm, b, is a positive real number with $b \neq 1$
  - The logarithm with base b of x: $\log_b x = y \Leftrightarrow b^y = x$
  - The **logarithmic function with base b**:

$$\log_b x : \mathbf{R}^+ \rightarrow \mathbf{R}$$

Examples:

$\log_3 9 = 2$	because	$3^2 = 9$
$\log_{10}(1) = 0$	because	$10^0 = 1$
$\log_2 ½ = -1$	because	$2^{-1} = ½$
$\log_2 (2^m) = m$		

More example functions (I)

- **Encoding and decoding functions** on sequences of 0's and 1's

  also called bit strings

Encoding function E: For each string s,

E(s) = the string obtained from s by

replacing each bit of s by the same bit written 3 times

Decoding function D: For each string t in the range of E,

D(t) = the string obtained from t by

replacing each consecutive 3 identical bits of t

by a single copy of that bit

Redundancy helps with error detection and fix.

More example functions (II)

- **The Hamming distance function**

Let S_n be the set of all strings of 0's and 1's of length n.

$H: S_n \times S_n \rightarrow Z^{nonneg}$

For each pair of strings $(s, t) \in S_n \times S_n$

$H(s, t)$ = number of positions in which s and t differ

Examples: For $n = 5$, $H(11111, 00000) = 5$

$H(10101, 00000) = 3$

$H(01010, 00000) = 2$

It is important in coding theory: gives a measure of "difference".

More example functions (III)

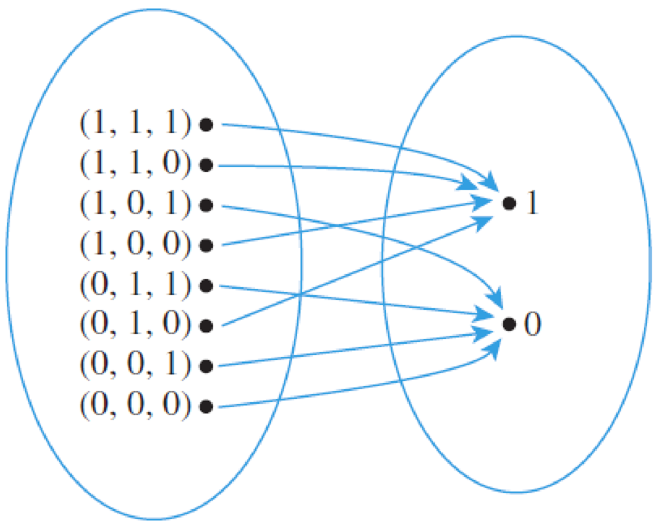
- **Boolean functions: (n-place) Boolean function**

$$f : \{0, 1\}^n \to \{0, 1\}$$ Cartesian product

domain = set of all ordered n-tuples of 0's and 1's

co-domain = {0, 1}

Input			Output
P	*Q*	*R*	*S*
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0



The input/output tables correspond to some circuits.

More example functions (IV)

- **Boolean functions example:**

$$f : \{0, 1\}^3 \rightarrow \{0, 1\}$$

$$f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \bmod 2$$

$$f(0, 0, 0) = (0 + 0 + 0) \bmod 2 = 0 \bmod 2 = 0$$
$$f(0, 0, 1) = (0 + 0 + 1) \bmod 2 = 1 \bmod 2 = 1$$
$$f(0, 1, 0) = (0 + 1 + 0) \bmod 2 = 1 \bmod 2 = 1$$
$$f(0, 1, 1) = (0 + 1 + 1) \bmod 2 = 2 \bmod 2 = 0$$
$$f(1, 0, 0) = (1 + 0 + 0) \bmod 2 = 1 \bmod 2 = 1$$
$$f(1, 0, 1) = (1 + 0 + 1) \bmod 2 = 2 \bmod 2 = 0$$
$$f(1, 1, 0) = (1 + 1 + 0) \bmod 2 = 2 \bmod 2 = 0$$
$$f(1, 1, 1) = (1 + 1 + 1) \bmod 2 = 3 \bmod 2 = 1$$

Checking well-definedness

- A "function" f is **not well defined** if:

  (1) there is no element y in the co-domain that satisfies $f(x) = y$ for some element x in the domain, or

  (2) there are two different values of y that satisfy $f(x) = y$

- **Example:**

  $f : \mathbf{R} \rightarrow \mathbf{R}$, $f(x)$ is the real number y such that $x^2 + y^2 = 1$

  f is not well defined:

  (1) $x = 2$, there is no real number y such that $2^2 + y^2 = 1$

  (2) $x = 0$, there are 2 real numbers $y=1$ and $y=-1$ such that $0^2 + y^2 = 1$

Checking well-definedness: example 2

- $f : \mathbf{Q} \to \mathbf{Z}$,

  $f(m/n) = m$, for all integers m and n with $n \neq 0$

f is not well defined:

$1/2 = 2/4 \rightarrow f(1/2) = f(2/4)$

but

$f(1/2) = 1 \quad \neq \quad 2 = f(2/4)$

That is, there are two different values of y that satisfy $f(x) = y$

Functions acting on sets

- If $f : X \to Y$ is a function and $A \subseteq X$ and $C \subseteq Y$, then

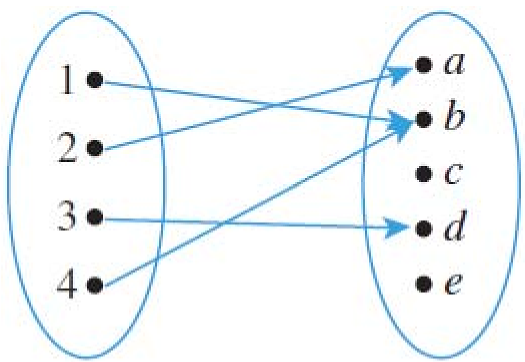
  $f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \text{ in } A\}$

  is the image of A

  $f^{-1}(C) = \{x \in X \mid f(x) \in C\}$

  is the inverse image of C

Example: $X = \{1, 2, 3, 4\}$, $Y = \{a, b, c, d, e\}$, $f : X \to Y$



$f(\{1,4\}) = \{b\}$ $\quad f^{-1}(\{a,b\}) = \{1, 2, 4\}$

$f(X) = \{a, b, d\}$ $\quad f^{-1}(\{c,e\}) = \emptyset$

Functions acting on sets: an example proof

- Let X and Y be sets, let $F : X \rightarrow Y$ be a function, $A \subseteq X$, and $B \subseteq X$, then $F(A \cup B) \subseteq F(A) \cup F(B)$

  Proof:

  Suppose $y \in F(A \cup B)$.

  By definition of function, $y = F(x)$ for some $x \in A \cup B$.

  By definition of union, $x \in A$ or $x \in B$.

  Case 1, $x \in A$: $F(x) = y$, so $y \in F(A)$.

  By definition of union: $y \in F(A) \cup F(B)$

  Case 2, $x \in B$: $F(x) = y$, so $y \in F(B)$.

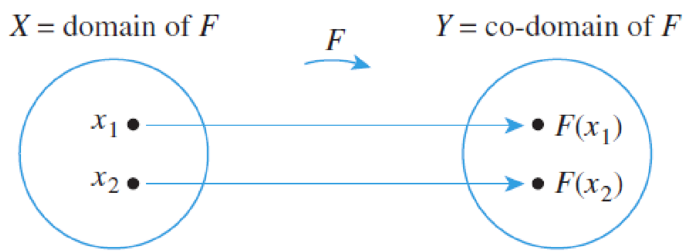
  By definition of union: $y \in F(A) \cup F(B)$ ■

One-to-one, onto, inverse functions

- $F : X \rightarrow Y$ is **one-to-one** (or **injective**) (often written 1-1) $\Leftrightarrow$

  for all $x_1 \in X$ and $x_2 \in X$, $F(x_1) = F(x_2) \rightarrow x_1 = x_2$

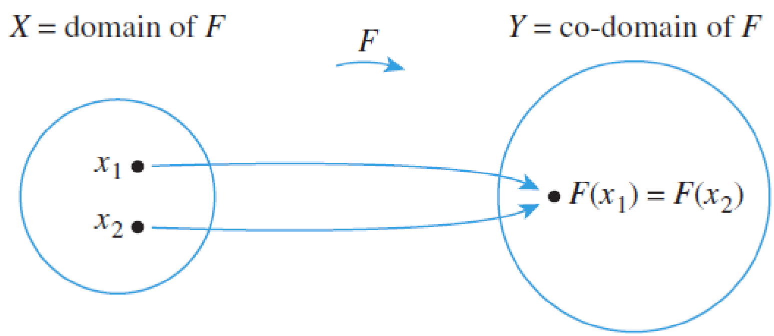
  or, equivalently (by contraposition), $x_1 \neq x_2 \rightarrow F(x_1) \neq F(x_2)$



Any two distinct elements of X are sent to two distinct elements of Y.

- $F : X \rightarrow Y$ is **not one-to-one** $\Leftrightarrow$

  $\exists\ x_1 \in X$ and $x_2 \in X$, such that $x_1 \neq x_2$ and $F(x_1) = F(x_2)$.

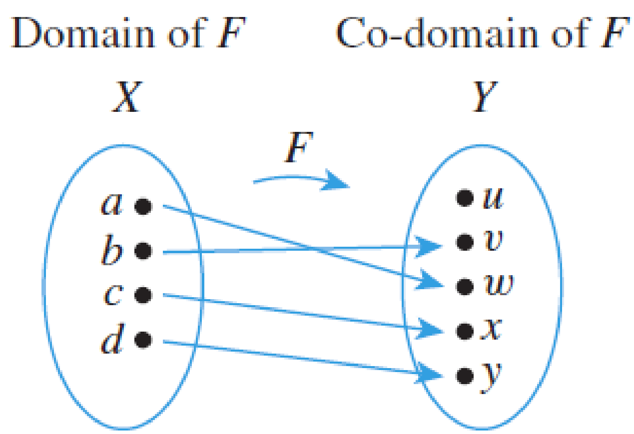


Two distinct elements of X are sent to the same element of Y.

One-to-one functions on finite sets

- **Example 1:**

  F: $\{a,b,c,d\} \rightarrow \{u,v,w,x,y\}$ defined by the following arrow diagram is one-to-one:

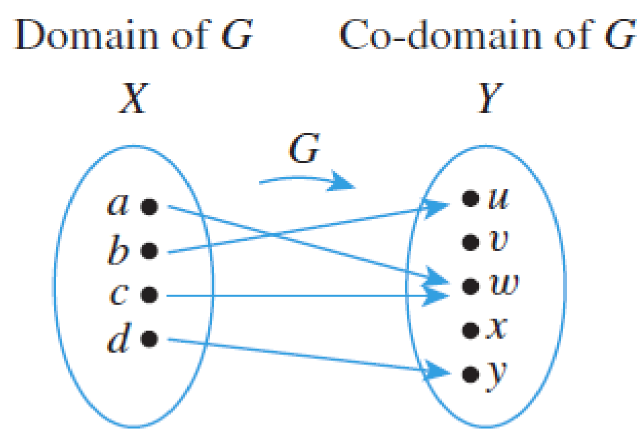


$$\forall\ x_1 \in X \text{ and } x_2 \in X, \quad x_1 \neq x_2 \Rightarrow F(x_1) \neq F(x_2)$$

One-to-one functions on finite sets

- **Example 2:**

G: {a,b,c,d} $\rightarrow${u,v,w,x,y} defined by the following arrow diagram is not one-to-one:



$G(a) = G(c) = w$

$\exists$ elements $x_1 \in X$ and $x_2 \in X$, such that $x_1 \neq x_2$ and $G(x_1) = G(x_2)$

that is, $a \in X$ and $c \in X$, such that $a \neq c$ and $G(a) = G(c)$

One-to-one functions on finite sets

- **Example 3:**

$H: \{1, 2, 3\} \rightarrow \{a, b, c, d\}, \; H(1) = c, \; H(2) = a, \; H(3) = d$

H is one-to-one:

$$\forall\, x_1 \in X \text{ and } x_2 \in X, \; x_1 \neq x_2 \Rightarrow H(x_1) \neq H(x_2)$$

- **Example 4:**

$K: \{1, 2, 3\} \rightarrow \{a, b, c, d\}, \; K(1) = d, \; K(2) = b, \; K(3) = d$

K is not one-to-one:

$$K(1) = K(3) = d$$

That is, $\exists\, x_1 \in X$ and $x_2 \in X$, such that $x_1 \neq x_2$ and $K(x_1) = K(x_2)$

One-to-one functions on infinite sets

- Copied definition:

  f is one-to-one $\Leftrightarrow$ $\forall x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$

- To show f is one-to-one, generally use direct proof:
  - suppose x_1 and x_2 are elements of X such that $f(x_1)=f(x_2)$
  - show that $x_1 = x_2$.

- To show f is **not** one-to-one, generally use 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 on infinite sets

copied: f is one-to-one $\Leftrightarrow \forall x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$

- **Example 1**: $f : \mathbf{R} \to \mathbf{R}$,

  $f(x) = 4x - 1$ for all $x \in \mathbf{R}$ is f one-to-one?

  Suppose x_1 and x_2 are any real numbers such that $4x_1 - 1 = 4x_2 - 1$.

  Adding 1 to both sides and and dividing by 4 both sides gives $x_1 = x_2$.

  Yes, f is one-to-one ■

- **Example 2**: $g : \mathbf{Z} \to \mathbf{Z}$,

  $g(n) = n^2$ for all $n \in \mathbf{Z}$ is g one-to-one?

  Start by trying to show that g is one-to-one

  Suppose n_1 and n_2 are integers such that $n_1^2 = n_2^2$ and try to show $n_1 = n_2$. but $1^2 = (-1)^2 = 1$.

  No, g is not one-to-one ■

Application: hash functions

- **Hash functions** are functions defined from larger to smaller sets of integers used in identifying documents.
- **Example**: Hash: SSN $\rightarrow \{0, 1, 2, 3, 4, 5, 6\}$

  SSN = set of all social security numbers (ignoring hyphens)

  Hash(n) = n mod 7 for all social security numbers n

  e.g., Hash(328343419) = 328343419 − (7·46906202) = 5

- Hash is not one-to one: called a **collision** for hash functions.

  e.g., Hash(328343412) = 328343412 − (7· 46906201) = 5

Collision resolution:

if position Hash(n) is already occupied, then start from that position and search downward to place the record in the first empty position.

Onto functions

- F: $X \to Y$ is **onto** (**surjective**) $\Leftrightarrow$

$$\forall y \in Y, \quad \exists x \in X \text{ such that } F(x) = y.$$

For arrow diagrams, a function is onto if each element in the co-domain has an arrow to it from some element in the domain.

- F: $X \to Y$ is **not onto** (**surjective**) $\Leftrightarrow$

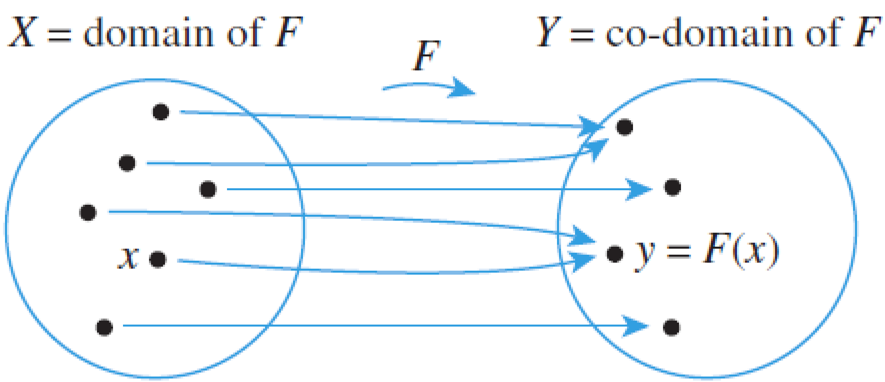
$$\exists y \in Y \text{ such that } \forall x \in X, F(x) \neq y.$$

There is some element in Y that is not the image of any element in X.

For arrow diagrams, a function is not onto if at least one element in its co-domain does not have an arrow pointing to it.

Onto functions with arrow diagrams

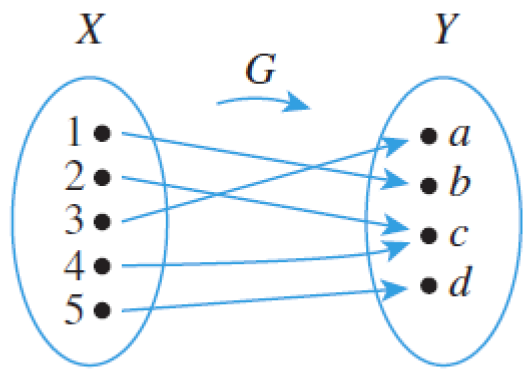
- F is onto:



Each element y in Y equals $F(x)$ for at least one x in X.

Onto functions: example 1

- G: $\{1,2,3,4,5\} \rightarrow \{a,b,c,d\}$

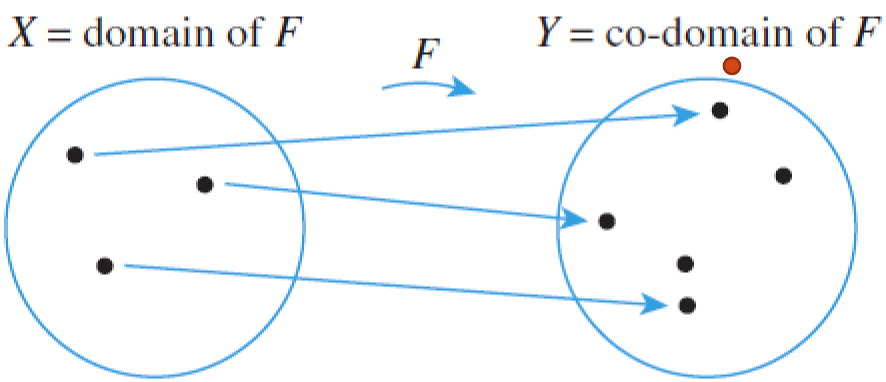


G is onto

because $\forall y \in Y,\ \exists x \in X$, such that $G(x) = y$

Not onto functions

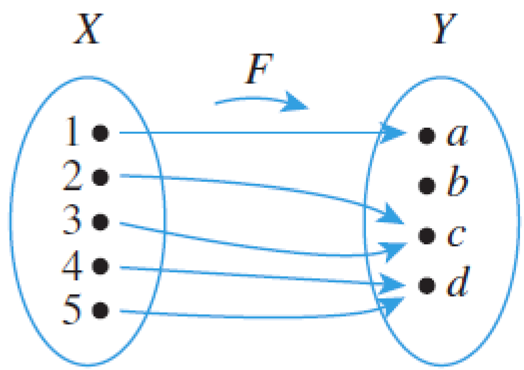
- F is not onto



At least one element in Y does not equal $F(x)$ for any x in X.

Onto functions: example 2

- F: {1,2,3,4,5} → {a,b,c,d}



F is not onto

because b ≠ F(x) for any x in X

that is, $\exists y \in Y$ such that $\forall x \in X$, $F(x) \neq y$

Onto functions: more examples

- $H: \{1,2,3,4\} \to \{a,b,c\}$

  $H(1) = c, \quad H(2) = a, \quad H(3) = c$, and $\quad H(4) = b$

  H is onto because $\forall y \in Y, \; \exists x \in X$ such that $H(x) = y$:

  $a = H(2)$

  $b = H(4)$

  $c = H(1) = H(3)$

- $K: \{1,2,3,4\} \to \{a,b,c\}$

  $K(1) = c, \quad K(2) = b, \quad K(3) = b$, and $\quad K(4) = c$

  H is not onto because $a \neq K(x)$ for any $x \in \{1, 2, 3, 4\}$.

Onto functions on infinite sets

- Copied definition:

  F is onto $\Leftrightarrow \forall y \in Y, \exists x \in X$ such that $F(x) = y$.

- To prove F is onto, generally use direct proof:
  - suppose y is any element of Y,
  - show there is an element x of X with $F(x)=y$.

- To prove F is **not** onto, use counterexample:
  - find an element y of Y such that $y \neq F(x)$ for any x in X.

Onto functions on infinite sets: examples

- Prove that a function is onto or give counterexample

- $f : \mathbf{R} \to \mathbf{R}$

$$f(x) = 4x - 1 \text{ for all } x \in \mathbf{R}$$

Suppose $y \in R$. Show there is a real number x such that $y = 4x - 1$.

$4x - 1 = y \Leftrightarrow x = (y + 1)/4 \in R$. So, f is onto $\blacksquare$

- $h : \mathbf{Z} \to \mathbf{Z}$

$$h(n) = 4n - 1 \text{ for all } n \in \mathbf{Z}$$

$0 \in \mathbf{Z}$, $h(n) = 0 \Leftrightarrow 4n - 1 = 0 \Leftrightarrow n = 1/4 \notin \mathbf{Z}$

$h(n) \neq 0$ for any integer n. So h is not onto $\blacksquare$

Exponential functions

- The exponential function with base b: $\exp_b : \mathbf{R} \rightarrow \mathbf{R}^+$

$$\exp_b(x) = b^x$$

$\exp_b(0) = b^0 = 1$

$\exp_b(-x) = b^{-x} = 1/b^x$

- The exponential function is one-to-one and onto:

for any positive real number $b \neq 1$, $b^v = b^u \rightarrow u = v, \ \forall\, u,v \in \mathbf{R}$

- Laws of exponents: $\forall$ b, c $\in \mathbf{R}^+$ and u,v $\in \mathbf{R}$

$$b^u b^v = b^{u+v}$$

$$b^u/b^v = b^{u-v}$$

$$(b^u)^v = b^{uv}$$

$$(bc)^u = b^u c^u$$

Logarithmic functions

- The logarithmic function with base b: $\log_b : \mathbf{R}^+ \rightarrow \mathbf{R}$

$$\log_b(x) = y \Leftrightarrow b^y = x$$

- The logarithmic function is one-to-one and onto:

for any positive real number $b \neq 1$,

$$\log_b u = \log_b v \rightarrow u = v, \quad \forall u, v \in \mathbf{R}^+$$

- Properties of logarithms: $\forall$ b, c, x $\in \mathbf{R}^+$, with $b \neq 1$ and $c \neq 1$

$$\log_b(xy) = \log_b x + \log_b y$$

$$\log_b(x/y) = \log_b x - \log_b y$$

$$\log_b(x^a) = a \log_b x$$

$$\log_c x = \log_b x / \log_b c$$

Logarithmic functions: example proofs

- $\forall$ b, c, x $\in \mathbf{R}^+$, with b $\neq$ 1 and c $\neq$ 1: $\log_c x = \log_b x \,/\, \log_b c$

Proof:

Suppose positive real numbers b, c, and x are given, s.t.

(1) $u = \log_b c$ (2) $v = \log_c x$ (3) $w = \log_b x$

By definition of logarithm: $c = b^u$, $x = c^v$ and $x = b^w$

$x = c^v = (b^u)^v = b^{uv}$, by laws of exponents

So $x = b^w = b^{uv}$, so $uv = w$

That is, $(\log_b c)(\log_c x) = \log_b x$, by (1), (2), and (3)

By dividing both sides by $\log_b c$: $\log_c x = \log_b x \,/\, \log_b c$ $\blacksquare$

Logarithmic functions: notations

- Logarithms with base 10 are called **common logarithms** and are denoted by simply log.

- Logarithms with base e are called **natural logarithms** and are denoted by ln.

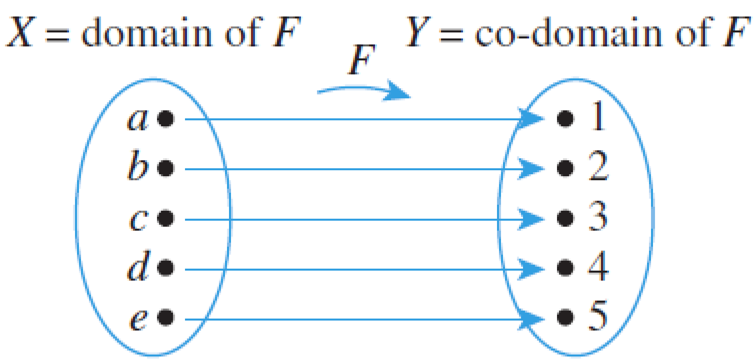
- **Example:**

$$\log_2 5 = \log 5 \;/\; \log 2 = \ln 5 \;/\; \ln 2$$

One-to-one correspondences

- A **one-to-one correspondence** (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**.

- **Example:**



One-to-one correspondences: example 2

- A function from a power set to a set of strings

$$h : P(\{a, b\}) \rightarrow \{00, 01, 10, 11\}$$

If a is in A, write a 1 in the 1^{st} position of the string h(A).

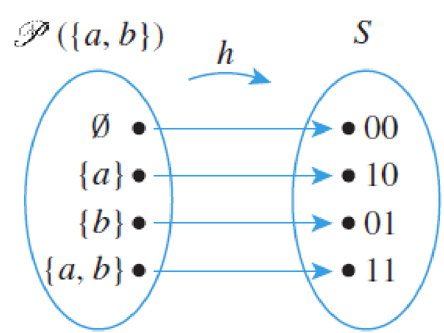
If a is not in A, write a 0 in the 1^{st} position of the string h(A).

If b is in A, write a 1 in the 2^{nd} position of the string h(A).

If b is not in A, write a 0 in the 2^{nd} position of the string h(A).

h

Subset of $\{a, b\}$	**Status of a**	**Status of b**	**String in S**
$\emptyset$	not in	not in	00
$\{a\}$	in	not in	10
$\{b\}$	not in	in	01
$\{a, b\}$	in	in	11



One-to-one correspondences: example 3

- **Example:** F: $\mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$

  $F(x, y) = (x + y, x - y)$, for all $(x, y) \in \mathbf{R} \times \mathbf{R}$

  Proof that F is one-to-one:

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

  $\Leftrightarrow (x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2)$, by definition of F

  $\Leftrightarrow$ (1) $x_1 + y_1 = x_2 + y_2$ and (2) $x_1 - y_1 = x_2 - y_2$, by pair equalty

  (1) + (2) $\rightarrow$ $2x_1 = 2x_2$ $\rightarrow$ (3) $x_1 = x_2$

  Substituting (3) in (2) $\rightarrow$ $x_1 + y_1 = x_1 + y_2$ $\rightarrow$ $y_1 = y_2$

  So, $(x_1, y_1) = (x_2, y_2)$

  So, F is one-to-one.

One-to-one correspondences: example 3

- **Example:** F: $\mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \times \mathbf{R}$

  $F(x, y) = (x + y, x - y)$, for all $(x, y) \in \mathbf{R} \times \mathbf{R}$

Proof that F is onto:

Let (u,v) be any ordered pair in $\mathbf{R} \times \mathbf{R}$

Suppose that we found $(r, s) \in \mathbf{R} \times \mathbf{R}$ such that $F(r, s) = (u, v)$.

$\Leftrightarrow (r + s, r - s) = (u, v) \Leftrightarrow r + s = u$ and $r - s = v$

$\Leftrightarrow 2r = u + v$ and $2s = u - v$

$\Leftrightarrow r = (u + v)/2$ and $s = (u - v)/2$

We found $(r, s) \in \mathbf{R} \times \mathbf{R}$ such that $F(r, s) = (u,v)$

So, F is onto.

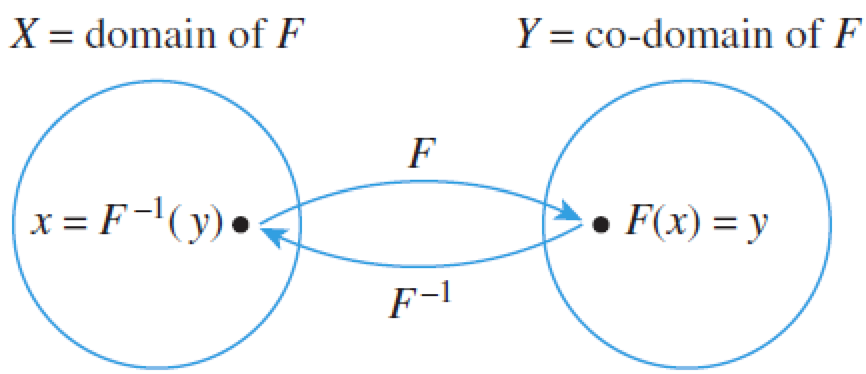
Thus, F is a One-to-One correspondence. $\blacksquare$

Inverse functions

- If F: X $\longrightarrow$ Y is a one-to-one correspondence, then there is an **inverse function** for F, $F^{-1}: Y \rightarrow X$, such that for any element $y \in Y$,

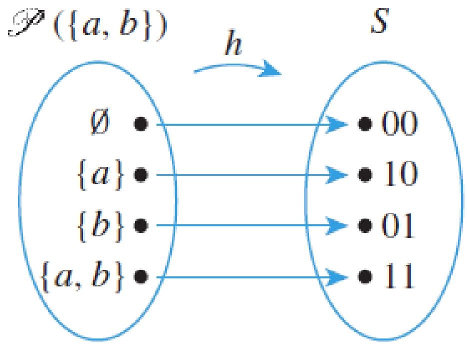
  $F^{-1}(y)$ = that unique element $x \in X$ such that $F(x) = y$

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

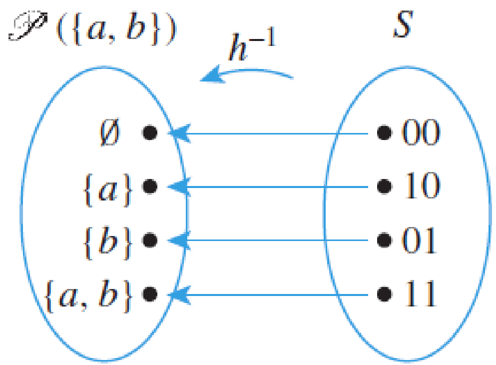


Inverse functions: example 1

- Function h:



The inverse function for h is h^{-1}:



$h^{-1}(00) = \emptyset \quad h^{-1}(10) = \{a\}$

$h^{-1}(01) = \{b\} \quad h^{-1}(11) = \{a, b\}$

Inverse functions: example 2

- Function $f : \mathbf{R} \to \mathbf{R}$

  $f(x) = 4x - 1$ for all real numbers x.

  The inverse function for f is $f^{-1} : \mathbf{R} \to \mathbf{R}$,

  for any y in $\mathbf{R}$,

  $f^{-1}(y)$ is that unique real number x such that $f(x) = y$.

  $f(x) = y \iff 4x - 1 = y \iff x = (y + 1)/4$

  Hence, $f^{-1}(y) = (y + 1)/4$.

Inverse functions: one-to-one, onto

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

Proof:

F^{-1} is one-to-one:

Suppose y_1 and y_2 are elements of Y, such that $F^{-1}(y_1) = F^{-1}(y_2)$

Let $x = F^{-1}(y_1) = F^{-1}(y_2)$. Then $x \in X$.

By definition of F^{-1}, $F(x) = y_1$ and $F(x) = y_2$, so $y_1 = y_2$

F^{-1} is onto:

Suppose $x \in X$. Need to find y in Y, such that $F^{-1}(y) = x$

Let $y = F(x)$. Then $y \in Y$.

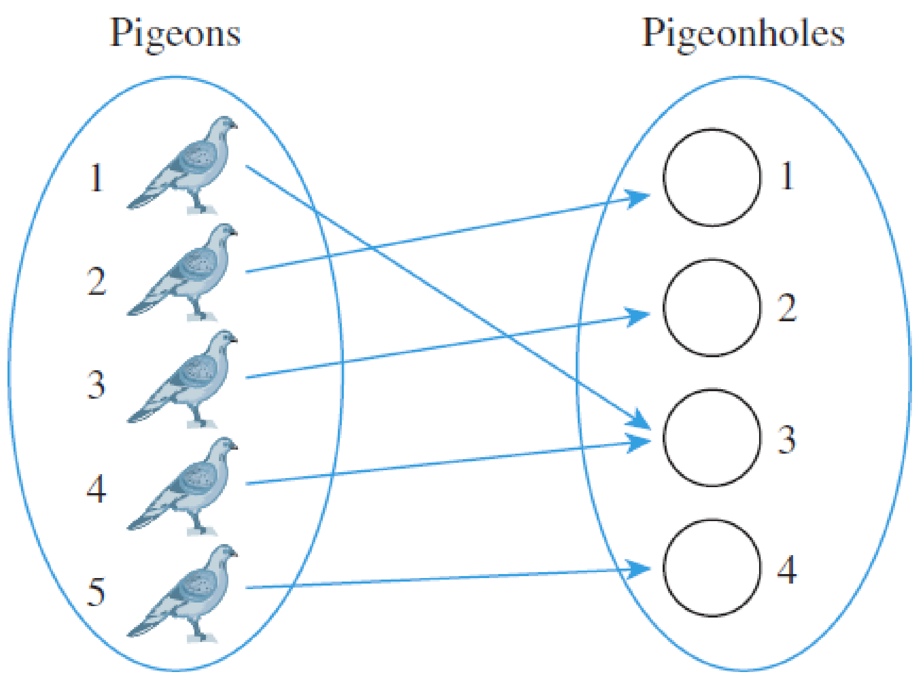
By definition of F^{-1}, $F^{-1}(y) = x$.

The Pigeonhole principle (sec 9.4)

- **A function from a finite set to a smaller set cannot be 1-1:** at least 2 elements in the domain have the same image in co-domain

If n pigeons fly into m pigeonholes with n > m,

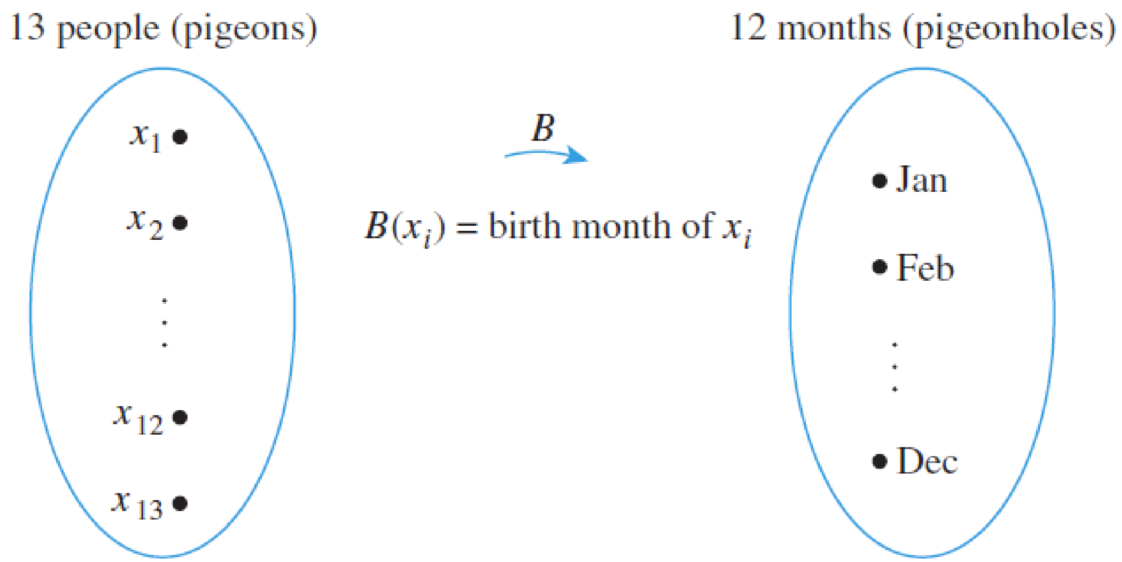
then at least one hole contains two or more pigeons.



at least 2 arrows point to the same element in co-domain

The Pigeonhole principle: example 1

- In a group of 6 people, must there be at least two who were born in the same month?
- In a group of 13 people, must there be at least two who were born in the same month



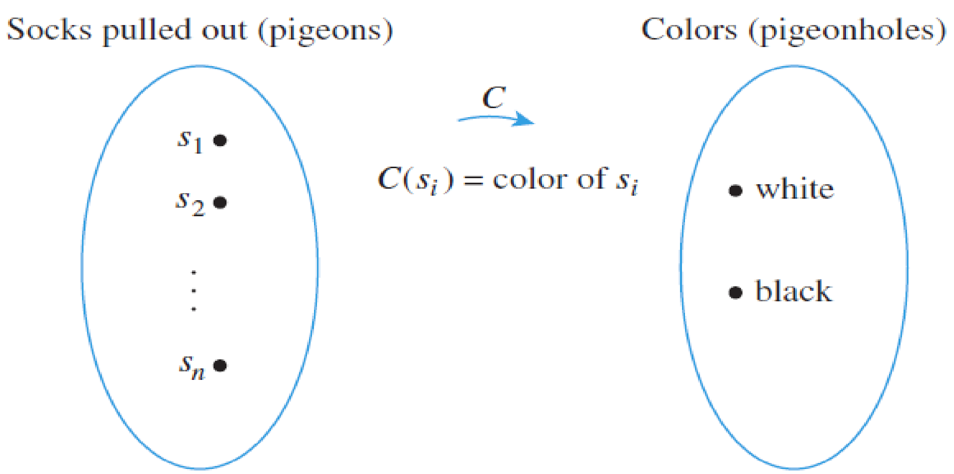
The Pigeonhole principle: example 2

- **Finding the number to pick to ensure a result:**

  at least the cardinality of the co-domain + 1

- A drawer contains black and white socks.

  What is the least number of socks you must pull out to be sure to get a matched pair?



2 socks are not enough:

one white and one black

3 socks are enough by the pigeonhole principle

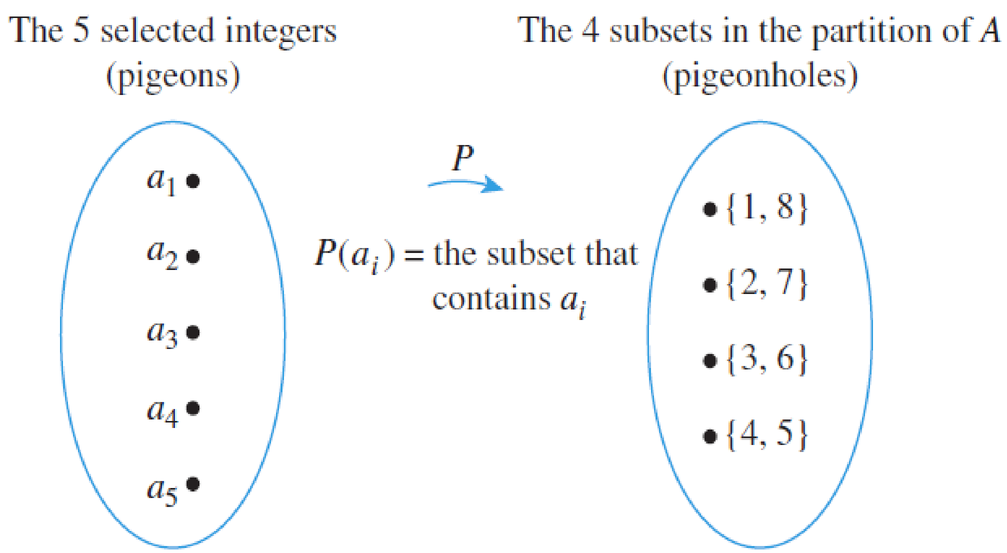
The Pigeonhole principle: example 3

- **Reach a certain sum:** Let A = {1, 2, 3, 4, 5, 6, 7, 8}
- If we select 4 integers from A, must at least one pair of the integers have a sum of 9?

  No. Let B = {1,2,3,4}

  1+2 = 3 ; 1+3 = 4 ; 1+4 = 5 ; 2+3 = 5 ; 2+4 = 6 ; 3+4 = 7
- If we select 5 integers from A, must at least one pair of the integers have a sum of 9?

  Yes.



Generalized Pigeonhole principle

- For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k,

  if $k < n/m$ (i.e., $km < n$), then there is some $y \in Y$ such that

  y is the image of at least $k + 1$ distinct elements of X.

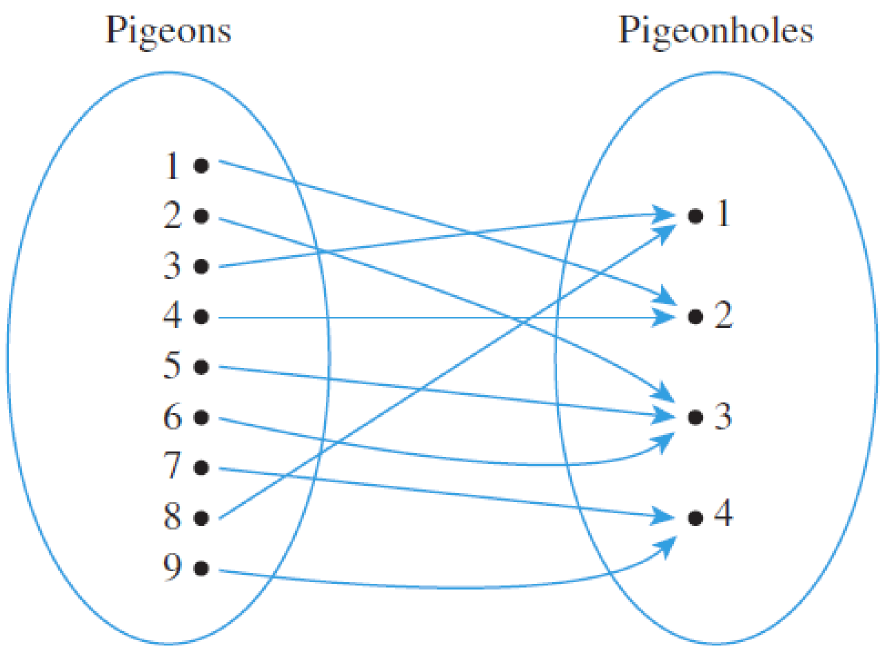
- **Example:**

  $n = 9$ pigeons

  $m = 4$ holes

  a least one pigeonhole

  contains 3 or more pigeons.



$k = 2 < 9/4$, $k+1 = 3$

One-to-one and onto for finite sets

- Let X and Y be finite sets with the **same number of elements** and f is a function from X to Y. Then **f is 1-1 $\Leftrightarrow$ f is onto**

Proof : Let $X = \{x_1, x_2, \ldots, x_m\}$ and $Y = \{y_1, y_2, \ldots, y_m\}$

($\rightarrow$) If f is 1-1, then $f(x_i)$ for $i = 1, \ldots m$ are all distinct.

Let $S = \{y \in Y \mid \forall x \in X, f(x) \neq y\}$; all $\{f(x_i)\}$ and S are mutually disjoint.

$m = |Y| = |\{f(x_1)\}| + |\{f(x_2)\}| + \ldots + |\{f(x_m)\}| + |S| = m + |S|$

$\Leftrightarrow$ $|S| = 0$, no element of Y is not the image of some element of X.

That is, f is onto.

($\leftarrow$) If f is onto, then $|f^{-1}(y_i)| \geq 1$ for all $i = 1, \ldots, m$.

all $\{f^{-1}(y_i)\}$ are mutually disjoint by f.

$m = |X| >= |f^{-1}(y_1)| + \ldots + |f^{-1}(y_m)|$. m terms, so $|f^{-1}(y_i)| = 1$.

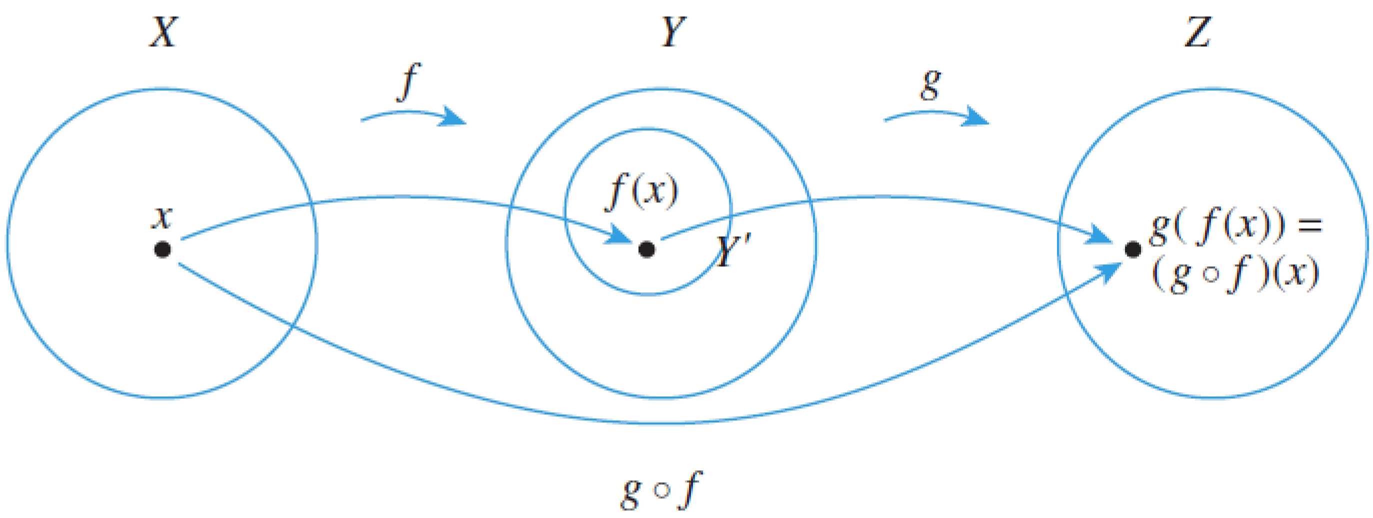
That is, f is 1-1.

Composition of functions

- Let f : X $\longrightarrow$Y' and g:Y $\longrightarrow$ Z be functions with the property that the range of f is a subset of the domain of g: Y' $\subseteq$ Y

The composition of f and g is a function $g \circ f : X \longrightarrow Z$:

$(g \circ f)(x) = g(f(x))$ for all $x \in X$



Composition of functions: example 1

- $f : \mathbf{Z} \rightarrow \mathbf{Z}$ and $g : \mathbf{Z} \rightarrow \mathbf{Z}$

$$f(n) = n + 1, \text{ for all } n \in \mathbf{Z}$$

$$g(n) = n^2, \text{ for all } n \in \mathbf{Z}$$

$$(g \circ f)(n) = g(f(n)) = g(n+1) = (n+1)^2, \text{ for all } n \in \mathbf{Z}$$

$$(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1, \text{ for all } n \in \mathbf{Z}$$

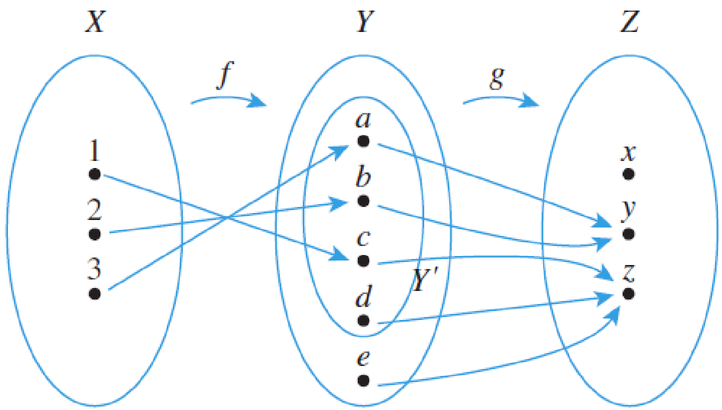
$$(g \circ f)(1) = (1 + 1)^2 = 4$$

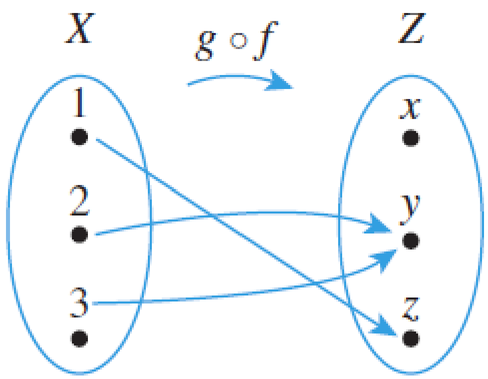
$$(f \circ g)(1) = 1^2 + 1 = 2$$

So, $f \circ g \neq g \circ f$

Composition of functions: example 2

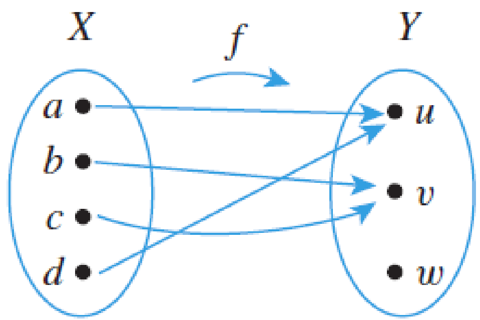
- f : {1,2,3} → {a,b,c,d} and g: {a,b,c,d,e} → {x,y,z}





Composition of functions: example 3

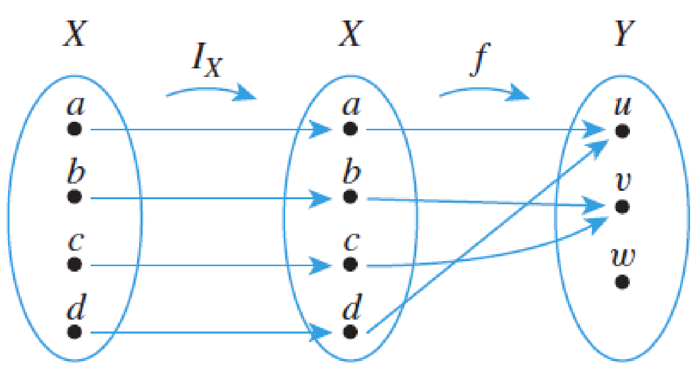
- $X = \{a, b, c, d\}$ and $Y = \{u, v, w\}$, $f : X \rightarrow Y$



$I_X : X \rightarrow X$ is an identity function

$I_X(x) = x$, for all $x \in X$

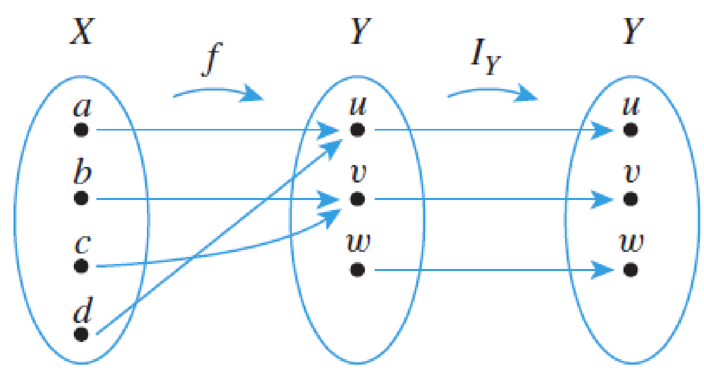
$(f \circ I_X)(x) = f(I_X(x)) = f(x)$, for all $x \in X$



$I_Y : Y \rightarrow Y$ is an identity function

$I_Y(y) = y$, for all $y \in Y$

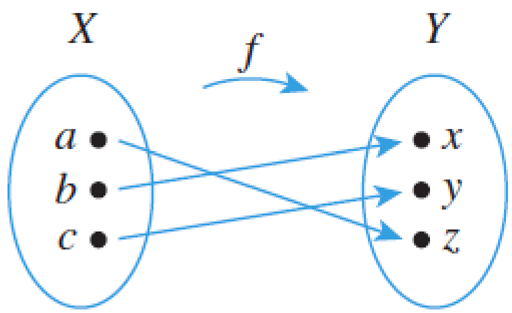
$(I_Y \circ f)(x) = I_Y(f(x)) = f(x)$, for all $x \in X$



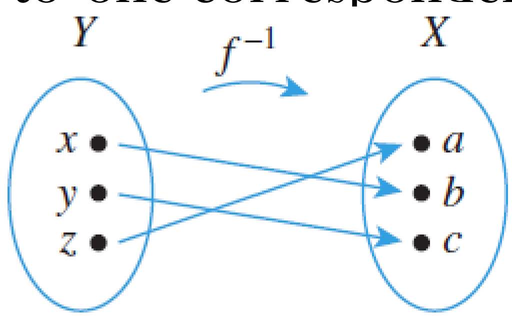
Composition of functions: example 4

- **Composing a function with its inverse:**

Let f : {a, b, c} $\longrightarrow$ {x, y, z} be a one-to-one and onto function



f is one-to-one correspondence ➔ f^{-1} : {x, y, z} $\longrightarrow$ {a, b, c}



$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(z) = a$

$(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(x) = b$ ➔ $\mathbf{f^{-1} \circ f = I_X}$

$(f^{-1} \circ f)(c) = f^{-1}(f(c)) = f^{-1}(y) = c$ **also** $\mathbf{f \circ f^{-1} = I_Y}$

Composition of functions: example 4

- **Composing a function with its inverse:**

  If $f : X \longrightarrow Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \longrightarrow X$, then (1) $f^{-1} \circ f = I_X$ and (2) $f \circ f^{-1} = I_Y$

  Proof of (1):

  Let x be any element in X: $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x' \in X$ (*)

  Definition of inverse function:

  $f^{-1}(b) = a \Leftrightarrow f(a) = b$ for all $a \in X$ and $b \in Y$

  ➔ $f^{-1}(f(x)) = x' \Leftrightarrow f(x') = f(x)$

  Since f is one-to-one, this implies that $x' = x$.

  (*) → $(f^{-1} \circ f)(x) = x$

Composition of one-to-one functions

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

  Proof (by direct proof):

  Suppose $f: X \to Y$ and $g: Y \to Z$ are both one-to-one functions.

  Suppose $x_1, x_2 \in X$ such that: $(g \circ f)(x_1) = (g \circ f)(x_2)$

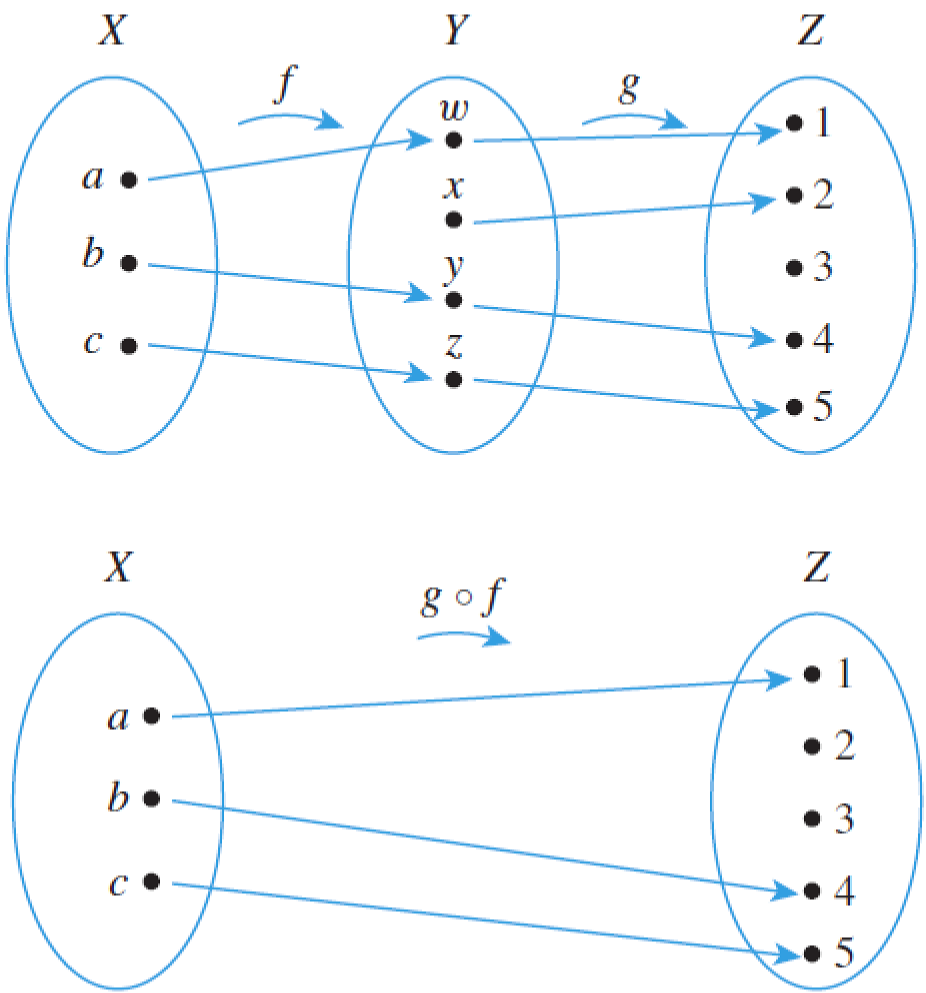
  By definition of composition of functions, $g(f(x_1)) = g(f(x_2))$.

  Since g is one-to-one, $f(x_1) = f(x_2)$.

  Since f is one-to-one, $x_1 = x_2$.

Composition of one-to-one functions

- **Example:**



Composition of onto functions

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

Proof:

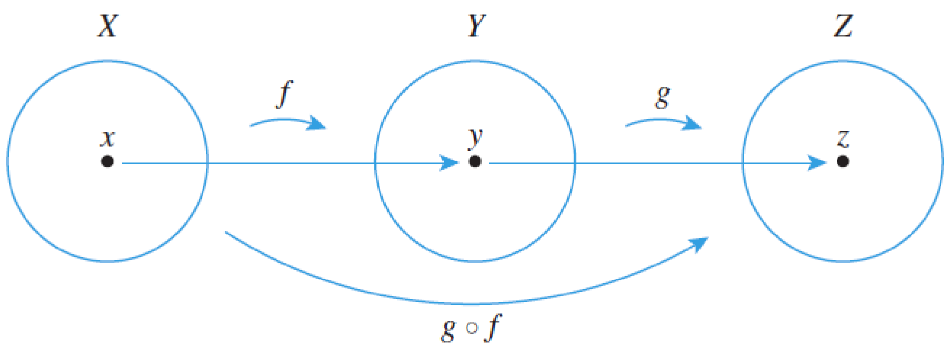
Suppose $f : X \to Y$ and $g : Y \to Z$ are both onto functions.

Let z be an element of Z.

Since g is onto, there is an element y in Y such that $g(y) = z$.

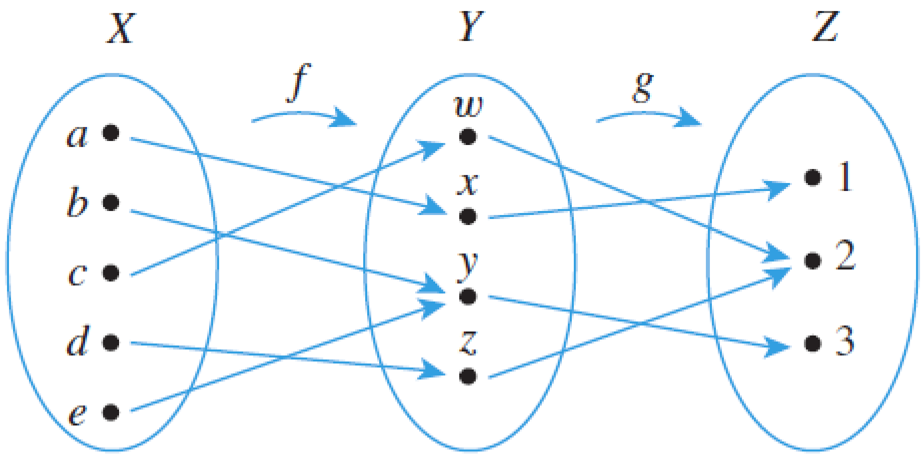
Since f is onto, there is an element x in X such that $f(x) = y$.

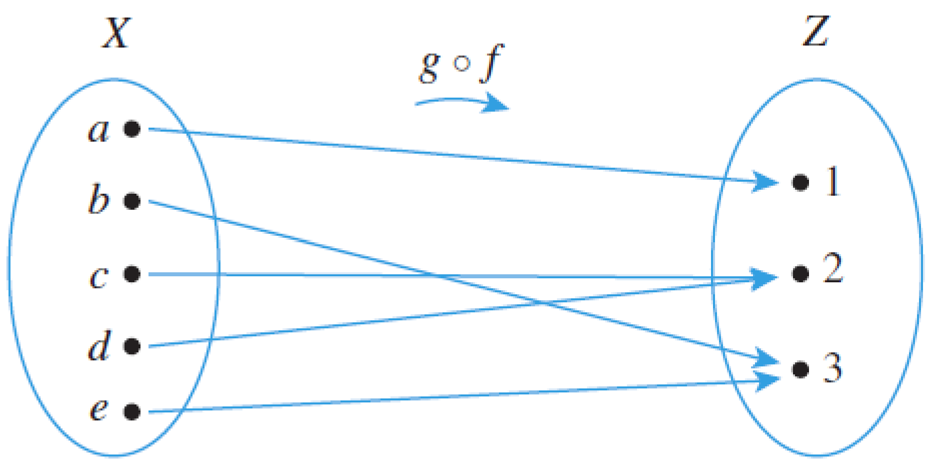
$z = g(y) = g(f(x)) = (g \circ f)(x)$ ➔ $g \circ f$ is onto



Composition of onto functions

- **Example:**





Cardinality and sizes of infinity

- **cardinal number** (**cardinal**): describe number of elements in a set.

  ordinal number (**ordinal**): describe order of elements in an ordered set.

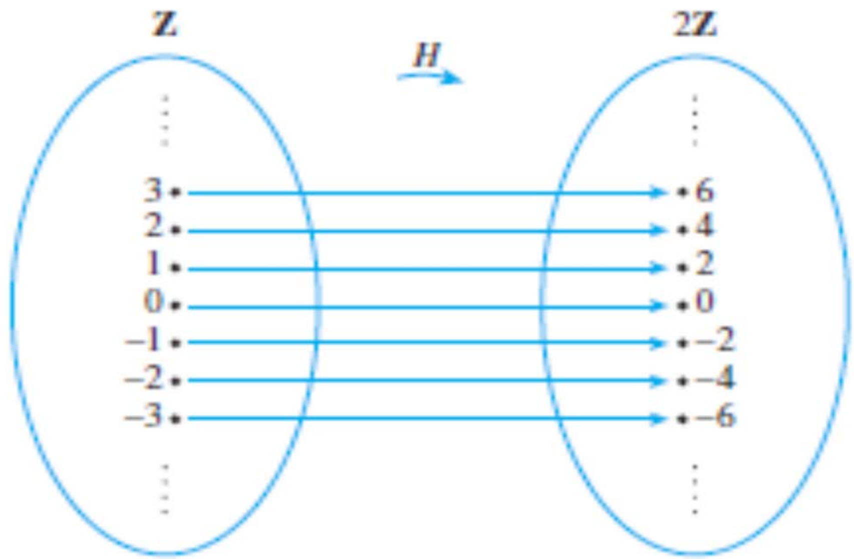
- **finite set**: the empty set or a set that can be put into
  1-1 correspondence with $\{1,2,\ldots,n\}$ for some positive integer n.

  infinite set: a nonempty set that cannot be put into
  1-1 correspondence with $\{1,2,\ldots,n\}$ for any positive integer n.

- a set A **has the same cardinality a** set B if, and only if, there is a 1-1 correspondence from A to B.
  - reflexivity: A has same cardinality as A
  - symmetry: if A has same cardinality as B, then B has same cardinality as A
  - transitivity: if A has same cardinality as B, and B has same cardinality as C, then A has same cardinality as C.

Cardinality: surprising example

- **An infinite set and a proper subset can have the same cardinality**



- **Example:**

  Z, the set of integers, and

  2Z, the set of even numbers

  have the same cardinality.

Proof: define function H: **Z** → **2Z** as H(n) = 2n for all n ∈ **Z**.

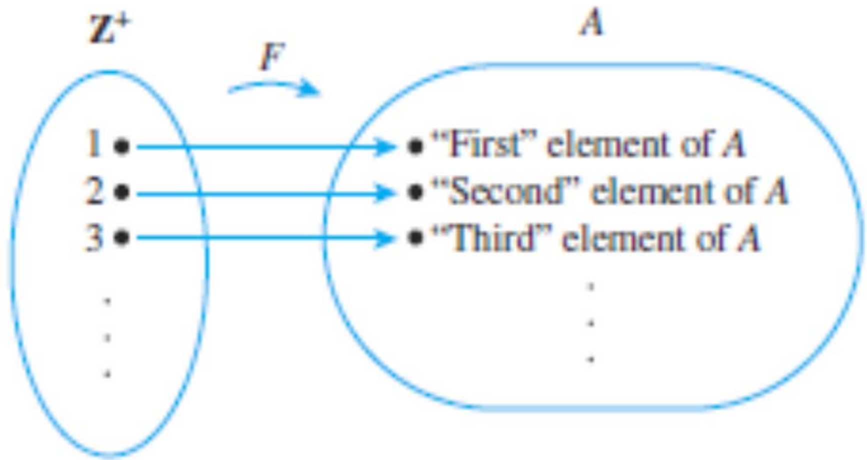
H is 1-1: if H(n1) = H(n2) then n1 = n2, by def of H and div by 2.

H is onto : any m ∈ **2Z**, m is even, so m= 2k for some k ∈ **Z**

Thus H is a 1-1 correspondence.

Countable sets

- Counting

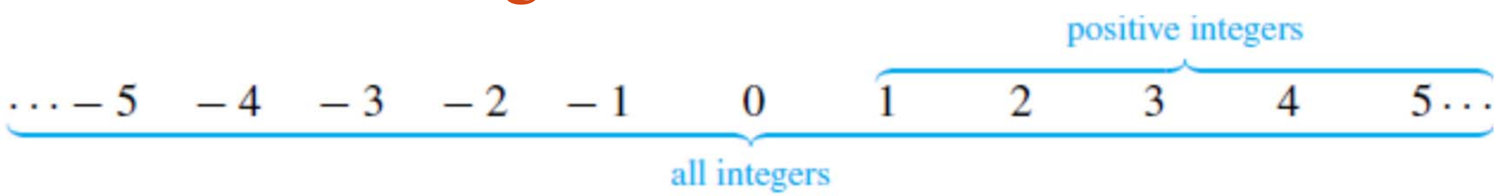


- A set is **countably infinite** if, and only if, it has the same cardinality as $\mathbf{Z}^+$, the set of positive integers.

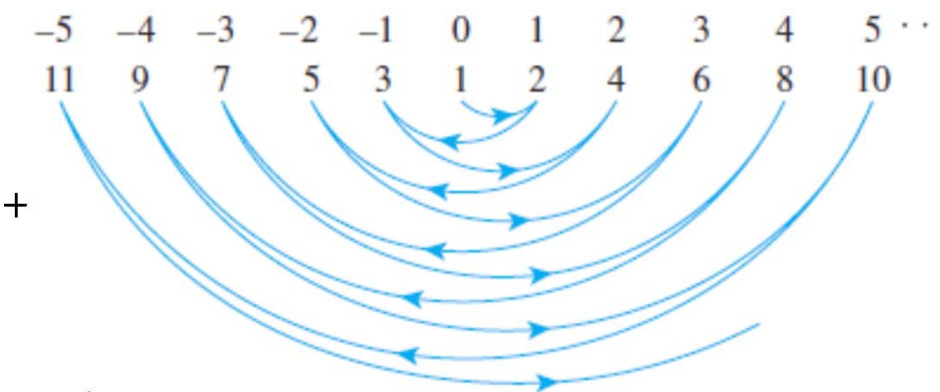
- A set is **countable** if, and only if, it is finite or countbly infinite.
- A set is **uncountable** if and only if it is not countable.

Countable sets: easy example

- **The set Z of all integers is countable** (and so **2Z** is too)



Proof:



No n in Z is counted twice:

1-1: n in Z -- at most 1 m in Z^+

All n in Z is counted:

onto: each n in Z -- some m in Z^+

Formally, define function F: $\mathbf{Z}^+ \rightarrow \mathbf{Z}$ as

F(n) = n/2 if n is an even positive integer

-(n-1)/2 if n is an odd positive integer

Countable sets of same cardinality

- For function f: $A \rightarrow B$, where A and B have the same cardinality,

  if A and B are finite, then f is 1-1 $\Leftrightarrow$ f is onto (slide 53)

- If A and B are infinite, then there exist

  functions that are both 1-1 and onto,

  functions that are 1-1 but not onto,

  functions that are onto but not 1-1.

Examples: $\mathbf{Z}^+$ and $\mathbf{Z}$ have the same cardinality (previous slide)

i: $\mathbf{Z}^+ \rightarrow \mathbf{Z}$ with $i(n)=n$ is 1-1 but not onto

j: $\mathbf{Z} \rightarrow \mathbf{Z}^+$ with $j(n)=|n|+1$ is onto but not 1-1

Larger infinities? surprising example

- **The set Q^+ of all positive rational numbers is countable**

Rational number are dense:

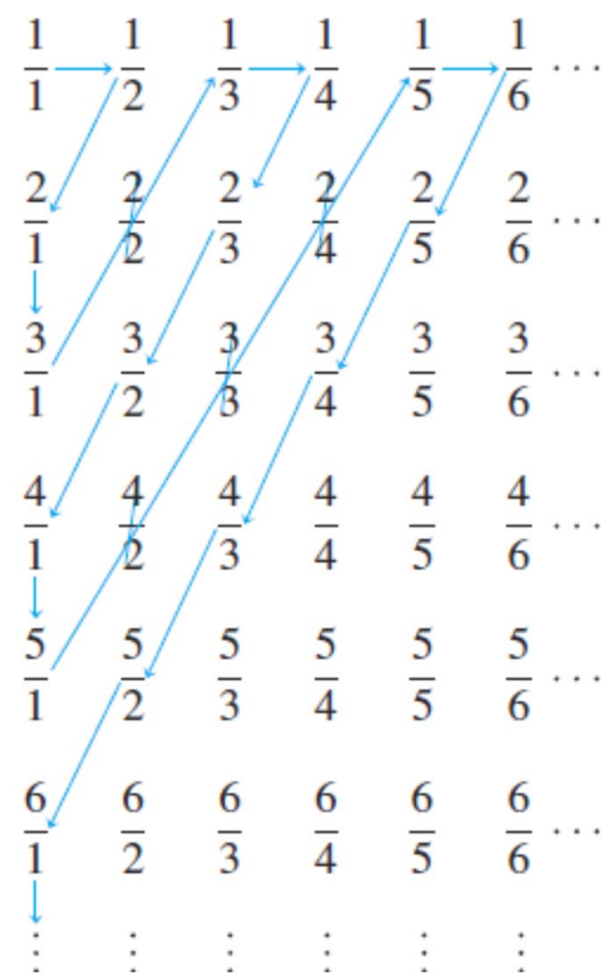
between any two, there is another!

Proof:

Count following arrows, skipping duplicates

F(1)=1/1, F(2)=1/2, F(3)=2/1,F(4)=3/1,

skip 2/2=1/1, F(t)=1/3, …



F is onto: all q in $\mathbf{Q}^+$ will be counted

F is 1-1: no q in $\mathbf{Q}^+$ is counted twice

Larger infinities: famous example

- **The set of all real numbers between 0 and 1 is uncountable**

Proof (by contradiction): Suppose the set [0,1] is countable.

Then decimal representations of all these numbers can be written in a list, on right:

$$\begin{array}{l} 0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots \\ 0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots \\ 0.a_{31}a_{32}a_{33}\cdots a_{3n}\cdots \\ \vdots \\ 0.a_{n1}a_{n2}a_{n3}\cdots a_{nn}\cdots \\ \vdots \end{array}$$

The i-th number's j-th decimal digit is a_{ij}:

e.g., $a_{11}=2$, $a_{22}=1$, $a_{33}=3$, …

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

Construct a decimal number $d = 0.d_1d_2d_3\cdots d_n\cdots$ $\quad d_n = \begin{cases} 1 & \text{if } a_{nn} \neq 1 \\ 2 & \text{if } a_{nn} = 1 \end{cases}$

e.g., $d_1=1$, $d_2=2$, $d_3=1$, … so d = 0.12112…

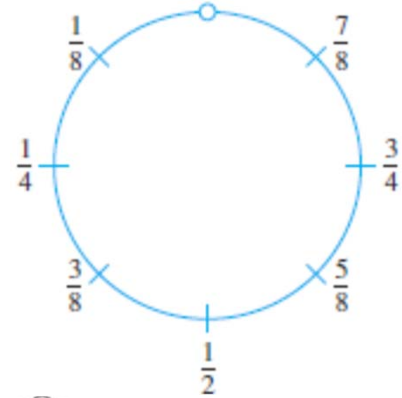
Each n, d differs from the n-th number on list in n-th decimal digit.

d is not in the list, contradiction! Cantor diagonalization process

Larger infinities: famous example 2

- **The set of all real numbers and the set of real numbers between 0 and 1 have the same cardinality**

Proof:

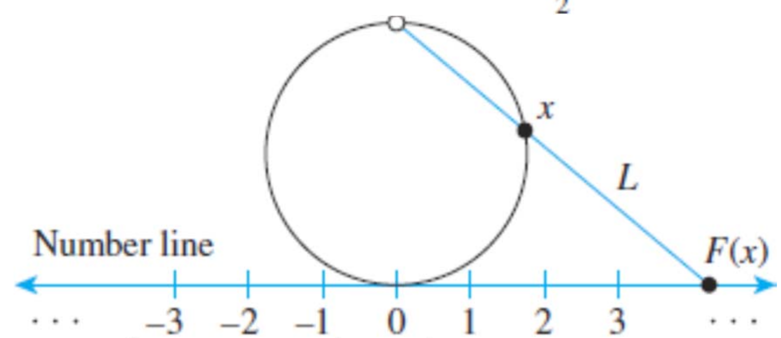


Let $S = \{x \in \mathbf{R} \mid 0 < x < 1\}$. Make a circle:

no 0 or 1, so top-most point of circle is omitted

Define function F: $S \rightarrow \mathbf{R}$ where F(x)

is projection of x on number line.



F is 1-1: different points on circle go

to distinct points on number line

F is onto: for any point on number line, a line can be drawn

to top of circle and intersect circle at some point.

Thus, F is a 1-1 correspondence from S to **R.**

More countable sets and infinities

- The set of all bit strings (strings of 0's and 1's) **is countable** (think of mapping each positive integer to its binary representation)
- The set of all computer programs in a language is **countable** (finite alphabet, each symbol translated to bit string)
- The set of all functions from integers to $\{0,1\}$ is **uncountable**

- Any subset of any countable set is **countable**
- Any set with an uncountable subset is **uncountable**

- There is an infinite sequence of larger infinities.
  Example: Z, *P*(Z), *P*(*P*(Z)), *P*(*P*(*P*(Z))), …