COMP233 Discrete Mathematics

Chapter 7
Functions

Functions

7.1 Introduction to Functions

In this lecture:

- ❑Part 1: **What is a function**
- ❑Part 2: Equality of Functions
- ❑Part 3: Examples of Functions
- ❑Part 3: Checking Well Defined Functions

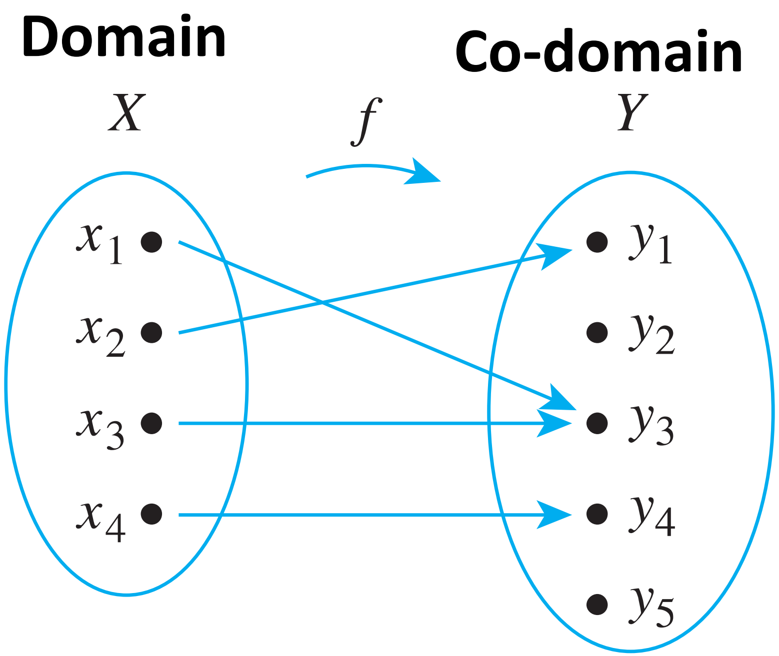
Motivation

Many issues in life can be mathematized and used as functions:

- Div(x), mod(x), ….
- FatherOf(x), TruthTable (x)

- In this chapter we focus on **discrete functions**

What is a Function



علاقة بين عنصرين
كل عنصر في المجال يجب ان
يكون له صورة واحدة في المدى.
كل عنصر في المدى هو صورة
لعنصر (او اكثر) في المجال

A function is a relation from X, the domain, to Y, the co-domain, that satisfies 2 properties:

1) Every element x is related to some element in Y;
2) No element in X is related to more than one element in Y

Function Definition

• Definition

A **function f from a set X to a set Y**, denoted $f: X \to Y$, is a relation from X, the **domain**, to Y, the **co-domain**, that satisfies two properties: (1) every element in X is related to some element in Y, and (2) no element in X is related to more than one element in Y. Thus, given any element x in X, there is a unique element in Y that is related to x by f. If we call this element y, then we say that "f sends x to y" or "f maps x to y" and write $x \xrightarrow{f} y$ or $f: x \to y$. The unique element to which f sends x is denoted

$\boldsymbol{f(x)}$ and is called **f of x**, or
the output of f for the input x, or
the value of f at x, or
the image of x under f.

The set of all values of f taken together is called the *range of f* or the *image of X under f*. Symbolically,

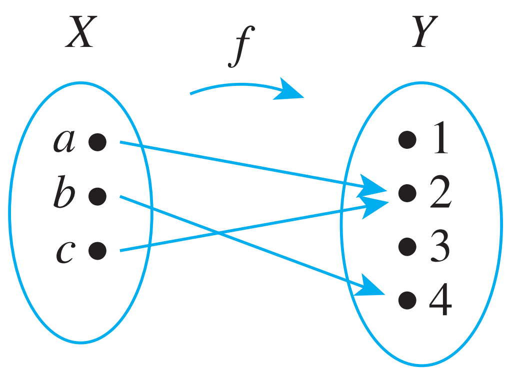
$$\textbf{range of } f = \textbf{image of } X \textbf{ under } f = \{y \in Y \mid y = f(x), \text{ for some } x \text{ in } X\}.$$

Given an element y in Y, there may exist elements in X with y as their image. If $f(x) = y$, then x is called **a preimage of y** or **an inverse image of y**. The set of all inverse images of y is called *the inverse image of y*. Symbolically,

$$\textbf{the inverse image of } y = \{x \in X \mid f(x) = y\}.$$

Example

Let $X = \{a, b, c\}$ and $Y = \{1,2,3,4\}$. Define a function $\boldsymbol{f}$ from X to Y



a. Write the domain and co-domain of f.

b. Find $f(a)$, $f(b)$, and $f(c)$.

c. What is the range of f?

d. Is c an inverse image of 2? Is b an inverse image of 3?

e. Find the inverse images of 2, 4, and 1.

f. Represent f as a set of ordered pairs.

Solution

a. domain of f = {a, b, c}, co-domain of f = {1, 2, 3, 4}

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

c. range of f = {2, 4}

d. Yes, No

e. inverse image of 2 = {a, c}

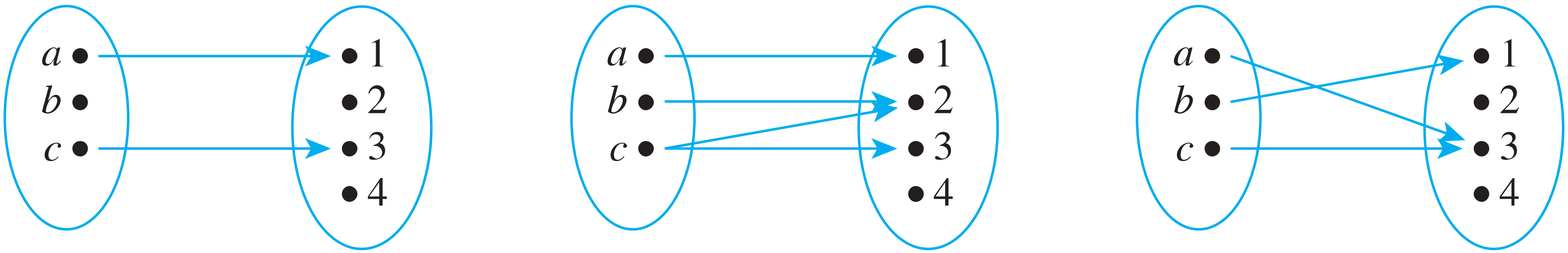
inverse image of 4 = {b}

inverse image of 1 = ∅ (since no arrows point to 1)

f. {(a, 2), (b, 4), (c, 2) }

Example

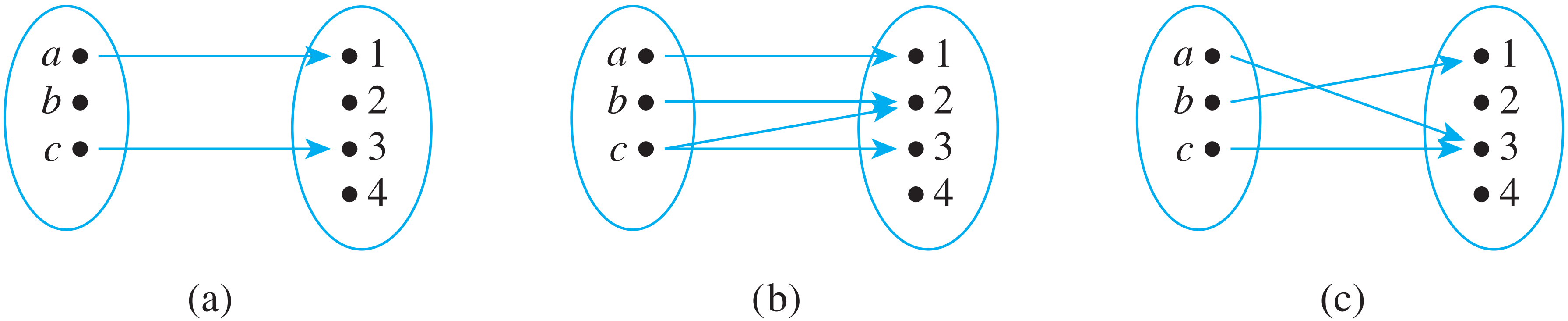
Which are functions?



(a) (b) (c)

Example

Which are functions?



(a) There is an element x, namely b, that is not sent to any element in of Y (i.e., there is no arrow coming out of Y)

(b) The element c isn't sent to a unique element of Y: that is, there are two arrows coming out of c; one pointing to 2 and the other is pointing to 3

Functions

7.1 Introduction to Functions

In this lecture:

- ❑Part 1: What is a function
- ❑Part 2: **Equality of Functions**
- ❑Part 3: Examples of Functions
- ❑Part 3: Checking Well Defined Functions

Equality of Functions

Theorem 7.1.1 A Test for Function Equality

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 $x \in X$.

Example:

Let $L = \{0, 1, 2\}$, and define functions f and g:
For all x *in* L

$$f(x) = (x^2 + x + 1) \; mod \; 3 \quad \text{and} \quad g(x) = (x + 2)^2 \; mod \; 3.$$

Does *f*= *g* ?

Equality of Functions

Theorem 7.1.1 A Test for Function Equality

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 $x \in X$.

Example:

Let $L = \{0, 1, 2\}$, and define functions f and g:
For all x *in* L

$$f(x) = (x^2 + x + 1) \bmod 3 \quad \text{and } g(x) = (x + 2)^2 \bmod 3.$$

Does *f = g* ?

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

Equal functions in reality?

Equality of Functions

Theorem 7.1.1 A Test for Function Equality

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 $x \in X$.

Example:

Let $F: \mathbf{R} \to \mathbf{R}$ and $G: \mathbf{R} \to \mathbf{R}$ be functions. Define new functions $F + G: \mathbf{R} \to \mathbf{R}$ and $G + F: \mathbf{R} \to \mathbf{R}$ as follows: For all $x \in \mathbf{R}$,

$$(F + G)(x) = F(x) + G(x) \quad \text{and} \quad (G + F)(x) = G(x) + F(x).$$

Does $F + G = G + F$?

Equality of Functions

Theorem 7.1.1 A Test for Function Equality

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 $x \in X$.

Example:

Let $F: \mathbf{R} \to \mathbf{R}$ and $G: \mathbf{R} \to \mathbf{R}$ be functions. Define new functions $F + G: \mathbf{R} \to \mathbf{R}$ and $G + F: \mathbf{R} \to \mathbf{R}$ as follows: For all $x \in \mathbf{R}$,

$$(F + G)(x) = F(x) + G(x) \quad \text{and} \quad (G + F)(x) = G(x) + F(x).$$

Does $F + G = G + F$?

$$\begin{aligned} (F+G)(x) &= F(x) + G(x) && \text{by definition of } F + G \\ &= G(x) + F(x) && \text{by the commutative law for addition of real numbers} \\ &= (G + F)(x) && \text{by definition of } G + F \end{aligned}$$

Hence $F + G = G + F$.

Functions

7.1 Introduction to Functions

In this lecture:

- ❑ Part 1: What is a function
- ❑ Part 2: Equality of Functions
- ❑ Part 3: **Examples of Functions**
- ❑ Part 3: Checking Well Defined Functions

Examples of Functions

Identity Function

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

Identity function send each element of X to the element that is identical to it

E.g., $I_x(y) = y$

Examples of Functions

Sequences

An infinite sequence is a function defined on set of integers that are greater than or equal to a particular integer.

E.g., Define the following sequence as a function from the set of positive integers to the set of real numbers

$$1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, \ldots, \frac{(-1)^n}{n+1}, \ldots$$

can be thought as a function *f* from the nonnegative integers to the real numbers that associate 0 → 1, 1 → -1/2, 2 → 1/3, …

$$\text{Send each integer } n \geq 0 \text{ to } f(n) = \frac{(-1)^n}{n+1}.$$

$$g(n+1) = \frac{(-1)^{n+2}}{n+1}$$

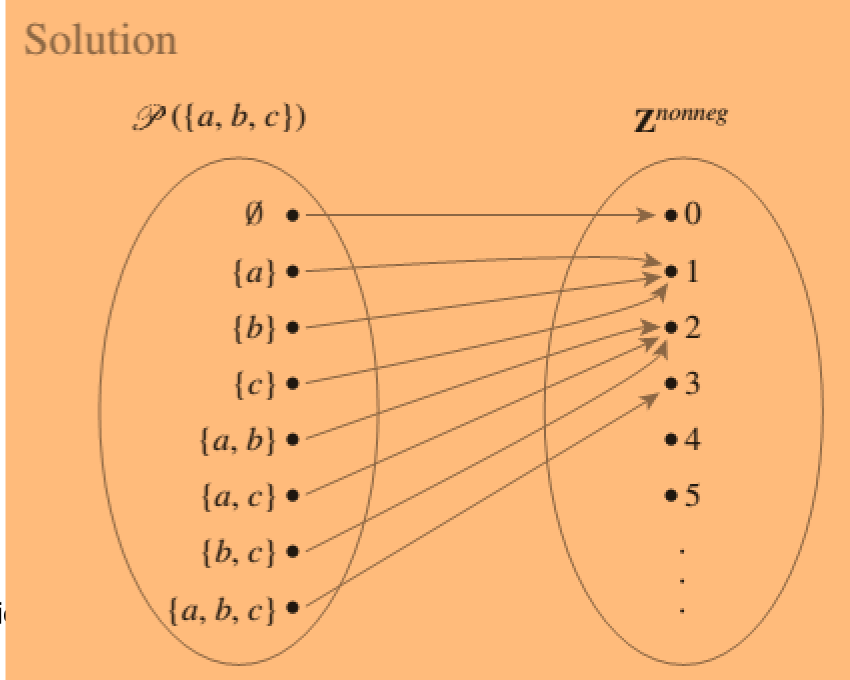
Examples of Functions

Function Defined on a Power Set

Recall from Section 6.1 that P(A) denotes the set of all subsets of the set A.

Define a function F: P({a, b, c}) → $\mathbf{Z}^{nonneg}$
as follows: For each $X \in$ P({a, b, c}),

F(X) = the number of elements in *X*.
Draw an arrow diagram for *F*.



Examples of Functions

Cartesian product

Define functions $M: \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ and $R: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ as follows: For all ordered pairs (a, b) of integers,

$$M(a, b) = ab \quad \text{and} \quad R(a, b) = (-a, b).$$

M is the multiplication function that sends each pair of real numbers to the product of the two.
R is the reflection function that 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.

Find the following

a. $M(-1, -1)$ b. $M\left(\frac{1}{2}, \frac{1}{2}\right)$ c. $M(\sqrt{2}, \sqrt{2})$
d. $R(2, 5)$ e. $R(-2, 5)$ f. $R(3, -4)$

a. $(-1)(-1) = 1$ b. $(1/2)(1/2) = 1/4$ c. $\sqrt{2} \cdot \sqrt{2} = 2$
d. $(-2, 5)$ e. $(-(-2), 5) = (2, 5)$ f. $(-3, -4)$

Examples of Functions

Logarithmic functions

- **Definition Logarithms and Logarithmic Functions**

Let b be a positive real number with $b \neq 1$. For each positive real number x, the **logarithm with base *b* of *x***, written $\log_b x$, is the exponent to which b must be raised to obtain x. Symbolically,

$$\log_b x = y \quad \Leftrightarrow \quad b^y = x.$$

The **logarithmic function with base *b*** is the function from $\mathbf{R}^+$ to $\mathbf{R}$ that takes each positive real number x to $\log_b x$.

- $\log_3 9 = 2$ because $3^2 = 9$.
- $\log_2 (1/2) = -1$ because $2^{-1} = ½$.
- $\log_{10}(1) = 0$ because $10^0 = 1$.
- $\log_2(2^m) = m$ because the exponent to which 2 must be raised to obtain 2^m is m.
- $2^{\log_2 m} = m$ because $\log_2 m$ is the exponent to which 2 must be raised to obtain m.

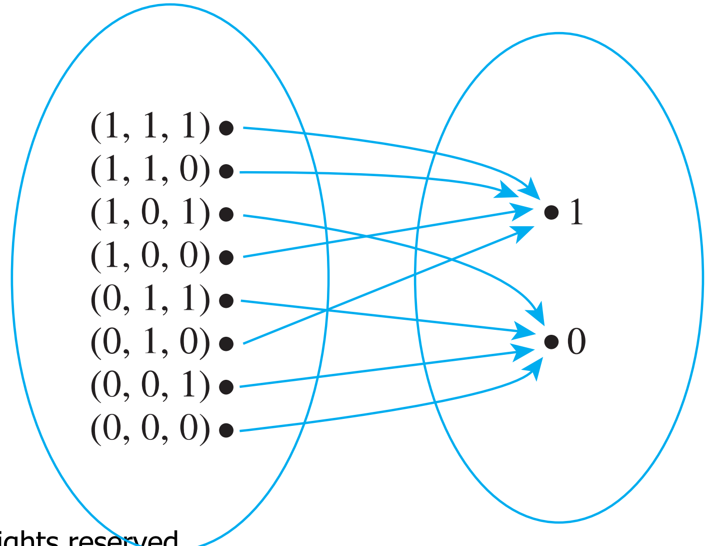
Examples of Functions

Boolean Functions

- **Definition**

An **(n-place) Boolean function** f is a function whose domain is the set of all ordered n-tuples of 0's and 1's and whose co-domain is the set {0, 1}. More formally, the domain of a Boolean function can be described as the Cartesian product of n copies of the set {0, 1}, which is denoted $\{0, 1\}^n$. Thus $f: \{0, 1\}^n \to \{0, 1\}$.

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



Examples of Functions

Boolean Functions

Consider the three-place Boolean function defined from the set of all 3-tuples of 0's and 1's to {0, 1} as follows: For each triple (x_1, x_2, x_3) of 0's and 1's,

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

Describe f using an input/output table.

$f(1, 1, 1) = (1 + 1 + 1)\ mod\ 2 = 3\ mod\ 2 = 1$
$f(1, 1, 0) = (1 + 1 + 0)\ mod\ 2 = 2\ mod\ 2 = 0$
and so on to calculate the other values

Input			Output
x_1	x_2	x_3	$(x_1 + x_2 + x_3)\ mod\ 2$
1	1	1	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
0	0	0	0

Functions

7.1 Introduction to Functions

In this lecture:

- ❑ Part 1: What is a function
- ❑ Part 2: Equality of Functions
- ❑ Part 3: Examples of Functions
- ❑ Part 3: **Checking Well Defined Functions**

Well-defined Functions

Checking Whether a Function Is Well Defined

A function is **NOT** well defined if it fails to satisfy at least one of the requirements of being a function

E.g., Define a function f: **R** → **R** by specifying that for all real numbers x, $f(x)$ is the real number y such that $x^2+y^2=1$.

There are two reasons why this function is not well defined:
For almost all values of x either (1) there is no y that satisfies the given equation or (2) there are two different values of y that satisfy the equation

Consider when x=2
Consider when x=0

Well-defined Functions

Checking Whether a Function Is Well Defined

$f : \mathbf{Q} \to \mathbf{Z}$ defines this formula:

$$f\left(\frac{m}{n}\right) = m \quad \text{for all integers } m \text{ and } n \text{ with } n \neq 0.$$

Is f a well defined function?

It is not a well defined function since fractions have more than one representation as quotients of integers.

$$f\left(\tfrac{1}{2}\right) = 1 \quad \text{and} \quad f\left(\tfrac{3}{6}\right) = 3,$$

$$f\left(\tfrac{1}{2}\right) \neq f\left(\tfrac{3}{6}\right).$$

Well-defined Functions

Checking Whether a Function or not

Y= BortherOf(x)

Y= SonOf(x)

Y= FatherOf(x)

Y= Wife Of(x)

.

.

.

Functions

7.2 Properties of Functions

In this lecture:

- ❑ Part 1: **One-to-one Functions**
- ❑ Part 2: Onto Functions
- ❑ Part 3: one-to-one Correspondence Functions
- ❑ Part 4: Inverse Functions
- ❑ Part 5: Applications: Hash and Logarithmic Functions

One-to-One Functions

- **Definition**

Let F be a function from a set X to a set Y. F is **one-to-one** (or **injective**) if, and only if, for all elements x_1 and x_2 in X,

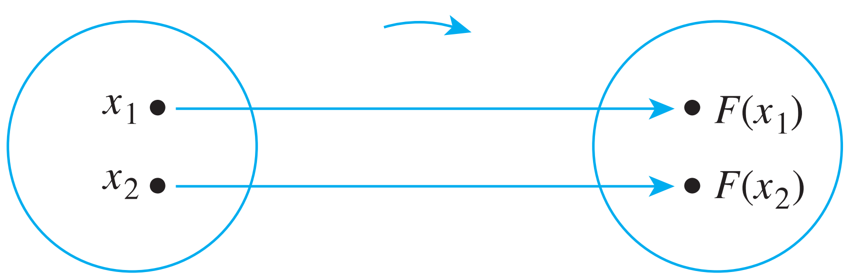
$$\text{if } F(x_1) = F(x_2), \text{ then } x_1 = x_2,$$

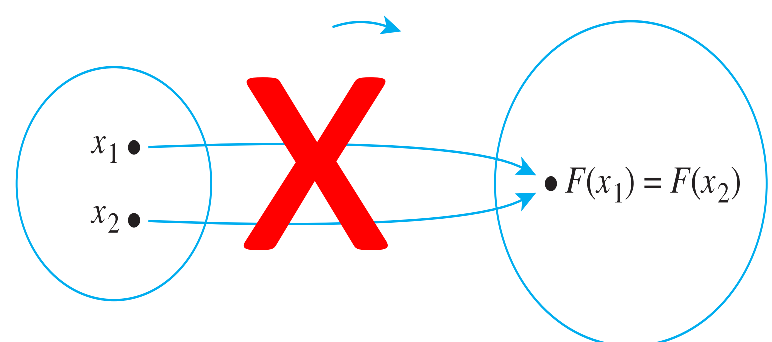
or, equivalently, $$\text{if } x_1 \neq x_2, \text{ then } F(x_1) \neq F(x_2).$$

Symbolically,

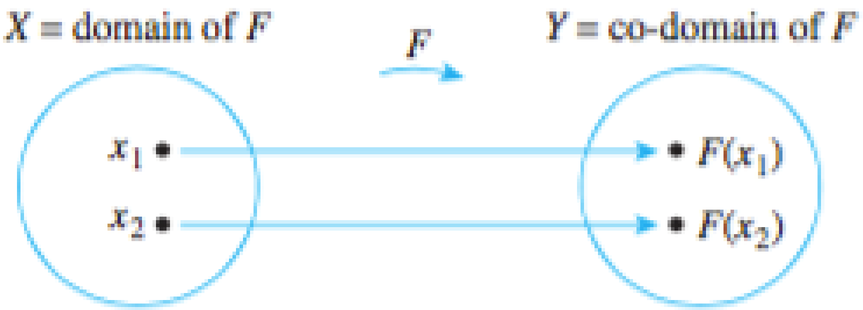
$$F\colon X \to Y \text{ is one-to-one} \quad \Leftrightarrow \quad \forall x_1, x_2 \in X, \text{if } F(x_1) = F(x_2) \text{ then } x_1 = x_2.$$

لا يوجد عنصرين في المجال لهما نفس الصورة في المدى



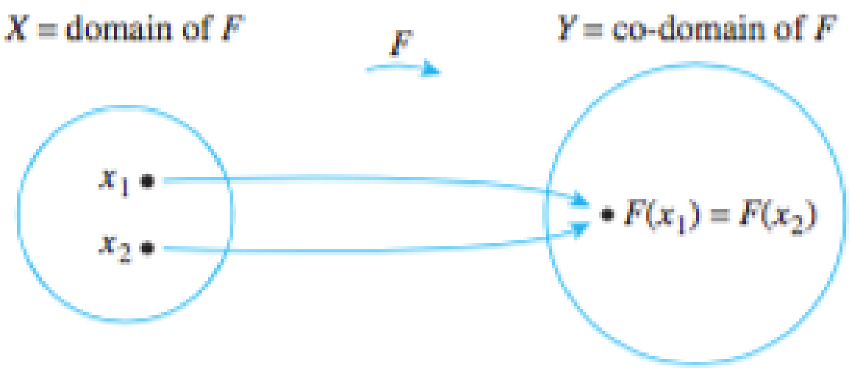


One-to-One Functions



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

A One-to-One Function Separates Points



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

A Function That Is Not One-to-One

One-to-One Functions

a. Do either of the arrow diagrams in Figure 7.2.2 define one-to-one functions?

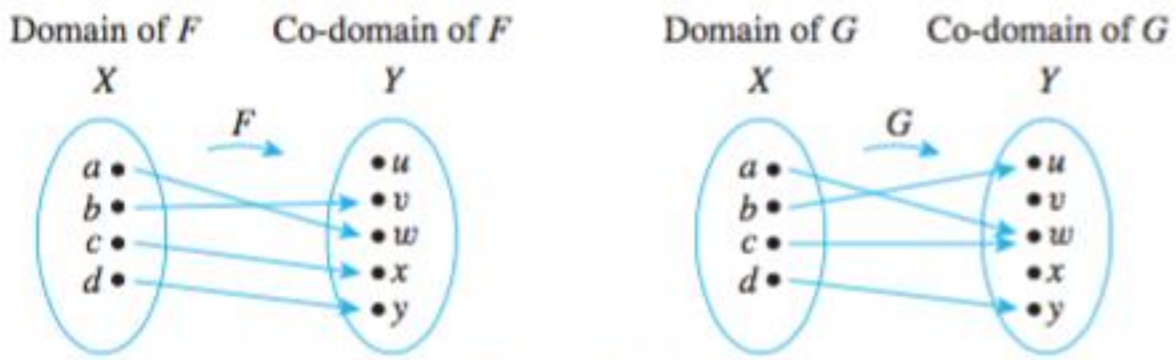


Figure 7.2.2

b. Let $X = \{1, 2, 3\}$ and $Y = \{a, b, c, d\}$. Define $H: X \to Y$ as follows: $H(1) = c$, $H(2) = a$, and $H(3) = d$. Define $K: X \to Y$ as follows: $K(1) = d$, $K(2) = b$, and $K(3) = d$. Is either H or K one-to-one?

One-to-One Functions

a. Do either of the arrow diagrams in Figure 7.2.2 define one-to-one functions?

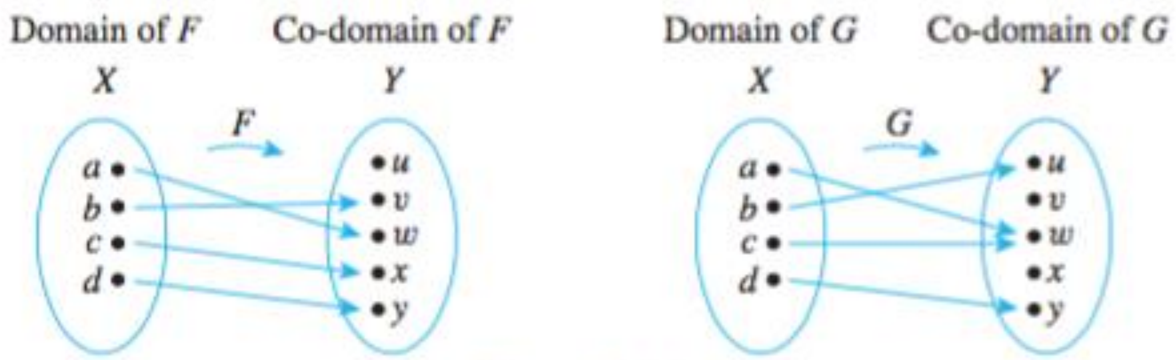


Figure 7.2.2

b. Let $X = \{1, 2, 3\}$ and $Y = \{a, b, c, d\}$. Define $H: X \to Y$ as follows: $H(1) = c$, $H(2) = a$, and $H(3) = d$. Define $K: X \to Y$ as follows: $K(1) = d$, $K(2) = b$, and $K(3) = d$. Is either H or K one-to-one?

(a) F is one-to-one but G is not. F is one-to-one because no two different elements of X are sent by F to the same element of Y. G is not one-to-one because the elements a and c are both sent by G to the same element of Y: $G(a) = G(c) = \text{w}$ but $a \neq c$.

(b) H is one-to-one but K is not. H is one-to-one because each of the three elements of the domain of H is sent by H to a different element of the co-domain: $H(1) \neq H(2)$, $H(1) \neq H(3)$, and $H(2) \neq H(3)$. K, however, is not one-to-one because $K(1) = K(3) = d$ but $1 \neq 3$.

Proving/Disproving Functions are One-to-One

To prove f is one-to-one (Direct Method):

suppose x_1 and x_2 are elements of $X \mid f(x_1) = f(x_2)$, and **show** that $x_1 = x_2$.

To show that f is *not* one-to-one:

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

Proving/Disproving Functions are One-to-One

Example 1

Define f: $\mathbf{R} \to \mathbf{R}$ by the rule

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

Is f one-to-one? Prove or give a counterexample.

Proving/Disproving Functions are One-to-One

Example 1

Define f: $\mathbf{R} \to \mathbf{R}$ by the rule

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

Is f one-to-one? Prove or give a counterexample.

Suppose x_1 and x_2 are real numbers such that $f(x_1) = f(x_2)$. *[We must show that $x_1 = x_2$.]* By definition of f,

$4x_1 - 1 = 4x_2 - 1$. Adding 1 to both sides gives

$4x_1 = 4x_2$, and dividing both sides by 4 gives

$x_1 = x_2$, which is what was to be shown.

Proving/Disproving Functions are One-to-One

Example 2

Define $g: \mathbf{Z} \to \mathbf{Z}$ by the rule

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

Is g one-to-one? Prove or give a counterexample.

Proving/Disproving Functions are One-to-One

Example 2

Define $g : \mathbf{Z} \to \mathbf{Z}$ by the rule

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

Is g one-to-one? Prove or give a counterexample.

Counterexample:

Let $n_1 = 2$ and $n_2 = -2$. Then by definition of g,

$$g(n_1) = g(2) = 2^2 = 4 \text{ and also}$$

$$g(n_2) = g(-2) = (-2)^2 = 4.$$

Hence $g(n_1) = g(n_2)$ but $n_1 \neq n_2$,

and so g is not one-to-one.

Proving/Disproving Functions are One-to-One

Example 3

Define g : **MobileNumber** → **People** by the rule

$g(x) = Person$ for all $x \in$ **MobileNumber**

Is g one-to-one? Prove or give a counterexample.

Counter example:

0599123456 and 0569123456 are both for Sami

Proving/Disproving Functions are One-to-One

Example 4

Define g : **Fingerprints** → **People** by the rule

$g(x) = Person$ for all $x \in$ **R** **Fingerprint**

Is g one-to-one? Prove or give a counterexample.

Prove:
In biology and forensic science: “The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail” [w].

Functions

7.2 Properties of Functions

In this lecture:

- Part 1: One-to-one Functions
- Part 2: **Onto Functions**
- Part 3: one-to-one Correspondence Functions
- Part 4: Inverse Functions
- Part 5: Applications: Hash and Logarithmic Functions

Onto Functions

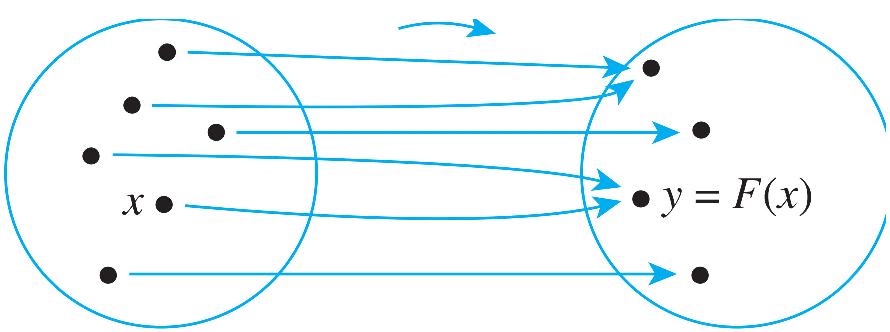
- **Definition**

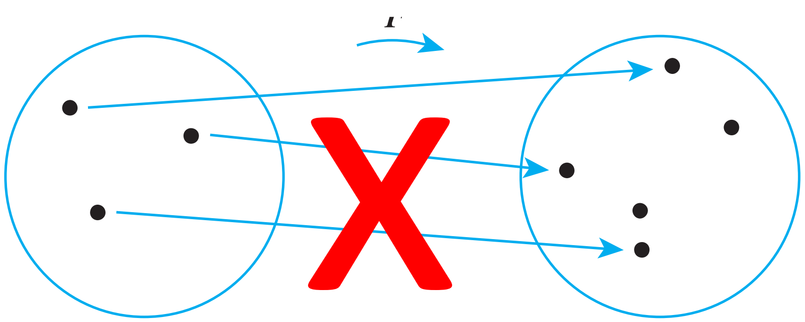
Let F be a function from a set X to a set Y. F is **onto** (or **surjective**) if, and only if, given any element y in Y, it is possible to find an element x in X with the property that $y = F(x)$.

Symbolically:

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

لا يوجد عنصر في المجال المقابل ليس صورة لعنصر في المجال





Onto Functions

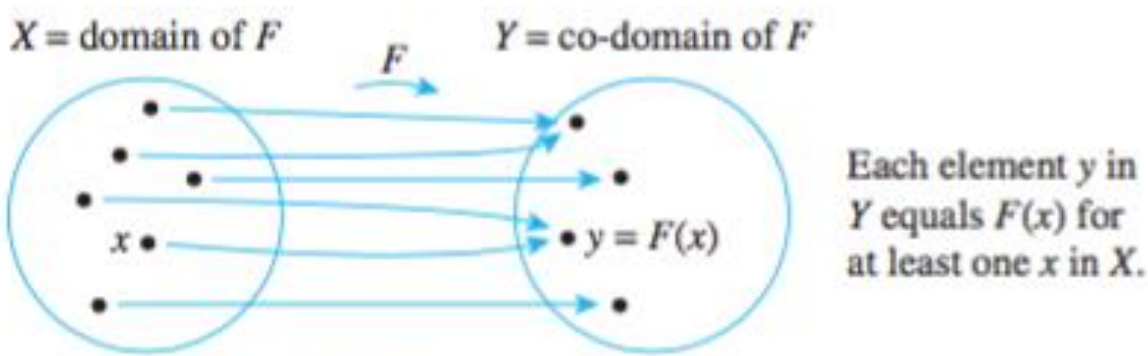


Figure 7.2.3(a) A Function That Is Onto

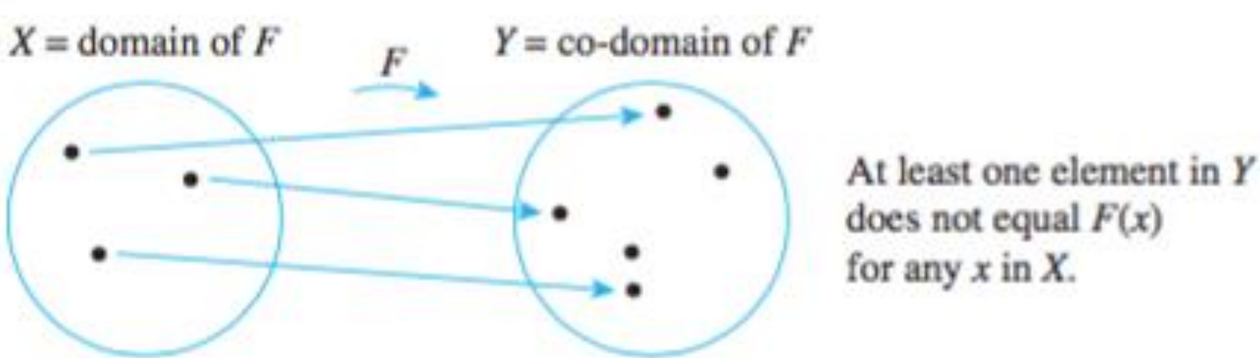


Figure 7.2.3(b) A Function That Is Not Onto

Onto Functions

a. Do either of the arrow diagrams in Figure 7.2.4 define onto functions?

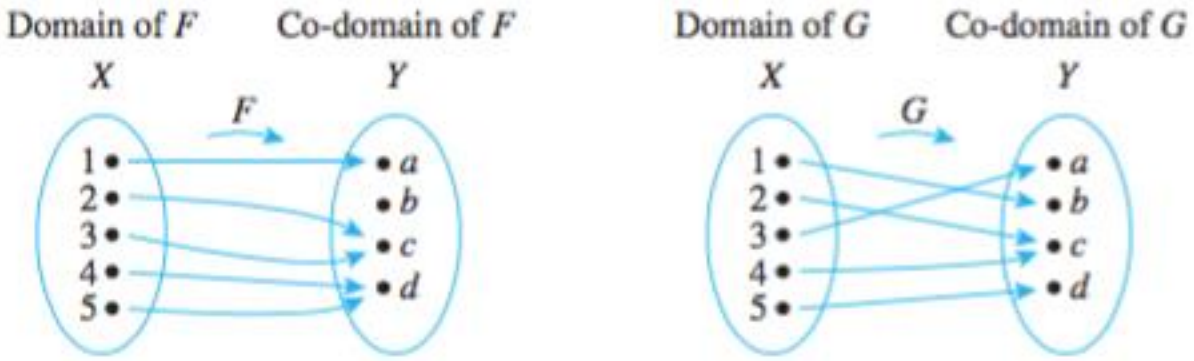


Figure 7.2.4

b. Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c\}$. Define $H: X \to Y$ as follows: $H(1) = c$, $H(2) = a$, $H(3) = c$, $H(4) = b$. Define $K: X \to Y$ as follows: $K(1) = c$, $K(2) = b$, $K(3) = b$, and $K(4) = c$. Is either H or K onto?

Onto Functions

a. Do either of the arrow diagrams in Figure 7.2.4 define onto functions?

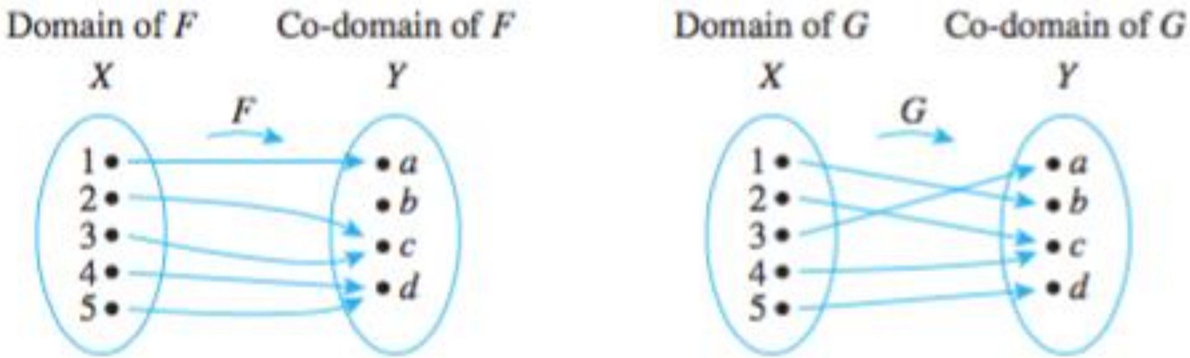


Figure 7.2.4

b. Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c\}$. Define $H: X \to Y$ as follows: $H(1) = c$, $H(2) = a$, $H(3) = c$, $H(4) = b$. Define $K: X \to Y$ as follows: $K(1) = c$, $K(2) = b$, $K(3) = b$, and $K(4) = c$. Is either H or K onto?

***(a) F* is not onto** because $b \neq F(x)$ for any x in X.

***G* is onto** because each element of Y equals $G(x)$ for some x in X:

$a = G(3)$, $b = G(1)$, $c = G(2) = G(4)$, and $d = G(5)$.

(b) ***H* is onto but *K* is not.**

H is onto because each of the three elements of the co-domain of H is the image of some element of the domain of H: $a = H(2), b = H(4)$, and $c=H(1)=H(3)$.

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

Proving/Disproving Functions are Onto

To prove F is onto, (**method of generalizing from the generic particular**)

suppose that y is any element of Y

show that there is an element x of X with $F(x) = y$.

To prove F is *not* onto, you will usually

find an element y of Y | $y \neq F(x)$ for *any* x in X.

Proving/Disproving Functions are Onto

Example 1

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

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

Is f onto? Prove or give a counterexample.

Proving/Disproving Functions are Onto

Example 1

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

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

Is f onto? Prove or give a counterexample.

Let $y \in \mathbf{R}$. *[We must show that* $\exists x$ *in* $\mathbf{R}$ *such that* $f(x) = y$*.]* Let $x = (y + 1)/4$. Then x is a real number since sums and quotients (other than by 0) of real numbers are real numbers. It follows that

$$
\begin{aligned}
f(x) &= f\left(\frac{y+1}{4}\right) && \text{by substitution} \\
&= 4 \cdot \left(\frac{y+1}{4}\right) - 1 && \text{by definition of } f \\
&= (y + 1) - 1 = y && \text{by basic algebra.}
\end{aligned}
$$

[This is what was to be shown.]

Proving/Disproving Functions are Onto

Example 2

Define $h : \mathbf{Z} \rightarrow \mathbf{Z}$ by the rules

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

Is h onto? Prove or give a counterexample.

Proving/Disproving Functions are Onto
Example 2

Define $h: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rules

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

Is h onto? Prove or give a counterexample.

Counterexample:

The co-domain of h is $\mathbf{Z}$ and $0 \in \mathbf{Z}$. But $h(n) \neq 0$ for any integer n. For if $h(n) = 0$, then

$$4n - 1 = 0 \qquad \text{by definition of } h$$

which implies that

$$4n = 1 \qquad \text{by adding 1 to both sides}$$

and so

$$n = \frac{1}{4} \qquad \text{by dividing both sides by 4.}$$

But $1/4$ is not an integer. Hence there is no integer n for which $f(n) = 0$, and thus f is not onto.

Proving/Disproving Functions are Onto

Example 3

Define g : **MobileNumber** → **People** by the rule

$g(x) = Person$ for all $x \in$ **MobileNumber**

Is g onto? Prove or give a counterexample.

Counter example:

Sami does not have a mobile number

Proving/Disproving Functions are Onto

Example 4

Define g : **Fingerprints** $\rightarrow$ **People** by the rule

$g(x) = Person$ for all $x \in$ **Fingerprint**

Is g onto? Prove or give a counterexample.

Prove:

In biology and forensic science: there is no person without fingerprint

Functions

7.2 Properties of Functions

In this lecture:

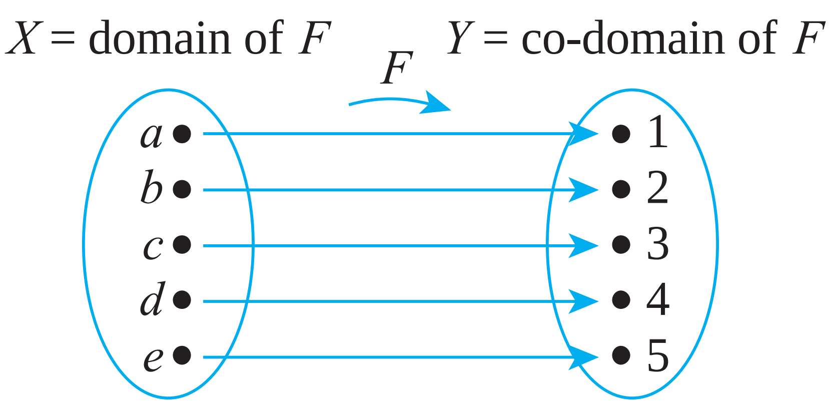
- Part 1: One-to-one Functions
- Part 2: Onto Functions
- Part 3: **one-to-one Correspondence Functions**
- Part 4: Inverse Functions
- Part 5: Applications: Hash and Logarithmic Functions

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.

لا يوجد عنصر في المجال المقابل ليس صورة لعنصر في المجال، او صورة لعنصرين في المجال



String-Reversing Function

Let T be the set of all finite strings of x's and y's.

Define

$g: T \rightarrow T$ by the rule: For all strings $s \in T$,

$g(s)$ = the string obtained by writing the characters of ***s*** in reverse order.

E.g., g("Ali") = "ilA"

Is g a one-to-one correspondence from T to itself?

(a)one-to-one:

(b)onto

String-Reversing Function

Let T be the set of all finite strings of x's and y's. Define

$g: T \to T$ by the rule: For all strings $s \in T$,

$g(s)$ = the string obtained by writing the characters of s in reverse order. E.g., g("Ali") = "ilA"

(a) one-to-one:

- suppose that for some strings $s1$ and $s2$ in T, $g(s1) = g(s2)$. *[We must show that $s1 = s2$.]*
- Now to say that $g(s1) = g(s2)$ is the same as saying that the string obtained by writing the characters of ***s*1** in reverse order equals the string obtained by writing the characters of ***s*2** in reverse order.
- But if ***s*1** and ***s*2** are equal when written in reverse order, then they must be equal to original.

  In other words, $s1 = s2$ *[as was to be shown].*

String-Reversing Function

(b) onto: suppose $\boldsymbol{t}$ is a string in T.

- *[We must find a string* $\boldsymbol{s}$ *in* T *such that* $g(s) = t$*.]*
- Let $\boldsymbol{s} = \boldsymbol{g}(\boldsymbol{t})$.
- By definition of g, $s = g(t)$ is the string in T obtained by writing the characters of $\boldsymbol{t}$ in reverse order.
- But when the order of the characters of a string is reversed once and then reversed again, the original string is recovered.
- $g(\boldsymbol{s}) = g(g(\boldsymbol{t}))$

  = the string obtained by writing the characters of $\boldsymbol{t}$ in reverse order and then writing those characters in reverse order again

  = $\boldsymbol{t}$

This is what was to be shown.

A Function of Two Variables

Define a function $F: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ as follows: For all $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$F(x, y) = (x + y, x - y).$$

Is F a one-to-one correspondence from $\mathbf{R} \times \mathbf{R}$ to itself?

A Function of Two Variables

Define a function $F: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ as follows: For all $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$F(x, y) = (x + y, x - y).$$

Is F a one-to-one correspondence from $\mathbf{R} \times \mathbf{R}$ to itself?

Functions

7.2 Properties of Functions

In this lecture:

- ❑ Part 1: One-to-one Functions
- ❑ Part 2: Onto Functions
- ❑ Part 3: one-to-one Correspondence Functions
- ❑ Part 4: **Inverse Functions**
- ❑ Part 5: Applications: Hash and Logarithmic Functions

Inverse Functions

Theorem 7.2.2

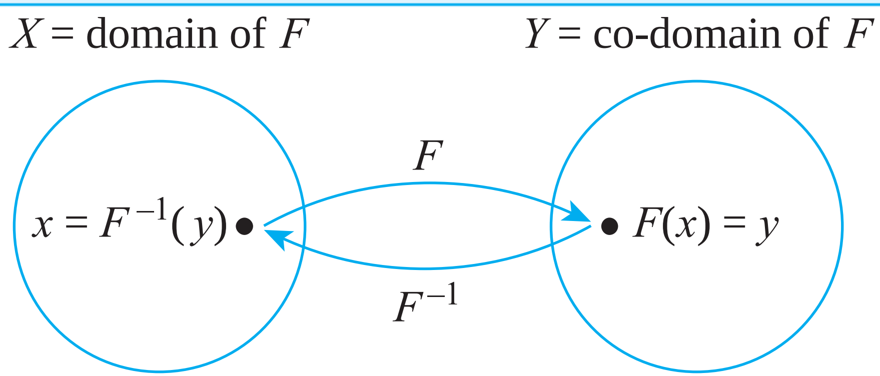
Suppose $F: X \to Y$ is a one-to-one correspondence; that is, suppose F is one-to-one and onto. Then there is a function $F^{-1}: Y \to X$ that is defined as follows:

Given any element y in Y,

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

In other words,

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



➔ Is it always that the inverse of a function is a function?

Finding Inverse Functions

The function f: $\mathbf{R} \rightarrow \mathbf{R}$ defined by the formula

$$f(x) = 4x - 1 \text{ for all real numbers } x$$

(was shown one-to-one and onto)

Find its inverse function?

Finding Inverse Functions

The function f: $\mathbf{R} \to \mathbf{R}$ defined by the formula

$$f(x) = 4x - 1 \text{ for all real numbers } x$$

(was shown one-to-one and onto)

Find its inverse function?

Solution For any *[particular but arbitrarily chosen]* y in $\mathbf{R}$, by definition of f^{-1},

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

But

$$\begin{aligned} & f(x) = y \\ \Leftrightarrow \quad & 4x - 1 = y && \text{by definition of } f \\ \Leftrightarrow \quad & x = \frac{y+1}{4} && \text{by algebra.} \end{aligned}$$

Hence $f^{-1}(y) = \dfrac{y+1}{4}$.

Functions

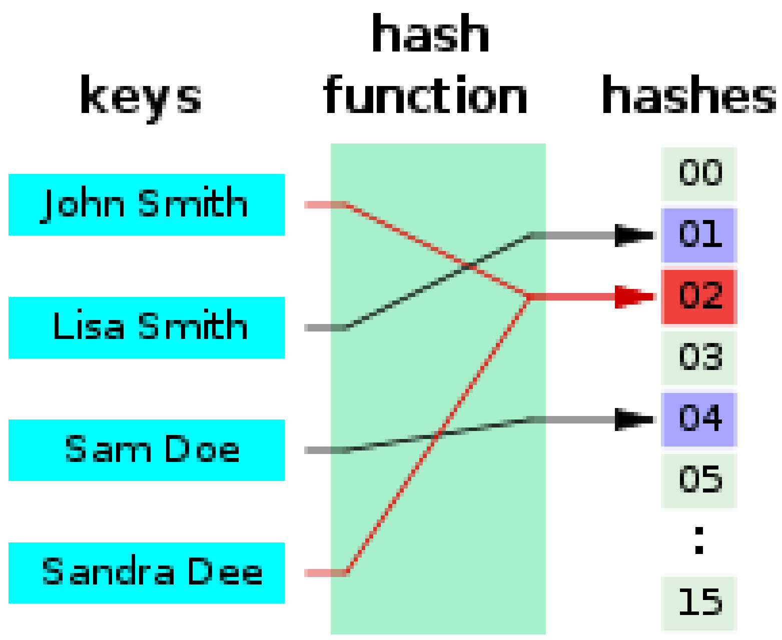
7.2 Properties of Functions

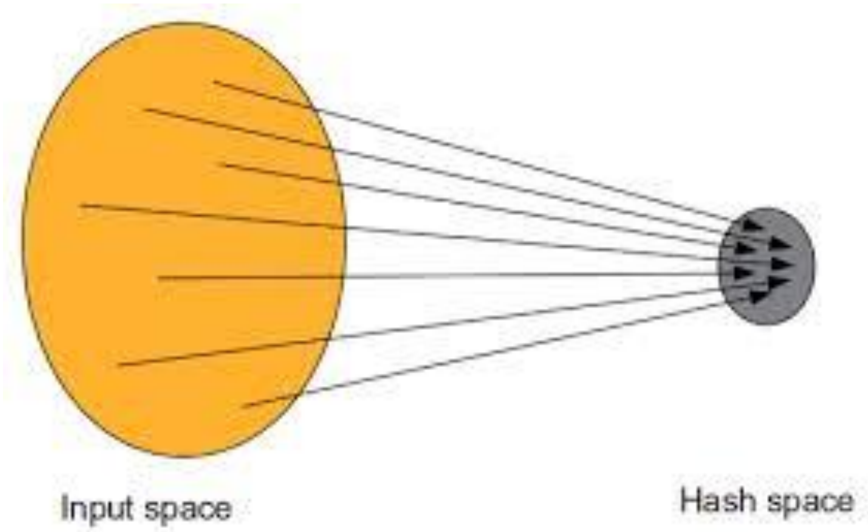
In this lecture:

- ❑ Part 1: One-to-one Functions
- ❑ Part 2: Onto Functions
- ❑ Part 3: one-to-one Correspondence Functions
- ❑ Part 4: Inverse Functions
- ❑ Part 5: **Applications: Hash and Logarithmic Functions**

Hash Functions

- Maps data of arbitrary length to data of a fixed length.
- Very much used in databases and security





Hash Functions

How to store long (ID numbers) for a small set of people

For example: ***n*** is an ID number, and ***m*** is number of people we have

$$\text{Hash}(n) = n \bmod m$$

$Hash(n) = n \ mod \ 7$ for all numbers *n.*

0	356-63-3102
1	
2	513-40-8716
3	223-79-9061
4	
5	328-34-3419
6	

collision?

Exponential and Logarithmic Functions

$$\text{Log}_b\, x = y \iff b^y = x$$

Relations between Exponential and Logarithmic Functions

Laws of Exponents

If b and c are any positive real numbers and u and v are any real numbers, the following laws of exponents hold true:

$$b^u b^v = b^{u+v} \quad 7.2.1$$

$$(b^u)^v = b^{uv} \quad 7.2.2$$

$$\frac{b^u}{b^v} = b^{u-v} \quad 7.2.3$$

$$(bc)^u = b^u c^u \quad 7.2.4$$

The exponential and logarithmic functions are one-to-one and onto. Thus the following properties hold:

For any positive real number b with $b \neq 1$,

if $b^u = b^v$ then $u = v$ for all real numbers u and v, 7.2.5

and

if $\log_b u = \log_b v$ then $u = v$ for all positive real numbers u and v. 7.2.6

Relations between Exponential and Logarithmic Functions

We can derive additional facts about exponents and logarithms, e.g.:

Theorem 7.2.1 Properties of Logarithms

For any positive real numbers b, c and x with $b \neq 1$ and $c \neq 1$:

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

b. $\log_b\left(\frac{x}{y}\right) = \log_b x - \log_b y$

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

d. $\log_c x = \frac{\log_b x}{\log_b c}$

How to prove this?

Using the One-to-Oneness of the Exponential Function

Prove that:

$$\log_c x = \frac{\log_b x}{\log_b c}.$$

Solution Suppose positive real numbers b, c, and x are given. Let

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

Then, by definition of logarithm,

$$(1')\ \ c = b^u \qquad (2')\ \ x = c^v \qquad (3')\ \ x = b^w.$$

Substituting (1′) into (2′) and using one of the laws of exponents gives

$$x = c^v = (b^u)^v = b^{uv}$$ by 7.2.2

But by (3), $x = b^w$ also. Hence

$$b^{uv} = b^w,$$

and so by the one-to-oneness of the exponential function (property 7.2.5),

$$uv = w.$$

Substituting from (1), (2), and (3) gives that

$$(\log_b c)(\log_c x) = \log_b x.$$

And dividing both sides by $\log_b c$ (which is nonzero because $c \neq 1$) results in

$$\log_c x = \frac{\log_b x}{\log_b c}.$$