# Discrete Structures (Monsoon 2021)


**Ashok Kumar Das**

**Associate Professor**
**IEEE Senior Member**
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad (IIIT Hyderabad)

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/view/iitkgpakdas/`

# Topic: **Functions**

# Function

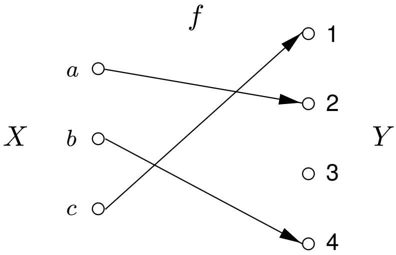
## Definition

A function or mapping or map or transformation is defined by two sets $X$ and $Y$, and a rule (relation) $f$ which assigns to each element of $X$ to exactly one element of $Y$.
In other words, a (binary) relation $f$ from $X$ to $Y$ is called a function from $X$ to $Y$, if each element of $X$ is related to exactly one element of $Y$.

- The set $X$ is called the *domain* and $Y$ the *co-domain (range)* of the function $f$.
- The image $y \in Y$ ($y$ in $Y$) of an element $x \in X$ is denoted by $y = f(x)$.
- For a function $f$ from set $X$ to set $Y$ is $f : X \to Y$, if $y \in Y$, then a pre-image of $y$ is an element $x \in X$ for which $f(x) = y$.
- The set of all elements in $Y$ which have at least one pre-image is called the *image* of $f$, denoted by $Im(f)$.

# Function

- Consider the sets $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$, and the relation (rule) $f$ from $X$ to $Y$ defined as $f(a) = 2, f(b) = 4, f(c) = 1$.




- The pre-image of 2 is $a$.
- Note that 3 does not have any pre-image.
- The image of $f$ is $Im(f) = \{1, 2, 4\}$.
- $f(X) =$ Image of $f$ = $Im(f) = \{f(x) | x \in X\} \subseteq Y$

**NOTE:** All functions are RELATIONS; however, a relation may or may not be a FUNCTION

# Functions

## Definition (Partial Function)

A **partial function** $f : X \to Y$ is a rule which assigns to every element $x \in D$ ($D$ is a proper subset of $X$, that is, $D \subset X$) a unique value in $Y$.

# Types of Functions

## Definition (One-to-One Function)

A function $f : X \rightarrow Y$ is **1-1 (one-to-one) or injective** if each element in the co-domain $Y$ is the image of at most one element in the domain $X$.

In other words, $f : X \rightarrow Y$ is 1-1 if distinct elements in the domain $X$ have distinct images in the co-domain $Y$, i.e., if $a, b \in X$ such that $a \neq b$, then $f(a) \neq f(b)$ or, equivalently, if $f(a) = f(b)$, then $a = b$.

If a function $f : X \rightarrow Y$ is NOT 1-1, it is called **many-one** function.

## Definition (Onto Function)

A function $f : X \rightarrow Y$ is **onto or surjective**, if each element in the co-domain $Y$ is the image of at least one element in the domain $X$.

In other words, $f : X \rightarrow Y$ is called onto if $Im(f) = Y$.

## Definition (Bijective Function)

A function $f : X \rightarrow Y$ is **bijective**, if it is both 1-1 and onto.

# Types of Functions

**Theorem**

*If a function $f : X \to Y$ is 1-1, then $f : X \to Im(f)$ is a bijection.*

**Theorem**

*If a function $f : X \to Y$ is 1-1, and $X$ and $Y$ are finite sets of the same size, then $f : X \to Y$ is a bijection.*

# Types of Functions

- Let $f : X \to Y$ is a function with $|X| = m$ and $|Y| = n$. Then
  - The total number of functions from $X$ to $Y$ is $n^m$
  - The total number of injective (1-1) functions from $X$ to $Y$ with $m < n$ is ${}^nC_m.m!$
  - The total number of surjective (onto) functions from $X$ to $Y$ with $m > n$ is

    $$n!S(m, n)$$

    where the Stirling number is given by

    $$S(m, m) = S(m, 1) = 1$$

    $$S(m, n) = n.S(m - 1, n) + S(m - 1, n - 1)$$
  - The total number of bijective functions from $X$ to $Y$ with $m = n$ is $n!$

# Types of Functions

## Problem:

Let $A = \{1, 2, 3\}$ and $B = \{8, 9\}$. How many mappings are there of $A$ into $B$? How many of these are one-one mappings? How many are onto?
**Solution:** Here $m = |A| = 3$ and $n = |B| = 2$.
There will be the following $n^m = 2^3 = 8$ mappings:

1. $\{(1, 8), (2, 9), (3, 9)\}$
2. $\{(1, 8), (2, 8), (3, 9)\}$
3. $\{(1, 9), (2, 8), (3, 9)\}$
4. $\{(1, 9), (2, 8), (3, 8)\}$
5. $\{(1, 8), (2, 9), (3, 8)\}$
6. $\{(1, 9), (2, 9), (3, 8)\}$
7. $\{(1, 8), (2, 8), (3, 8)\}$
8. $\{(1, 9), (2, 9), (3, 9)\}$

- Of these 8 mappings, NONE is one-one mapping.
- All but the last two (7 and 8) are onto mappings (SIX functions are onto).
- **Verification:**
  No. of onto functions $= n!S(m, n) = 2!S(3, 2) = 2 * 3 = 6$
  as $S(3, 2) = 2 * S(2, 2) + S(2, 1) = 2 * 1 + 1 = 3$

# Inverse Function

## Definition (Inverse Function)

A function $f : X \to Y$ is a bijection, then it is a simple matter to define a bijection $g : Y \to X$ as follows:
for each $y \in Y$ define $g(y) = x$ where $x \in X$ and $f(x) = y$.
This function $g$ obtained from $f$ is called the **inverse function** of $f$ and is denoted by $g = f^{-1}$.

Consider the sets $X = \{a, b, c, d, e\}$ and $Y = \{1, 2, 3, 4, 5\}$.

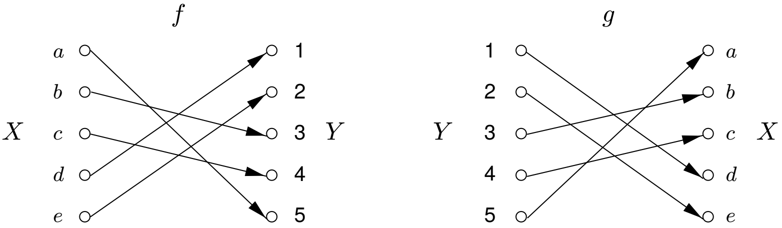



Figure: A bijection $f$ and its inverse $g = f^{-1}$

# One-Way Function

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

## Definition (One-Way Function)

A function $f : X \rightarrow Y$ is called a **one-way function** if $f(x)$ is *easy* to compute for all $x \in X$, but for *essentially all* elements $y \in Im(f)$ it is *computationally infeasible* to find any $x \in X$ such that $f(x) = y$.
In other words, a one-way function which is easily computed, but the calculation of its inverse is infeasible.

**NOTE:** The phrase "for essentially all elements in $Y$" refers to the fact that there are a few values $y \in Y$ for which it is easy to find an $x \in X$ such that $y = f(x)$.

# Trap-Door One-Way Function

**Definition (Trap-door One-way Function)**

A **trap-door one-way function** is a one-way function $f : X \to Y$ with the additional property that given some extra information (called the trap-door information) it becomes feasible to find for any given $y \in Im(f)$, an $x \in X$ such that $f(x) = y$.

In other words, a trap-door one-way function is a function that is easily computed; the calculation of its inverse is infeasible unless certain privileged information is known.