Discrete Structures (Monsoon 2022)

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/

Recap: Functions

Function

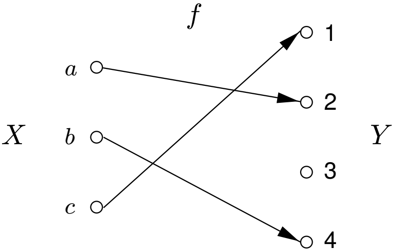
Definition

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

Definition (Onto Function)

A function $f : X \to Y$ 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, $f : X \to Y$ is called onto if $Im(f) = Y$.

Definition (Bijective Function)

A function $f : X \to Y$ 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, that is, $|X| = |Y|$, 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 $n!$

Permutations

Permutations

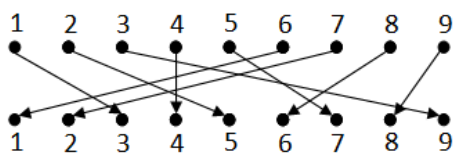
Definition (Permutation)

Let S be a finite set of elements. A permutation p on S is a bijection from S to itself (i.e., $p : S \to S$).

Example: Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. A permutation $p : S \to S$ is defined as follows:

$$p(1) = 3, p(2) = 5, p(3) = 9, p(4) = 4, p(5) = 7, p(6) = 1,$$

$$p(7) = 2, p(8) = 6, p(9) = 8$$



Permutations

- A permutation $p : S \to S$ on a finite set $S = \{a_1, a_2, \ldots, a_n\}$ is displayed as an array:

$$p = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}$$

where $p(a_i)$ is the p-image of a_i.

Definition (Identity Permutation)

The permutation which maps each element of S onto itself is said to be the *identity permutation* and is denoted by I. Thus, if $S = \{a_1, a_2, \ldots, a_n\}$, then

$$I = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Multiplication of Permutations

- Let $f : S \to S$ and $g : S \to S$ be two permutations on S. Since $range.f = dom.g$, where $range.f$ and $dom.g$ denote the range of f and domain of g respectively, the composition is defined.
- Since f and g are both bijective, $g \circ f : S \to S$ is also bijective. Therefore, $g \circ f$ is a permutation on S. Similarly, $f \circ g$ is also a permutation on S.
- The products gf and fg are defined by the composite $g \circ f$ and $f \circ g$, respectively.

Multiplication of Permutations

- If

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$$

and

$$g = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(a_1) & g(a_2) & \cdots & g(a_n) \end{pmatrix}$$

then

$$fg = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f[g(a_1)] & f[g(a_2)] & \cdots & f[g(a_n)] \end{pmatrix}$$

and

$$gf = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g[f(a_1)] & g[f(a_2)] & \cdots & g[f(a_n)] \end{pmatrix}$$

Inverse of a permutation

- The inverse of $p : S \to S$, where $S = \{a_1, a_2, \ldots, a_n\}$ is

$$p^{-1} = \begin{pmatrix} p(a_1) & p(a_2) & \cdots & p(a_n) \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

where

$$p = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}$$

- If

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

then

$$p^{-1} = \begin{pmatrix} 3 & 5 & 4 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

Permutations

Definition (Cycle)

Let $S = \{a_1, a_2, \ldots, a_n\}$. A permutation $f : S \to S$ is said to be a cycle of length r or an r-cycle, if there are r elements $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ in S such that
$f(a_{i_1}) = a_{i_2}, f(a_{i_2}) = a_{i_3}, \cdots, f(a_{i_{r-1}}) = a_{i_r}, f(a_{i_r}) = a_{i_1}$, and $f(a_j) = a_{i_1}$, $j \neq i_1, i_2, \cdots, i_r$.
The cycle is denoted by $(a_{i_1}\ a_{i_2}\ \cdots a_{i_r})$ or by $(a_{i_2}\ a_{i_3}\ \cdots a_{i_r}\ a_{i_1})$ or any other form provided the elements appear in a fixed cyclic order.

Permutations

Index Laws

- $f^m.f^n = f^{m+n}$
- $(f^m)^n = f^{mn}$

hold for integral values of m and n.

- By the law $f^m.g^m = (fg)^m$ does not hold, since $fg \neq gf$, in general.
- The identity permutation

$$I = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

on a set $S = \{a_1, a_2, \ldots, a_n\}$, is the product of n cycles (a_1), (a_2), $\ldots$, (a_n), each of length 1.

Permutations

Definition (Transposition)

A 2-cycle is called a transposition.

Definition (Even Permutation)

If a permutation contains even number of transpositions, it is called an even permutation.

Definition (Odd Permutation)

If a permutation contains odd number of transpositions, it is called an odd permutation.

Permutations

Problem. Examine whether the permutation

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{pmatrix}$$

is odd or even.

Solution. Given p can be written as

$$p = \begin{pmatrix} 1 & 2 & 4 & 6 & 3 & 5 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$$

$= (\ 1\ 2\ 4\ 6\ )\ (\ 3\ 5\ )$
$= (1\ 6)\ (1\ 4)\ (1\ 2)\ (3\ 5)$
Since p has four transpositions, that is, even number of transpositions, therefore it is EVEN.

Permutations

Problem. Prove that $(1\ 2\ 3 \cdots\ n) \circ (1\ i) = (1\ i+1\ i+2 \cdots\ n) \circ (2\ 3 \cdots\ i-1\ i)$.

Solution.

LHS $= (1\ 2\ 3 \cdots\ n) \circ (1\ i)$

$$= \begin{pmatrix} 1 & 2 & 3 & \cdots & i-1 & i & i+1 & \cdots & n \\ 2 & 3 & 4 & \cdots & i & i+1 & i+2 & \cdots & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & i-1 & i & i+1 & \cdots & n \\ i & 2 & 3 & \cdots & i-1 & 1 & i+1 & \cdots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \cdots & i-1 & i & i+1 & \cdots & n \\ i+1 & 3 & 4 & \cdots & i & 2 & i+2 & \cdots & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & i+1 & \cdots & n & 2 & 3 & 4 & \cdots & i-1 & i \\ i+1 & i+2 & \cdots & 1 & 3 & 4 & 5 & \cdots & i & 2 \end{pmatrix}$$

$= (1\ i+1\ i+2 \cdots\ n) \circ (2\ 3\ 4 \cdots\ i-1\ i)$

$=$ RHS.

Permutations

Problem. Let f, g be given permutations on a finite set S on which there is a unique permutation p on S such that $fp = g$ and there is a unique permutation q on S such that $qf = g$. Determine p, q, when $S = \{1, 2, 3\}$, $f = (1\ 2\ 3)$, $g = (1\ 3\ 2)$.

Solution.

- Given $fp = g$. Then, $f^{-1}(fp) = f^{-1}g \Rightarrow (f^{-1}f)p = f^{-1}g$
$\Rightarrow I.p = f^{-1}.g$, since $f^{-1}.f = I$, the identity permutation.
Thus, $p = f^{-1}.g = (1\ 2\ 3)$.
- Given $qf = g$. Then, $(qf).f^{-1} = g.f^{-1} \Rightarrow q.(f.f^{-1}) = g.f^{-1}$
$\Rightarrow q.I = g.f^{-1}$, since $f.f^{-1} = I$, the identity permutation.
Thus, $q = g.f^{-1} = (1\ 2\ 3)$.

Permutations

Theorem

Let $S = \{a_1, a_2, \cdots, a_n\}$ be a finite set with n elements, $n \geq 2$. Then, there are $\frac{n!}{2}$ even permutations and $\frac{n!}{2}$ odd permutations.

Proof. Let A_n be the set of all even permutations on S and B_n the set of all odd permutations on S.
Task: We shall define a function $f : A_n \to B_n$, which we show is one-one and onto (bijective), and this will show that A_n ad B_n have the same number of elements, that is, $|A_n| = |B_n|$.
Since $n \geq 2$, we can choose a particular transposition (2-cycle) q_0 of S, say that $q_0 = (a_{n-1}\ a_n)$. We now define the function $f : A_n \to B_n$ by

$$f(p) = q_0 \cdot p, \forall p \in A_n.$$

Note that if $p \in A_n$, then p is an even permutation, and since q_0 is a transposition, so $q_0 \cdot p$ is an odd permutation (because $q_0 \circ p$ has odd number of transpositions now), and thus $f(p) \in B_n$.

Permutations

- **Claim 1. *f* in one-one**
  Suppose now that $p_1 \in A_n$ and $p_2 \in A_n$ such that $f(p_1) = f(p_2)$.
  Then,
  $$q_0 \cdot p_1 = q_0 \cdot p_2 \qquad (1)$$
  Thus, $q_0 \cdot (q_0 \cdot p_1) = q_0 \cdot (q_0 \cdot p_2)$
  $$q_0 \cdot q_0 = (a_{n-1}\ a_n) \cdot (a_{n-1}\ a_n) \qquad (2)$$
  by the associative property.
  We have, $q_0 \cdot q_0 = (a_{n-1}\ a_n) \cdot (a_{n-1}\ a_n)$
  $= \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_1 & a_2 & \cdots & a_n & a_{n-1} \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_1 & a_2 & \cdots & a_n & a_{n-1} \end{pmatrix}$
  $= \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \end{pmatrix}$
  $= I$, the identity permutation on S.

Permutations

- **Claim 1. f in one-one (Cont...)**
  From Eq. (2), we have:

  $$I \cdot p_1 = I \cdot p_2$$

  This implies that

  $$p_1 = p_2$$

  Thus, whenever $f(p_1) = f(p_2)$, then $p_1 = p_2$.
  Hence, f is one-one.

Permutations

- **Claim 2. f in onto**
  Now, let $q \in B_n$. Then, $q_0 \cdot q \in A_n$, since q is an odd permutation. Thus,

$$\begin{aligned} f(q_0 \cdot q) &= q_0 \cdot (q_0 \cdot q) \\ &= (q_0 \cdot q_0) \cdot q \\ &= I \cdot q \\ &= q. \end{aligned}$$

  This shows that f is also onto.

Since f is both one-one and onto, f is bijective and we conclude that A_n and B_n have the same number of elements, that is, $|A_n| = |B_n|$.

Permutations

Note that $A_n \cap B_n = \emptyset$ since no permutation can be both even and odd. Also, we have,

$$|A_n \cup B_n| = n!$$

Thus,

$$\begin{aligned} n! &= |A_n \cup B_n| \\ &= |A_n| + |B_n| - |A_n \cap B_n| \\ &= |A_n| + |B_n| \\ &= 2|A_n| \end{aligned}$$

Then,

$$|A_n| = \frac{n!}{2}$$

and

$$|B_n| = \frac{n!}{2}$$