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/`

Involutions

Definition

Let S be a finite set and let f be a bijection from S to itself (i.e., $f : S \rightarrow S$). The function f is called an **involution** if $f = f^{-1}$. An equivalently, $f(f(x)) = x$, for all $x \in S$.

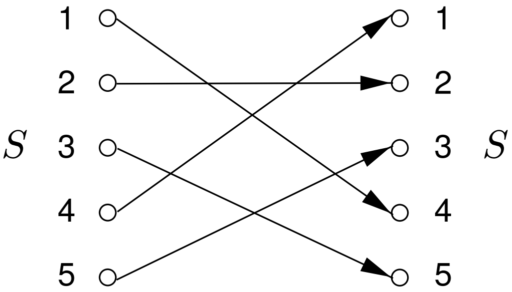


Figure: An involution on a set of five elements, $S = \{1, 2, 3, 4, 5\}$

Functions

Composition of Functions

Definition

Let $f : A \to B$ and $g : B \to C$ be two functions. The composition of f by g is the function $g \circ f : A \to C$ defined by

$$(g \circ f)(a) = g[f(a)], \forall a \in A.$$

Lemma

Let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be functions. Whenever the composites involved are defined, composition of functions obeys the associate law:

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Functions

Problem [Composition of Functions]

Let $f : x \to 2x$, $g : x \to x^2$ and $h : x \to (x+1)$ defined over a set of real numbers. Then, find $h \circ (g \circ f)$ and $(h \circ g) \circ f$, and prove that each of them is $(4x^2 + 1)$.

Proof. Here $f(x) = 2x$, $g(x) = x^2$ and $h(x) = x + 1$.

Now,

$$\begin{aligned}
[h \circ (g \circ f)](x) &= h \circ (g \circ f)(x) \\
&= h \circ [g(f(x)] \\
&= (h \circ g)(2x) \\
&= h[g(2x)] \\
&= h[(2x)^2] \\
&= h(4x^2) \\
&= 4x^2 + 1.
\end{aligned}$$

Functions

Problem [Composition of Functions]

Let $f : x \to 2x$, $g : x \to x^2$ and $h : x \to (x+1)$ defined over a set of real numbers. Then, find $h \circ (g \circ f)$ and $(h \circ g) \circ f$, and prove that each of them is $(4x^2 + 1)$.

Proof. Again,

$$
\begin{aligned}
((h \circ g) \circ f)(x) &= (h \circ g)f(x) \\
&= (h \circ g)(2x) \\
&= h[g(2x)] \\
&= h[(2x)^2] \\
&= h(4x^2) \\
&= 4x^2 + 1.
\end{aligned}
$$

Hence, $h \circ (g \circ f)(x) = ((h \circ g) \circ f)(x)$, for all x in the set of real numbers. Thus, $(h \circ g) \circ f = h \circ (g \circ f)$.

Identity Function

Definition

The identity function $I_S : S \to S$ maps each element of S onto itself. That is, $I_S(x) = x, \forall x \in S$.

Theorem (Identity Law)

Let $f : S \to T$, and 1_S and 1_T be the identity functions of S and T respectively. Then,

$$f \circ 1_S = 1_T \circ f = f.$$

Proof.

Given $1_S : S \to S$, $1_T : T \to T$ are identity functions. So, $1_S(s) = s, \forall s \in S$ and $1_T(t) = t, \forall t \in T$.

Therefore, $f \circ 1_S : S \to T$ and $1_T \circ f : S \to T$. Let $s \in S$. Then,

$$\begin{aligned} (f \circ 1_S)(s) &= f[1_S(s)] \\ &= f(s), \forall s \in S \end{aligned}$$

Identity Function

Thus,

$$f \circ 1_S = f \tag{1}$$

Again,

$$\begin{aligned} (1_T \circ f)(s) &= 1_T[f(s)] \\ &= f(s), \forall s \in S \end{aligned}$$

Therefore,

$$1_T \circ f = f \tag{2}$$

Combining both Eqs. (1) and (2), we have:

$$f \circ 1_S = 1_T \circ f = f.$$

Characteristic Function

Definition (Characteristic Function)

Any set S which is a subset of a set U ($S \subseteq U$) can be associated with a function, called its characteristic function:
$e_S : U \to \{0, 1\}$ defined by

$$e_S(x) = \begin{cases} 1, \text{ if } x \in S \\ 0, \text{ if } x \notin S \end{cases}$$

In other words, if $S \subseteq U = \{u_1, u_2, \ldots, u_n\}$, then $e_S : U \to \{0, 1\}$ is defined by

$$e_S(u_i) = \begin{cases} 1, \text{ if } u_i \in S \\ 0, \text{ if } u_i \notin S \end{cases}$$

Example: If $S = \{4, 7, 9\}$ and $U = \{1, 2, 3, \ldots, 10\}$, then $e_S(2) = 0$, $e_S(4) = 1$, $e_S(7) = 1$, and $e_S(12)$ is undefined since $12 \notin U$.

Inverses of Function

Definition

Let $f : S \to T$ and $g : T \to S$ ($g = f^{-1}$) be two mappings such that $g \circ f = 1_S$ and $f \circ g = 1_T$. Then, g is called the ***left inverse*** of f with respect to left composition and g is called the ***right inverse*** of f with respect to right composition.

Definition

A function which has a two-sided inverse if called **invertible**.

Theorem

(a) A function is ***left-invertible*** *iff it is one-one (injective).*
(b) A function is ***right-invertible*** *iff it is onto (surjective).*

Inverses of Function

Corollary

*A function $f : A \to B$ is a **bijective** iff it has both a left-inverse and right inverse.*

Corollary

If $g \circ f$ is defined, and both f and g have left inverses, then $g \circ f$ has a left inverse.

Functions

Definition

For all $f : S \to S$,

$$f^2 = f \circ f.$$

If $f^2 = f$, then f is said to be an **idempotent** or a **projection.**

Problem: Let $f : S \to S$ be a function defined as follows:

$$f(x) = x, \forall x \in S.$$

Then,

$$\begin{aligned} f^2(x) &= (f \circ f)(x) \\ &= f[f(x)] \\ &= f(x) \end{aligned}$$

Therefore, $f^2(x) = f(x), \forall x \in S$. Hence, $f^2 = f$. As a result, f is an "idempotent" or a "projection" mapping.

Functions

Theorem

(a) If f and g are both injective, then $g \circ f$ is injective too.
(b) If f and g are both surjective, then $g \circ f$ is surjective too.
(c) If f and g are both bijective, then $g \circ f$ is bijective too. In addition,

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

(d) If $g \circ f$ is injective, f is injective too.
(e) If $g \circ f$ is surjective, g is surjective too.

Proof.

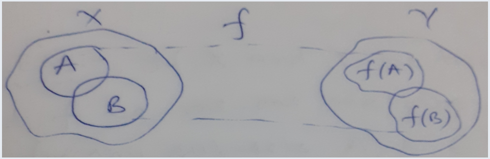
(a) Let $a_1, a_2 \in A$ and $a_1 \neq a_2$. RTP: $(g \circ f)(a_1)] \neq (g \circ f)(a_2)$.
Then, $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$, since f is injective (one-one).
$\Rightarrow g[f(a_1)] \neq g[f(a_2)]$, since g is injective (one-one)
$[f(a_1) \in B, f(a_2) \in B$ and $f(a_1) \neq f(a_2)]$
$\Rightarrow (g \circ f)(a_1)] \neq (g \circ f)(a_2)$.
Hence, $g \circ f$ is injective. □

Functions

Theorem

If X and Y be two non-empty sets and f be a mapping of X into Y. Then, for any sub-sets $A, B \in X$, $f(A \cup B) = f(A) \cup f(B)$. Also, $A \subseteq B \Rightarrow f(A) \subseteq f(B)$.

Proof.



RTP: (i) $f(A \cup B) \subseteq f(A) \cup f(B)$ and (ii) $f(A) \cup f(B) = f(A \cup B)$.
(i) Let $y \in f(A \cup B)$ be an arbitrary element.
Then, $y \in f(A \cup B)$
$\Rightarrow y = f(x)$, for some $x \in A \cup B$
$\Rightarrow y = f(x)$, for some $x \in A$ or $x \in B$
$\Rightarrow y = f(x)$, for some $f(x) \in f(A)$ or $f(x) \in f(B)$
$\Rightarrow y \in f(A)$ or $y \in f(B) \Rightarrow y \in (f(A) \cup f(B))$
Thus,

Functions

(ii) To prove other direction, let $y \in f(A) \cup f(B)$ be an arbitrary element.
Then, $y \in f(A) \cup f(B)$
$\Rightarrow y \in f(A)$ or $y \in f(B)$
$\Rightarrow y = f(x)$, for some $x \in A$ or $x \in B$
$\Rightarrow y = f(x)$, for some $x \in A \cup B$
$\Rightarrow y = f(x)$, for $f(x) \in f(A \cup B)$
$\Rightarrow y \in f(A \cup B)$.
Thus,

$$f(A) \cup f(B) \subseteq f(A \cup B) \tag{4}$$

By combining Eqs. (3) and (4), we have:

$$f(A \cup B) = f(A) \cup f(B).$$

Functions

Theorem

If X and Y be two non-empty sets and f be one-one mapping of X onto Y (f is bijective). Then, for any sub-sets $A, B \in Y$, $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

Theorem

If $f : X \rightarrow Y$ be a mapping and A, B be subsets of X. Then, $f(A \cap B) \subseteq f(A) \cap f(B)$. The equality holds, if f is one-one (injective).

Theorem

If X and Y be two non-empty sets and f be one-one mapping of X onto Y (f is bijective). Then, for any sub-sets $A, B \in Y$, $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

Functions

Problem: If N be the set of natural numbers, E be the set of even natural numbers, and a mapping $f : N \to E$ be defined by

$$f(x) = 2x, \forall x \in N$$

then show that f is one-one (injective) onto (surjective) map, that is, f is bijective.

Proof.

- **Claim 1:** f is one-one.
  Let $x_1, x_2 \in N$ such that $x_1 \neq x_2$. Then, $2x_1 \neq 2x_2 \Rightarrow f(x_1) \neq f(x_2)$.
- **Claim 2:** f is onto.
  If $y \in E$, then y is an even positive number. Thus, $\frac{y}{2}$ is a natural number.
  Now, $y = f(x) = 2x \Rightarrow x = \frac{y}{2} \in N$, for all $y \in E$.

Since f is both one-one and onto, f is also bijective.

Functions

Problem: Show that the mapping $f : R \to R$ defined by $f(x) = \cos x, x \in R$, where R is the set of real numbers, is neither one-one nor onto.

Proof.

- **Claim 1:** f is NOT one-one.

  Let $x_1, x_2 \in R$ be two arbitrary elements in R (domain set). Now, $x_1 \neq x_2 \not\Rightarrow \cos x_1 \neq \cos x_2 \not\Rightarrow f(x_1) \neq f(x_2)$.

  For example, let $x_1 = 0$ and $x_2 = 2\pi$. Then, $f(x_1) = \cos 0 = 1$ and $f(x_2) = \cos 2\pi = 1$. Thus, $x_1 \neq x_2$, but $f(x_1) = f(x_2)$.

  In fact, f is many-one mapping.

- **Claim 2:** f is NOT onto.

  Let $y \in R$ (co-domain set). Then, $y = f(x) = \cos x \Rightarrow x = \cos^{-1}(y)$.

  Since $-1 \leq \cos x \leq +1$, so $f : R \to [-1, +1] \subset R$, and $f(R) \neq R$. Thus, $f : R \to R$ is not onto (surjective). In fact, f in into mapping.

Conclusion: $f : R \to R$ defined by $f(x) = \cos x$ is many-one into mapping.