Functions

Aritra Hazra

Department of Computer Science and Engineering,
Indian Institute of Technology Kharagpur,
Paschim Medinipur, West Bengal, India - 721302.

Email: *aritrah@cse.iitkgp.ac.in*

Autumn 2020

Basics of Functions

Functions: For two sets, $\mathcal{A}, \mathcal{B} \neq \phi$, a function (or mapping) f from $\mathcal{A}$ to $\mathcal{B}$, denoted as $f : \mathcal{A} \rightarrow \mathcal{B}$, is a relation from $\mathcal{A}$ to $\mathcal{B}$ in which every element of $\mathcal{A}$ appears exactly once in the first component of an ordered pair in the relation.

$f(a) = b$ $(a \in \mathcal{A}, b \in \mathcal{B})$ when (a, b) is an ordered pair in the function f associating each a to an unique b. Thus, $(a, b), (a, c) \in f \Rightarrow b = c$.

Example: **(1)** Access function of 2-D array in memory, $f : \mathcal{A} \rightarrow \mathbb{N}$ ($\mathcal{A} = (a_{ij})_{m \times n}$ is an $m \times n$ array) is defined by, $f(a_{ij}) = (i - 1)n + j$.

(2) Floor and ceiling functions, $f : \mathbb{R} \rightarrow \mathbb{Z}$, are defined by,

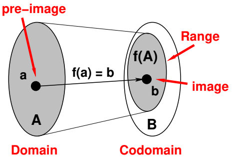
$$f(x) = \lfloor x \rfloor \text{ and } g(y) = \lceil y \rceil \ (x, y \in \mathbb{R}).$$

$$f(2.7) = 2, f(-2.7) = -3, f(2) = 2, f(-2) = -2 \text{ and}$$
$$g(2.7) = 3, g(-2.7) = -2, g(2) = 2, g(-2) = -2.$$

Image and Pre-image: If $f(a) = b$, then b is the image of a under f and a is the pre-image of b.

Domain and Codomain: In $f : \mathcal{A} \rightarrow \mathcal{B}$, $\mathcal{A}$ is the domain of f and $\mathcal{B}$ is the codomain of f.

Range: Set of all images for elements of $\mathcal{A}$ in $\mathcal{B}$, $f(\mathcal{A}) \subseteq \mathcal{B}$.



Properties of Functions

Number of Functions: Let $\mathcal{A} = \{a_1, \ldots, a_m\}$ ($|\mathcal{A}| = m$) and $\mathcal{B} = \{b_1, \ldots, b_n\}$ ($|\mathcal{B}| = n$). $f : \mathcal{A} \to \mathcal{B}$ is described as, $\{(a_1, x_1), (a_2, x_2), \ldots, (a_m, x_m)\}$.
So, Total Count $= n^m = |\mathcal{B}|^{|\mathcal{A}|}$ (by rule-of-product).

Image of Subset: If $f : \mathcal{A} \to \mathcal{B}$ and $\mathcal{A}' \subseteq \mathcal{A}$, then $f(\mathcal{A}') = \{b \in \mathcal{B} \mid b = f(a)\}$ (for some $a \in \mathcal{A}'$), and $f(\mathcal{A}')$ is called the image of $\mathcal{A}'$ under f.

Restriction: If $f : \mathcal{A} \to \mathcal{B}$ and $\mathcal{A}' \subseteq \mathcal{A}$, then $f|_{\mathcal{A}'} : \mathcal{A}' \to \mathcal{B}$ is called the restriction of f to $\mathcal{A}'$ if $f|_{\mathcal{A}'}(a) = f(a)$ for all $a \in \mathcal{A}'$.

Extension: Let $\mathcal{A}' \subseteq \mathcal{A}$ and $f : \mathcal{A}' \to \mathcal{B}$. If $g : \mathcal{A} \to \mathcal{B}$ and $g(a) = f(a)$ for all $a \in \mathcal{A}'$, then g is called an extension of f to $\mathcal{A}$.

Let $f : \mathcal{A} \to \mathcal{B}$, with $\mathcal{A}_1, \mathcal{A}_2 \subseteq \mathcal{A}$. Then, **(i)** If $\mathcal{A}_1 \subset \mathcal{A}_2 \Rightarrow f(\mathcal{A}_1) \subseteq f(\mathcal{A}_2)$, **(ii)** $f(\mathcal{A}_1 \cup \mathcal{A}_2) = f(\mathcal{A}_1) \cup f(\mathcal{A}_2)$, and **(iii)** $f(\mathcal{A}_1 \cap \mathcal{A}_2) \subseteq f(\mathcal{A}_1) \cap f(\mathcal{A}_2)$.

Proof: **(ii)** For each $b \in \mathcal{B}$, $b \in f(\mathcal{A}_1 \cap \mathcal{A}_2) \Rightarrow b = f(a)$, for some $a \in (\mathcal{A}_1 \cap \mathcal{A}_2)$
$\Rightarrow [b = f(a)$ for some $a \in \mathcal{A}_1] \wedge [b = f(a)$ for some $a \in \mathcal{A}_2] \Rightarrow b \in f(\mathcal{A}_1) \wedge b \in f(\mathcal{A}_2)$
$\Rightarrow b \in f(\mathcal{A}_1) \cap f(\mathcal{A}_2)$, implying the result.

(i) and (ii) *Left for You as an Exercise!*

One-to-One or Injective Functions

One-to-one (Injective) Function: $f : \mathcal{A} \to \mathcal{B}$ is a one-to-one (or injective) function, if each element in $\mathcal{B}$ appears at most once as image of an element of $\mathcal{A}$.

- For arbitrary sets $\mathcal{A}, \mathcal{B}$, $f : \mathcal{A} \to \mathcal{B}$ is one-to-one if and only if $\forall a_1, a_2 \in \mathcal{A}, f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.
- If $f : \mathcal{A} \to \mathcal{B}$ is one-to-one with $\mathcal{A}, \mathcal{B}$ finite, then $|\mathcal{A}| \leq |\mathcal{B}|$.

Examples: **(i)** $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = 2x + 1, \ \forall x \in \mathbb{R}$ is one-to-one; because for all $x_1, x_2 \in \mathbb{R}$, we have $f(x_1) = f(x_2) \Rightarrow 2x_1 + 1 = 2x_2 + 1 \Rightarrow x_1 = x_2$.
(ii) $g : \mathbb{R} \to \mathbb{R}$ where $g(x) = x^2 + x, \ \forall x \in \mathbb{R}$ is NOT one-to-one; because $g(-1) = 0$ and $g(0) = 0$.

Number of Injective Functions: Let $\mathcal{A} = \{a_1, \ldots, a_m\}$ $(|\mathcal{A}| = m)$ and $\mathcal{B} = \{b_1, \ldots, b_n\}$ $(|\mathcal{B}| = n)$ $(m \leq n)$. $f : \mathcal{A} \to \mathcal{B}$ is described as, $\{(a_1, x_1), (a_2, x_2), \ldots, (a_m, x_m)\}$.
So, Total Count $= n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!} = P(|\mathcal{B}|, |\mathcal{A}|)$.

$f : \mathcal{A} \to \mathcal{B}$, with $\mathcal{A}_1, \mathcal{A}_2 \subseteq \mathcal{A}$. Then, $f(\mathcal{A}_1 \cap \mathcal{A}_2) = f(\mathcal{A}_1) \cap f(\mathcal{A}_2)$, if f is one-to-one.

Onto or Surjective Functions

Onto (Surjective) Function: $f : \mathcal{A} \to \mathcal{B}$ is a onto (or surjective) function, if $f(\mathcal{A}) = \mathcal{B}$, i.e. for all $b \in \mathcal{B}$ there is at least one $a \in \mathcal{A}$ with $f(a) = b$.

- For arbitrary sets $\mathcal{A}, \mathcal{B}$, $f : \mathcal{A} \to \mathcal{B}$ is onto if and only if $\forall b \in \mathcal{B},\ \exists a \in \mathcal{A},$ so that $f(a) = b$.
- If $f : \mathcal{A} \to \mathcal{B}$ is onto with $\mathcal{A}, \mathcal{B}$ finite, then $|\mathcal{A}| \geq |\mathcal{B}|$.

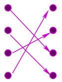
Examples: **(i)** $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^3 + 1,\ \forall x \in \mathbb{R}$ is onto; because for each $y = x^3 + 1 \in \mathbb{R}$, there is an $x = \sqrt[3]{y-1}$.
(ii) $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2,\ \forall x \in \mathbb{R}$ is NOT onto; because for an $y = -4 \in \mathbb{R}$, we get $x = \sqrt{y} = 2i$ or $-2i \notin \mathbb{R}$.

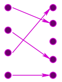
Number of Onto Functions: Counting is *non-trivial* and will be addressed later!

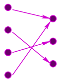
One-to-one & Onto (Bijective) Function:

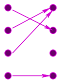
$f : \mathcal{A} \to \mathcal{B}$ is bijective if it is both one-to-one (injective) and onto (surjective).

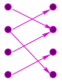
- For arbitrary sets $\mathcal{A}, \mathcal{B}$, $f : \mathcal{A} \to \mathcal{B}$ is bijective if and only if $\forall b \in \mathcal{B},\ \exists a \in \mathcal{A},$ so that $f(a) = b$ and $\forall a'(\neq a) \in \mathcal{A}, f(a') \neq b$.
- If $f : \mathcal{A} \to \mathcal{B}$ is bijective with $\mathcal{A}, \mathcal{B}$ finite, then $|\mathcal{A}| = |\mathcal{B}|$.


One-to-one and Onto


One-to-one, but not Onto


Onto, but not One-to-one


Neither One-to-one, nor Onto


Not a Function (but a Relation)

(Binary) Operations and Properties

Definition

Binary Operation: For non-empty sets, $\mathcal{A}, \mathcal{B}$, any function $f : \mathcal{A} \times \mathcal{A} \to \mathcal{B}$ is called a binary operation on $\mathcal{A}$. If $\mathcal{B} \subseteq \mathcal{A}$ then the binary operation is closed on $\mathcal{A}$ (also $\mathcal{A}$ is closed under f). (Count: $|\mathcal{B}|^{|\mathcal{A}|^2}$)

Unary Operation: A function $g : \mathcal{A} \to \mathcal{A}$ is called unary (or monary) operation on $\mathcal{A}$.

Properties: *Let $f : \mathcal{A} \times \mathcal{A} \to \mathcal{B}$ is a binary operation.*

Commutativity: If $\forall (x, y) \in \mathcal{A} \times \mathcal{A},\ f(x, y) = f(y, x)$ then f is commutative.

Associativity: If f is closed and $\forall x, y, z \in \mathcal{A},\ f(f(x, y), z) = f(x, f(y, z))$, then f is associative.

Example

1. $g : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}$ defined as $g(x, y) = x - y$, is a binary operation on $\mathbb{Z}$ which is NOT closed as $g(1, 2) = -1 \notin \mathbb{Z}^+$, though $1, 2 \in \mathbb{Z}^+$.
2. $h : \mathbb{R}^+ \to \mathbb{R}^+$ defined as $h(x) = \frac{1}{x}$ is an unary operation on $\mathbb{R}^+$.
3. $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined as $f(x, y) = x - y$, is a closed binary operation on $\mathbb{Z}$ which is neither commutative nor associative. (Why?)
4. $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined as $f(a, b) = a + b - ab$ is both commutative and associative.

More Properties of Binary Operation

Properties: *Let $f : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{B}$ is a binary operation.*

Identity: $x \in \mathcal{A}$ is an identity (or identity element) for f if $f(a, x) = f(x, a) = a, \ \forall a \in \mathcal{A}$.

Property: If f has an identity, then that identity is *unique*.
(**Proof:** Let two identities, $x_1, x_2 \in \mathcal{A}$. Then, by definition $f(x_1, x_2) = x_1 = f(x_2, x_1) = x_2$, leading to contradiction!)

Example: $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(a, b) = a + b - ab$ has 0 as the unique identity, because $f(a, 0) = a + 0 + a.0 = a = 0 + a + 0.a = f(0, a)$.

Projection: For sets $\mathcal{A}, \mathcal{B}$, if $\mathcal{C} \subseteq \mathcal{A} \times \mathcal{B}$, then –
(i) $\pi_{\mathcal{A}} : \mathcal{C} \rightarrow \mathcal{A}$ defined by $\pi_{\mathcal{A}}(a, b) = a$, is called the projection on the first coordinate. **(ii)** $\pi_{\mathcal{B}} : \mathcal{C} \rightarrow \mathcal{B}$ defined by $\pi_{\mathcal{B}}(a, b) = b$, is called the projection on the second coordinate.

Property: If $\mathcal{C} = \mathcal{A} \times \mathcal{B}$, then $\pi_{\mathcal{A}}$ and $\pi_{\mathcal{B}}$ both are *onto* functions.

Example: Let $\mathcal{A} = \mathcal{B} = \mathbb{R}$ and $\mathcal{C} \subseteq \mathcal{A} \times \mathcal{B}$ where $\mathcal{C} = \{(x, y) \mid y = x^2, \ x, y \in \mathbb{R}\}$ representing the Euclidean plane that contains points on the parabola $y = x^2$. Here, $\pi_{\mathcal{A}}(3, 9) = 3$ and $\pi_{\mathcal{B}}(3, 9) = 9$. Note that, $\pi_{\mathcal{A}}(\mathcal{C}) = \mathbb{R}$ and hence $\pi_{\mathcal{A}}$ is onto (and one-to-one as well). Whereas, $\pi_{\mathcal{B}}(\mathcal{C}) = [0, +\infty] \subset \mathbb{R}$ and hence $\pi_{\mathcal{B}}$ is NOT onto (nor it is one-to-one as $\pi_{\mathcal{B}}(2, 4) = 4 = \pi_{\mathcal{B}}(-2, 4)$).

Equal, Identity and Composite Functions

Identity Function: The function, $1_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ defined by $1_{\mathcal{A}}(a) = a$ $(\forall a \in \mathcal{A})$, is called the identity function for $\mathcal{A}$.

Equal Functions: Two functions $f, g : \mathcal{A} \to \mathcal{B}$ are said to be equal (denoted as $f = g$) if $f(a) = g(a)$, $\forall a \in \mathcal{A}$.

Note: Domain and Codomain of f, g must also be the same!

Example: $f, g : \mathbb{R} \to \mathbb{Z}$ are defined as, $f(x) = \begin{cases} x, & \text{if } x \in \mathbb{Z} \\ \lfloor x \rfloor + 1, & \text{if } x \in \mathbb{R} - \mathbb{Z} \end{cases}$ and $g(x) = \lceil x \rceil$, then $f(x) = g(x)$ for every $x \in \mathbb{R}$ (Why?). So, $f = g$.

Composite Function: If $f : \mathcal{A} \to \mathcal{B}$ and $g : \mathcal{B} \to \mathcal{C}$, we define the composite function, $g \circ f : \mathcal{A} \to \mathcal{C}$ by $(g \circ f)(a) = g(f(a))$, $\forall a \in \mathcal{A}$.

- Range of $f \subseteq$ Domain of g – sufficient for Function Composition!
- For two identity functions $1_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ and $1_{\mathcal{B}} : \mathcal{B} \to \mathcal{B}$,
$$f \circ 1_{\mathcal{A}} = f = 1_{\mathcal{B}} \circ f.$$

Example: Let $f, g : \mathbb{R} \to \mathbb{R}$ defined as, $f(x) = x^2$ and $g(x) = x + 1$. Then, $(f \circ g)(x) = x^2 + 2x + 1$ and $(g \circ f)(x) = x^2 + 1$. So, $(f \circ g)(x) \neq (g \circ f)(x)$.

Commutativity of Function Compositions: *Does NOT Hold!*

Function Composition is NOT Commutative, that is, we shall NOT always have $f \circ g(x) \neq g \circ f(x)$ for any two functions, $f, g : \mathcal{A} \to \mathcal{A}$ (and $x \in \mathcal{A}$).

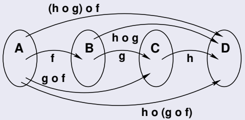
Composite Function Properties

Associativity of Function Compositions

If $f : \mathcal{A} \to \mathcal{B}$, $g : \mathcal{B} \to \mathcal{C}$ and $h : \mathcal{C} \to \mathcal{D}$, then $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof: For every $x \in \mathcal{A}$, we can show,

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



Recursive Compositions of Functions

Let $f : \mathcal{A} \to \mathcal{A}$. Then, $f^1 = f$, and for $n \in \mathbb{Z}^+$, $f^{n+1} = f \circ (f^n) = (f^n) \circ f$.

Bijective Nature of Function Compositions

If $f : \mathcal{A} \to \mathcal{B}$ and $g : \mathcal{B} \to \mathcal{C}$ both are one-to-one , then $g \circ f : \mathcal{A} \to \mathcal{C}$ is one-to-one.

Proof: Let $a_1, a_2 \in \mathcal{A}$.

$(g \circ f)(a_1) = (g \circ f)(a_2) \Rightarrow g(f(a_1)) = g(f(a_2)) \Rightarrow f(a_1) = f(a_2)$ (as g is one-to-one).

Again, $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ (as f is one-to-one). Hence, $g \circ f$ is one-to-one.

If $f : \mathcal{A} \to \mathcal{B}$ and $g : \mathcal{B} \to \mathcal{C}$ both are onto, then $g \circ f : \mathcal{A} \to \mathcal{C}$ is onto.

Proof: For any $z \in \mathcal{C}$, $\exists y \in \mathcal{B}$ (as g is onto) and $y \in \mathcal{B}$, $\exists x \in \mathcal{A}$ (as f is onto).

So, $z = g(y) = g(f(x)) = (g \circ f)(x)$ and Range of $(g \circ f) = \mathcal{C} =$ Codomain of $(g \circ f)$.

Composite Function Properties

Bijective Nature of Function Compositions

Let $f : \mathcal{A} \rightarrow \mathcal{B}$ and $g : \mathcal{B} \rightarrow \mathcal{C}$ and the composition $g \circ f : \mathcal{A} \rightarrow \mathcal{C}$ is a one-to-one (injective) function. Then, f is one-to-one (however, g need NOT be one-to-one).

Explanation:

f is one-to-one (Proof): Assuming f is NOT one-to-one, implies $\exists x_1, x_2 \in \mathcal{A}$ such that $f(x_1) = f(x_2)$. So, $g \circ f(x_1) = g \circ f(x_2)$, contradicting $g \circ f$ is injective!

g is not one-to-one (Example): $f, g : \mathbb{R} \rightarrow \mathbb{R}$ are defined as, $f(x) = e^x$ and $g(x) = x^2$ $(x \in \mathbb{R})$. Here, $g \circ f : \mathbb{R} \rightarrow \mathbb{R}$ is defined as, $g \circ f(x) = e^{2x}$. So, $(g \circ f)$ is one-to-one, but g is NOT (note that, f is one-to-one as proven)!

Let $f : \mathcal{A} \rightarrow \mathcal{B}$ and $g : \mathcal{B} \rightarrow \mathcal{C}$ and the composition $g \circ f : \mathcal{A} \rightarrow \mathcal{C}$ is a onto (surjective) function. Then, g is onto (however, f need NOT be onto).

Explanation:

g is onto (Proof): As $(g \circ f)$ is onto, for any $z \in \mathcal{C}$, $\exists x \in \mathcal{A}$ such that, $z = g \circ f(x) = g(f(x))$, implying that z has a pre-image defined as $f(x) \in \mathcal{B}$ – thus making g onto.

f is not onto (Example): $f, g : \mathbb{Z} \rightarrow \mathbb{Z}$ are defined as, $f(x) = 2x$ and $g(x) = \lfloor \frac{x}{2} \rfloor$ $(x \in \mathbb{Z})$. Here, $g \circ f : \mathbb{Z} \rightarrow \mathbb{Z}$ is defined as, $g \circ f(x) = x$. So, $(g \circ f)$ is onto, but f is NOT (note that, g is onto as proven)!

Inverse Functions and Invertibility

Inverse Functions: For a function $f : \mathcal{A} \to \mathcal{B}$, if $f_L^{-1}, f_R^{-1} : \mathcal{B} \to \mathcal{A}$ are defined such that $f_L^{-1} \circ f = 1_{\mathcal{A}}$ and $f \circ f_R^{-1} = 1_{\mathcal{B}}$, then f_L^{-1} and f_R^{-1} are called the left inverse and right inverse of f, respectively.

Invertible Functions: A function $f : \mathcal{A} \to \mathcal{B}$ is said to be invertible if there exist a function $f^{-1} : \mathcal{B} \to \mathcal{A}$ such that $f^{-1} \circ f = 1_{\mathcal{A}}$ and $f \circ f^{-1} = 1_{\mathcal{B}}$.
f^{-1} is called the inverse function of f.

Unique Inverse: An invertible function $f : \mathcal{A} \to \mathcal{B}$ has a unique inverse $f^{-1} : \mathcal{B} \to \mathcal{A}$.

(**Proof:** Assume two inverses, f_1^{-1} and f_2^{-1}. Using the definition, we get, $f_1^{-1} = f_1^{-1} \circ 1_{\mathcal{B}} = f_1^{-1} \circ (f \circ f_2^{-1}) = (f_1^{-1} \circ f) \circ f_2^{-1} = 1_{\mathcal{A}} \circ f_2^{-1} = f_2^{-1}$.)

Examples: **(1)** Let $f, g : \mathbb{Z} \to \mathbb{Z}$ are defined as $f(x) = 2x$ and $g(x) = \lfloor \frac{x+1}{2} \rfloor$ $(x \in \mathbb{Z})$. So, $g \circ f, f \circ g : \mathbb{Z} \to \mathbb{Z}$ are defined by, $g \circ f(x) = g(2x) = x$ and $f \circ g(x) = f(\lfloor \frac{x+1}{2} \rfloor) = \begin{cases} x+1, & \text{if } x \text{ is odd} \\ x, & \text{if } x \text{ is even} \end{cases}$. So, $g \circ f = 1_{\mathbb{Z}}$ meaning g is the left inverse of f, but $f \circ g \neq 1_{\mathbb{Z}}$ meaning g is NOT the right inverse of f.

(2) Let $f, g : \mathbb{R} \to \mathbb{R}$ are defined as $f(x) = 2x$ and $g(x) = \frac{x}{2}$ $(x \in \mathbb{R})$. So, $g \circ f, f \circ g : \mathbb{R} \to \mathbb{R}$ are defined by, $g \circ f(x) = g(2x) = x$ and $f \circ g(x) = f(\frac{x}{2}) = x$. So, $g \circ f = f \circ g = 1_{\mathbb{R}}$ meaning g is inverse of f.

Properties of Invertible Functions

Properties

- $f : \mathcal{A} \to \mathcal{B}$ is invertible if and only if it is bijective (one-to-one + onto).

  Proof: [If] f is invertible means inverse function $f^{-1} : \mathcal{B} \to \mathcal{A}$ exists.
  $f^{-1} \circ f = 1_{\mathcal{A}}$ and $1_{\mathcal{A}}$ is injective, so f is injective.
  $f \circ f^{-1} = 1_{\mathcal{B}}$ and $1_{\mathcal{B}}$ is surjective, so f is surjective.

  [Only-If] Since f is bijective, $y \in \mathcal{B}$ has one and only one pre-image $x \in \mathcal{A}$.
  We define $f^{-1} : \mathcal{B} \to \mathcal{A}$ as $f^{-1}(y) = x$ (pre-image of y under f), $y \in \mathcal{B}$.
  So, $f^{-1} \circ f(x) = f^{-1}(y) = x$ and $f \circ f^{-1}(y) = f(x) = y$,
  implying $f^{-1} \circ f = 1_{\mathcal{A}}$ and $f \circ f^{-1} = 1_{\mathcal{B}} \Rightarrow f$ is invertible.

- If $f : \mathcal{A} \to \mathcal{B}$, $g : \mathcal{B} \to \mathcal{C}$ are invertible, then $g \circ f : \mathcal{A} \to \mathcal{C}$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

  Proof: f, g are invertible implies that f, g are bijective functions.
  So, $(g \circ f)$ is also bijective and hence invertible (using above property).
  $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ 1_{\mathcal{B}} \circ f = f^{-1} \circ f = 1_{\mathcal{A}}$.
  $(g \circ f) \circ (f^{-1} \circ g^{-1}) = 1_{\mathcal{B}}$. So, $(f^{-1} \circ g^{-1})$ is the inverse of $(g \circ f)$.

Example

$f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = 3x + 1$ ($x \in \mathbb{R}$). Note that, f is bijective (Why?) and hence invertible. Now, $f^{-1} : \mathbb{R} \to \mathbb{R}$ defined by $f^{-1}(y) = \frac{y-1}{3}$, $y \in \mathbb{R}$.

Properties with Direct and Inverse Images

Direct Image: Let $f : \mathcal{A} \to \mathcal{B}$ and (non-empty) $\mathcal{A}' \subseteq \mathcal{A}$. The direct image of $\mathcal{A}'$ under f is $f(\mathcal{A}') \subseteq \mathcal{B}$ given by, $f(\mathcal{A}') = \{f(x) \mid x \in \mathcal{A}'\}$.

Inverse Image: Let $f : \mathcal{A} \to \mathcal{B}$ and (non-empty) $\mathcal{B}' \subseteq \mathcal{B}$. The inverse image (pre-image) of $\mathcal{B}'$ under f is $f^{-1}(\mathcal{B}') \subseteq \mathcal{A}$ given by, $f^{-1}(\mathcal{B}') = \{x \mid f(x) \in \mathcal{B}'\}$.

Example: $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = x^2$ $(x \in \mathbb{R})$. Let $\mathcal{P} = \{x \in \mathbb{R} \mid x \in [0, 2]\}$. The direct image $f(\mathcal{P}) = \{y \mid y \in [0, 4]\}$ $(y \in \mathbb{R})$ and the inverse image of set $f(\mathcal{P})$ is $f^{-1}(f(\mathcal{P})) = \{x \mid x \in [-2, 2]\}$. So, $f^{-1}(f(\mathcal{P})) \neq \mathcal{P}$ and f is not a bijection / invertible.

Properties:

- (RECAP) Let $f : \mathcal{A} \to \mathcal{B}$, with $\mathcal{A}_1, \mathcal{A}_2 \subseteq \mathcal{A}$. Then, **(i)** If $\mathcal{A}_1 \subset \mathcal{A}_2 \Rightarrow f(\mathcal{A}_1) \subset f(\mathcal{A}_2)$, **(ii)** $f(\mathcal{A}_1 \cup \mathcal{A}_2) = f(\mathcal{A}_1) \cup f(\mathcal{A}_2)$, and **(iii)** $f(\mathcal{A}_1 \cap \mathcal{A}_2) \subset f(\mathcal{A}_1) \cap f(\mathcal{A}_2)$.

  Note: In general, $f(\mathcal{A}_1 \cap \mathcal{A}_2) \neq f(\mathcal{A}_1) \cap f(\mathcal{A}_2)$. Consider, $f : \mathbb{R} \to \mathbb{R}$ as $f(x) = x^2$ and $\mathcal{A}_1 = \{0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\}$, $\mathcal{A}_2 = \{0, -1, -\frac{1}{2}, -\frac{1}{3}, \ldots\}$. Here, $f(\mathcal{A}_1 \cap \mathcal{A}_2) = \{0\} \neq \{0, 1, \frac{1}{2^2}, \frac{1}{3^2}\} = f(\mathcal{A}_1) \cap f(\mathcal{A}_2)$.

- Let $f : \mathcal{A} \to \mathcal{B}$ be an onto mapping, with $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{B}$. Then, **(i)** If $\mathcal{B}_1 \subset \mathcal{B}_2 \Rightarrow f^{-1}(\mathcal{B}_1) \subset f^{-1}(\mathcal{B}_2)$, **(ii)** $\overline{f^{-1}(\mathcal{B}_1)} = f^{-1}(\overline{\mathcal{B}_1})$, **(iii)** $f^{-1}(\mathcal{B}_1 \cup \mathcal{B}_2) = f^{-1}(\mathcal{B}_1) \cup f^{-1}(\mathcal{B}_2)$, and **(iv)** $f^{-1}(\mathcal{B}_1 \cap \mathcal{B}_2) = f^{-1}(\mathcal{B}_1) \cap f^{-1}(\mathcal{B}_2)$.

  Proof: **(i)** Let $x \in f^{-1}(\mathcal{B}_1) \Rightarrow f(x) \in \mathcal{B}_1$. Since $\mathcal{B}_1 \subset \mathcal{B}_2$, therefore $f(x) \in \mathcal{B}_1 \Rightarrow f(x) \in \mathcal{B}_2$. So, $x \in f^{-1}(\mathcal{B}_2)$ implying $f^{-1}(\mathcal{B}_1) \subset f^{-1}(\mathcal{B}_2)$.

  (ii), (iii) and (iv) *Left for You as an Exercise!*

The Leftover: *Number of Onto Functions under $f : \mathcal{A} \rightarrow \mathcal{B}$*

If $0 < |\mathcal{A}| = m < n = |\mathcal{B}|$, how many Onto functions? $= 0$

If $|\mathcal{A}| = m = 1 = n = |\mathcal{B}|$, how many Onto functions? $= 1$

If $|\mathcal{A}| = m \geq n = 2 = |\mathcal{B}|$, how many Onto functions? $= 2^m - 2$

If $\mathcal{A} = \{x, y, z\}$, $\mathcal{B} = \{1, 2\}$, then all possible functions $= |\mathcal{B}|^{|\mathcal{A}|} = 2^3$; but $f_1 = \{(x,1),(y,1),(z,1)\}$ and $f_2 = \{(x,2),(y,2),(z,2)\}$ are NOT onto. Hence, number of onto functions $= 2^3 - 2 = 6$.

If $|\mathcal{A}| = m \geq n = 3 = |\mathcal{B}|$, how many Onto functions? $= \binom{3}{3}3^m - \binom{3}{2}2^m + \binom{3}{1}1^m$

If $\mathcal{A} = \{w, x, y, z\}$, $\mathcal{B} = \{1, 2, 3\}$, then all possible functions $= 3^4$; this includes 2^4 non-onto functions each from $\mathcal{A} \rightarrow \{1,2\}$, $\mathcal{A} \rightarrow \{1,3\}$ and $\mathcal{A} \rightarrow \{2,3\}$. Now, the running count for onto functions $= 3^4 - 3.2^4$. But, we removed the constant function $\{(w,2),(x,2),(y,2),(z,2)\}$ twice – both during function removal from $\mathcal{A} \rightarrow \{1,2\}$, $\mathcal{A} \rightarrow \{2,3\}$. So, the final onto functions count $= 3^4 - 3.2^4 + 3 = \binom{3}{3}3^4 - \binom{3}{2}2^4 + \binom{3}{1}1^4$.

If $|\mathcal{A}| = m \geq n = |\mathcal{B}|$, how many Onto functions? $= O(m, n)$

What do the above steps reveal? $\Rightarrow$ Principle of Inclusion-Exclusion!

$$O(m,n) = \binom{n}{n}n^m - \binom{n}{n-1}(n-1)^m + \binom{n}{n-2}(n-2)^m - \cdots + (-1)^{n-2}\binom{n}{2}2^m + (-1)^{n-1}\binom{n}{1}1^m$$
$$= \sum_{i=0}^{n-1}(-1)^i\binom{n}{n-i}(n-i)^m = \sum_{i=0}^{n}(-1)^i\binom{n}{n-i}(n-i)^m$$

Stirling Number of the Second Kind

Combinatorial Definition

- For $m \geq n$, Number of ways to distribute m objects into n identical (but numbered) containers with no container empty $= \sum_{i=0}^{n}(-1)^i \binom{n}{n-i}(n-i)^m$.
- Removing numbering in containers yields the number of ways to distribute m objects into n perfectly identical containers with no container empty $= \frac{1}{n!}\sum_{i=0}^{n}(-1)^i \binom{n}{n-i}(n-i)^m = S(m,n) =$ Stirling Number of Second Kind.
- Therefore, in $f : \mathcal{A} \rightarrow \mathcal{B}$, number of onto functions, $O(m,n) = n!.S(m,n)$.

Combinatorial Derivation: *A Primer to 'Principle of Inclusion-Exclusion'*

Let $m, n \in \mathbb{Z}^+$ with $1 < n \leq m$. Then, $S(m+1,n) = S(m,n-1) + n.S(m,n)$.

Proof:

- $S(m,n-1)$ ways to distribute m objects into $(n-1)$ identical containers with none left empty and putting the $(m+1)^{th}$ object into n^{th} container alone $\Rightarrow$ *contributing* $S(m,n-1)$ *ways to* $S(m+1,n)$.
- $S(m,n)$ ways to distribute m objects into n identical containers with none left empty and then placing $(m+1)^{th}$ object in any of the already filled n containers $\Rightarrow$ *contributing* $n.S(m,n)$ *ways to* $S(m+1,n)$.

Corollary: $\frac{1}{n}[n!.S(m+1,n)] = [(n-1)!.S(m,n-1)] + [n!.S(m,n)]$ (multiply by $(n-1)!$)
$\Rightarrow \frac{1}{n}.O(m+1,n) = O(m,n-1) + O(m,n)$

Counting Problems: *Are these problems well-recognized now?*

1. Suppose you set your computer password of length m from a fixed chosen set of n different characters available in the keyboard ($m \geq n$). How many different passwords can you set so that at least one occurrence of each symbol (from the n chosen set of keyboard symbols) will be present?
2. An $m \times n$ 2-dimensional (2-D) array, $(a_{ij})_{m \times n}$ having m rows and n columns, is filled up with only 0 and 1 values. How many different 2-D arrays you can construct so that exactly one 1 is present in each row and at least one 1 is present at each column?

   (Such arrays / adjacency-matrices are used to represent graph data structures!)
3. m different component manufacturing contracts of a high-security project is to be executed by n different companies so that every company works on some components of the project. How many possible ways these m contracts can get assigned to n companies?
4. For $m, n \in \mathbb{Z}^+$ with $m < n$, prove that, $\sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^m = 0$.
5. For $n \in \mathbb{Z}^+$, verify that, $\sum_{k=0}^{n} (-1)^n \binom{n}{n-k} (n-k)^n = n!$.

Thank You!