More on Proofs

Another widely used proof technique is Induction

- Typically, when a statement requires that a property works for all natural numbers ($n \in \mathbb{N}$)
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

  Mathematical Induction is a good method.

- Two steps ~~needed~~ for Mathematical Induction

  1. Show that the statement is true for $n=0$ or 1

  2. often known as INDUCTION STEP

     Show that if the statement is true for k, it is also true for $n=k+1$.

     This is an implication.
     - We assume that it is true for $n=k$, (Hypothesis)
     - Using this assumption, we show that it is true when $n=k+1$ conclusion

Before trying, one should see if direct method or other methods do work.

Prove for any integer n, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof: STEP 1: Let $n=1$, $\sum_{i=1}^{1} i = 1$, and

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

so, it is true for "1"

STEP 2:

We assume that it holds for $n=k$.

So, $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ is true

Now, for $n=k+1$, we obtain

$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$, and we must show that it is true.

So,

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2} = \frac{k^2+k+2k+2}{2}$$

$$= \frac{k^2+k}{2} + \frac{2k+2}{2} = \frac{k(k+1)}{2} + (k+1)$$

$$=$$

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$= \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

So, $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$ as expected

Proved

Uniqueness Proofs:

Often some theories assert the existence of a unique element with certain type of property.

↓ in other words

Only one element is available with such property.

↳ To prove, we must show that an element with this property exist and

No other element has the same property.

- There are two parts of a uniqueness proof:

  1. We show that an element with the desired property x exists, and
  2. If $y \neq x$, then y does not have the same property.

Example: Given a, b are realnumber, and $a \neq 0$. Then, there is an unique real number r such that $ar + b = 0$.

Given

$ar + b = 0$ $\Rightarrow r = -b/a$	Step 1 existence	Suppose, s is a realnumber So, $as + b = 0$. Then,

$$as + b = ar + b = 0$$
$$\Rightarrow as = ar$$
$$\Rightarrow s = r$$

Therefore, if $s \neq r$, then $as + b \neq 0$.

↳ uniqueness

SETS, FUNCTIONS

SEQUENCE AND SUMS

Union

A, B sets.

union $\equiv A \cup B$

$\equiv \{x \mid x \in A \vee x \in B\}$

$\equiv \{x \mid x \in A \text{ or } x \in B\}$

$\equiv$ x such that x belongs to A, or x belongs to B

Let $A = \{1, 3, 5\}$
$B = \{1, 2, 3\}$

so, $A \cup B = \{1, 2, 3, 5\}$

Intersection

$A \cap B \equiv \{x \mid x \in A \wedge x \in B\}$

$\equiv \{x \mid x \in A \text{ and } x \in B\}$

$\equiv$ x such that x belongs to A and x belongs to B

$A \cap B = \{1, 3, 5\}$

Disjont

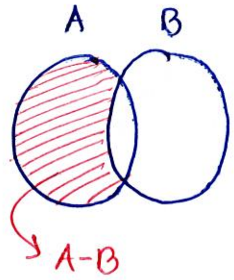
if empty set is the intersection, then the sets are disjoint

$A \cap B = \{\phi\}$

Difference

Difference of A and B, denoted as A−B, is the set of elements that are in A but not in B

So, $A - B = \{x \mid x \in A \wedge x \notin B\}$



Let $A = \{1, 3, 5\}$

$B = \{1, 2, 3\}$

$A - B = \{5\}$

Complement

Complement of A is $\bar{A}$

So, $\bar{A} = \{x \mid x \notin \bar{A}\}$

That is, $U - A = \bar{A}$, where U is the universal set.

Prove $\overline{A \cap B} = \bar{A} \cup \bar{B}$

$= \{x \mid x \notin (A \cap B)\}$ definition of complement

$= \{x \mid \neg\, x \in (A \cap B)\}$ " of $\notin$

$= \{x \mid \neg (x \in A \text{ and } x \in B)\}$ definition of $\wedge$

$= \{x \mid \neg (x \in A) \underset{\text{or}}{\vee} \neg (x \in B)\}$ De Morgan's Law

$= \{x \mid x \notin A \text{ or } x \notin B\}$ definition of $\notin$

$= \{x \mid x \in \bar{A} \text{ or } x \in \bar{B}\}$ " of complement

$= \{x \mid x \in \bar{A} \cup \bar{B}\}$ definition of Union

$= \bar{A} \cup B$ by meaning of set builder notation.

For sets A, B, C, show that

$$\overline{A \cup B \cap C} = (\bar{C} \cup \bar{B}) \cap \bar{A}$$

We have

$$\overline{A \cup B \cap C} = \overline{A \cup (B \cap C)} = \bar{A} \cap \overline{(B \cap C)}$$ De Morgan's

$$= \bar{A} \cap (\bar{B} \cup \bar{C})$$ De Morgan's

$$= (\bar{B} \cup \bar{C}) \cap \bar{A}$$ Commutative Law for intersection

$$= (\bar{C} \cup \bar{B}) \cap \bar{A}$$ Commutative law for Union.

Power set :

Given a set S, power set of S is the set of all subsets of S. It is denoted as P(S)

Example: Find power set of $\{0, 1, 2\}$

$$P\{0,1,2\} = \{ \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}, \{\phi\} \}$$

it is always a subset of a given set.

* If a set has n elements, its power set has 2^n elements.

Cartesian Product

Given A and B are two sets, their cartesian product is $A \times B$, is the set of all ordered pairs (a, b). Here, $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Example:

$A = \{1, 2\}$, $B = \{a, b, c\}$

So, $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b)$
$(2, c)\}$

Now, $B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$

As we see, $A \times B \neq (B \times A)$

$A \times A = A^2$, $A^2 \times A = A^3$, $A^4 = A^3 \times A$ ...

$A = \{1, 2\}$ $A \times A = \{1, 2\} \times \{1, 2\}$

$= \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

$A^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

Find $A^3 = ?$

Set Notation with Quantifiers :

$\forall x \in S\,(P(x))$, where S is the set.

Universal quantification of $(P(x))$

$\Downarrow$ Shorthand

$$\forall x\,(x \in S \rightarrow P(x))$$

Similarly, $\exists x \in S\; P(x)$ denotes the existential quantification of $P(x)$ over all elements in S

$\Downarrow$ Short hand

$$\exists x\,(x \in S \wedge P(x))$$

Example : $\forall x \in \mathbb{R}\,(x^2 \geq 0)$

The square of every real number is non-negative.

$\exists x \in \mathbb{Z}\,(x^2 = 1)$

There's an integer whose square is 1.

⊞ If f is a fn^c from A to B, then we say that

A is the domain

B is the codomain of f

Again $f(a) = b$

b → image of a

a → Preimage

So, Range, or image, of f is the set of all images of elements of A.

⊞ Two fn^c's are equal when they have same domain

they have same codomain

and

Map each element of their common domain to the same element in their common co-domain.

⊞ Given. f_1 and f_2 be functions from A to $\mathbb{R}$.

Then. $f_1 + f_2$ and $f_1 f_2$ are also fn^c from A to $\mathbb{R}$, and defined for all $x \in A$ by

$$(f_1 + f_2)x = f_1(x) + f_2(x)$$

$$(f_1 f_2)(x) = f_1(x)\, f_2(x)$$

Two real valued fn^c with same domain can be added and multiplied.

Given $A = \{0, 2, 4, 6, 8\}$, $B = \{0, 1, 2, 3, 4\}$ and $C = \{0, 3, 6, 9\}$

so, $A \cup B \cup C = \{0, 1, 2, 3, 4, 6, 8, 9\}$

$A \cap B \cap C = \{0\}$

Union of a collection of sets is :

$$A_1 \cup A_2 \cup A_3 \cup A_4 \cdots \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

Intersection of a collection of sets is :

$$A_1 \cap A_2 \cap A_3 \cap A_4 \cdots \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

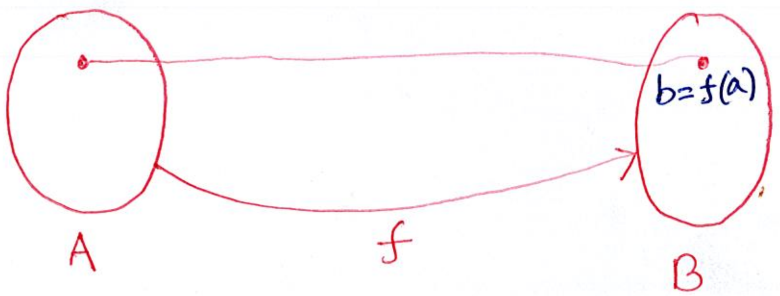
Functions

Let us assume that A and B are two non-empty sets. Any fn^c f from A to B is an assignment of exaclly one element of B to each element of A.

$$f(a) = b$$

$\hookrightarrow$ Unique element of B

Now, we use $f : A \to B$ to manifest that f is a function from A to B



It's a Kind of mapping : Function 'f' Maps A to B

Example:

$$f_1, f_2 : \mathbb{R} \to \mathbb{R}$$

$$f_1(x) = x^2, \quad f_2(x) = x - x^2$$

So, $f_1 + f_2 = x^2 + x - x^2 = x$

and $(f_1 f_2)(x) = x^2(x - x^2) = x^3 - x^4$

Image of a subset:

When f is a fn^c from set A to B, the image of a subset of A can also be defined.

$\downarrow$ Definition

Let's assume that f is a fn^c from A to B and let's consider "S" be a subset of A.

So, the image of "S" under the fn^c f is the subset of B that consists of the images of the elements of S.

Image of S is denoted by $f(S)$

$$f(S) = \{t \mid \exists s \in S \,(t = f(s))\}$$

Example: Given

$A = \{a, b, c, d, e\}$

$B = \{1, 2, 3, 4\}$

$f(a) = 2$
$f(b) = 1$
$f(c) = 4$
$f(d) = 1$
$f(e) = 1$

S is the subset $\{b, c, d\}$

$\downarrow$ image

$f(S) = \{1, 4\}$

Types of fn^c :

One-to-one : if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain.

$\downarrow$ also known as

injective

$\downarrow$ Contrapositive way

A fn^c f is one-to-one iff $f(a) \neq f(b)$ whenever $a \neq b$

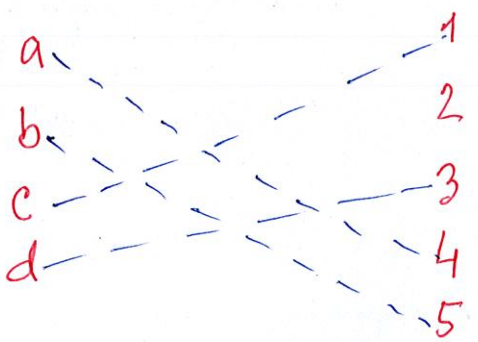
Q. Use Predicates, quantifier to represent the definition of one-to-one fn^c?

$$\forall a \forall b \, (f(a) = f(b) \rightarrow a = b)$$

$\downarrow$ contrapositive

$$\forall a \forall b \, (a \neq b \rightarrow f(a) \neq f(b))$$

Example: A fn^c from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$



Given $f(a) = 4$

$f(b) = 5$

$f(c) = 1$

$f(d) = 3$

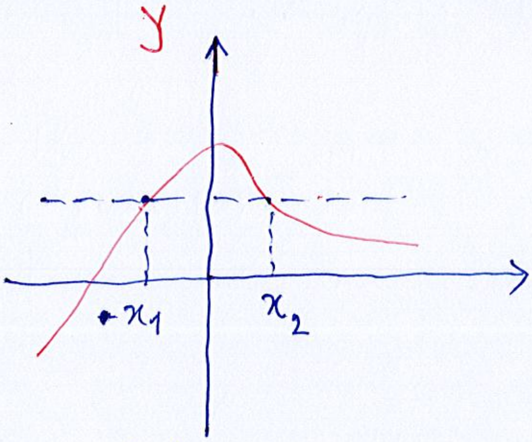
This fn^c is one-to-one because f takes on different values at the four elements of its domain.

A few example $f(x) = x^2$; $f(x) = x^3$; $f(x) = \frac{1}{x}$

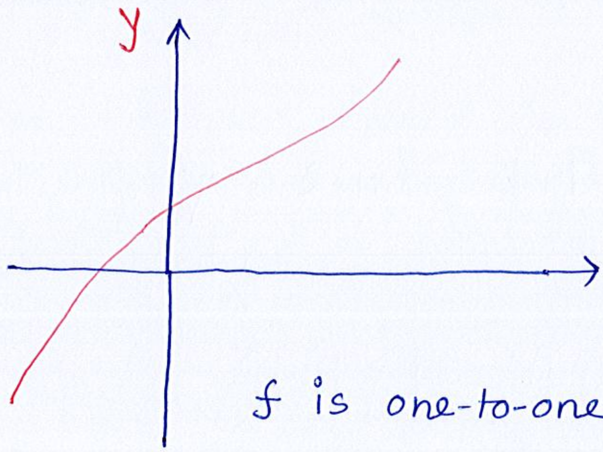
$f(x)=x^2 \xrightarrow{\text{not}}$ one-to-one

$f(x)=x^3 \xrightarrow{\text{YES}}$ one-to-one

$f(x)=\frac{1}{x} \xrightarrow{\text{YES}}$ one-to-one



f is not one-to-one



f is one-to-one

If some horizontal lines intersect the graph of fn^c "f" more than once, then the fn^c is not one-to-one. → GRAPHICAL WAY to decide one-to-one.

Also, fn^{c}s that are increasing or decreasing are one-to-one.

increasing : A fn^c "f" is increasing if $\forall x \forall y\,(x<y \rightarrow f(x) \leq f(y))$

$\xrightarrow{\text{strictly}}$ $\forall x \forall y\,(x<y \rightarrow f(x) < f(y))$

decreasing :

A fn^c "f" is decreasing if

$$\forall x \forall y\,(x<y \rightarrow f(x) \geq f(y))$$

$$\Big\downarrow \text{strictly}$$

$$\forall x \forall y\,(x<y \rightarrow f(x) > f(y))$$

On-to function

A fn^c from A to B is called onto, or surjective, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$.

Using Predicates & quantifiers

$$\forall y \, \exists x \, (f(x) = y)$$

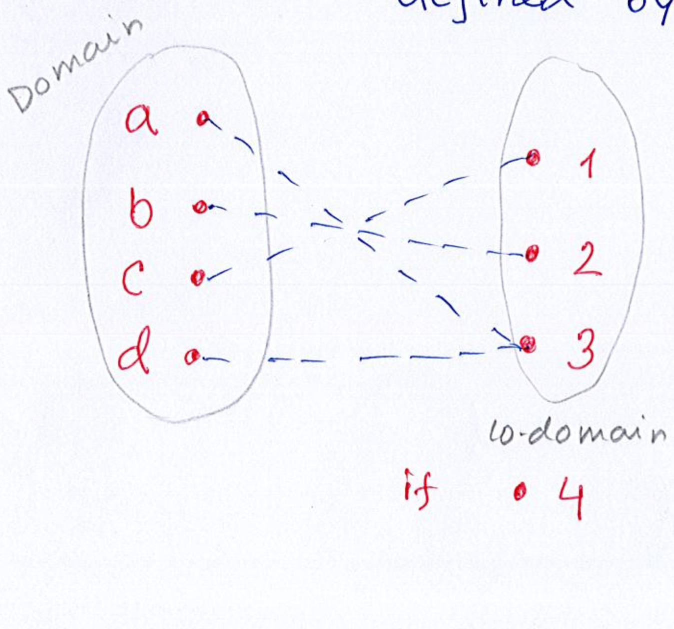
On-to fn^c → x is domain → y is co-domain

In case of on-to fn^c,

co-domain and range are equal.

Example :

f be the fn^c from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ defined by $f(a) = 3$, $f(b) = 2$, $f(c) = 1$



Here, all the three elements of the codomain are images of elements in the domain

if • 4 $\Longrightarrow$ Not an On-to fn^c

Example

$f(x) = x^2$ from the set of integers to the set of integers

This is NOT on-to

→ Because, there's no integer that can give $x^2 = -1$

$f: \mathbb{N} \to \mathbb{N}$ (Natural numbers) $[1, 2, 3, 4 \ldots]$

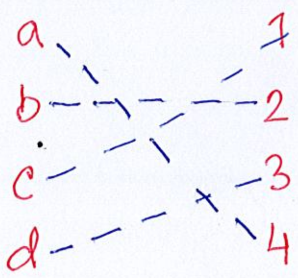
fn^c	One-to-One	On-to
$f(n) = n^2$	YES	NO
$f(n) = n+3$	YES	NO
$f(n) = \begin{cases} n-1, & n \text{ is odd} \\ n+1, & n \text{ is even} \end{cases}$	YES	YES

Bijection fn^c

If a fn^c is bijection, it is both one-to-one and on-to fn^c

example: Given, fn^c f is form $\{a, b, c, d\} \xrightarrow{f} \{1, 2, 3, 4\}$

$f(a) = 4$, $f(b) = 2$, $f(c) = 1$
$f(d) = 3$



This is one-one /multiple

→ no dual assignment of b

This is on-to

→ All 'b' are images

Composition of functions

Let g be a function from the set A to the set B and let "f" be a fn^c from the set B to the set C.

Given the above,

Composition of the functions f and g, denoted as "$f \circ g$", is defined by :

$$(f \circ g)(a) = f(g(a))$$

To find $(f \circ g)(a)$

W We first apply g to a, and then, f to the result $g(a)$.

f use $g(a)$ as the domain

Example :

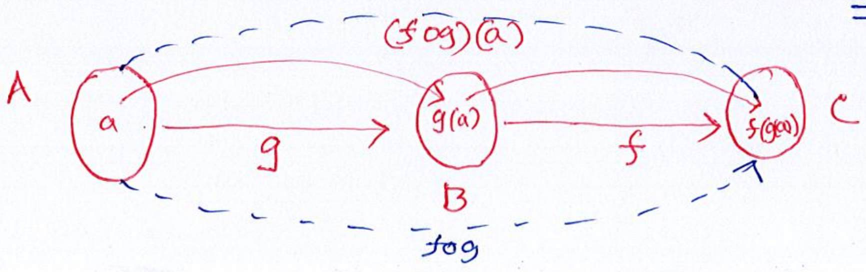
Given, f and g are fn^c from the set of integers defined by $f(x) = 2x+3$ and $g(x) = 3x+2$.

Find $f \circ g$ and $g \circ f$

$$f \circ g(x) = f(g(x)) = f(3x+2) = 2 \cdot 3x+2 + 3$$
$$= 6x+4+3$$
$$= 6x+7$$

and

$$g \circ f(x) = g(f(x)) = g(2x+3) = 3(2x+3)+2$$
$$= 6x+11$$



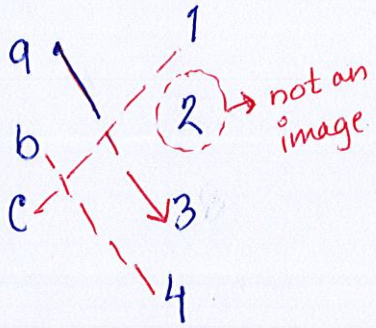
All fn^c graphically

$\{a, b, c, d\} \downarrow \{1, 2, 3, 4\}$

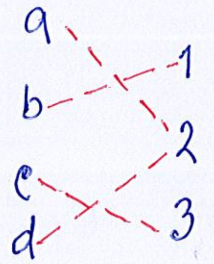
$f(a) = 4$
$f(b) = 2$
$f(c) = 1$
$f(d) = 3$

Not necessary for below explanations.

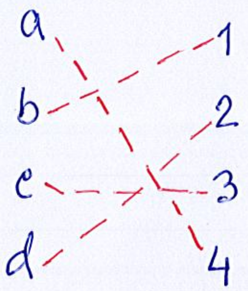
one-to-one but NOT on-to



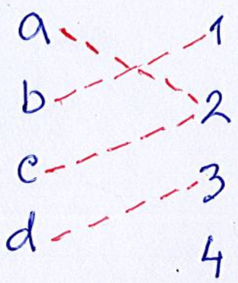
Onto, NOT one-to-one



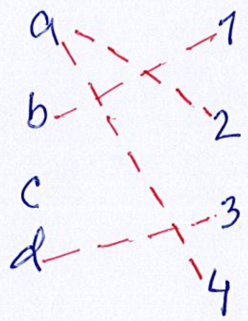
One-to-one and onto



Neither one-to-one nor on-to



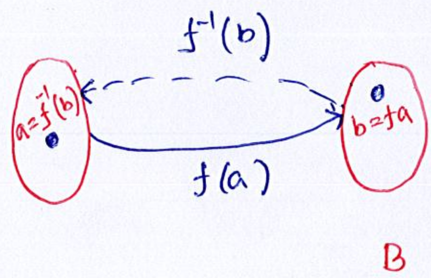
Not a fn^c



Inverse Functions

Let's consider "f" be the one-to-one correspondence from set A to B.
bijection

The inverse fn^c of "f" is ~~that~~ the fn^c that assigns to, an element b belonging to ~~the~~ B, the unique element a in A such that $f(a) = b$.

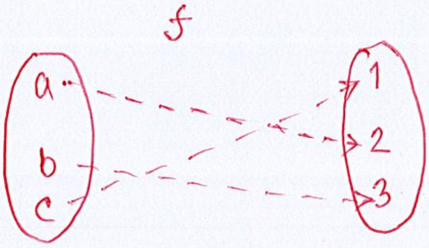


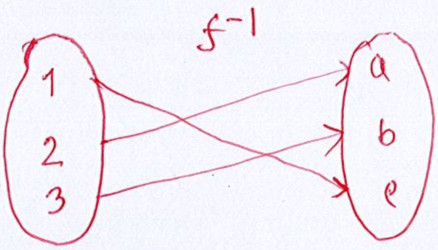
Inverse fn^c of f is denoted as f^{-1}. $f^{-1}(b) = a$ when $f(a) = b$

Let f is fn^c from $\{a, b, c\}$ to $\{1, 2, 3\}$ such that $f(a) = 2$, $f(b) = 3$, $f(c) = 1$

So, f is invertible as the fn^c is one-to-one correspondence.

$$f^{-1}(1) = c, \quad f^{-1}(2) = a, \quad f^{-1}(3) = b$$





Caution:

If a fn^c is not one-to-one correspondence, we cannot define an inverse.

Find the inverse of $f(x) = 3x - 2$. That is— $f^{-1}(x) = ?$

Let's assume $y = f(x) \Rightarrow x = f^{-1}(y)$

$$\Rightarrow y = 3x - 2$$

Now, replace "y" by "x" & x by "y". We obtain.

$$x = 3y - 2$$

$$\Rightarrow 3y = x + 2$$

$$\Rightarrow y = \frac{1}{3}(x + 2)$$

$\equiv x = f(y)$
$\equiv y = f^{-1}(x)$.
Using this

So, $\Rightarrow f^{-1}(x) = \frac{1}{3}(x+2)$