Sets and Functions

Reading for COMP364 and CSIT571

Cunsheng Ding
Department of Computer Science
HKUST, Kowloon, CHINA

Acknowledgments: Materials from Prof. Sanjain Jain at NUS

Sets and Functions for Cryptography

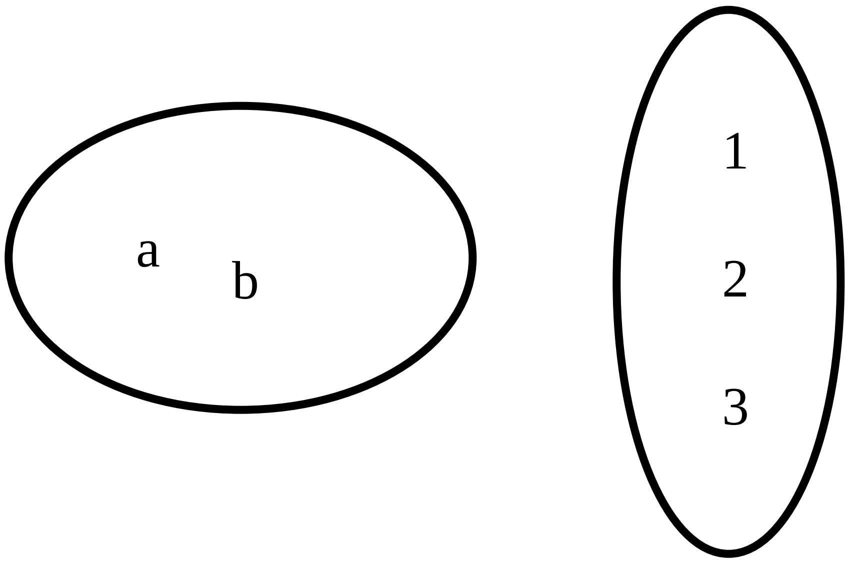
- Sets and functions are basic building blocks of cryptographic systems. There is no way to learn cryptography and computer security without the knowledge of sets and functions.
- Sets and functions are covered in school math., and also in any university course on discrete math.
- Every student should read this material as you may have forgotten sets and functions even if you learnt them as people do forget.

Lecture Topics

- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- Equality of Sets by Mutual Inclusion
- Universal Sets, Venn Diagrams
- Set Operations
- Set Identities
- Proving Set Identities

Sets

- A <u>set</u> is a collection of (distinct) objects.
- For example,



Members, Elements

- The objects that make up a set are called members or elements of the set.

- An object can be anything that is “meaningful”. For example,
  - a number
  - an equation
  - a person
  - another set

Equality of Sets

- Two sets are equal iff they have the same members.
  - That is, a set is completely determined by its members.
- This is known as the principle of extension.

Pause and Think ...

- Does the statement “a set is a collection of objects” define what a set is?
- Let
  - the members of set A be -1 and 1,
  - the members of set B be the roots of the equation $x^2 - 1 = 0$.
  - Are sets A and B equal?

Lecture Topics

- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- Equality of Sets by Mutual Inclusion
- Universal Sets, Venn Diagrams
- Set Operations
- Set Identities
- Proving Set Identities

The Notation { … } Describes a Set

- A set can be described by listing the comma separated members of the set within a pair of curly braces.

- An example
  - Let $S = \{ 1, 3, 9 \}$.
  - S is a set.
  - The members of S are 1, 3, 9.

Order and Repetition Do Not Matter in { … }

- By the principle of extension, a set is determined by its members.
- For example, the following expressions are equivalent
  - { 1, 3, 9 }
  - { 9, 1, 3 }
  - { 1, 1, 9, 9, 3, 3, 9, 1 }
  - They denote the set whose members are 1, 3, 9.

The Membership Symbol $\in$

- The fact that x is a member of S can be expressed as
  - $x \in S$
- The membership symbol $\in$ can be read as
  - is in, is a member of, belongs to
- An Example
  - $S = \{ 7, 13, 21, 47 \}$
  - $7 \in S$, $13 \in S$, $21 \in S$, $47 \in S$
- The negation of $\in$ is written $\notin$.

Defining a Set by Membership Properties

- Notation
  - $S = \{ x \in T \mid P(x) \}$
  - The members of S are members of a already known set T that satisfy property P.

- An example
  - Let **Z** be the set of integers.
  - Let $\mathbf{Z}_{+}$ be the set of positive integers.
  - $\mathbf{Z}_{+} = \{ x \in \mathbf{Z} \mid x > 0 \}$

Pause and Think ...

- Can you simplify the following expression?
  - { {2,2}, { {2} }, {1,1,1}, 1 , { 1 } , 2, 2 }

- What does the following expression say?
  - X = { X }

- Find an expression equivalent to S = { . . . , x , . . . }.

Lecture Topics

- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- Equality of Sets by Mutual Inclusion
- Universal Sets, Venn Diagrams
- Set Operations
- Set Identities
- Proving Set Identities

The Empty Set

- The empty set is also called the null set.
- It is the set that has no members.
- It is denoted as $\emptyset$.
- Clearly, $\emptyset = \{ \}$.
- For any object x, $x \notin \emptyset$.

The Sets of Positive, Negative, and All Integers

- $\mathbf{Z}$ = The set of (all) integers
  - $\mathbf{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$
- $\mathbf{Z}_+$ = The set of (all) positive integers
  - $\mathbf{Z}_+ = \{ 1, 2, 3, \ldots \}$
  - $\mathbf{Z}_+ = \{ x \in \mathbf{Z} \mid x > 0 \}$
- $\mathbf{Z}_-$ = The set of (all) negative integers
  - $\mathbf{Z}_- = \{ \ldots, -3, -2, -1 \} = \{ -1, -2, -3, \ldots \}$
  - $\mathbf{Z}_- = \{ x \in \mathbf{Z} \mid x < 0 \}$

The Set of Real Numbers

- **R** = The set of (all) real numbers

The Set of Rational Numbers

- **Q** = The set of (all) rational numbers.
- **Q** $= \{ x \in \mathbf{R} \mid x = p/q;\ p,q \in \mathbf{Z};\ q \neq 0 \}$

Pause and Think ...

- What is the set of natural numbers?

Lecture Topics

- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- <u>Subsets and Power Sets</u>
- Equality of Sets by Mutual Inclusion
- Universal Sets, Venn Diagrams
- Set Operations
- Set Identities
- Proving Set Identities

Subsets

- A is a subset of B, or B is a superset of A iff every member of A is a member of B.

- Notationally,
  - $A \subseteq B$ iff $\forall$ x, if $x \in A$, then $x \in B$.

- An example
  - $\{ -2, 0, 8 \} \subseteq \{ -3, -2, -1, 0, 2, 4, 6, 8, 10 \}$

Negation of $\subseteq$

- A is not a subset of B, or B is not a superset of A iff there is a member of A that is not a member of B.

- Notationally
  - $A \not\subseteq B$ iff $\exists x,\ x \in A$ and $x \notin B$.

- Example
  - $\{ 2, 4 \} \not\subseteq \{ 2, 3 \}$

Obvious Subsets

- $S \subseteq S$
- $\varnothing \subseteq S$
- Vacuously true
  - The implication "if $x \in \varnothing$, then $x \in S$" is true
- By contradiction,
  - If $\varnothing \not\subseteq S$, then $\exists x$, $x \in \varnothing$ and $x \notin S$.

Proper Subsets

- A is a proper subset of B, or B is a proper superset of A iff A is a subset of B and A is not equal to B.

- Notationally
  - $A \subset B$ iff $A \subseteq B$ and $A \neq B$

- Examples
  - If $S \neq \emptyset$, then $\emptyset \subset S$.
  - $\mathbf{Z}_{+} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$

Power Sets

- The set of all subsets of a set is called the power set of the set.
- The power set of S is P(S).
- Examples
  - $P(\varnothing) = \{ \varnothing \}$
  - $P(\{1, 2\}) = \{ \varnothing, \{1\}, \{2\}, \{1, 2\} \}$
  - $P(S) = \{ \varnothing, \ldots, S \}$

$\in$ and $\subseteq$ are Different.

- Examples
  - $1 \in \{ 1 \}$ is true
  - $1 \subseteq \{ 1 \}$ is false
  - $\{ 1 \} \subseteq \{ 1 \}$ is true

Pause and Think ...

- Which of the following statements is true?
  - $S \subseteq P(S)$
  - $S \in P(S)$
- What is $P(\{ 1, 2, 3 \})$?

Lecture Topics

- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- <u>Equality of Sets by Mutual Inclusion</u>
- Universal Sets, Venn Diagrams
- Set Operations
- Set Identities
- Proving Set Identities

Mutual Inclusion

- Sets A and B have the same members iff they mutually include
  - $A \subseteq B$ and $B \subseteq A$
- That is, $A = B$ iff $A \subseteq B$ and $B \subseteq A$.

Equality by Mutual Inclusion

- Mutual inclusion is very useful for proving the equality of two sets.
- To prove an equality, we prove two subset relationships.

An Example Showing the Equality of Sets

- Recall that **Z** = The set of (all) integers.
- Let A = { $x \in \mathbf{Z}$ | $x = 2m$ for some $m \in \mathbf{Z}$ }
- Let B = { $y \in \mathbf{Z}$ | $y = 2n - 2$ for some $n \in \mathbf{Z}$ }
- To show $A \subseteq B$, note that
  - $2m = 2(m+1) - 2 = 2n-2$
- To show $B \subseteq A$, note that
  - $2n-2 = 2(n-1) = 2m$
- That is, A = B.
- In fact, A, B both denote the set of even integers.

Pause and Think ...

- Let
  - $A = \{ x \in \mathbf{Z} \mid x^2 - 1 = 0 \}$
  - $B = \{ x \in \mathbf{Z} \mid 2x^3 - x^2 - 2x + 1 = 0 \}$
  - Show that A = B by the method of mutual inclusion.

Lecture Topics

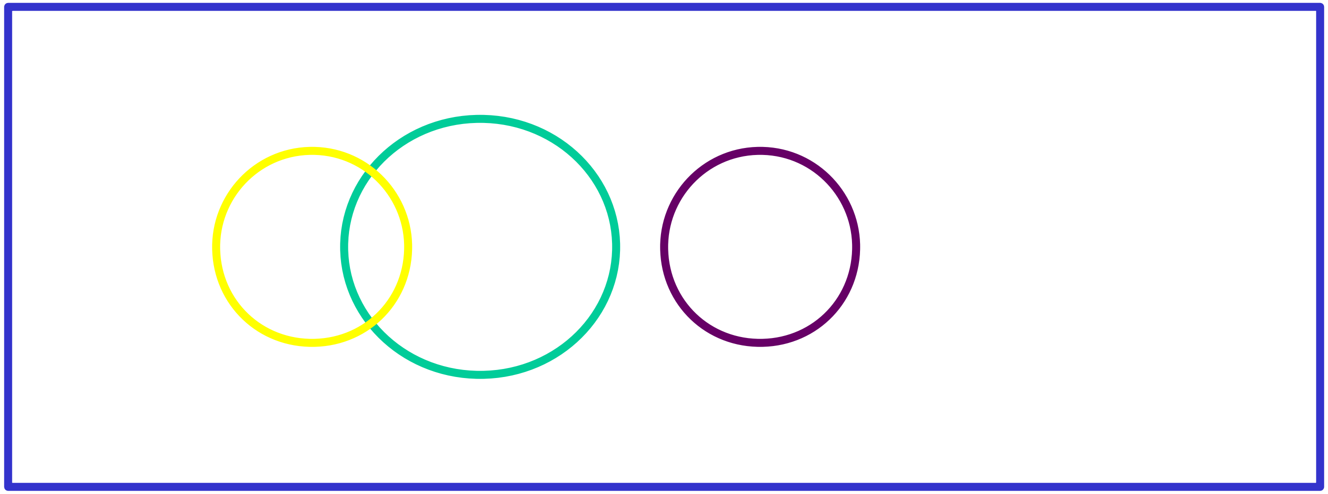
- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- Equality of Sets by Mutual Inclusion
- <u>Universal Sets, Venn Diagrams</u>
- Set Operations
- Set Identities
- Proving Set Identities

Universal Sets

- Depending on the context of discussion,
  - define a set U such that all sets of interest are subsets of U.
  - The set U is known as a universal set.
- For example,
  - when dealing with integers, U may be **Z**
  - when dealing with plane geometry, U may be the set of all points in the plane

Venn Diagrams

- To visualise relationships among some sets
- Each subset (of U) is represented by a circle inside the rectangle



Pause and Think ...

- If **Z** is a universal set, can we replace **Z** by **R** as the universal set?

Lecture Topics

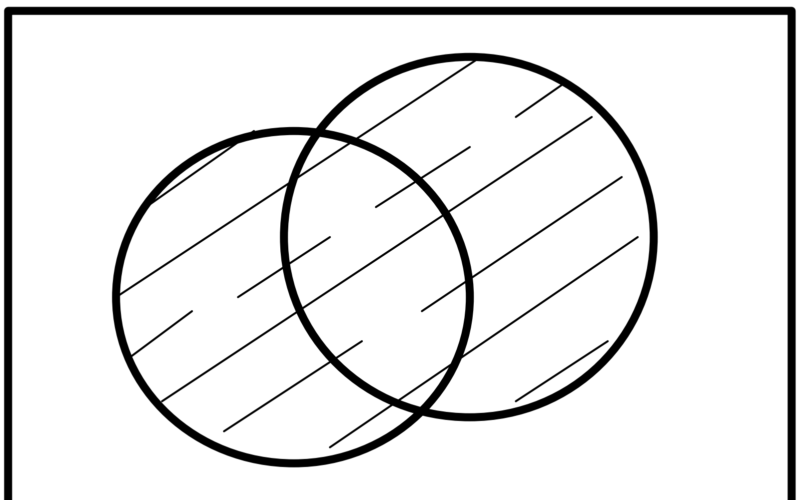
- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- Equality of Sets by Mutual Inclusion
- Universal Sets, Venn Diagrams
- Set Operations
- Set Identities
- Proving Set Identities

Set Operations

- Let A, B be subsets of some universal set U.
- The following set operations create new sets from A and B.
- Union
  - $A \cup B = \{ x \in U \mid x \in A \text{ or } x \in B \}$
- Intersection
  - $A \cap B = \{ x \in U \mid x \in A \text{ and } x \in B \}$
- Difference
  - $A - B = A \setminus B = \{ x \in U \mid x \in A \text{ and } x \notin B \}$
- Complement
  - $A^c = U - A = \{ x \in U \mid x \notin A \}$

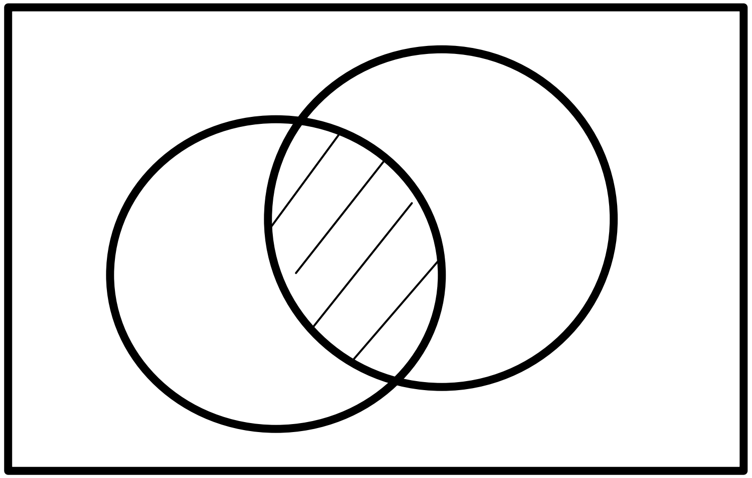
Set Union

- An example
  - { 1, 2, 3 } $\cup$ { 2, 3, 4, 5 } = { 1, 2, 3, 4, 5 }
- the Venn diagram



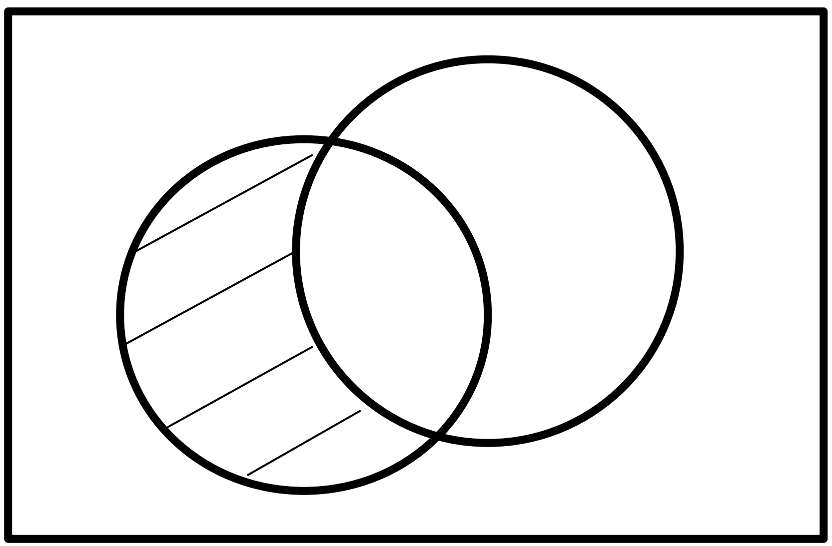
Set Intersection

- An example
  - $\{ 1, 2, 3 \} \cap \{ 2, 3, 4, 5 \} = \{ 2, 3 \}$
- the Venn diagram



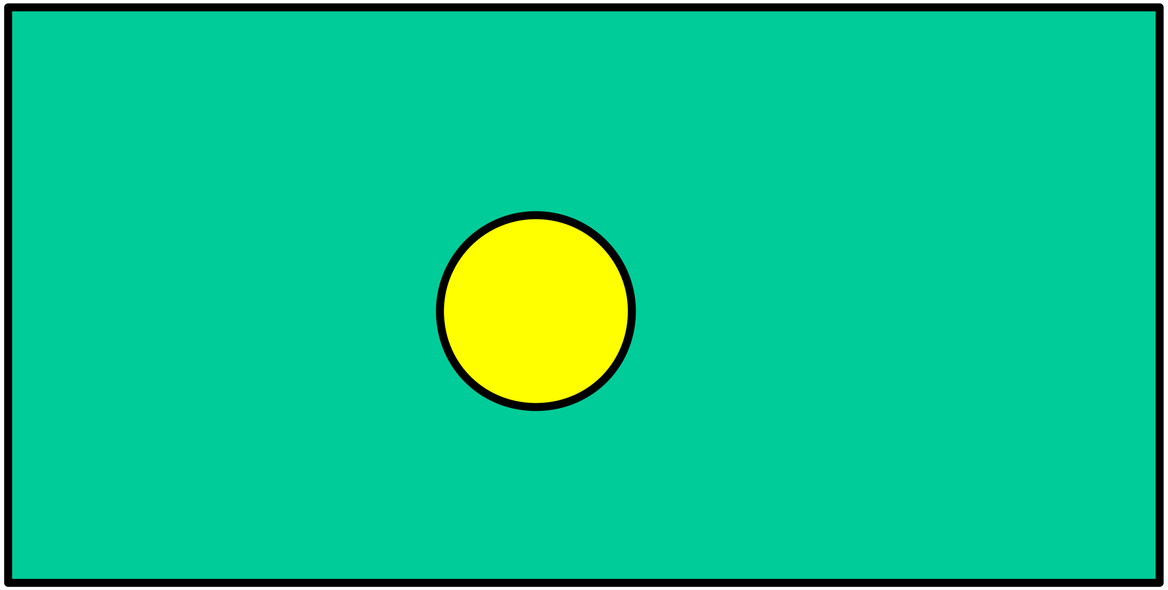
Set Difference

- An example
  - { 1, 2, 3 } - { 2, 3, 4, 5 } = { 1 }
- the Venn diagram



Set Complement

- The Venn diagram



Pause and Think ...

- Let $A \subseteq B$.
  - What is $A - B$?
  - What is $B - A$?
- If $A, B \subseteq C$, what can you say about $A \cup B$ and C?
- If $C \subseteq A, B$, what can you say about C and $A \cap B$?

Lecture Topics

- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- Equality of Sets by Mutual Inclusion
- Universal Sets, Venn Diagrams
- Set Operations
- <u>Set Identities</u>
- Proving Set Identities

Basic Set Identities

- Commutative laws
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Associative laws
  - $(A \cup B) \cup C = A \cup (B \cup C)$
  - $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributive laws
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Basic Set Identities (continued)

- $\varnothing$ is the identity for union
  - $\varnothing \cup A = A \cup \varnothing = A$
- U is the identity for intersection
  - $A \cap U = U \cap A = A$
- Double complement law
  - $(A^c)^c = A$
- Idempotent laws
  - $A \cup A = A$
  - $A \cap A = A$

Basic Set Identities (continued)

- De Morgan's laws
  - $(A \cup B)^c = A^c \cap B^c$
  - $(A \cap B)^c = A^c \cup B^c$

Pause and Think ...

- What is
  - $(A \cap B) \cap (A \cup B)$?

- What is
  - $(A \cup B) \cup (A \cap B)$?

Lecture Topics

- Sets and Members, Equality of Sets
- Set Notation
- The Empty Set and Sets of Numbers
- Subsets and Power Sets
- Equality of Sets by Mutual Inclusion
- Universal Sets, Venn Diagrams
- Set Operations
- Set Identities
- <u>Proving Set Identities</u>

Proof Methods

- There are many ways to prove set identities.
- The methods include
  - applying existing identities,
  - building a membership table,
  - using mutual inclusion.

A Proof by Mutual Inclusion

- Prove that $(A \cap B) \cap C = A \cap (B \cap C)$.
- First show that $(A \cap B) \cap C \subseteq A \cap (B \cap C)$.
- Let $x \in (A \cap B) \cap C$,
  - $x \in (A \cap B)$ and $x \in C$
  - $x \in A$ and $x \in B$ and $x \in C$
  - $x \in A$ and $x \in (B \cap C)$
  - $x \in A \cap (B \cap C)$
- Then show that $A \cap (B \cap C) \subseteq (A \cap B) \cap C$.

Pause and Think ...

- To prove that $A \cup A^c = U$ by mutual inclusion, do you have to prove the inclusion $A \cup A^c \subseteq U$?

- To prove that $A \cap A^c = \emptyset$ by mutual inclusion, do you have to prove the inclusion $\emptyset \subseteq A \cap A^c$?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- Equality of Functions
- Some Special Functions
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- The Values of Function Composition

“High School” Functions

- Functions are usually given by formulas.
- Examples
  - $f(x) = \sin(x)$
  - $f(x) = e^x$
  - $f(x) = x^n$
  - $f(x) = \log x$
- A function is a computation rule that changes one value to another value.
- Effectively, a function associates, or relates, one value to another value.

“General” Functions

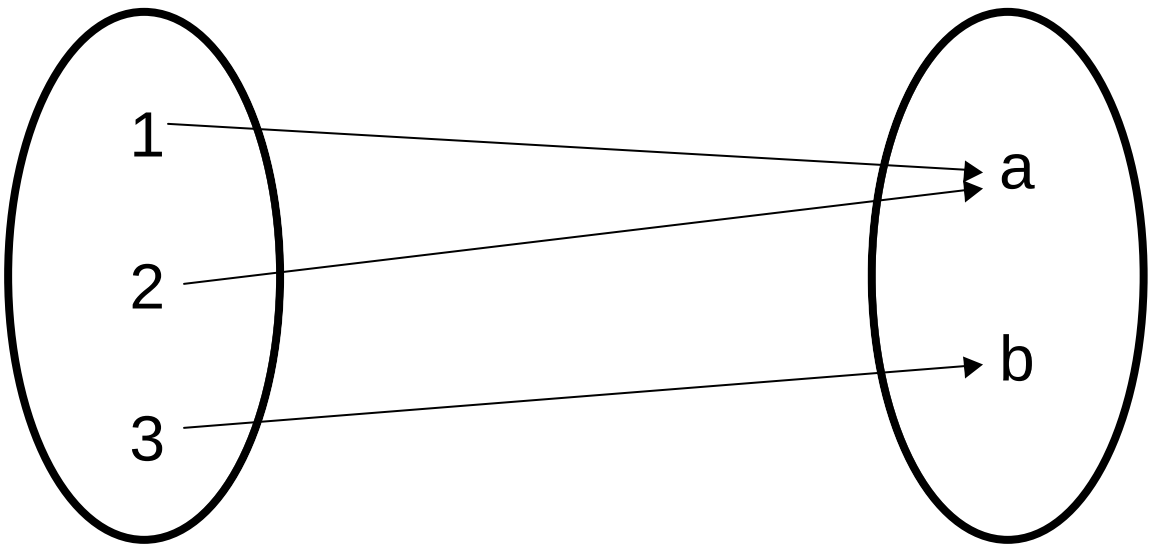
- Since a function relates one value to another, we can think of a function as relating one object to another object. Objects need not be numbers.
- In the previous examples, the function f relates the object x to the object f(x).
- Usually we want to be able to relate each object of interest to only one object.
- That is, a function is a single-valued and exhaustive relation.

Functions

- A relation f from A to B is a function from A to B iff
  - for every $x \in A$, there exists a unique $y \in B$ such that x f y, or equivalently, $(x,y) \in f$.
- Functions are also known as transformations, maps, and mappings.

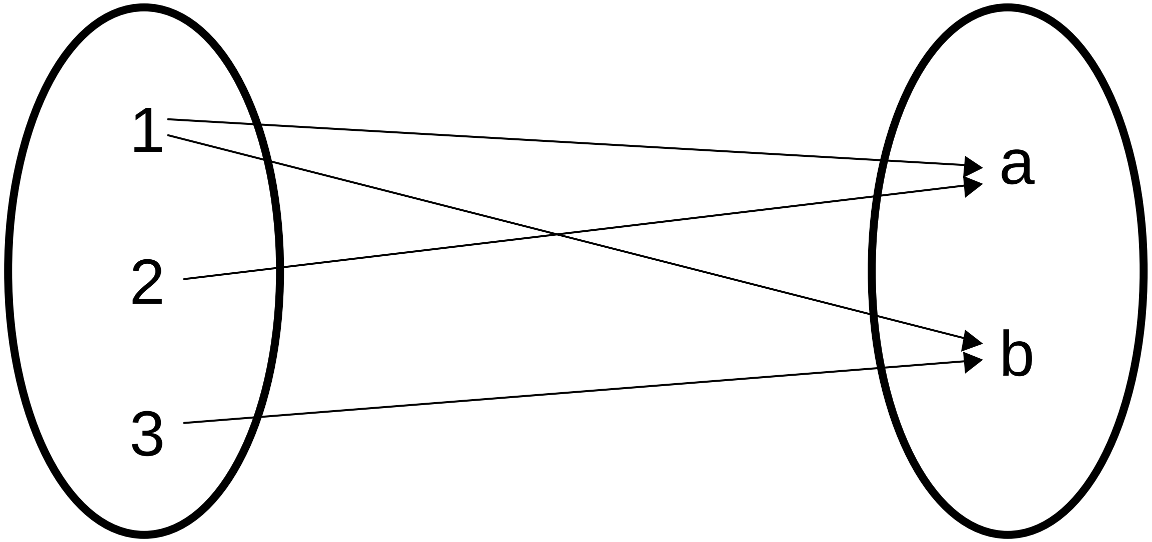
Example 1

- Let A = { 1, 2, 3 } and B = { a, b }.
- R = { (1,a), (2,a), (3,b) } is a function from A to B.



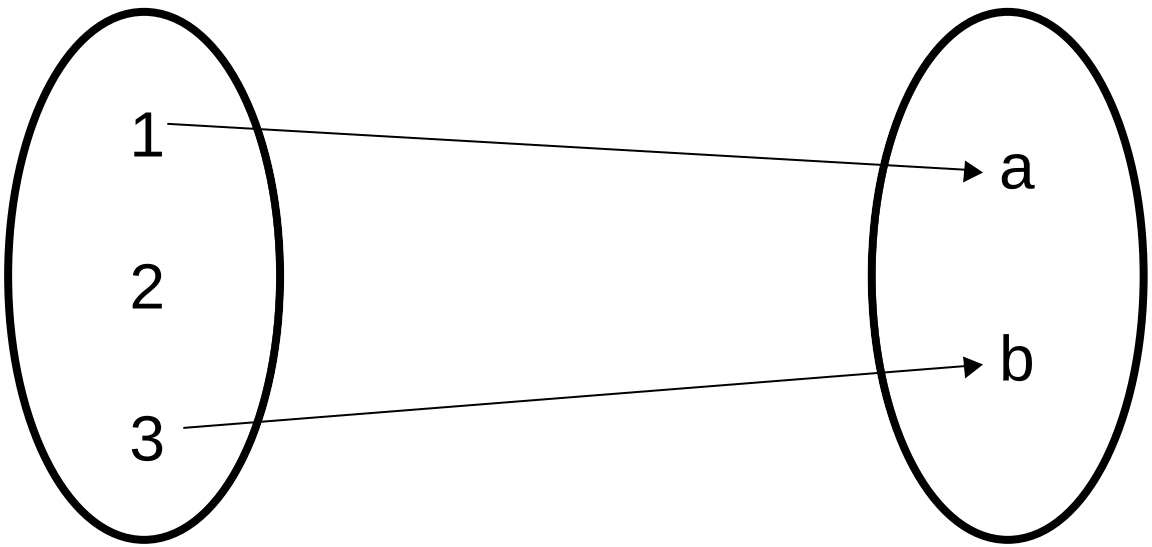
Example 2

- Let A = { 1, 2, 3 } and B = { a, b }.
- S = { (1,a), (1,b), (2,a), (3,b) } is not a function from A to B.



Example 3

- Let A = { 1, 2, 3 } and B = { a, b }.
- T = { (1,a), (3,b) } is not a function from A to B.



Pause and Think ...

- Is A x { a }, where a $\in$ A, a function from A to A?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- Equality of Functions
- Some Special Functions
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- The Values of Function Composition

Function Notation

- Let f be a relation from A to B. That is, $f \subseteq AxB$.
- If the relation f is a function,
  - we write $f : A \rightarrow B$.
  - If $(x,y) \in f$, we write $y = f(x)$.
- Usually we use f, g, h, … to denote relations that are functions.

Notational Convention

- Sometimes functions are given by stating the rule of transformation, for example, $f(x) = x+1$.

- This should be taken to mean

  - $f = \{ (x,f(x)) \in AxB \mid x \in A \}$

  - where A and B are some understood sets.

Pause and Think ...

- Let $f \subseteq A \times B$ be a relation and $(x,y) \in f$.
- Does the expression $f(x) = y$ make sense?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- <u>Values, images, inverse images, pre-images</u>
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- Equality of Functions
- Some Special Functions
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- The Values of Function Composition

Values, Images

- Let $f : A \rightarrow B$.
- Let $y = f(x)$.
  - That is, $x \, f \, y$, equivalently, $(x,y) \in f$.
- The object y is called
  - the image of x under the function f, or
  - the value of f at x.

Inverse Images, Pre-images

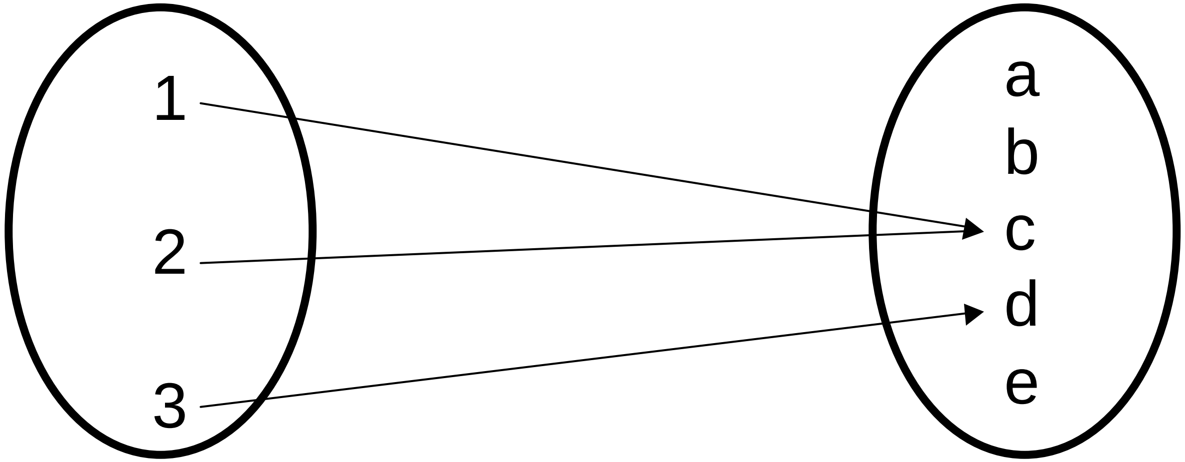
- Let $f : A \rightarrow B$ and $y \in B$.
- Define
  - $f^{-1}(y) = \{ x \in A \mid f(x) = y \}$
- The set $f^{-1}(y)$ is called the inverse image, or pre-image of y under f.

Images and Pre-images of Subsets

- Let $f : A \to B$ and $X \subseteq A$ and $Y \subseteq B$.
- We define
  - $f(X) = \{ f(x) \in B \mid x \in X \}$
  - $f^{-1}(Y) = \{ x \in A \mid f(x) \in Y \}$

Examples

- Let $f : A \rightarrow B$ be given as follows



- $f(\{1,3\}) = \{ c, d \}$
- $f^{-1}(\{ a, d \}) = \{ 3 \}$

Some Properties

- Let $f : A \to B$ and $X \subseteq A$ and $Y \subseteq B$.
- Clearly we have
  - $f(A) \subseteq B$
  - $f^{-1}(B) = A$ because every element of A has an image in B

Pause and Think ...

- Let $f : A \to B$ and $X \subseteq A$ and $Y \subseteq B$.

- If there are n elements in X, how many elements are there in f(X)?

- If there are n elements in Y, how many elements are there in $f^{-1}(Y)$?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- <u>Codomains, Domains, Ranges</u>
- Sets of Images and Pre-Images
- Equality of Functions
- Some Special Functions
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- The Values of Function Composition

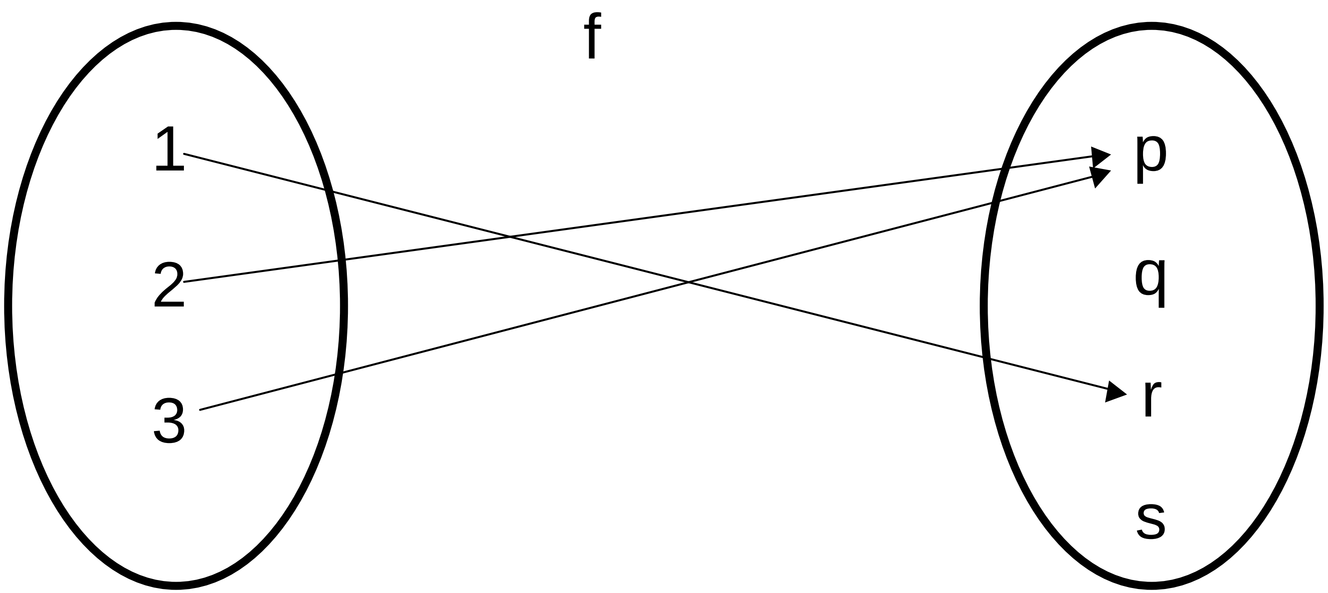
Domains

- Let f : A $\rightarrow$ B.
- The domain of function f is the set A.

Codomains and Ranges

- Let f : A $\rightarrow$ B.
- The codomain of function f is the set B.
- The range of function f is the set of images of f.
  - Clearly, the range of f is f(A).

Example 1



- The domain is { 1, 2, 3 }.
- The codomain is { p, q, r, s }.
- The range is { p, r }.

Example 2

- Consider exp : $\mathbf{R} \rightarrow \mathbf{R}$. That is, $\exp(x) = e^x$.
- The domain and codomain of exp are both $\mathbf{R}$.
- The range of exp is $\mathbf{R}_+$, the set of positive real numbers.

Pause and Think ...

- Consider cos : $\mathbf{R} \rightarrow \mathbf{R}$.
- What are the domain, codomain, and range of cos?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- <u>Sets of Images and Pre-Images</u>
- Equality of Functions
- Some Special Functions
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- The Values of Function Composition

Images and Pre-images of Subsets

- Let $f : A \to B$.
- Let $X, X' \subseteq A$ and $Y, Y' \subseteq B$.
- We shall call $f(X)$ the image of X instead of the set of images of members of X. Similarly, we shall simply call $f^{-1}(Y)$ the preimage of Y.
- We have
  - $f(f^{-1}(Y)) \subseteq Y$ and $X \subseteq f^{-1}(f(X))$
  - $f(X \cup X') = f(X) \cup f(X')$, $f(X \cap X') \subseteq f(X) \cap f(X')$
  - $f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y')$
  - $f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y')$

$f(f^{-1} (Y)) \subseteq Y$

- It is possible to have strict inclusion.
  - When the range of f is a proper subset of its codomain, we may take Y = B to obtain
  - $f(f^{-1} (B)) = f(A) \subset B$
- To show inclusion,
  - let $y \in f(f^{-1} (Y))$.
  - $\exists\, x \in f^{-1} (Y)$ such that $f(x) = y$.
  - We have $f(x) \in Y$.
  - That is, $y \in Y$

$f(X \cup X') = f(X) \cup f(X')$

- We can easily show that
  - $f(X \cup X') \supseteq f(X) \cup f(X')$.
- This is because $X \cup X' \supseteq X$, so
  - $f(X \cup X') \supseteq f(X)$.
- Similarly, we have $f(X \cup X') \supseteq f(X')$.
- Consequently, $f(X \cup X') \supseteq f(X) \cup f(X')$.

$f(X \cup X') = f(X) \cup f(X')$

- To show $f(X \cup X') \subseteq f(X) \cup f(X')$,
  - let $y \in f(X \cup X')$.
- $\exists\, x \in X \cup X'$ such that $f(x) = y$.
- If $x \in X$, then $y \in f(X)$; otherwise, $y \in f(X')$. This means $y \in f(X) \cup f(X')$.
- That is, $f(X \cup X') \subseteq f(X) \cup f(X')$.

Pause and Think ...

- What do the given set expressions become when f is the identity function?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- <u>Equality of Functions</u>
- Some Special Functions
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- The Values of Function Composition

Equality of Functions

- Let $f : A \rightarrow B$ and $g : C \rightarrow D$.
- We define function f = function g iff
  - set f = set g
- Note that this forces $A = C$ but allows $B \neq D$.
  - Some require $B = D$ as well.

A Proof that Set f = Set g Implies Domain f = Domain g

- Let $f : A \to B$ and $g : C \to D$ and set f = set g.
- Let $x \in A$.
  - $(x,f(x)) \in f$
  - But f = g as sets
  - $(x,f(x)) \in g$
  - That is $x \in C$.
  - Consequently, $A \subseteq C$.
- Similarly, we have $C \subseteq A$.
- That is, $A = C$.

A Proof that Set f = Set g Implies $f(x) = g(x)$ for all $x \in A$

- Let $f, g : A \to B$ and set f = set g.
- Let $x \in A$.
  - $(x,f(x)) \in f$
  - But f = g as sets
  - $(x,f(x)) \in g$
  - That is $(x,f(x)), (x,g(x)) \in g$.
  - Since g is a function, so $f(x) = g(x)$.

Example

- We consider
  - exp : $\mathbf{R} \to \mathbf{R}$ and
  - exp : $[0,1] \to \mathbf{R}$
  - as two different functions though the computation rule is the same --- $\exp(x) = e^x$.

Pause and Think ...

- Let f and g be functions such that $f(x) = g(x)$ on some set A. Can we conclude that function f = function g?

Lecture Topics

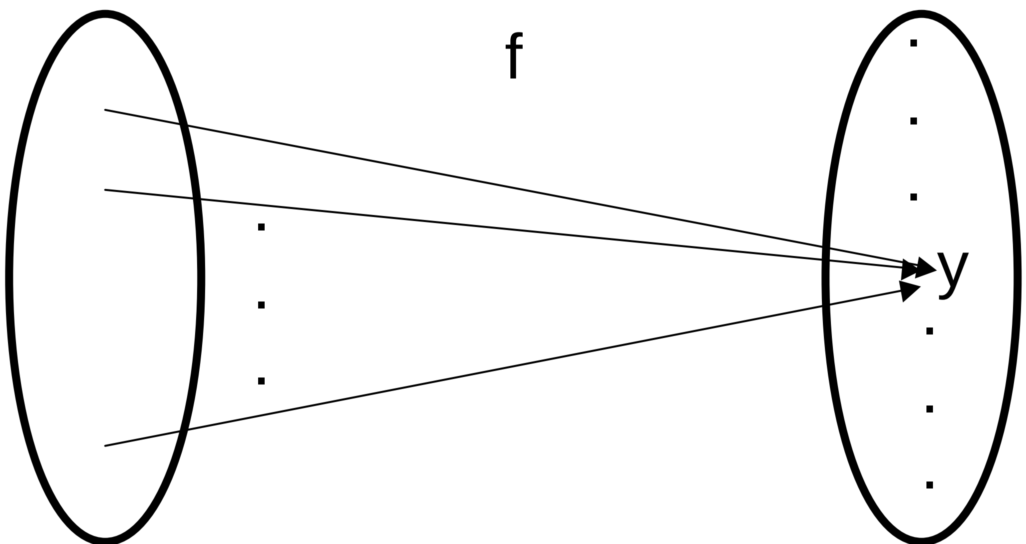
- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- Equality of Functions
- <u>Some Special Functions</u>
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- The Values of Function Composition

Identity Functions

- Consider the identity relation I_A on the set A.
- Clearly, for every $x \in A$, I_A relates x to an unique element of A that is itself.
- Consequently, we have $I_A : A \to A$.
- I_A is also called the identity function on A.

Constant Functions

- Let f : A $\rightarrow$ B.
- If f(A) = { y } for some y $\in$ B, f is called a constant function of value y.



Characteristics Functions

- Consider some universal set U.
- Let $A \subseteq U$.
- The function $\chi_A : U \to \{ 0, 1 \}$ defined by
  - $\chi_A(x) = 1$, if $x \in A$,
  - $\chi_A(x) = 0$, if $x \in A^c$;
  - is called the characteristic function of A.

Pause and Think ...

- Let f : **R** $\rightarrow$ **R**.
  - If f is a constant function, what does its graph on the Cartesian X-Y plane look like?
  - If f is the identity function, what does its graph on the Cartesian X-Y plane look like?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- Equality of Functions
- Some Special Functions
- <u>Unary and Binary Operations as Functions</u>
- The Composition of Two Functions is a Function
- The Values of Function Composition

Unary Operations

- A unary operation on a set A acts on an element of A and produces another element of A.
- Clearly, a unary operation uop can be thought of as a function $f : A \to A$ with $f(x) = uop(\ x\ )$.
- Conversely, a function from A to A can be regarded as a unary operation on A.

Example 1

- Let U be some universal set.
- The complement operation on P(U) can be represented as a function
  - f: $P(U) \rightarrow P(U)$ with $f(A) = A^c$.

Binary Operations

- A binary operation on a set A acts on two elements of A and produces another element of A.

- Clearly, a binary operation bop can be represented as a function
  - f : AxA $\rightarrow$ A with f((a,b)) = a bop b.
  - We write f(a,b) instead of f((a,b)).

- Conversely, a function from AxA to A can be regarded as a binary operation on A.

Example 1

- Let U be some universal set.
- The union operation on P(U) can be represented as a function f: P(U)xP(U)$\to$ P(U) with f(A,B) = A$\cup$B.

Pause and Think ...

- Let U = { 0, 1 }.
- Give the set representations of the functions for unary complement operation and the binary intersection operation.

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- Equality of Functions
- Some Special Functions
- Unary and Binary Operations as Functions
- <u>The Composition of Two Functions is a Function</u>
- The Values of Function Composition

Function Composition

- Let f : A $\to$ B and g : B $\to$ C.
- Since relations can be composed and functions are relations, so functions can be composed like relation composition.
- So relations f and g can be composed and their composition is gf.
- Clearly gf is a relation from A to C.
- But is gf a function?

Function Composition Gives a Function

- Let $f : A \to B$ and $g : B \to C$.
- We want to show that $gf : A \to C$.
  - That is, the composition of two functions is again a function.
- We have to show for any $x \in A$, there is a unique $z \in C$, such that $(x,z) \in gf$.

Existency Proof

- Let $x \in A$.
- Since f is a function from A to B, there is a unique $y \in B$ such that $(x,y) \in f$.
- For this $y \in B$, there is a unique $z \in C$ such that $(y,z) \in g$ because g is a function from B to C.
- That is, $(x,z) \in gf$.

Uniqueness Proof

- Let (x,z), (x,z') $\in$ gf.
- There exist y, y' $\in$ B such that
  - (x,y) $\in$ f, (y,z) $\in$ g
  - (x,y') $\in$ f, (y',z') $\in$ g
- But f is a function, so y = y'.
- Now we have (y,z), (y,z') $\in$ g.
- But g is a function, so z = z'.

Pause and Think ...

- Can you compose cos and log to obtain the composition (log cos)?

- Can you compose log and exp to obtain the composition (exp log)?

Lecture Topics

- From “High School” Functions to “General” Functions
- Function Notation
- Values, images, inverse images, pre-images
- Codomains, Domains, Ranges
- Sets of Images and Pre-Images
- Equality of Functions
- Some Special Functions
- Unary and Binary Operations as Functions
- The Composition of Two Functions is a Function
- <u>The Values of Function Composition</u>

The Values of Function Composition

- Let $f : A \rightarrow B$ and $g : B \rightarrow C$.
- Since $gf : A \rightarrow C$, for any $x \in A$, there is a $z \in C$, such that $(gf)(x) = z$.
- That is, $(x,z) \in gf$.
- By the definition of function composition, there is a $y \in B$, such that $(x,y) \in f$ and $(y,z) \in g$.
- Since f and g are function, we can write $f(x) = y$ and $g(y) = z$.
- Substituting $y = f(x)$ in $g(y) = z$, we have $g(f(x))=z$.
- That is,
  - $(gf)(x) = g(f(x))$.

The Values of Function Compositions

- Let $f : A \to B$, $g : B \to C$, $h : C \to D$.
- Since relation composition are associative and functions are relations, we have
  - $h(gf) = (hg)f$
- Furthermore, we have
  - $(h(gf))(x) = h((gf)(x)) = h(g (f(x)))$
  - and
  - $((hg)f)(x) = (hg)(f(x)) = h(g (f(x)))$
- That is,
  - $(h(gf))(x) = ((hg)f)(x) = h(g(f(x)))$

Pause and Think ...

- Let $f(x) = x+1$, $g(x) = x^2$, and $h(x) = 1/(1+x^2)$ be functions **R** from to **R**.
  - Is hgf a function?
  - If so, what is the value of (hgf)(x)?

Lecture Topics

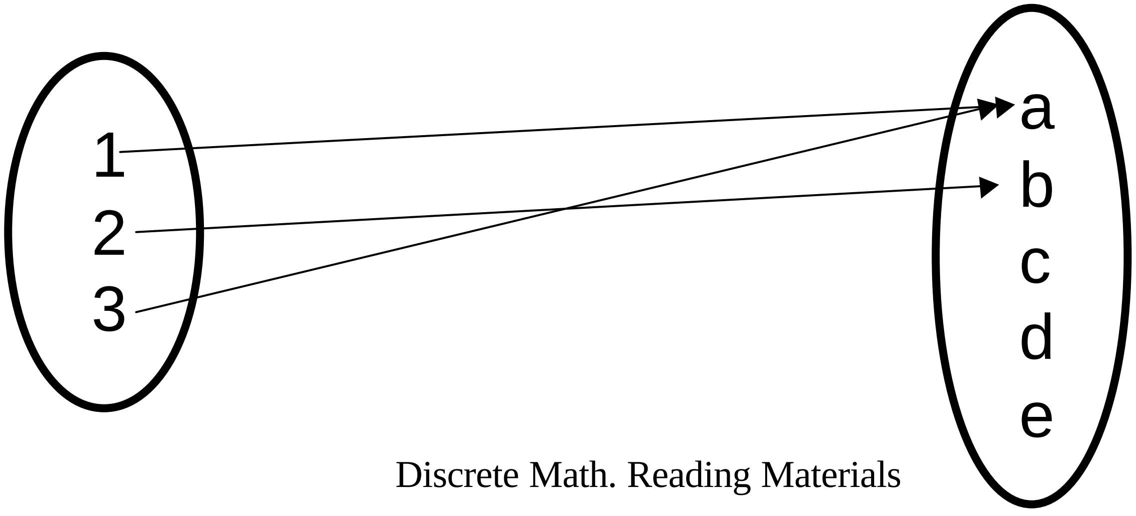
- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function.
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- Some Function Composition Properties

One-To-One Functions, Injections

- Let $f : A \to B$.
- The function f is one-to-one iff
  - for any $x, x' \in A$,
  - if $f(x) = f(x')$ then $x = x'$
  - Equivalently,
  - if $x \neq x'$ then $f(x) \neq f(x')$.
- In words, a function is one-to-one iff it maps distinct elements to distinct images.
- A one-to-one function is also called an injection.
- We abbreviate one-to-one as 1-1.

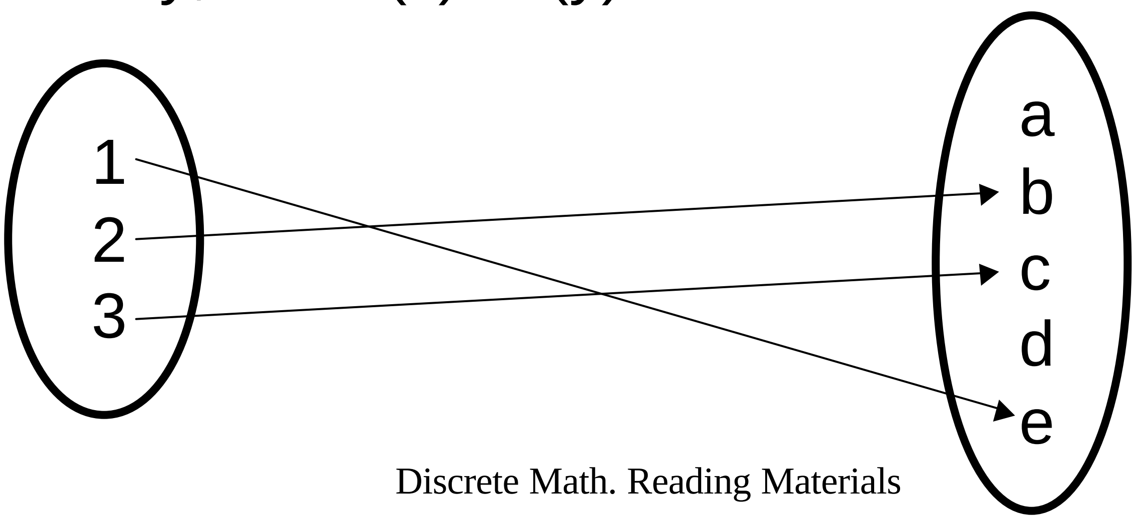
Example 1

- Let A = { 1, 2, 3 }.
- Let B = { a, b, c, d, e }
- Let f = { (1,a), (2,b), (3,a) }
- The function f is not 1-1 because
  - f(1) = f(3) = a but1 $\neq$ 3



Example 2

- Let A = { 1, 2, 3 }.
- Let B = { a, b, c, d, e }
- Let f = { (1,e), (2,b), (3,c) }
- The function f is 1-1 because
  - if $x \neq y$, then $f(x) \neq f(y)$



Example 3

- Let f : **Z** ® **Z** with $f(x) = x^2$.
- The function f is not 1-1 because $f(x) = f(-x)$.

- Let g : $\mathbf{Z}_+$ ® **Z** with $g(x) = x^2$.
- The function g is 1-1 because $x^2 = y^2$ implies $x = y$.

Pause and Think ...

- How many 1-1 functions are there from {1,2,3} to itself?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- Some Function Composition Properties

Composition of One-To-One Functions

- Theorem
  - Let $f : A \to B$, $g : B \to C$.
  - If both f and g are 1-1, then g f is also 1-1.
- That is, the composition of 1-1 functions is again 1-1.

Proof

- Let $(gf)(x) = (gf)(y)$
- $g(f(x)) = g(f(y))$
- Since g is 1-1, $f(x) = f(y)$
- Since f is 1-1, $x = y$
- That is, gf is a 1-1 function.

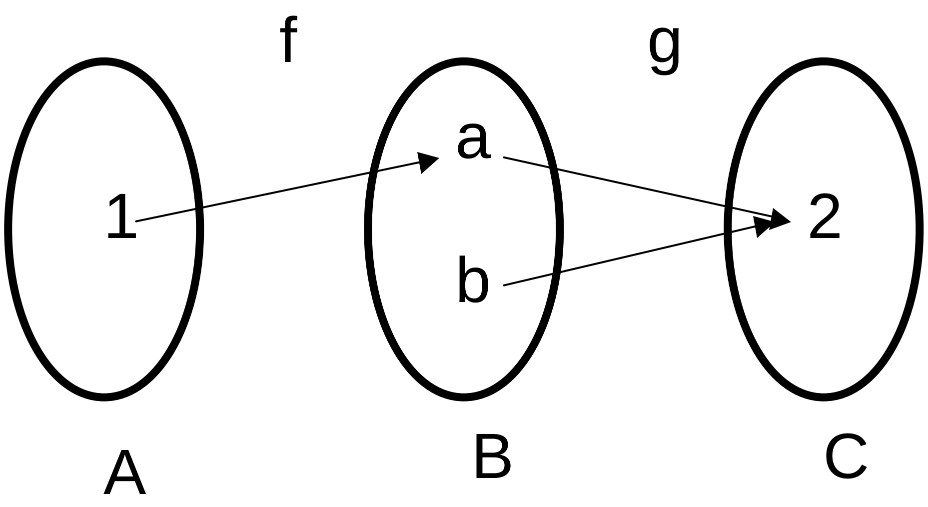
The Converse is Almost True

- Let $f : A \rightarrow B$, $g : B \rightarrow C$. Let $gf : A \rightarrow C$ be 1-1.

- Then f is 1-1 but g need not be 1-1.
- Proof
  - Let $f(x) = f(y)$
  - Then $g(f(x)) = g(f(y))$
  - $(gf)(x) = (gf)(y)$
  - $x = y$
  - That is, f is 1-1.

The Converse is False

- Let $f : A \to B$, $g : B \to C$. Let $gf : A \to C$ be 1-1.
- The following is an example that g is not 1-1.



Pause and Think ...

- Let $f : A \to B$, $g : B \to C$. Let $gf : A \to C$ be not 1-1.
  - Are f and g both not 1-1?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- Some Function Composition Properties

Onto Functions, Surjections

- Let $f : A \to B$.
- The function f is onto iff
  - for any $y \in B$,
  - there exists some $x \in A$,
  - such that $f(x) = y$.
- In words, a function is onto iff every element in the codomain has a non-empty pre-image.

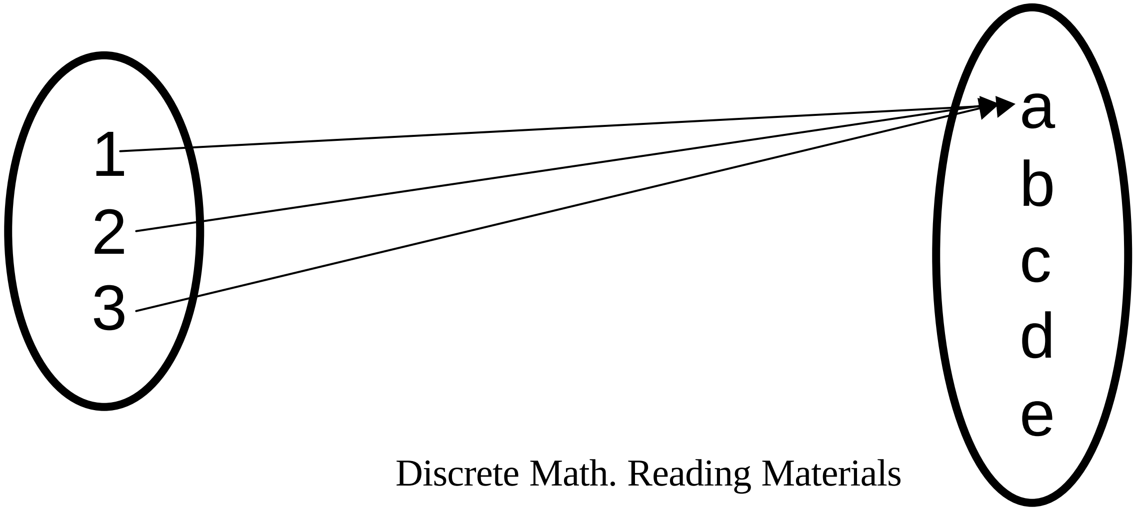
- A onto function is also called a surjection.

Onto Means Range is Codomain

- Let $f : A \to B$ be onto.
- Onto implies $B \subseteq f(A)$.
- Proof
  - Let $y \in B$.
  - There exists $x \in A$ such that $f(x) = y$.
  - $y \in f(A)$
  - That is, $B \subseteq f(A)$.
- But $f(A) \subseteq B$.
- That is, $B = f(A)$.

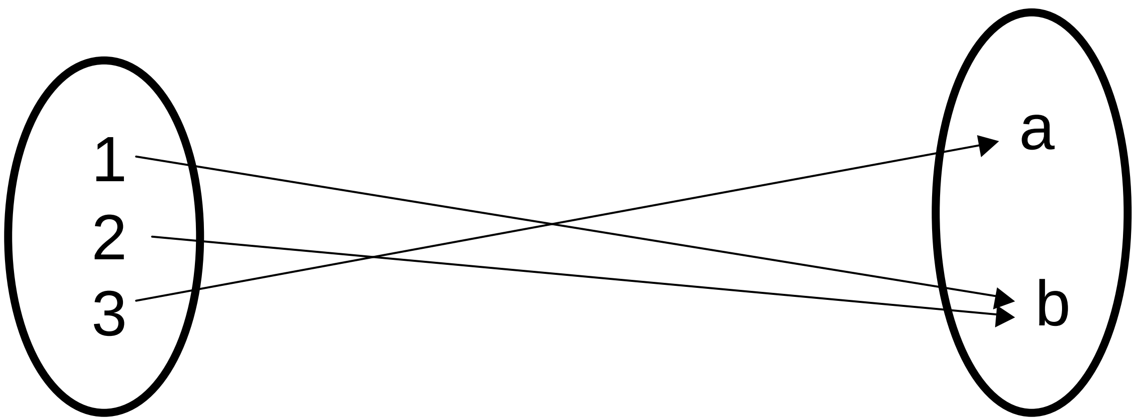
Example 1

- Let A = { 1, 2, 3 } and B = { a, b, c, d, e }
- Let f = { (1,a), (2,a), (3,a) }
- The function f is not onto because there is a b $\in$ B without any x $\in$ A such that f(x) = b.



Example 2

- Let $A = \{ 1, 2, 3 \}$ and $B = \{ a, b \}$
- Let $f = \{ (1,b), (2,b), (3,a) \}$
- The function f is onto because for any $y \in B$ there is a $x \in A$ such that $f(x) = y$.



Example 3

- Let f : **Z** ® **Z** with $f(x) = x^2$.
  - The function f is not onto because there is no integer x such that f(x) = -1.

- Let g : **Z** ® $\mathbf{Z}_+$ with g(x) = |x| + 1.
  - It is not hard to check that g is onto.

Pause and Think ...

- Let g : **Z** ® $\mathbf{Z}_+$ with $g(x) = |x|+2$. Is g onto?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- <u>Composition of Surjections</u>
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- Some Function Composition Properties

Composition of Onto Functions

- Theorem
  - Let $f : A \to B$, $g : B \to C$.
  - If both f and g are onto, then $g \circ f$ is also onto.
- That is, the composition of onto functions is again onto.

Proof

- Let $z \in C$.
- Since $g : B \to C$ is onto, there is a $y \in B$ such that
  - $g(y) = z$.
- Since $f : A \to B$ is onto, there is a $x \in A$ such that
  - $f(x) = y$.

- Combining, we have
  - $(gf)(x) = g(f(x)) = g(y) = z$

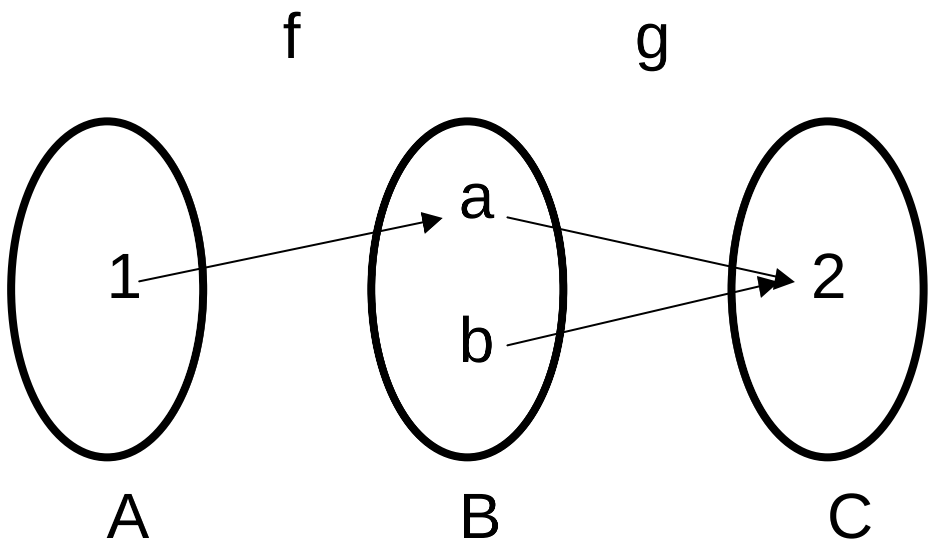
- That is, the composition gf is onto.

The Converse is Almost True

- Let $f : A \to B$, $g : B \to C$. Let $gf : A \to C$ be onto.
- Then g is onto but f need not be onto.
- Proof
  - Since gf is onto, for any $z \in C$, there is a $x \in A$ such that $(gf)(x) = z$.
  - That is $g(f(x)) = z$.
  - But $f(x) \in B$.
  - So for any $z \in C$, there is a $y = f(x) \in B$ such that $g(y) = x$.
  - That is, g is onto.

The Converse is False

- Let $f : A \to B$, $g : B \to C$. Let $gf : A \to C$ be onto.
- The following is an example that f is not onto.



Pause and Think ...

- Let $f : A \rightarrow B$, $g : B \rightarrow C$. Let $gf : A \rightarrow C$ be not onto.

  - Are f and g also not onto?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- <u>One-To-One Correspondences, Bijections</u>
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- Some Function Composition Properties

1-1 and Onto Functions, Bijections, 1-1 Correspondences

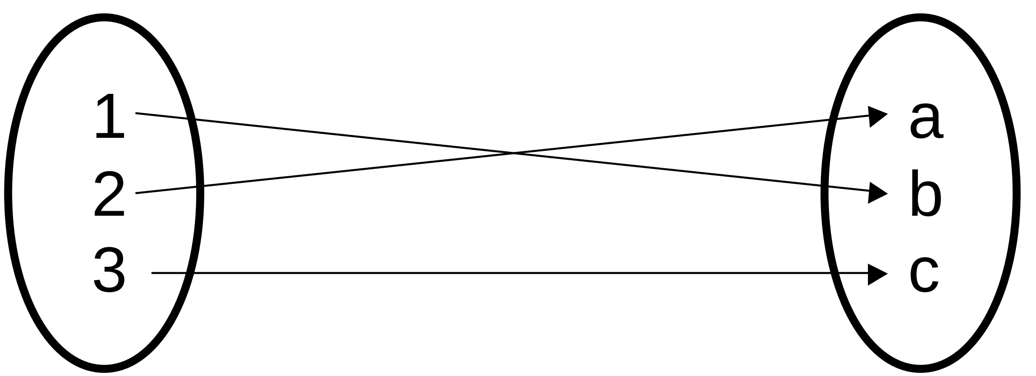
- Let $f : A \to B$.

- The function f is a 1-1 correspondence iff f is 1-1 and onto.

- A 1-1 correspondence is also called a bijection.

Example 1

- Let A = { 1, 2, 3 } and B = { a, b, c }.
- Let f = { (1,b), (2,a), (3,c) }.
- The function f is a 1-1 correspondence because it is 1-1 and onto.



Example 2

- Let f : **Z** ® **Z** and f(x) = x - 1.
- Since x-1 = y-1 implies x = y, so f is 1-1.
- Since f(y+1) = y, so f is onto.
- The function f is a 1-1 correspondence.

Example 3

- Let f : **Z** ® $\mathbf{Z}_{+}$ and f(x) = |x| + 1.
- Since f(-x) = f(x) but -x ≠ x for non-zero x, f is not 1-1.
- When y > 0, we have f(y-1) = y. This shows that f is onto.
- Since f is onto but not 1-1, so f is not a 1-1 correspondence.

Pause and Think ...

- How many 1-1 correspondences are there from {1,2,3} to itself?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- <u>Composition of Bijections</u>
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- Some Function Composition Properties

Composition of 1-1 Correspondences

- Theorem
  - Let f : A $\rightarrow$ B, g : B $\rightarrow$ C.
  - If both f and g are 1-1 correspondences, then g f is also a 1-1 correspondence.
- That is, the composition of 1-1 correspondences is a 1-1 correspondence.

Proof

- Since f and g are 1-1, so is gf.
- Since f and g are onto, so is gf.
- Since gf is 1-1 and onto, gf is a 1-1 correspondence.

The Converse is Almost True

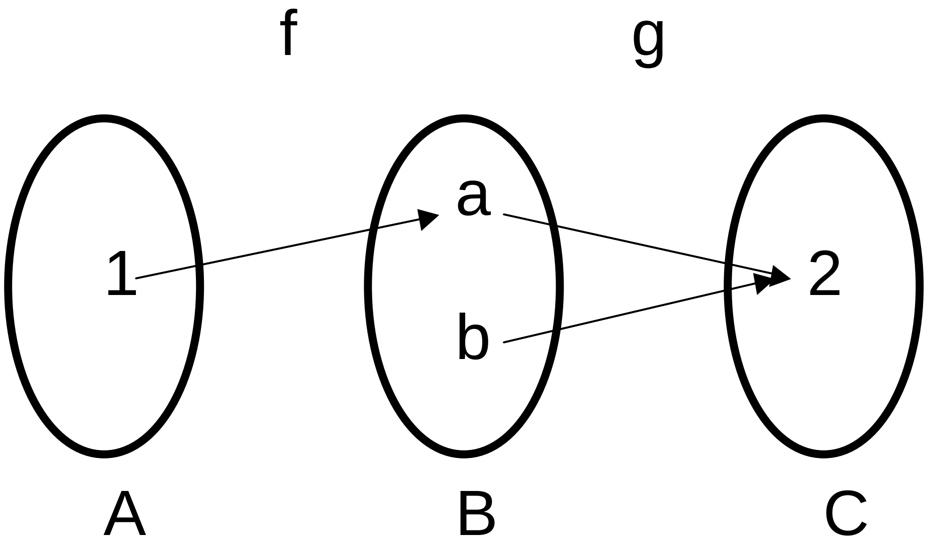
- Since gf is 1-1,
  - we have shown that f is 1-1,
  - but g need not be 1-1.

- Since gf is onto,
  - we have shown that g is onto,
  - but f need not be onto.

- That is, f and g need not be 1-1 correspondences.

The Converse is False

- The following example shows that gf is a 1-1 correspondence from A to C, but neither f nor g is a 1-1 correspondence.



Making an Injection a Bijection

- Let f : A $\rightarrow$ B be 1-1.
- Let C = f(B).
- Clearly, f : A $\rightarrow$ C is a bijection.
  - Proof:
  - f remains 1-1
  - f has become onto.

Pause and Think ...

- Let $f : A \rightarrow B$, $g : B \rightarrow C$. If $gf : A \rightarrow C$ is not a bijection, are f and g also not bijections?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- Some Function Composition Properties

Inverse Functions

- Let A = { 0, 1 }, B = { p, q }, f = { (0,p), (1,p) }.
- Clearly f is a function from A to B.
- Clearly f^{-1} = { (p,0), (p,1) } is a relation from B to A but it is not a function from B to A.
- A function is invertible iff its inverse is also a function.

Theorem

- Let f : A $\rightarrow$ B.
- If f is a 1-1 correspondence then f^{-1} is a function.

Proof

- Let $f : A \rightarrow B$ be 1-1 and onto.
- We want to show $f^{-1} \subseteq B \times A$ is a function.
- We need to show
  - For any $y \in B$, there is a $x \in A$ such that $(y,x) \in f^{-1}$.
  - If $(y,x), (y,x') \in f^{-1}$, then $x = x'$.

Proof --- Every Member of B Has an Image Under f^{-1}

- Let $y \in B$.
- Since f is onto, there is a $x \in A$ such that $f(x) = y$.
- That is, for any $y \in B$, there is a $x \in A$, such that
  - $(x,y) \in f$.
- But $(x,y) \in f$ implies $(y,x) \in f^{-1}$.

Proof --- The Image Under f^{-1} is Unique

- Let $y \in B$.

- Let $(y,x), (y,x') \in f^{-1}$.
  - We have $(x,y), (x',y) \in f$.
  - This gives $f(x) = y = f(x')$.
  - But f is 1-1 gives $x = x'$.

Pause and Think ...

- Consider A x B = { 1, 2, 3 } x { a, b, c }.
- Let f = { (1,a), (2,b), (3,a) }.
- Is f a function from A to B?
- Is f^{-1} a function from B to A?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- <u>f Inverse is a Function Implies f is a Bijection</u>
- Properties of Inverse Functions
- Some Function Composition Properties

Inverse Functions

- Let $f : A \rightarrow B$.
- Since f is a function, it is a relation.
- We know f^{-1} is a relation from B to A.
- If f^{-1} is a function, what can we say about f ?

Theorem

- Let f : A $\rightarrow$ B.

- If f^{-1} is a function, then f is 1-1 and onto.

Proof

- Given $f^{-1} : B \to A$ is a function.
- We want to show $f : A \to B$ is 1-1 and onto.
- We need to show
  - If $f(x) = f(x')$, then $x = x'$.
  - For any $y \in B$, there is a $x \in A$ such that $f(x) = y$.

Proof --- f is 1-1

- Let f(x) = f(x') = y.
- We have (x,y), (x',y) $\in$ f.
- (y,x), (y,x') $\in$ f^{-1}
  - But f^{-1} is a function, so the image of y under it is unique, that is, x = x'.
- Since x=x' whenever f(x) = f(x'), f is 1-1.

Proof --- f is Onto

- For any $y \in B$, let $f^{-1}(y) = x$.
  - That is, $(y,x) \in f^{-1}$.
  - $(x,y) \in f$ and thus $f(x) = y$.
- Since any member of B has a non-empty pre-image under f, f is onto.

Pause and Think ...

- Consider A x B = { 1, 2, 3 } x { a, b, c }.
- Let f = { (1,a), (2,b), (3,c) }.
- Is f a function from A to B?
- Is f^{-1} a function from B to A?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- <u>Properties of Inverse Functions</u>
- Some Function Composition Properties

The Inverse Image and the Pre-Image

- Let $f : A \to B$ and $f^{-1} : B \to A$.
- We have $(x,y) \in f$ iff $(y,x) \in f^{-1}$.
- Since both f and f^{-1} are functions, the above can be written as
  - $f(x) = y$ iff $f^{-1}(y) = x$.

Theorem

- If the inverse of a function is a function, the inverse function is a 1-1 correspondence.

- Proof
  - Let the function be f and f^{-1} be a function.
  - We have $(f^{-1})^{-1} = f$ is a function.
  - Since the inverse of f^{-1} is a function, by a previous theorem, f^{-1} is a 1-1 correspondence.

Pause and Think ...

- Let $f : A \to B$.
- Let $f(x) = y$.
- Can we write $f^{-1}(y) = x$?

Lecture Topics

- One-To-One (1-1) Functions, Injections
- Composition of Injections
- Onto Functions, Surjections
- Composition of Surjections
- One-To-One Correspondences, Bijections
- Composition of Bijections
- f is a Bijection Implies f Inverse is a Function
- f Inverse is a Function Implies f is a Bijection
- Properties of Inverse Functions
- <u>Some Function Composition Properties</u>

Function Composition

- Let $f : A \rightarrow B$ be 1-1 and onto.
- We have $f^{-1} : B \rightarrow A$ is also 1-1 and onto.
- We want to find
  - $f\, f^{-1}$
  - $f^{-1} f$
  - $f\, I_A$, $I_B\, f$
  - $I_A\, f^{-1}$, $f^{-1}\, I_B$

$f\,f^{-1}$

- We have $f^{-1} : B \to A$, $f : A \to B$.
- Let $(f\,f^{-1})(x) = y$.
  - $f(f^{-1}(x)) = y$
  - $f^{-1}(x) = f^{-1}(y)$
  - But f^{-1} is a 1-1 correspondence,
  - so $x = y$
  - and $f\,f^{-1}(x) = x$.
- That is, $f\,f^{-1} = I_B$.

$f^{-1} f$

- We have $f : A \rightarrow B$, $f^{-1} : B \rightarrow A$.
- Let $(f^{-1} f)(x) = y$.
  - $f^{-1}(f(x)) = y$
  - $f(x) = f(y)$
  - But f is a 1-1 correspondence,
  - so $x = y$
  - and $f^{-1} f(x) = x$.
- That is, $f^{-1} f = I_A$.

$f\ I_A$

- We have I_A: $A \to A$, $f : A \to B$.
- Let $(f\ I_A)(x) = y$.
  - $f\,(I_A\,(x)) = y$
  - $f\,(x) = y$
  - $(f\ I_A)(x) = f(x)$
- That is, $f\ I_A = f$.

$I_B f$

- We have $f : A \rightarrow B$, $I_B: B \rightarrow B$.
- Let $(I_B f)(x) = y$.
  - $I_B (f (x)) = y$
  - $f (x) = y$
  - $(I_B f)(x) = f(x)$
- That is, $I_B f = f$.

Pause and Think ...

- What are $I_A f^{-1}$ and $f^{-1} I_B$?