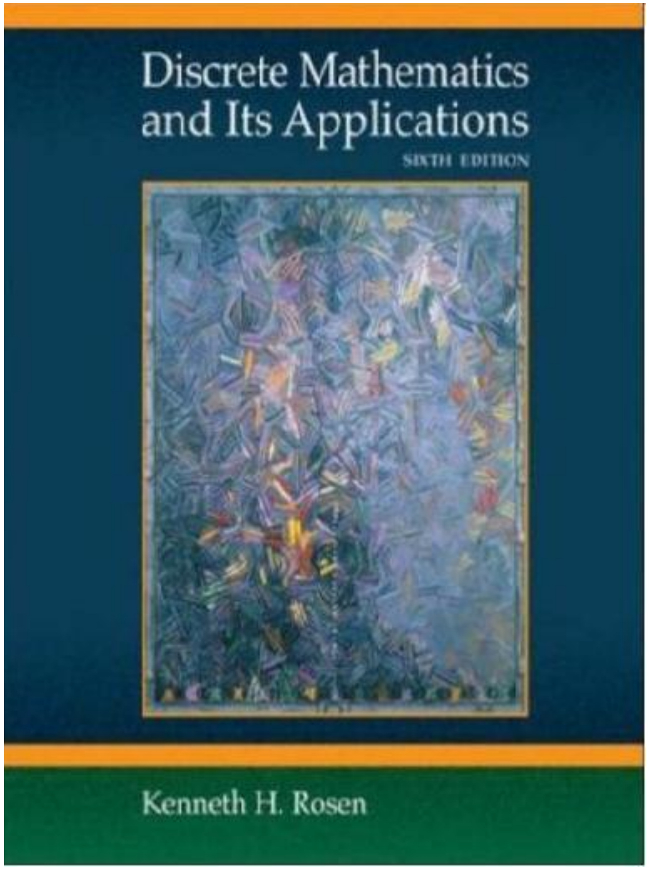
Jiangxi University of Science and Technology

Discrete Mathematics and Its Applications

Lecture010: Logic Module – Part II (proof methods)



Acknowledgement

- Most of these slides are adapted from ones created by Professor Bart Selman at Cornell University and Dr Johnnie Baker

Fallacies

- Fallacies are incorrect inferences. Some common fallacies:

1. The Fallacy of Affirming the Consequent
2. The Fallacy of Denying the Antecedent
3. Begging the question or circular reasoning

The Fallacy of Affirming the Consequent

If the butler did it he has blood on his hands.
The butler had blood on his hands.
Therefore, the butler did it.

This argument has the form

$$\begin{array}{l} P \to Q \\ \underline{Q \qquad\quad} \\ \therefore\ P \end{array}$$

or $((P \to Q) \wedge Q) \to P$ which is not a tautology and therefore not a valid rule of inference

The Fallacy of Denying the Antecedent

- *If the butler is nervous, he did it.*
- *The butler is really mellow.*
- *Therefore, the butler didn't do it.*

This argument has the form

$$P \to Q$$
$$\neg P$$
$$\therefore \neg Q$$

or $((P \to Q) \wedge \neg P) \to \neg Q$ which is not a tautology and therefore not a valid rule of inference

Begging the question or circular reasoning

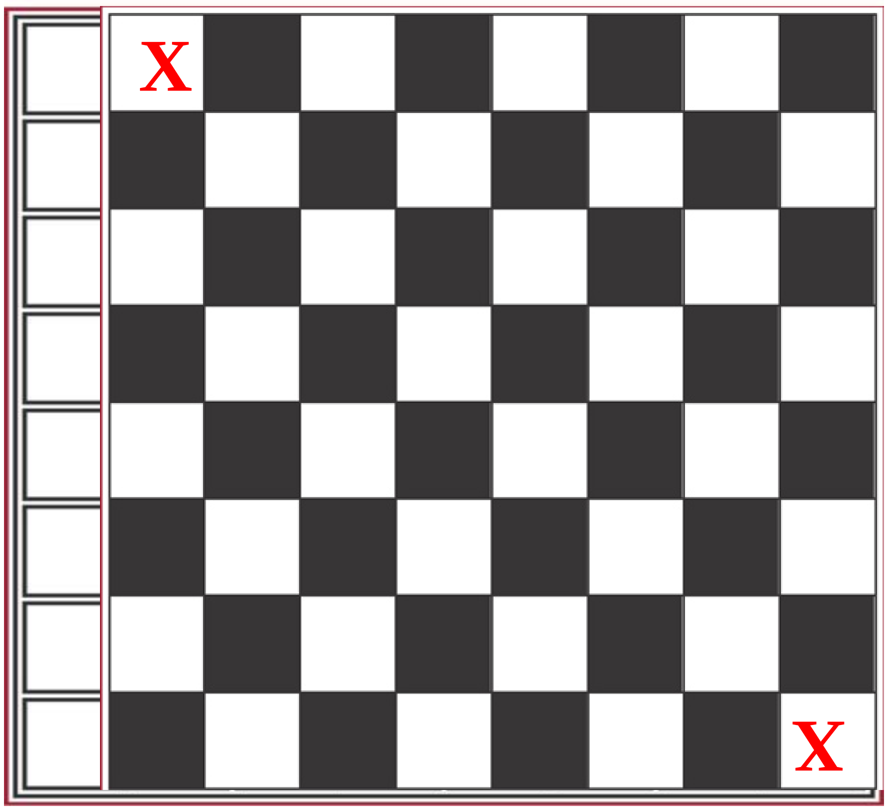
This occurs when we use the truth of the statement being proved (or something equivalent) in the proof itself.

Example:
Conjecture: *if n^2 is even then n is even.*
Proof: If n^2 is even then $n^2 = 2k$ for some k. Let $n = 2m$ for some m. Hence, x must be even.

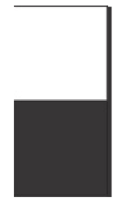
Note that the statement $n = 2m$ is introduced without any argument showing it.

Notoriously hard problem
automated theorem prover
--- requires “true cleverness”

Final example
Tiling



Standard checkerboard. 8x8 = 64 squares



A domino

62 squares: 32 black
30 white
31 doms.: 31 black
31 white squares!

Can you use 32 dominos to cover the board? Easily! (many ways!)

What about the mutilated checkerboard? Hmm… **No! Why?**
Use counting?

What is the proof based upon?
Proof uses clever coloring and counting argument.
Note: also valid for board and dominos without b&w pattern!
(use proof by contradiction)

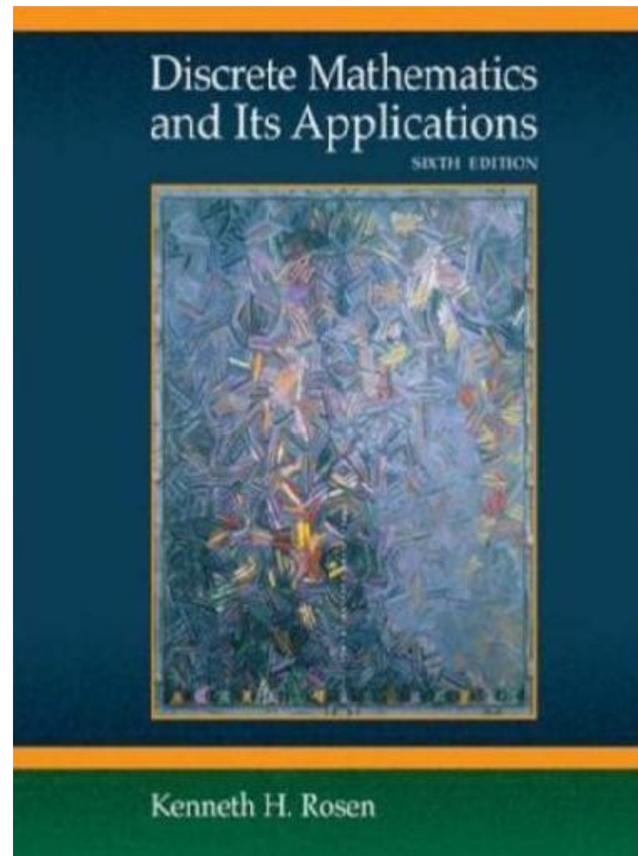
Additional Proof Methods Covered in CS23022

- Induction Proofs
- Combinatorial proofs
- But first we have to cover some basic notions on sets, functions, and counting.

Jiangxi University of Science and Technology

Module Topic

Basic Structures: Functions and Sequences

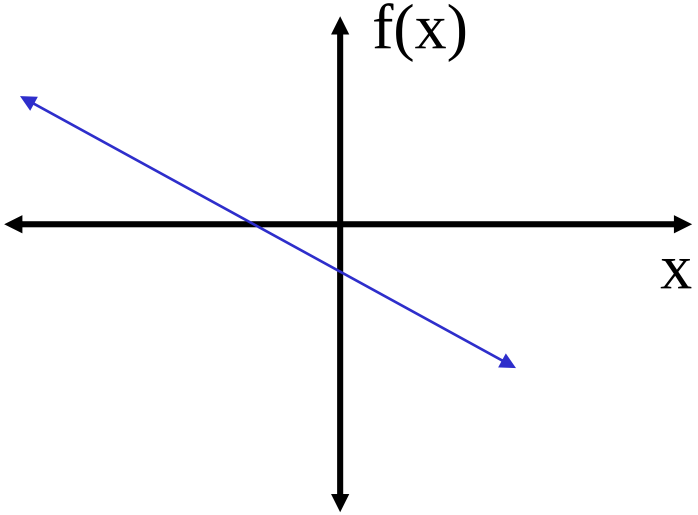


Functions

- Suppose we have:

How do you describe the yellow function?

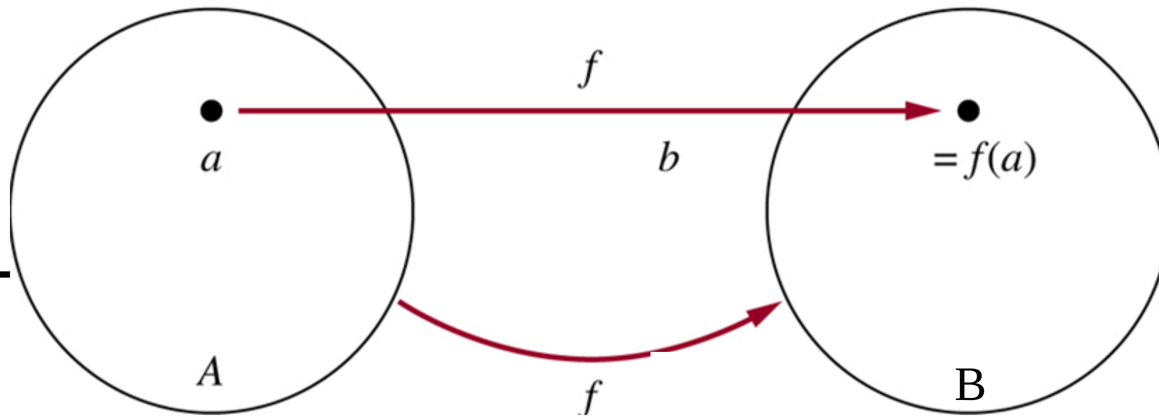
What's a function ?



$f(x) = -(1/2)x - 1/2$

Functions

- More generally:

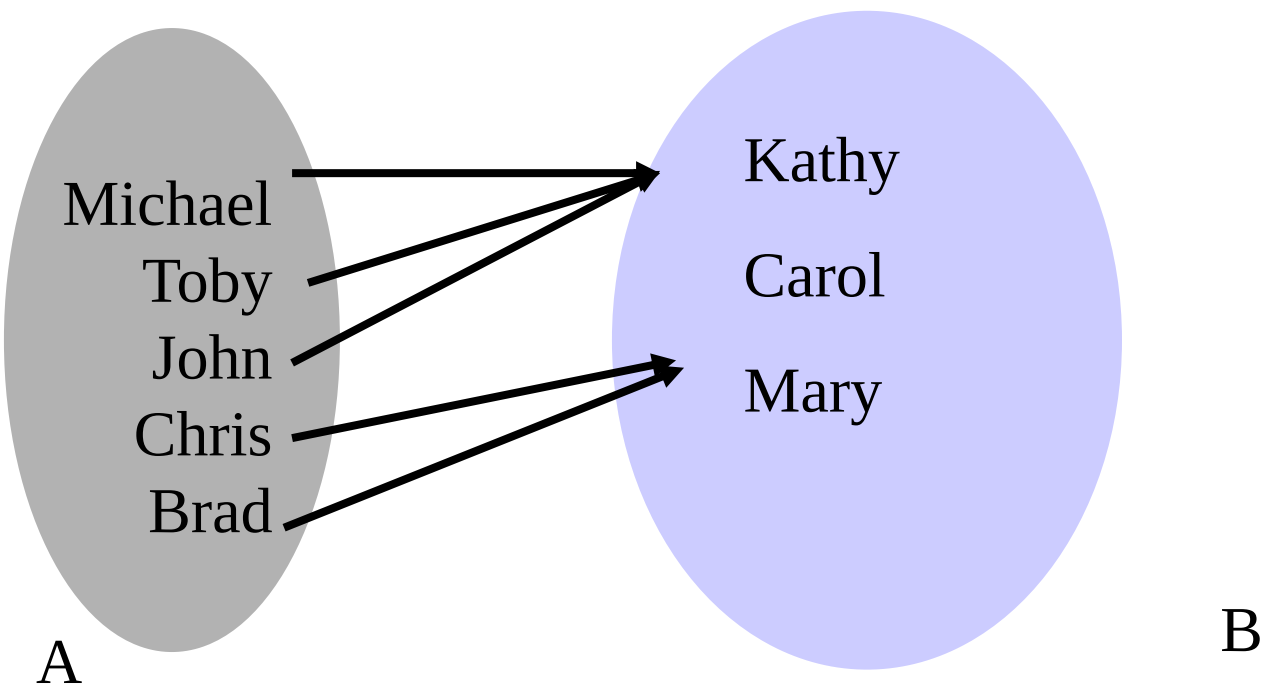


Definition:
Given A and B, nonempty sets, a **function** f from A to B is an assignment of exactly one element of B to each element of A.
We write f(a)=b if b is
the element of B assigned by function f to the element a of A.
If f is a function from A to B, we write $f : A \rightarrow B$.

Note: Functions are also called **mappings** or **transformations.**

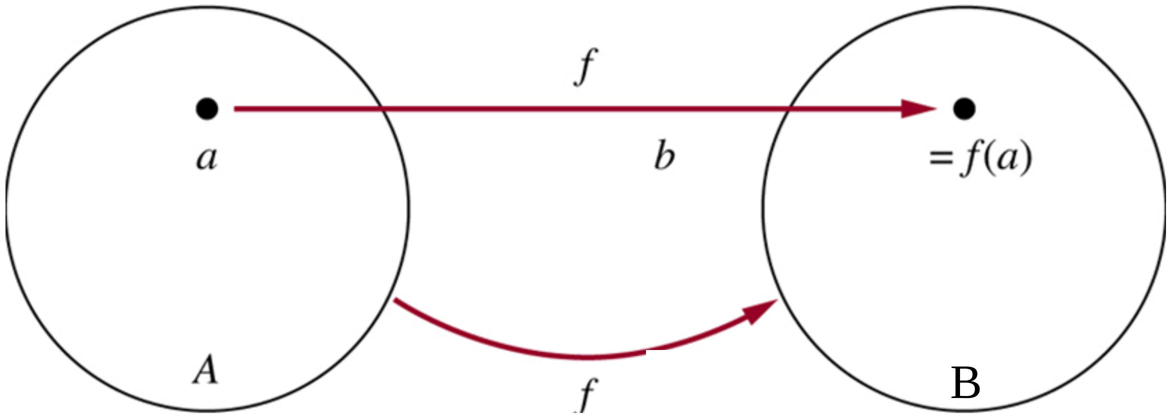
Functions

- A = {Michael, Toby , John , Chris , Brad }
- B = { Kathy, Carla, Mary}
- Let f: A $\rightarrow$ B be defined as f(a) = mother(a).



Functions

- More generally:



A - Domain of f B- Co-Domain of f

$f: \mathbb{R} \to \mathbb{R}$, $f(x) = -(1/2)x - 1/2$

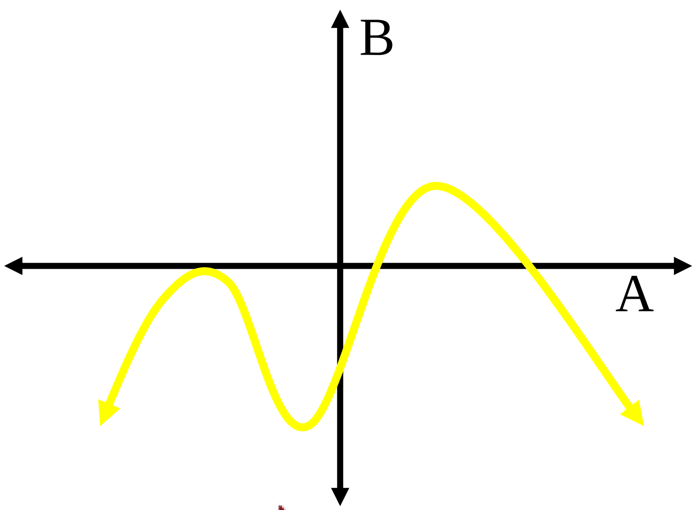
domain co-domain

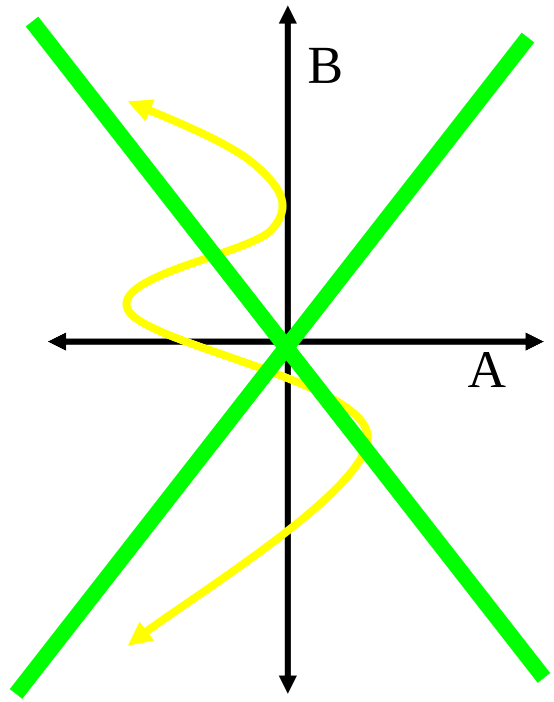
Functions

a collection of points!

- More formally: a function $f : A \rightarrow B$ is a subset of AxB where $\forall\ a \in A, \exists!\ b \in B$ and $\langle a,b \rangle \in f$.

a point!



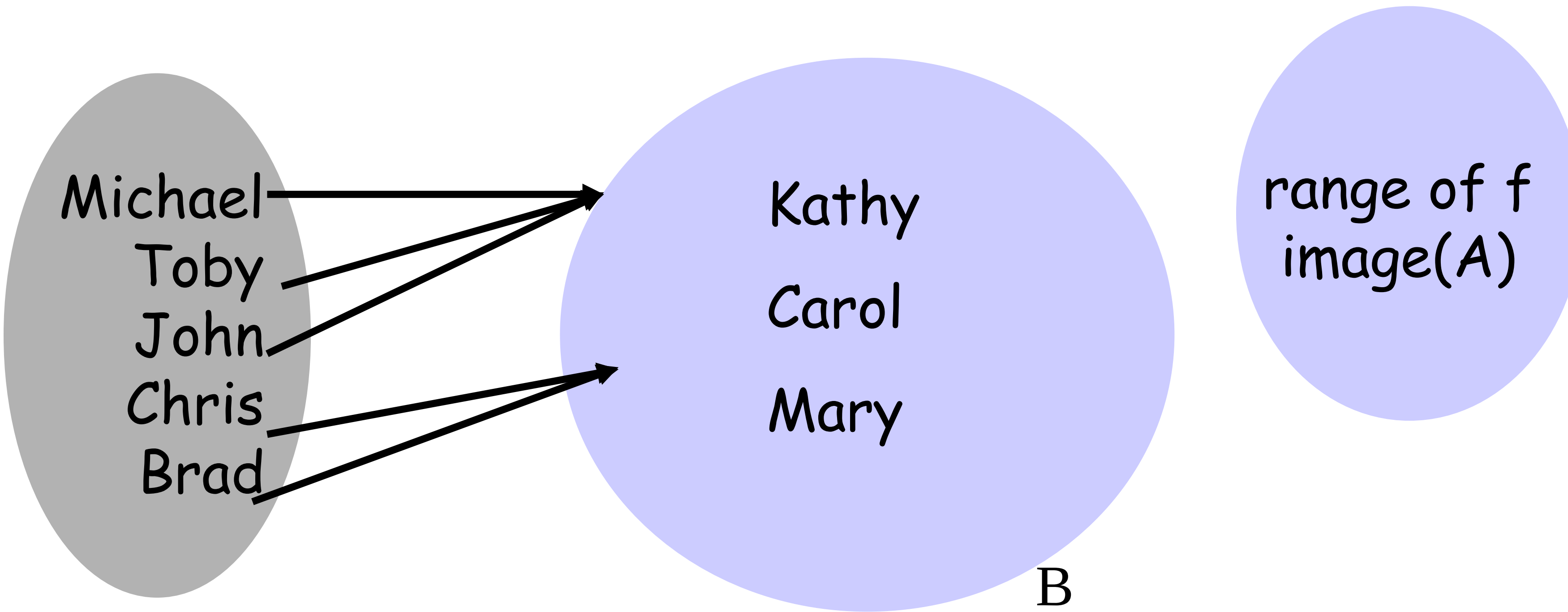


Why not?

Functions - image & preimage

image(S)

- **For any set S ⊆ A, image(S) = {b : ∃a ∈ S, f(a) = b}**
- **So, image({Michael, Toby}) = {Kathy} image(A) = B - {Carol}**

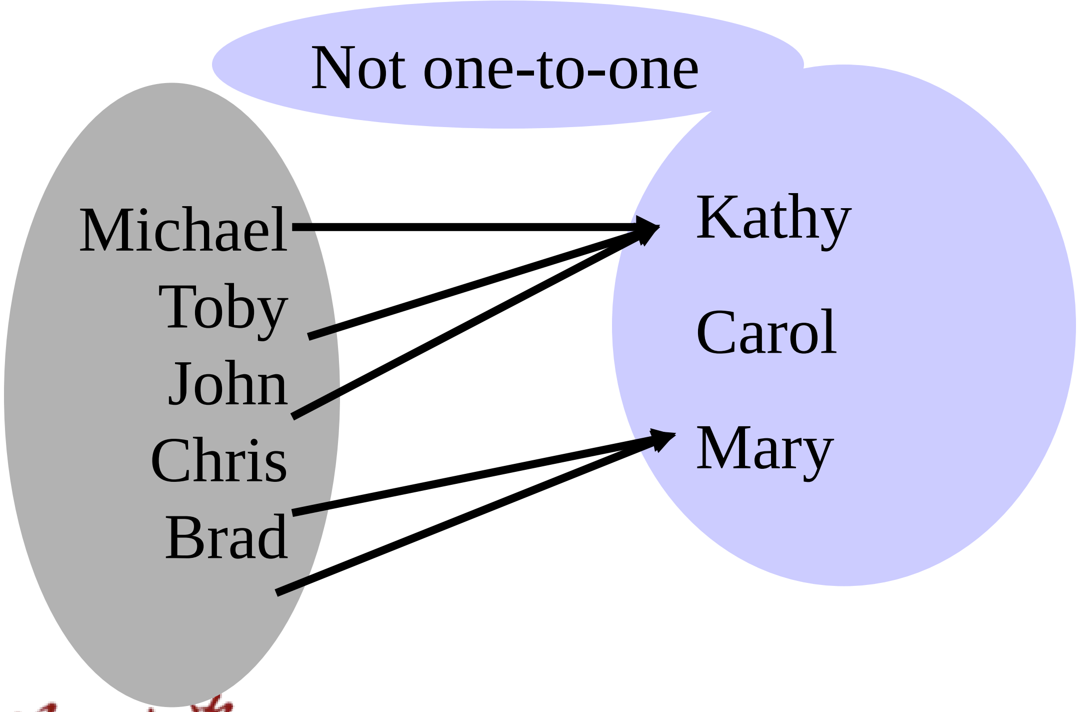


A image(John) = {Kathy} pre-image(Kathy) = {John, Toby, Michael}

Functions - injection

Every $b \in B$ has at most 1 preimage.

- A function $f: A \to B$ is one-to-one (injective, an injection) if $\forall a,b,c,\ (f(a) = b \wedge f(c) = b) \to a = c$

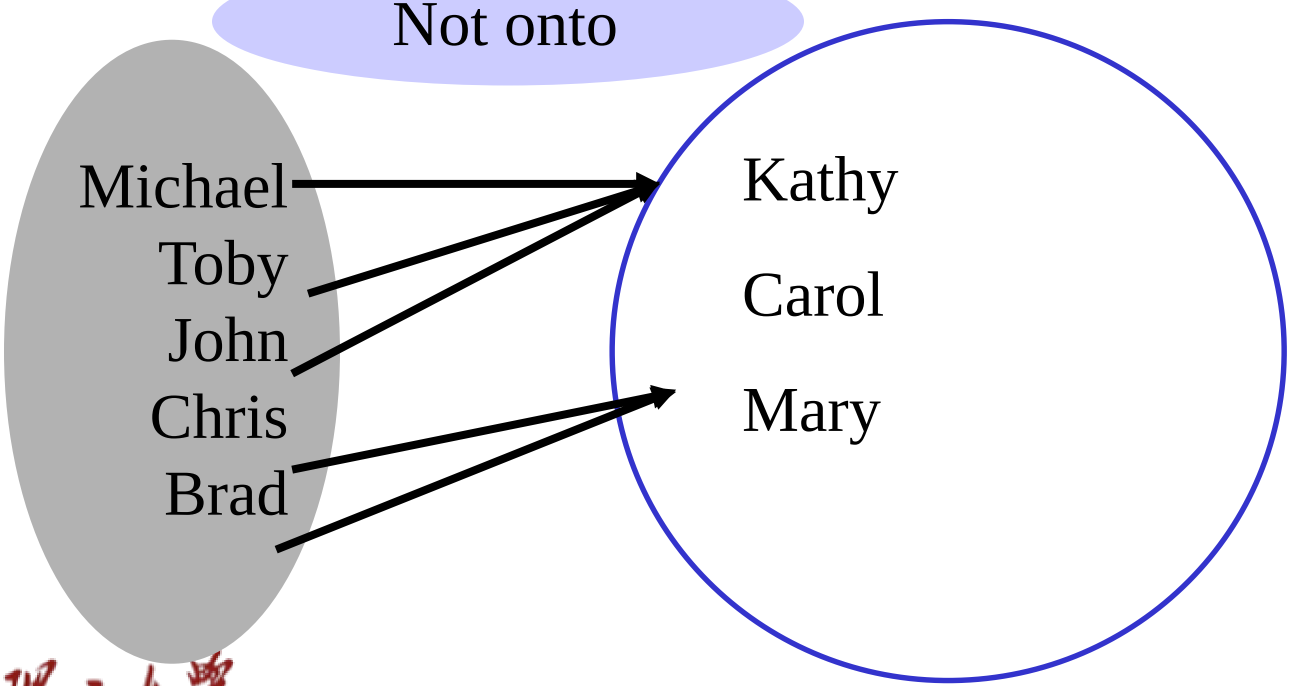


Every $b \in B$ has at least 1 preimage.

Functions - surjection

- A function $f: A \rightarrow B$ is onto (surjective, a surjection) if $\forall b \in B, \exists a \in A\ f(a) = b$

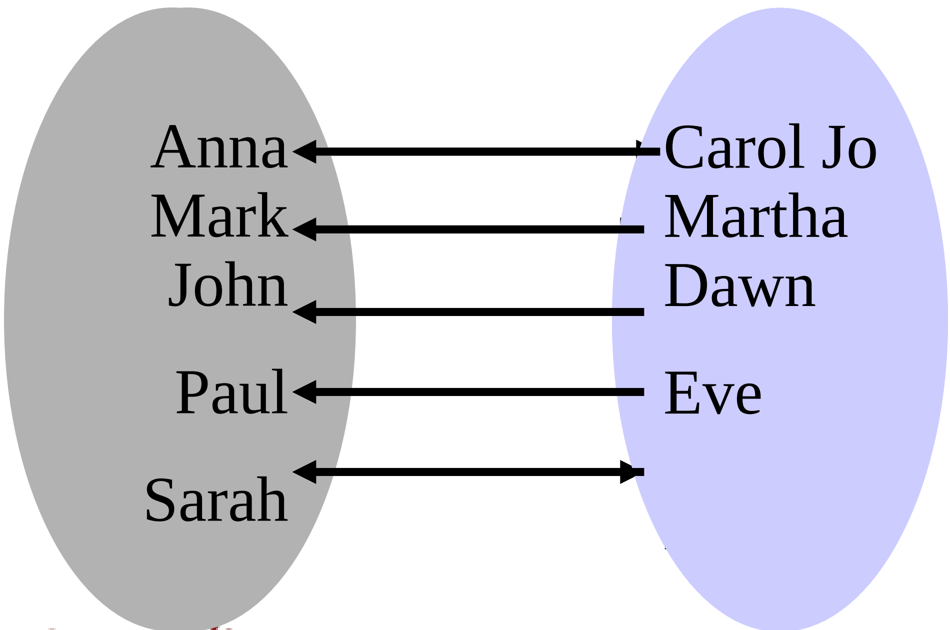
Not onto



Functions – one-to-one-correspondence or bijection

- A function f: $A \rightarrow B$ is bijective if it is one-to-one and onto.

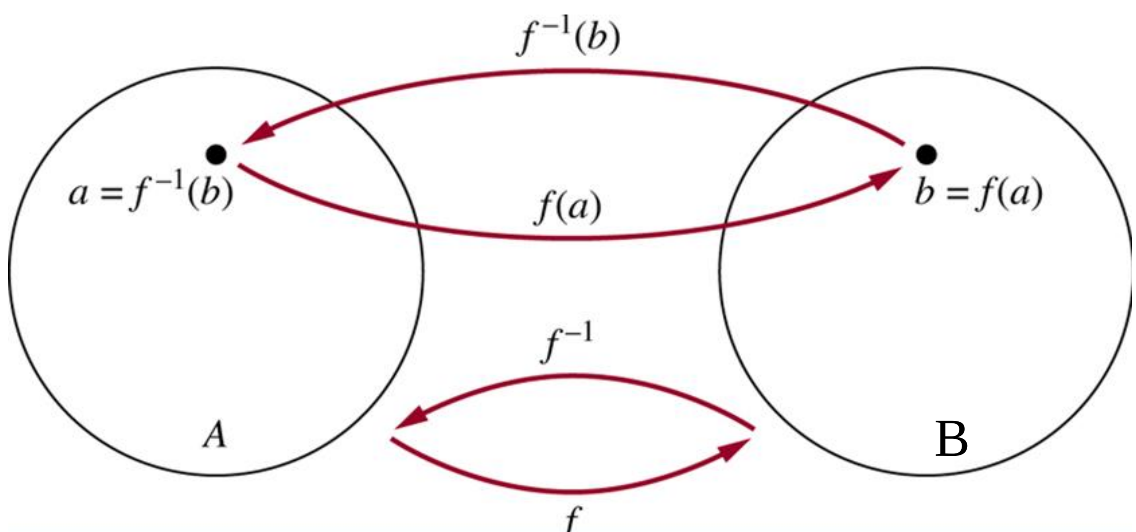
Every $b \in B$ has exactly 1 preimage.



An important implication of this characteristic:
The preimage (f^{-1}) is a function!
They are **invertible.**

Functions: inverse function

- Definition:
- Given f, a one-to-one correspondence from set A to set B, the **inverse**
- **function of f** is the function that assigns to an element b belonging to B the unique element a in A such that f(a)=b. The inverse function is denoted f^{-1} . f^{-1} (b)=a, when f(a)=b.

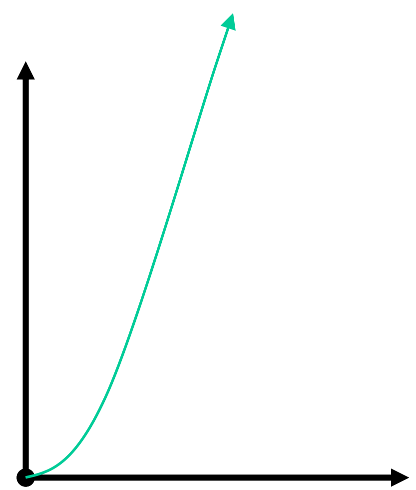


Functions - examples

- Suppose f: $R^+ \rightarrow R^+$, $f(x) = x^2$.

- Is f one-to-one? yes
- Is f onto? yes
- Is f bijective? yes

This function is invertible.



Functions - examples

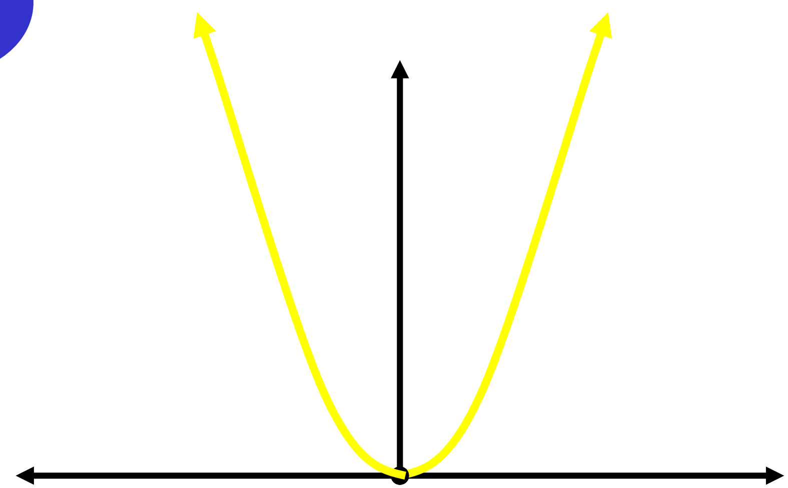
- Suppose f: R $\rightarrow$ R^+, $f(x) = x^2$.

- Is f one-to-one?
- Is f onto?
- Is f bijective?

yes

no

no



This function is not invertible.

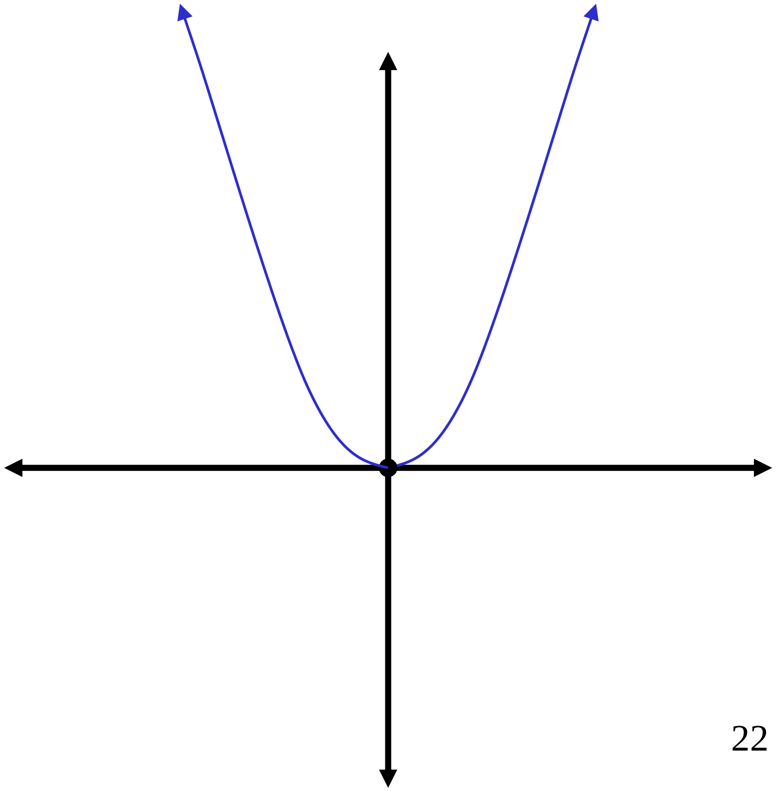
Functions - examples

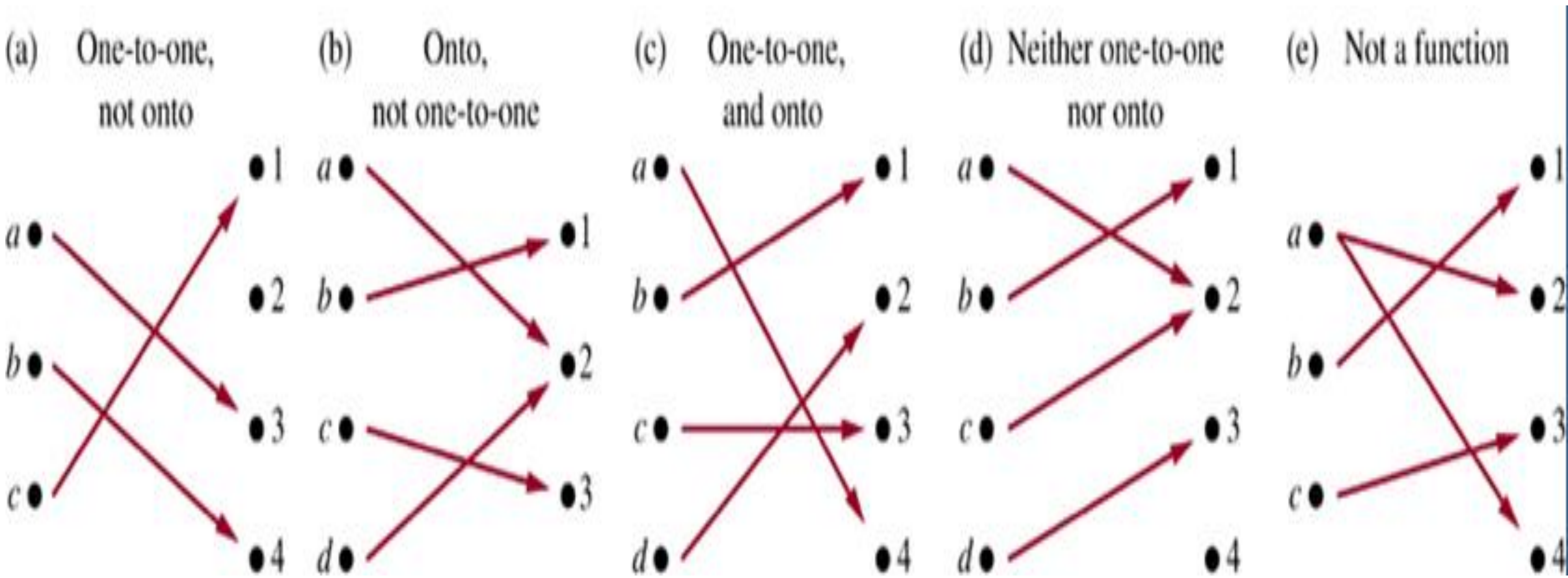
- Suppose f: R $\rightarrow$ R, $f(x) = x^2$.

Is f one-to-one? no

Is f onto? no

Is f bijective? no




(a) One-to-one, not onto
(b) Onto, not one-to-one
(c) One-to-one, and onto
(d) Neither one-to-one nor onto
(e) Not a function
a
b
c
d
1
2
3
4

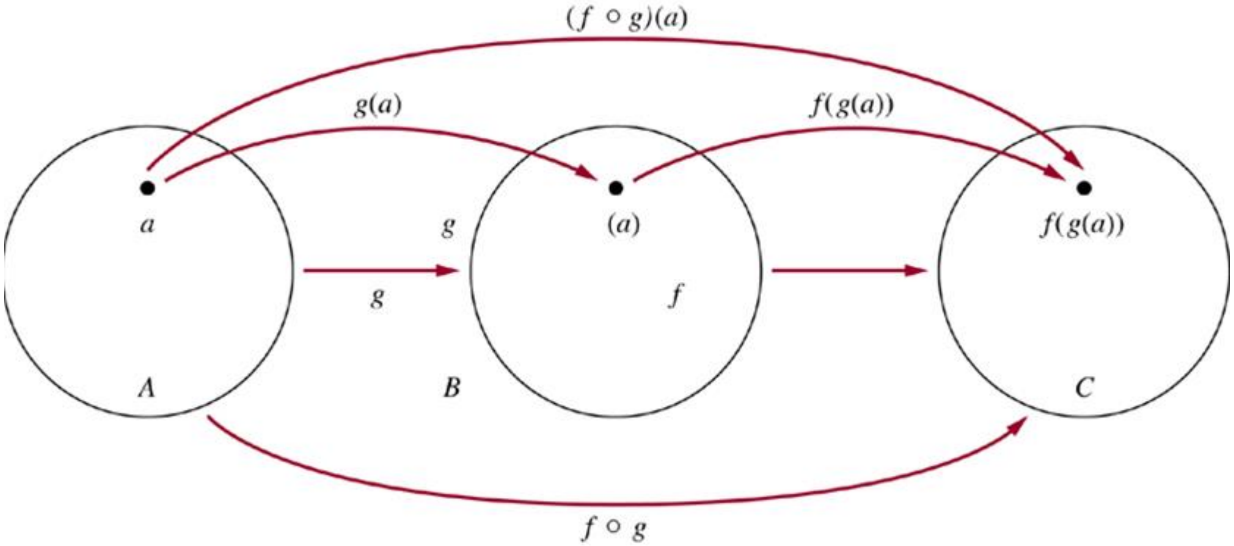
Functions - composition

"f composed with g"

- Let f: A→B, and g: B→C be functions.

Then the composition of f and g is:

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



Note: (f o g) cannot be defined unless the range of g is a subset of the domain of f.

Example:

Let $f(x) = 2x + 3$; $g(x) = 3x + 2$;

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

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

As this example shows, $(f \circ g)$ and $(g \circ f)$ are not necessarily equal – i.e, the composition of functions is not commutative.

Note:

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

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

Therefore $(f^{-1} \circ f) = I_A$ and $(f \circ f^{-1}) = I_B$ where I_A and I_B are the identity function on the sets A and B. $(f^{-1})^{-1} = f$

Some important functions

Absolute value:

Domain R; Co-Domain = $\{0\} \cup R^+$

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Ex: $|-3| = 3$; $|3| = 3$

Floor function (or greatest integer function):

Domain = R; Co-Domain = Z

$\lfloor x \rfloor$ = largest integer not greater than x

Ex: $\lfloor 3.2 \rfloor = 3$; $\lfloor -2.5 \rfloor = -3$

Some important functions

- **Ceiling function:**

  Domain = R;

  Co-Domain = Z

  $\lceil x \rceil$ = smallest integer greater than x

  Ex: $\lceil 3.2 \rceil = 4; \lceil -2.5 \rceil = -2$

TABLE 1 Useful Properties of the Floor and Ceiling Functions.

(n is an integer)

(1a)	$\lfloor x \rfloor = n$ if and only if $n \le x < n + 1$
(1b)	$\lceil x \rceil = n$ if and only if $n - 1 < x \le n$
(1c)	$\lfloor x \rfloor = n$ if and only if $x - 1 < n \le x$
(1d)	$\lceil x \rceil = n$ if and only if $x \le n < x + 1$
(2)	$x - 1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x + 1$
(3a)	$\lfloor -x \rfloor = -\lceil x \rceil$
(3b)	$\lceil -x \rceil = -\lfloor x \rfloor$
(4a)	$\lfloor x + n \rfloor = \lfloor x \rfloor + n$
(4b)	$\lceil x + n \rceil = \lceil x \rceil + n$

Some important functions

Factorial function: Domain = Range = N **Error on range**

n! = n (n-1)(n-2) …, 3 x 2 x 1

Ex: 5! = 5 x 4 x 3 x 2 x 1 = 120

Note: 0! = 1 by convention.

Some important functions

Mod (or remainder):

Domain = $N \times N^+ = \{(m,n) | m \in N, n \in N+ \}$

Co-domain Range = N

$$m \textit{ mod } n = m - \lfloor m/n \rfloor n$$

Ex: $8 \text{ mod } 3 = 8 - \lfloor 8/3 \rfloor 3 = 2$

$57 \text{ mod } 12 = 9$;

Note: This function computes the remainder when m is divided by n.
The name of this function is an abbreviation of m modulo n, where modulus means with respect to a modulus (size) of n, which is defined to be the remainder when m is divided by n. Note also that this function is an example in which the domain of the function is a 2-tuple.

Some important functions:Exponential Function

Exponential function:

- Domain = $R^+ \times R$ = $\{(a,x) | a \in R+, x \in R\}$

  Co-domain Range = R^+

  $f(x) = a^x$

Note: *a* is a **positive** constant; x varies.

Ex: $f(n) = a^n = a \times a \ldots, \times a$ (n times)

How do we define f(x) if x is not a positive integer?

Some important functions: Exponential function

Exponential function:
How do we define f(x) if x is not a positive integer?
Important properties of exponential functions:

(1) $a^{(x+y)} = a^x a^y$; (2) $a^1 = a$ (3) $a^0 = 1$

See:

$$a^2 = a^{1+1} = a^1 a^1 = a \times a;$$

$$a^3 = a^{2+1} = a^2 a^1 = a \times a \times a;$$

$$\ldots$$

$$a^n = a \times \cdots \times a \quad (n\ times)$$

We get:

$$a = a^1 = a^{1+0} = a \times a^0 \quad therefore \quad a^0 = 1$$

$$1 = a^0 = a^{b+(-b)} = a^b \times a^{-b} \quad therefore \quad a^{-b} = 1/a^b$$

$$a = a^1 = a^{\frac{1}{2}+\frac{1}{2}} = a^{\frac{1}{2}} \times a^{\frac{1}{2}} = (a^{\frac{1}{2}})^2 therefore \quad a^{\frac{1}{2}} = \sqrt{a}$$

By similar arguments:

$$a^{\frac{1}{k}} = \sqrt[k]{a}$$

$$a^{mx} = a^x \times \cdots a^x \ (m \quad times) = (a^x)^m, \quad therefore \quad a^{\frac{m}{n}} = (a^{\frac{1}{n}})^m = (\sqrt[n]{a})^m$$

Note: This determines a^x for all x rational. x is irrational by continuity (we'll skip "details").

Some important functions:Logarithm Function

Logarithm base a:

Domain = $R^+ \times R$ = $\{(a,x) | a \in R+, a>1, x \in R\}$

Co-domain Range = R

$y = \log_a (x) \Leftrightarrow a^y = x$

Ex: $\log_2 (8) =3$; $\log_2 (16) =3$; $3 < \log_2 (15) <4$.

Key properties of the log function (they follow from those for exponential):

1. $\log_a (1)=0$ (because $a^0 =1$)
2. $\log_a (a)=1$ (because $a^1 =a$)
3. $\log_a (xy) = \log_a (x) + \log_a (x)$ (similar arguments)
4. $\log_a (x^r) = r \log_a (x)$
5. $\log_a (1/x) = - \log_a (x)$ (note $1/x = x^{-1}$)
6. $\log_b (x) = \log_a (x) / \log_a (b)$

Logarithm Functions

Examples:

$\log_2(1/4) = -\log_2(4) = -2.$

$\log_2(-4)$ undefined

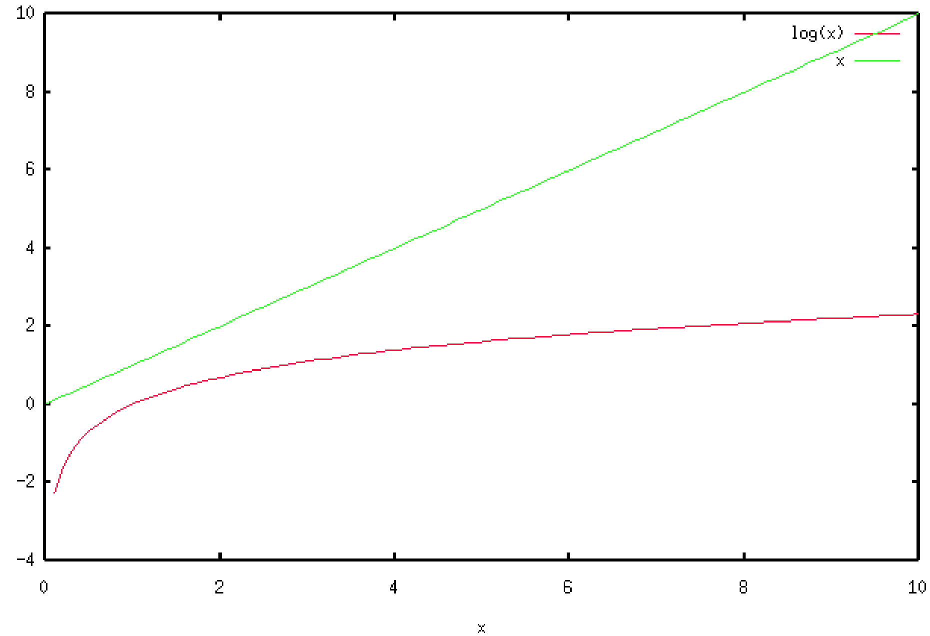
$\log_2(2^{10}\,3^5) = \log_2(2^{10}) + \log_2(3^5) = 10\log_2(2) + 5\log_2(3) =$

$= 10 + 5\log_2(3)$

Limit Properties of Log Function

$$\lim_{x \to \infty} \log(x) = \infty$$

$$\lim_{x \to \infty} \frac{\log(x)}{x} = 0$$



As x gets large, *log(x)* grows without bound.

But *x* grows **MUCH** faster than *log*(*x*)…more soon on growth rates.