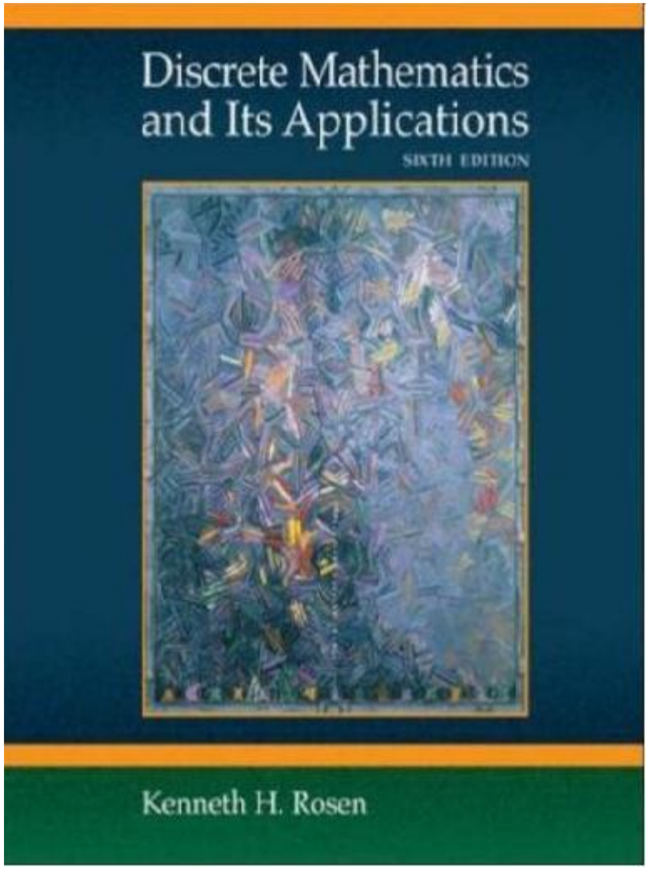
Jiangxi University of Science and Technology

Discrete Mathematics and Its Applications

Lecture010: Logic Module – Part II (proof methods)



Discrete Mathematics and Its Applications

SIXTH EDITION

Kenneth H. Rosen

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 $((P \to Q) \land Q) \to P$ 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

$$P\rightarrow Q$$
$$\neg P$$
$$\therefore\ \neg Q$$

or $((P\rightarrow Q) \wedge \neg P)\rightarrow \neg Q$ 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.

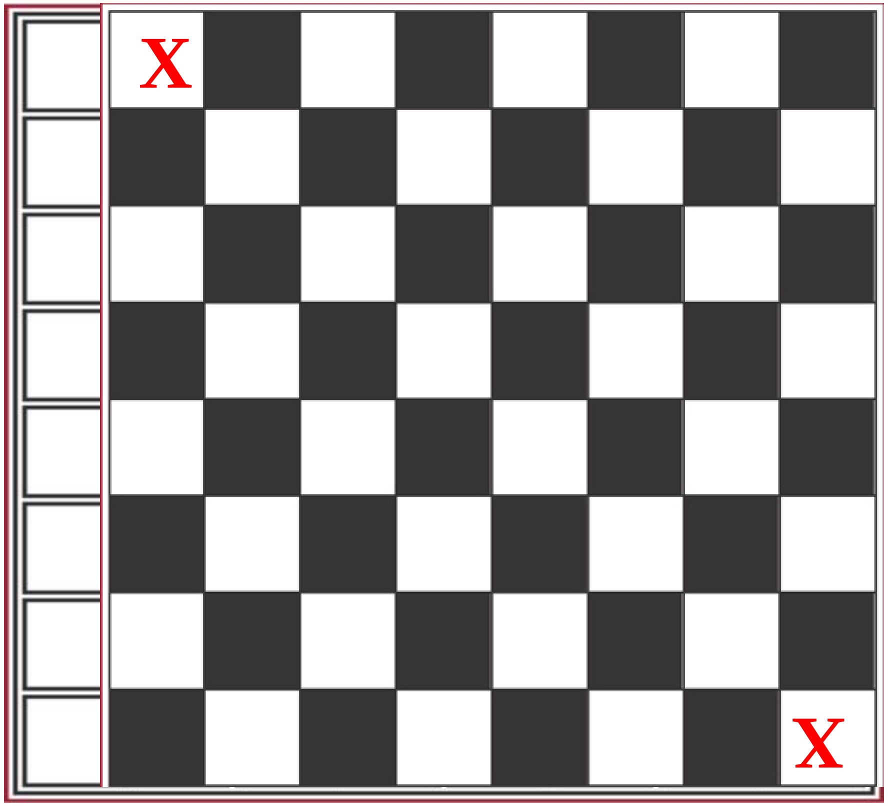
Example:
Conjecture: *if n^2 is even then n is even.*
Proof: If n^2 is even then $n^2 = 2k$ for some k. Let $n = 2m$ for some m. Hence, x must be even.

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

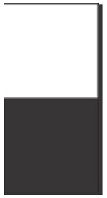
Final example
Tiling

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

© The McGraw-Hill Companies, Inc. all rights reserved.



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)

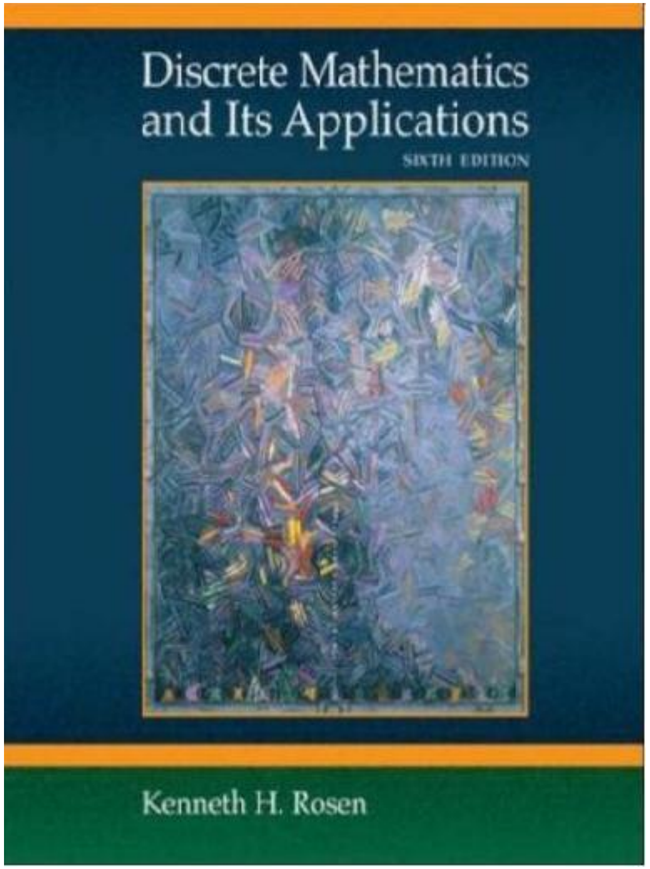
Additional Proof Methods Covered in CS23022

- 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



Discrete Mathematics and Its Applications

SIXTH EDITION

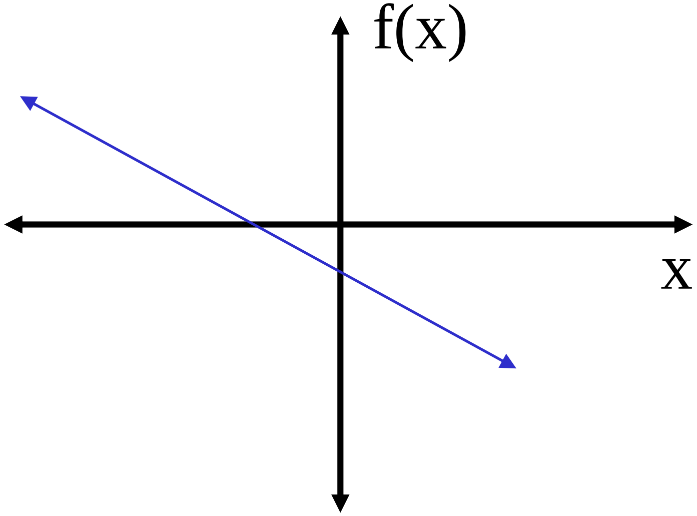
Kenneth H. Rosen

Functions

- Suppose we have:

How do you describe the yellow function?

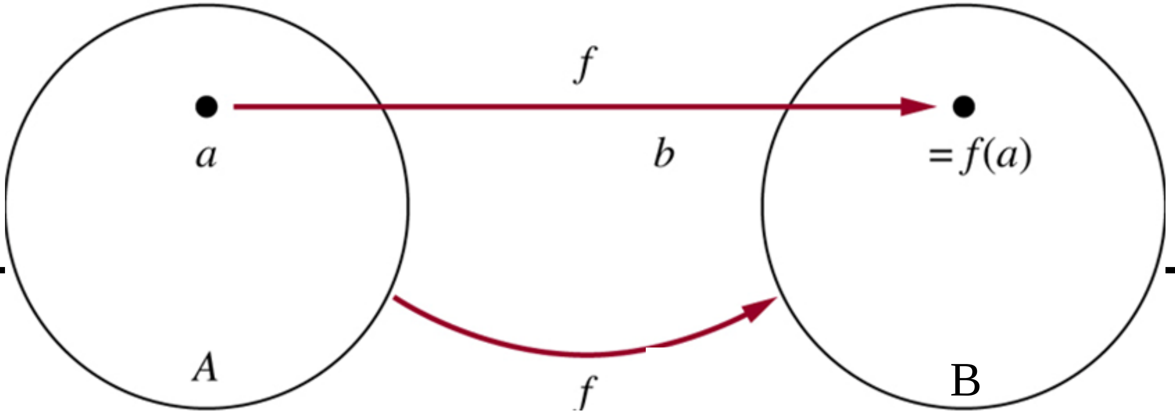
What’s a function ?



f(x) = -(1/2)x – 1/2

Functions

- More generally:

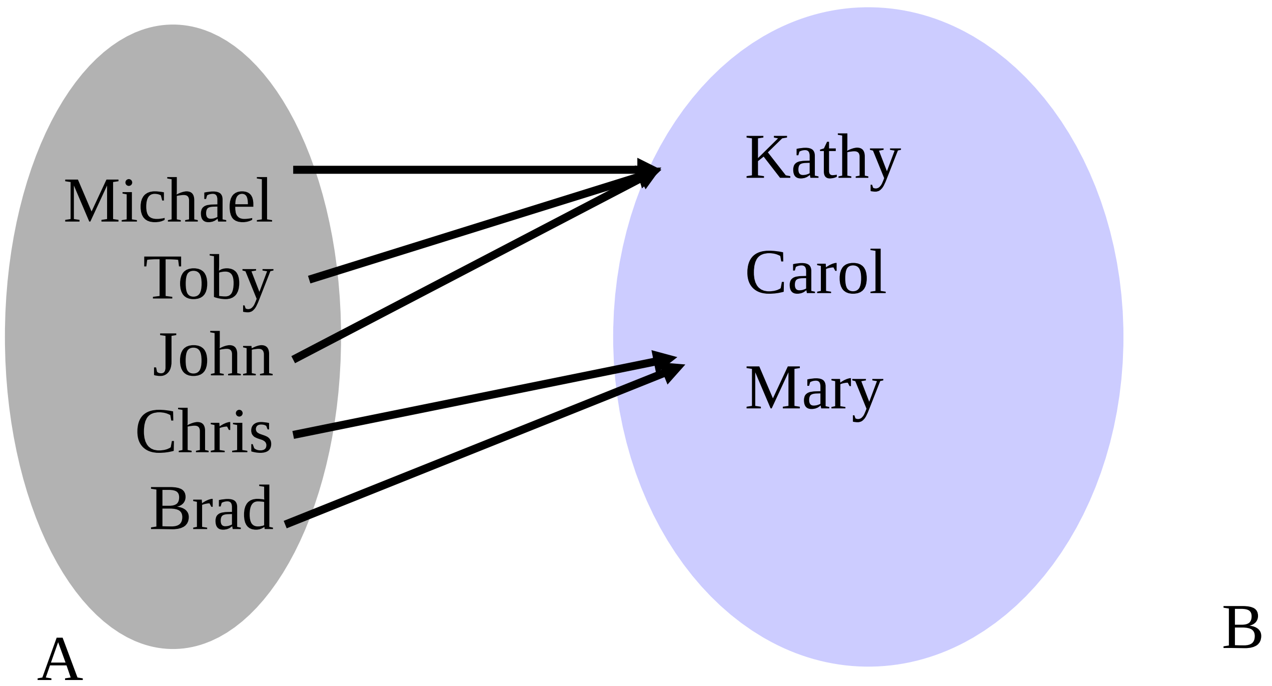


Definition:
Given A and B, nonempty sets, a **function** f from A to B is an assignment of exactly one element of B to each element of A.
We write f(a)=b if b is
the element of B assigned by function f to the element a of A.
If f is a function from A to B, we write f : A→B.

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

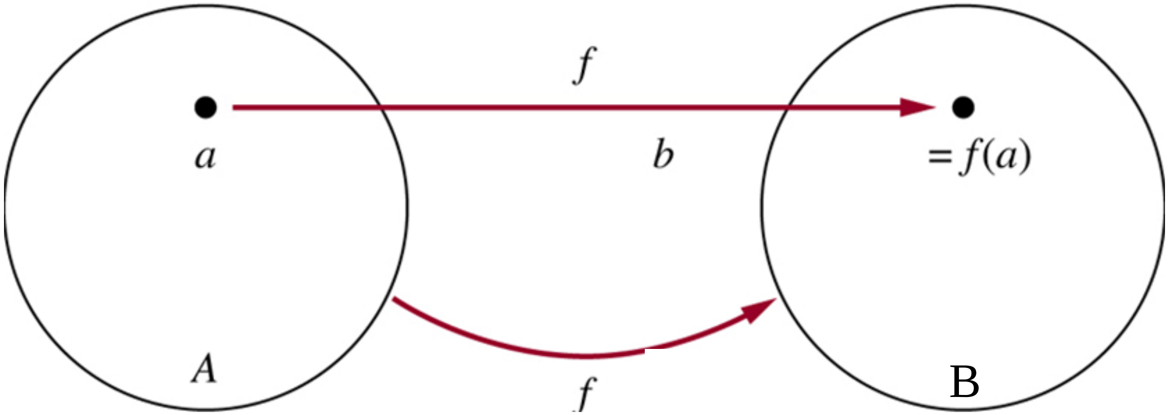
Functions

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



Functions

- More generally:



A - Domain of f

B- Co-Domain of f

f: R→R, f(x) = -(1/2)x – 1/2

domain

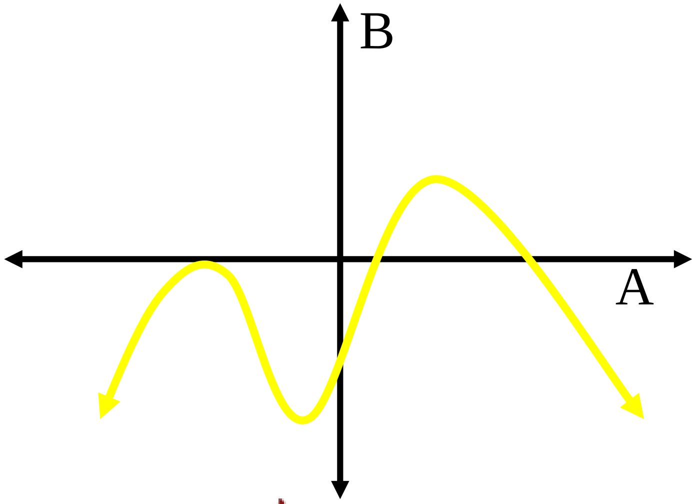
co-domain

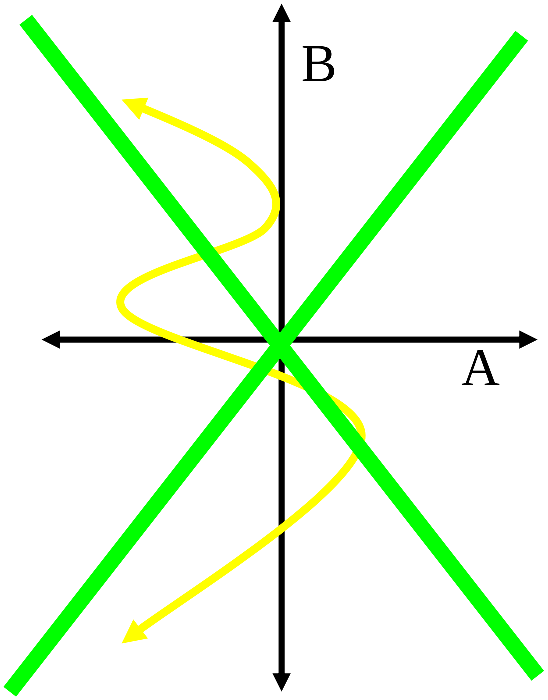
Functions

a collection of points!

- More formally: a function *f* : A → B is a subset of AxB where ∀ a ∈ A, ∃! b ∈ B and <a,b> ∈ *f*.

a point!



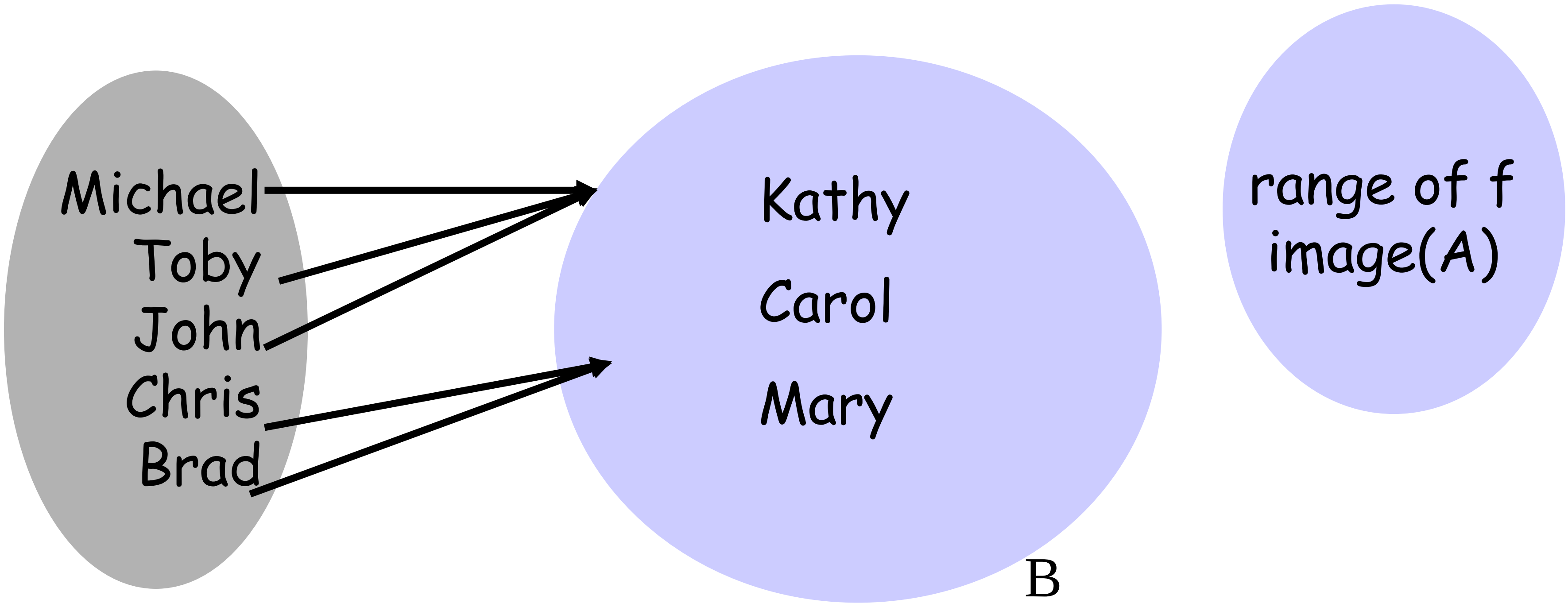


Why not?

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}**



Michael

Toby

John

Chris

Brad

Kathy

Carol

Mary

range of f
image(A)

B

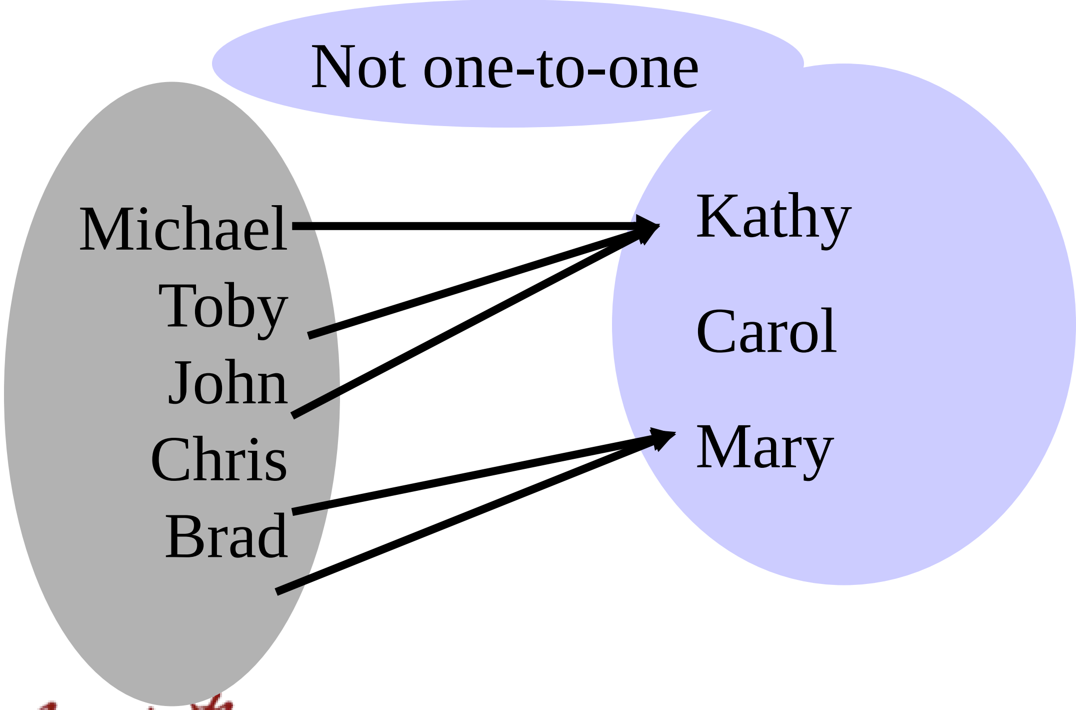
A image(John) = {Kathy}

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

Functions - injection

Every b ∈ B has at most 1 preimage.

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

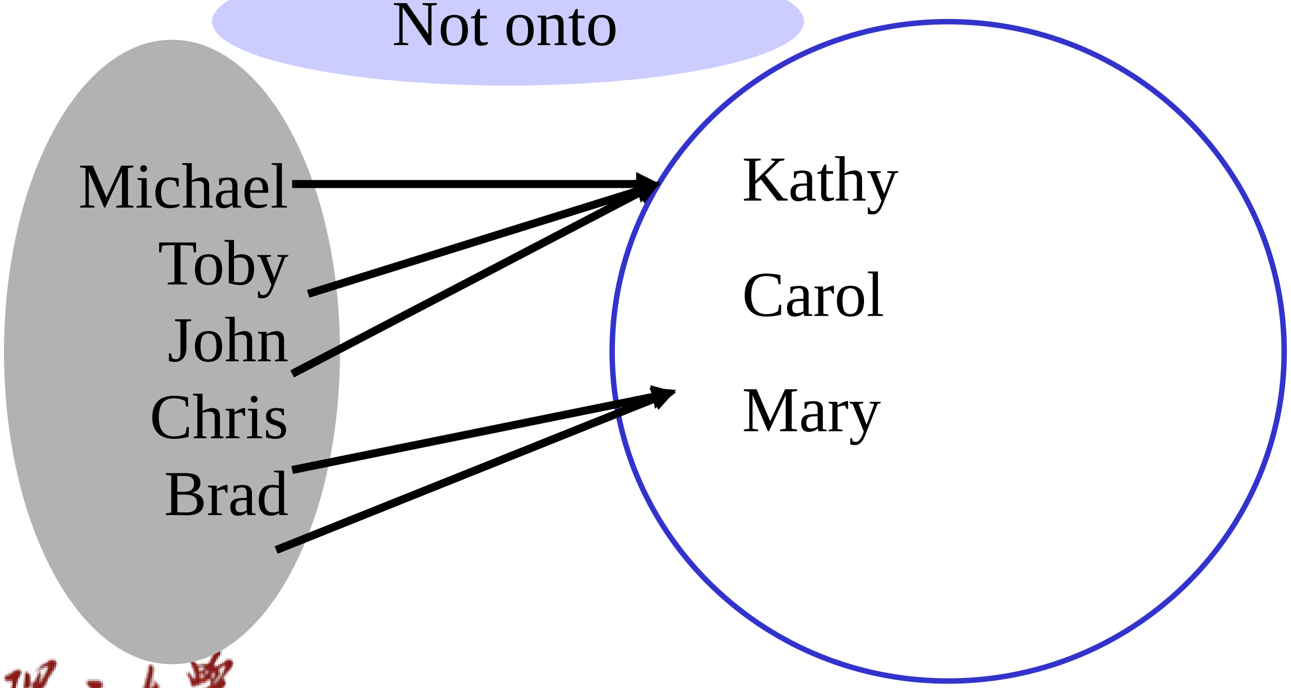


Functions - surjection

Every b ∈ B has at least 1 preimage.

- A function f: A → B is onto (surjective, a surjection) if ∀b ∈ B, ∃a ∈ A f(a) = b

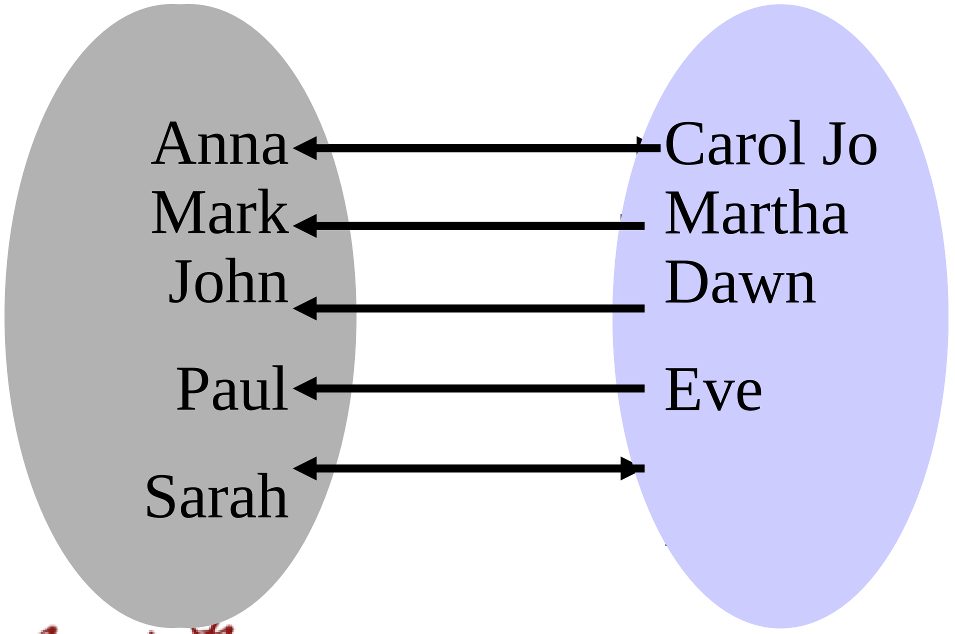
Not onto



Functions – one-to-one-correspondence or bijection

- A function f: A → B is bijective if it is one-to-one and onto.

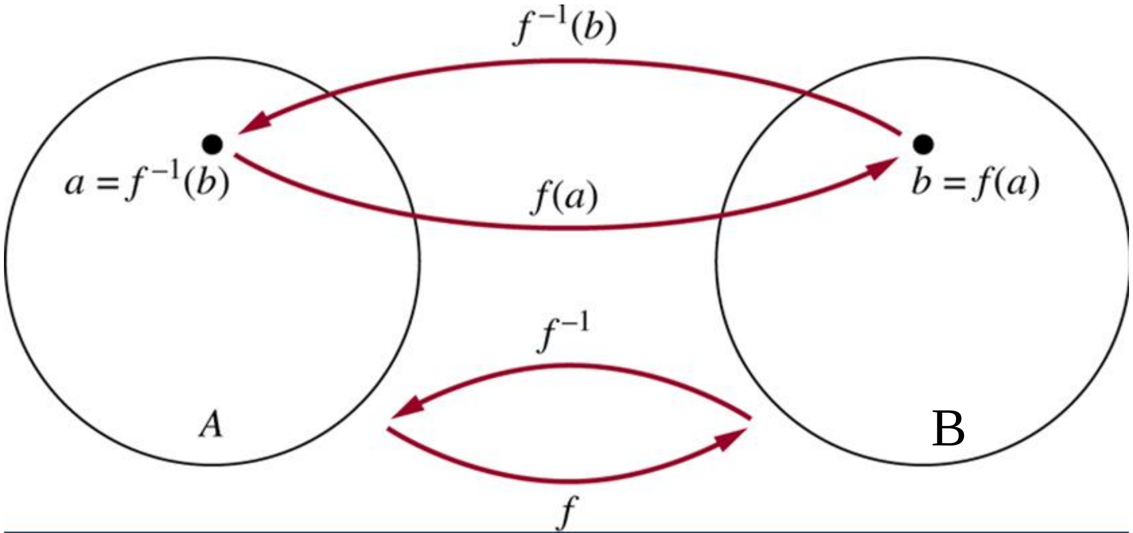
Every b ∈ B has exactly 1 preimage.



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

Functions: inverse function

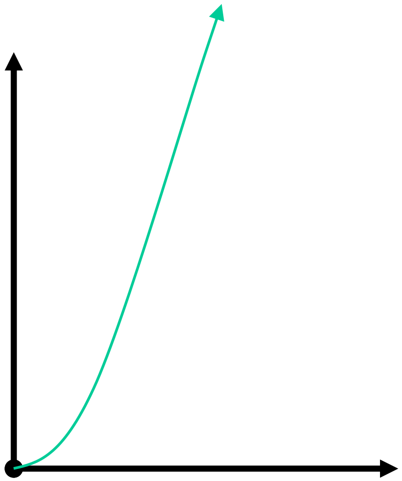
- Definition:
- Given f, a one-to-one correspondence from set A to set B, the **inverse**
- **function of f** is the function that assigns to an element b belonging to B the unique element a in A such that f(a)=b. The inverse function is denoted f^{-1} . f^{-1} (b)=a, when f(a)=b.



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

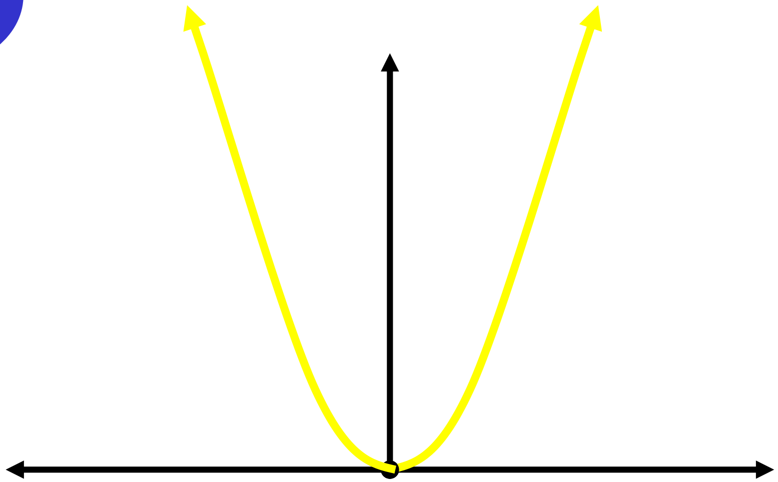
- Suppose f: R → R^+, $f(x) = x^2$.

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

no

yes

no



This function is not invertible.

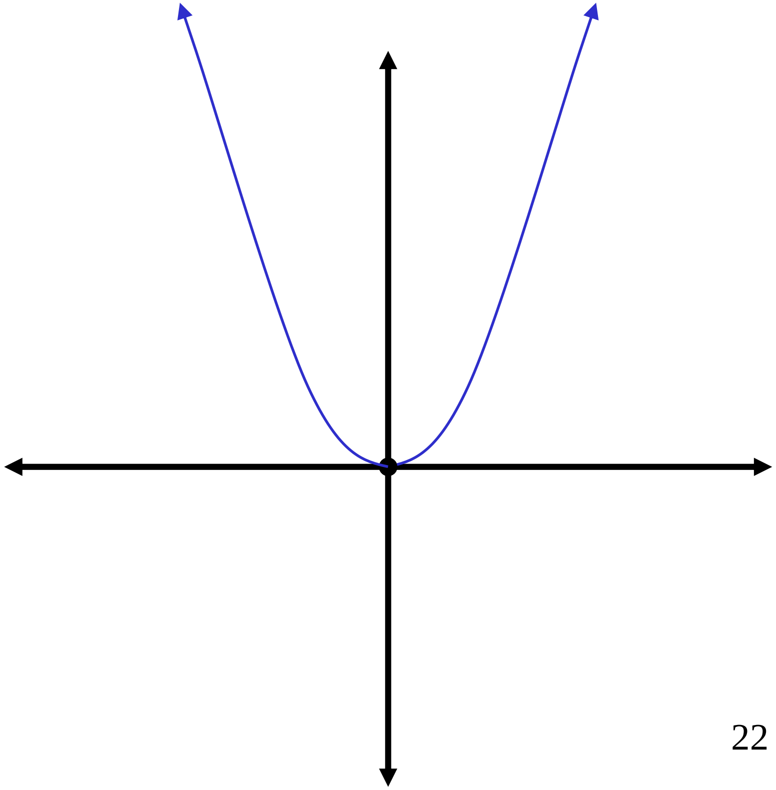
Functions - examples

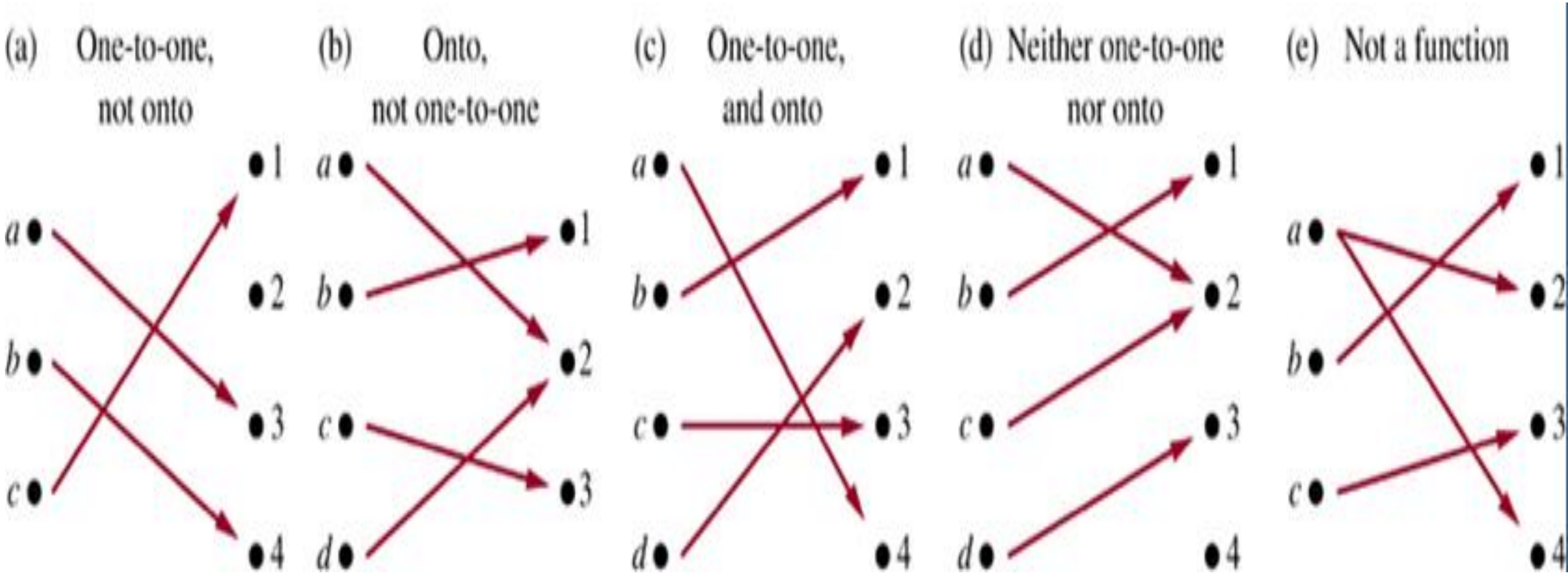
- Suppose f: R → R, $f(x) = x^2$.

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

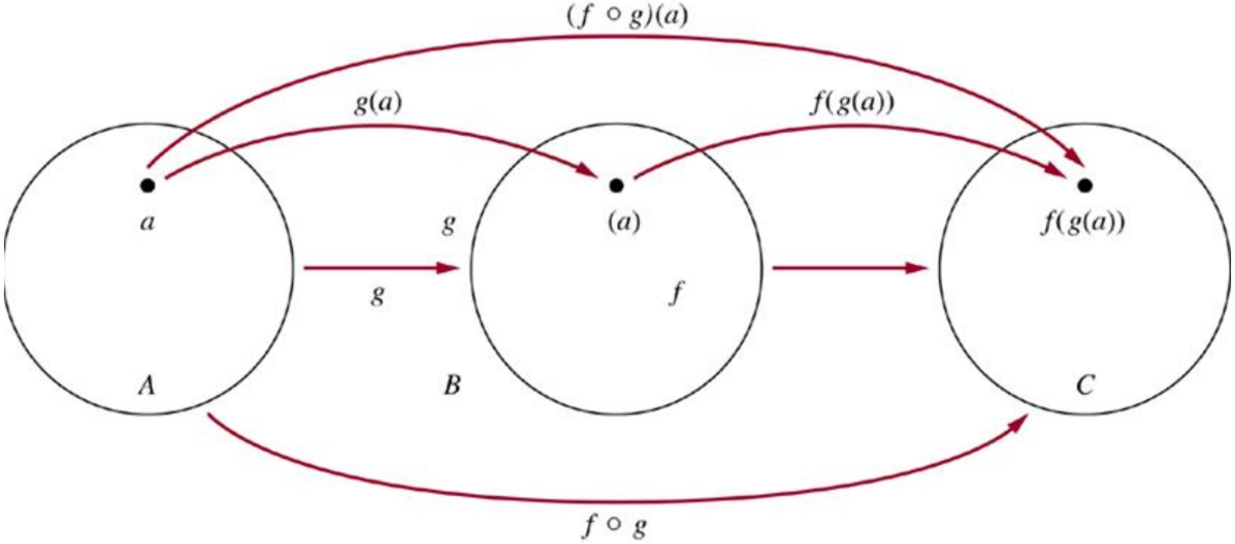
Functions - composition

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

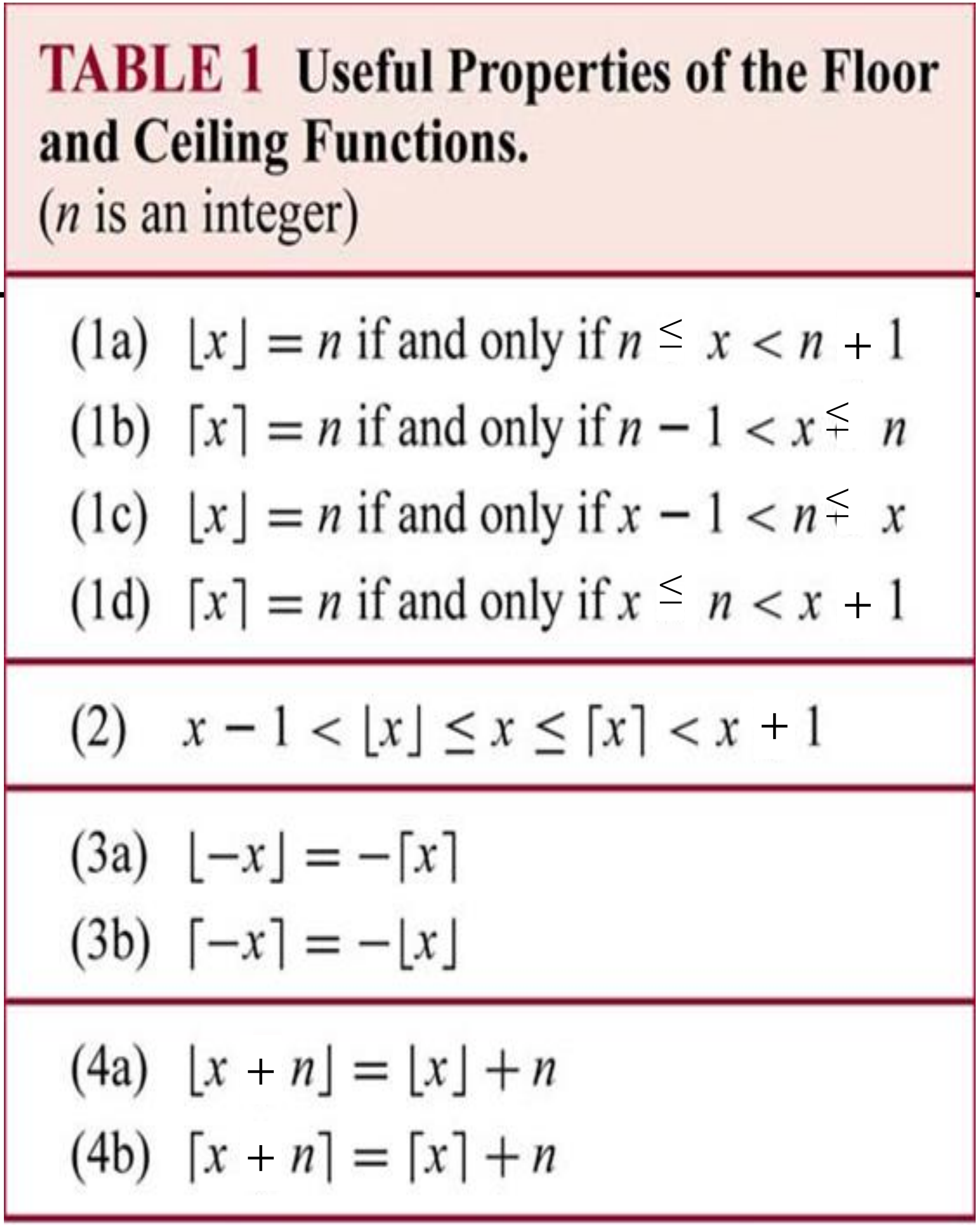


TABLE 1 **Useful Properties of the Floor and Ceiling Functions.**
(n is an integer)

(1a) $\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$

(1b) $\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$

(1c) $\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$

(1d) $\lceil x \rceil = n$ if and only if $x \leq n < x + 1$

(2) $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$

(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 x N^+ = {(m,n)| m ∈N, n ∈ N+ }

  Co-domain Range = N

  m *mod* n = m - $\lfloor m/n \rfloor$ n

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

57 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^+ x 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 x a …, x 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^+ x 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

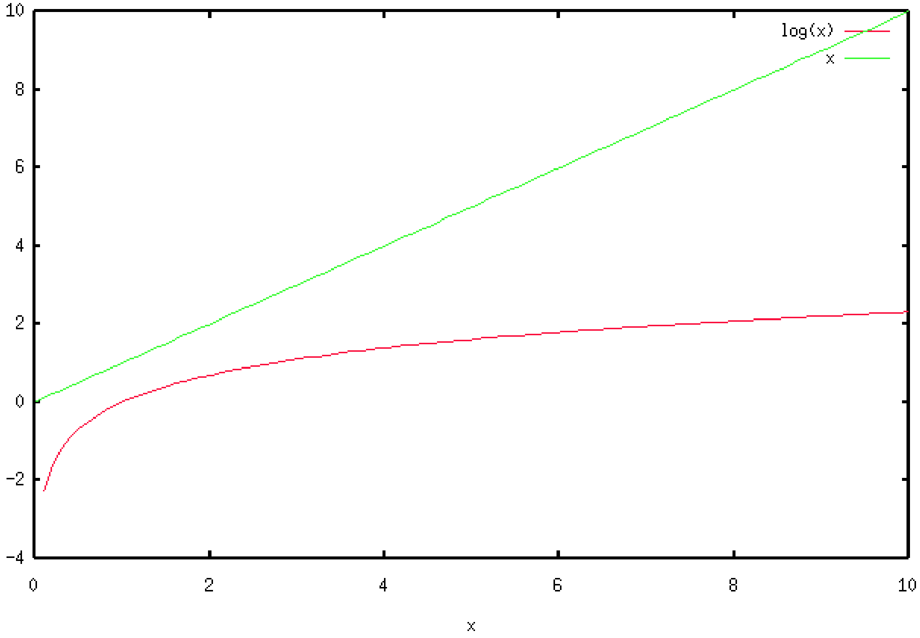
$\log_2 (2^{10}\,3^5) = \log_2 (2^{10}) + \log_2 (3^5) = 10 \log_2 (2) + 5\log_2 (3) =$

$= 10 + 5 \log_2 (3)$

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.

Some important functions:Polynomials

- **Polynomial function:**

  Domain = usually R

  Co-domain Range = usually R

  $P_n(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x^1 + a_0$

n, a nonnegative integer is the degree of the polynomial;
$a_n \neq 0$ (so that the term $a_n x^n$ actually appears)

$(a_n, a_{n-1}, \ldots, a_1, a_0)$ are the coefficients of the polynomial.

Ex:

$y = P_1(x) = a_1 x^1 + a_0$ linear function

$y = P_2(x) = a_2 x^2 + a_1 x^1 + a_0$ quadratic polynomial or function

- Exponentials grow MUCH faster than polynomials:

$$\lim_{x\to\infty} \frac{a_0 + \cdots + a_k x^k}{b^x} = 0 \; if \;\; b > 1$$

We’ll talk more about growth rates in the next module….

Sequences

- Definition:

  A sequence $\{a_i\}$ is a function $f: A \subseteq N \cup \{0\} \rightarrow S$, where we write a_i to indicate $f(i)$. We call a_i term I of the sequence.

- Examples:
- Sequence $\{a_i\}$, where $a_i = i$ is just $a_0 = 0, a_1 = 1, a_2 = 2, \ldots$
- Sequence $\{a_i\}$, where $a_i = i^2$ is just $a_0 = 0, a_1 = 1, a_2 = 4, \ldots$

Sequences of the form $a_1, a_2, \ldots, a_n$ are often used in computer science.
(always check whether sequence starts at a_0 or a_1)
These finite sequences are also called strings. The length of a string is the number of terms in the string. The empty string, denoted by λ, is the string that has no terms.

Geometric and Arithmetic Progressions

- Definition: A **geometric progression** is a sequence of the form

$$a, ar, ar^2, ar^3, \cdots, ar^n, \cdots$$

The **initial term *a*** and the common **ratio *r*** are real numbers

Definition: An **arithmetic progression** is a sequence of the form

$$a, a+d, a+2d, a+3d, \cdots, a+nd, \cdots$$

The **initial term *a*** and the common **difference *d*** are real numbers

Note: An arithmetic progression is a discrete analogue of the linear function f(x) = dx + a

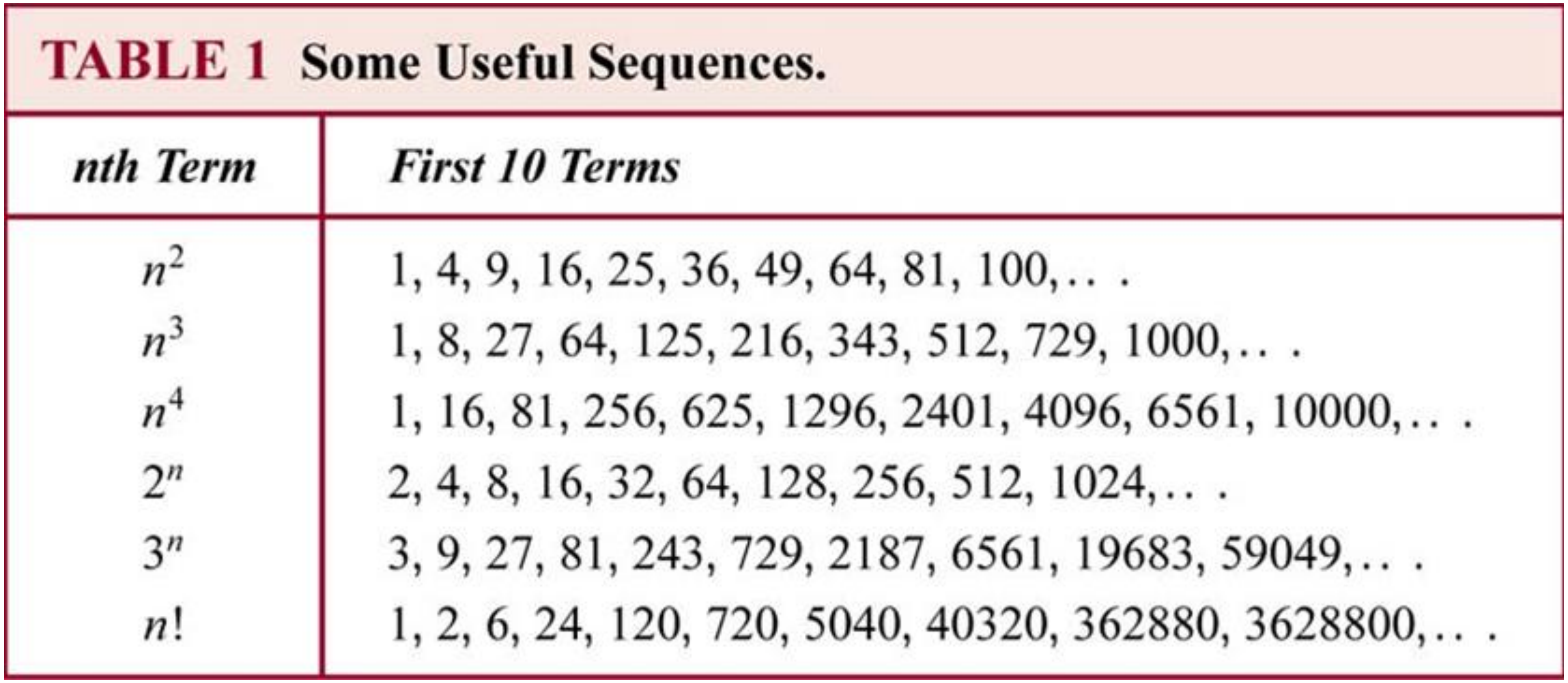


TABLE 1 Some Useful Sequences.

nth Term	*First 10 Terms*
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, . . .
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, . . .
n^4	1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, . . .
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, . . .
3^n	3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, . . .
$n!$	1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, . . .

Notice differences in growth rate.

Summation

- The symbol ∑ (Greek letter sigma) is used to denote summation.

$$\sum_{i=1}^{k} a_i = a_1 + a_2 + \ldots + a_k$$

i is the **index of the summation**, and the choice of letter *i* is arbitrary;

the index of the summation runs through all integers, with its **lower limit** 1 and ending **upper limit** k.

- The limit:

$$\sum_{i=1}^{\infty} a_i = \lim_{n \to \infty} \sum_{i=1}^{n} a_i$$

Summation

- The laws for arithmetic apply to summations

$$\sum_{i=1}^{k}(ca_i + b_i) = c\sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i$$

Use associativity to separate the b terms from the a terms.

Use distributivity to factor the c's.

Summations you should know…

- What is S = 1 + 2 + 3 + … + n?

(little) Gauss in 4th grade. ☺

$$
\begin{array}{ccccccccc}
S & = & 1 & + & 2 & + & \dots & + & n \\
S & = & n & + & n-1 & + & \dots & + & 1 \\
\hline
2s & = & n+1 & + & n+1 & + & \dots & + & n+1
\end{array}
$$

Write the sum.

Write it again.

Add together.

You get n copies of (n+1). But we’ve over added by a factor of 2.
So just divide by 2.

Why whole number?

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

Sum of first n odds.

- What is S = 1 + 3 + 5 + … + (2n - 1)?

$$\sum_{k=1}^{n}(2k-1) = 2\sum_{k=1}^{n}k - \sum_{k=1}^{n}1$$

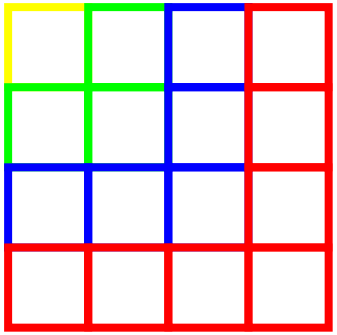
$$= 2\left(\frac{n(n+1)}{2}\right) - n$$

$$= n^2$$

Sum of first n odds.

- What is S = 1 + 3 + 5 + … + (2n - 1)?

$$= n^2$$



Geometric Series

- What is S = 1 + r + r² + … + rⁿ

$$\sum_{k=0}^{n} r^k = 1 + r + \ldots + r^n$$

Multiply by r

$$r\sum_{k=0}^{n} r^k = r + r^2 + \ldots + r^{n+1}$$

Subtract the summations

$$\sum_{k=0}^{n} r^k - r\sum_{k=0}^{n} r^k = 1 - r^{n+1}$$

factor

$$(1-r)\sum_{k=0}^{n} r^k = 1 - r^{n+1}$$

divide

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{(1-r)}$$

DONE!

- What about:

$$\sum_{k=0}^{\infty} r^k = 1 + r + \ldots + r^n + \ldots$$

If r ≥ 1 this blows up.

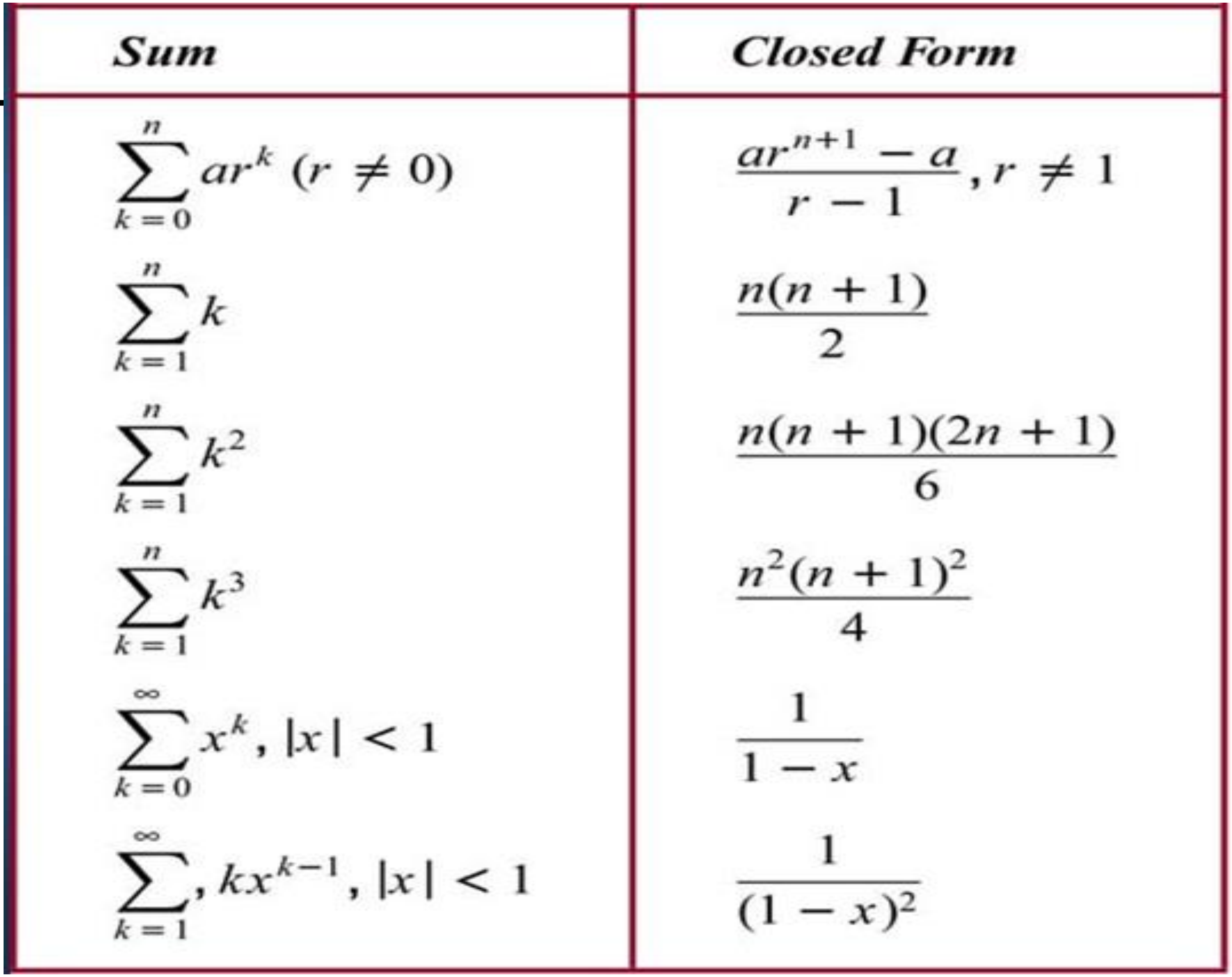
If r < 1 we can say something.

$$\sum_{k=0}^{\infty} r^k = \lim_{n\to\infty} \sum_{k=0}^{n} r^k$$

$$= \lim_{n\to\infty} \frac{1 - r^{n+1}}{(1-r)} \qquad = \frac{1}{(1-r)}$$

Try r = ½.

Useful Summations



Sum	Closed Form
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty}, kx^{k-1}, \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

Infinite Cardinality

- How can we extend the notion of cardinality to infinite sets?
- Definition: Two sets **A and B have the same cardinality** if and only if there exists a bijection (or a one-to-one correspondence) between them, A ~ B.

We split infinite sets into two groups:

1. Sets with the **same cardinality as the set of natural numbers**
2. Sets with **different cardinality as the set of natural numbers**

Infinite Cardinality

- Definition: A set is **countable** if it is **finite** or has the same **cardinality as the set of positive integers.**
- Definition: A set is un**countable** if it is **not countable.**
- Definition: The cardinality of an infinite set S that is countable is denotes by $\aleph_0$ (where $\aleph$ is aleph, the first letter of the Hebrew alphabet).
- We write $|S| = \aleph_0$ and say that S has cardinality “aleph null”

Note: Georg Cantor defined the notion of cardinality and was the first to realize that infinite sets can have different cardinalities. $\aleph_0$ is the cardinality of the natural numbers; the next larger cardinality is aleph-one $\aleph_1$, then, $\aleph_2$ and so on.

Infinite Cardinality: Odd Positive Integers

Example: The set of odd positive integers is a countable set.

Let’s define the function f, from Z^+ to the set of odd positive numbers,

$$f(n) = 2n - 1$$

We have to show that f is both one-to-one and onto.

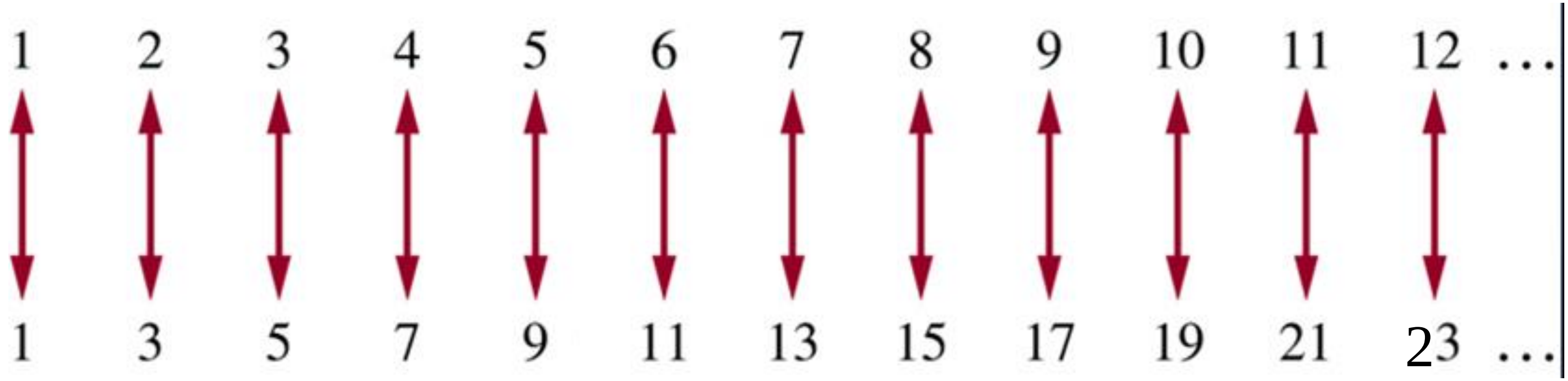
one-to-one

Suppose f(n)= f(m) → 2n-1 = 2m-1 → n=m

onto

Suppose that t is an odd positive integer. Then t is 1 less than an even integer 2k, where k is a natural number. hence t=2k-1= f(k).

Infinite Cardinality: Odd Positive Integers



1 2 3 4 5 6 7 8 9 10 11 12 . . .

1 3 5 7 9 11 13 15 17 19 21 23 . . .

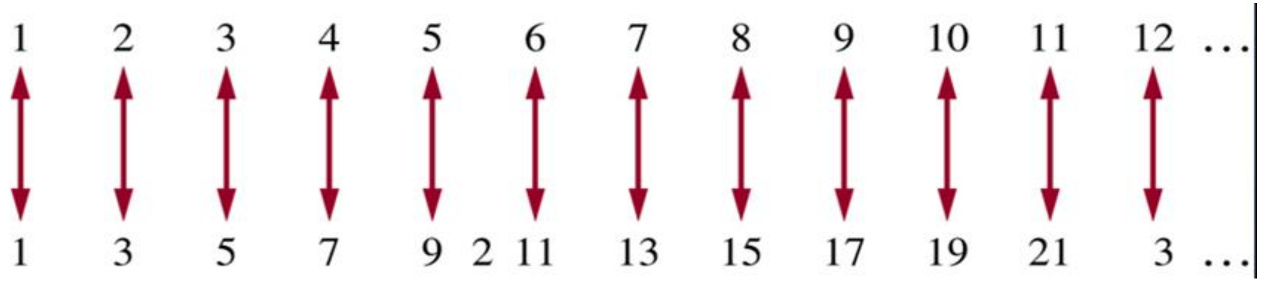
Infinite Cardinality:Integers

Example: **The set of integers is a countable set.**

Lets consider the sequence of all integers, starting with 0: 0,1,-1,2,-2,….

We can define this sequence as a function:

$$f(n) = \begin{cases} n/2 & n \in N, even \\ \dfrac{-(n-1)}{2} & n \in N, odd \end{cases}$$



0 1 -1 2 2

Show at home that it's one-to-one and onto

Infinite Cardinality: Rational Numbers

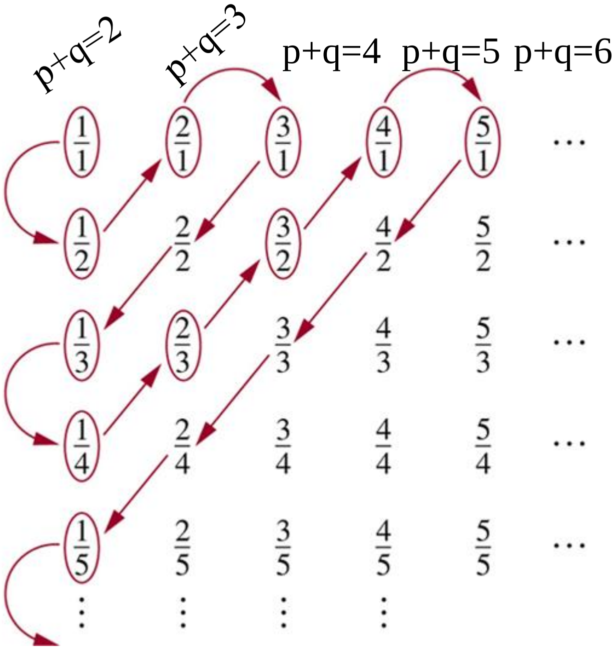
- Example: The set of **positive rational numbers** is a **countable** set.
- Hmm…

Infinite Cardinality: Rational Numbers

Example: The set of **positive rational numbers** is a **countable** set

Key aspect to list the rational numbers as a sequence – every positive number is the quotient p/q of two positive integers.

Visualization of the proof.



Terms not circled are not listed because they repeat previously listed terms

Since all positive rational numbers are listed once, the set of positive rational numbers is countable.

Uncountable Sets: Cantor's diagonal argument

The set of all **infinite sequences of zeros and ones** is **uncountable.**

Consider a sequence,

$$a_1, a_2, \cdots, a_n, n \to \infty, a_i = 0 \; or \; a_i = 1$$

For example:

$$s_1 = (0, 0, 0, 0, 0, 0, 0, \ldots)$$
$$s_2 = (1, 1, 1, 1, 1, 1, 1, \ldots)$$
$$s_3 = (0, 1, 0, 1, 0, 1, 0, \ldots)$$
$$s_4 = (1, 0, 1, 0, 1, 0, 1, \ldots)$$
$$s_5 = (1, 1, 0, 1, 0, 1, 1, \ldots)$$
$$s_6 = (0, 0, 1, 1, 0, 1, 1, \ldots)$$
$$s_7 = (1, 0, 0, 0, 1, 0, 0, \ldots)$$

So in general we have:

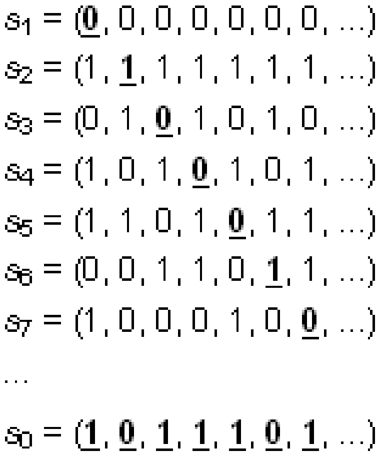
$$s_n = (s_{n,1}, s_{n,2}, s_{n,3}, s_{n,4}, \ldots)$$

i.e., $s_{n,m}$ is the mth element of the nth sequence on the list.

Uncountable Sets: Cantor's diagonal argument

- It is possible to build a sequence, say s_0, in such a way that its first element is different from the first element of the first sequence in the list, its second element is different from the second element of the second sequence in the list, and, in general, its *n*th element is different from the n^{th} element of the n^{th} sequence in the list. In other words, $s_{0,m}$ will be 0 if $s_{m,m}$ is 1, and $s_{0,m}$ will be 1 if $s_{m,m}$ is 0.

Uncountable Sets: Cantor's diagonal argument



$s_1 = (\underline{\mathbf{0}}, 0, 0, 0, 0, 0, 0, \ldots)$

$s_2 = (1, \underline{\mathbf{1}}, 1, 1, 1, 1, 1, \ldots)$

$s_3 = (0, 1, \underline{\mathbf{0}}, 1, 0, 1, 0, \ldots)$

$s_4 = (1, 0, 1, \underline{\mathbf{0}}, 1, 0, 1, \ldots)$

$s_5 = (1, 1, 0, 1, \underline{\mathbf{0}}, 1, 1, \ldots)$

$s_6 = (0, 0, 1, 1, 0, \underline{\mathbf{1}}, 1, \ldots)$

$s_7 = (1, 0, 0, 0, 1, 0, \underline{\mathbf{0}}, \ldots)$

...

$s_0 = (\underline{\mathbf{1}}, \underline{\mathbf{0}}, \underline{\mathbf{1}}, \underline{\mathbf{1}}, \underline{\mathbf{1}}, \underline{\mathbf{0}}, \underline{\mathbf{1}}, \ldots)$

Note: the diagonal elements are highlighted, showing why this is called the **diagonal argument**

- The sequence s_0 is distinct from all the sequences in the list. Why?
- Let’s say that s_0 is identical to the 100th sequence, therefore, $\mathrm{s}_{0,100}=\mathrm{s}_{100,100}$.
- In general, if it appeared as the *n*th sequence on the list, we would have $s_{0,\mathrm{n}} = s_{\mathrm{n,n}}$,
- which, due to the construction of s_0, is impossible.

Uncountable Sets: Cantor's diagonal argument

From this it follows that the set *T*, consisting of all infinite sequences of zeros and ones, cannot be put into a list s_1, s_2, s_3, ...

Otherwise, it would be possible by the above process to construct a sequence s_0 which would both be in *T* (because it is a sequence of 0's and 1's which is by the definition of *T* in *T*) and at the same time not in *T* (because we can deliberately construct it not to be in the list). *T*, containing all such

sequences, must contain s_0, which is just such a sequence. But since s_0 does not appear anywhere on the list, *T* cannot contain s_0.

Therefore *T* cannot be placed in one-to-one correspondence with the natural numbers. In other words, the set of infinite binary strings is **uncountable**.

Real Numbers

Example;

The set of real numbers is an uncountable set.

Let’s assume that the set of real numbers is countable.

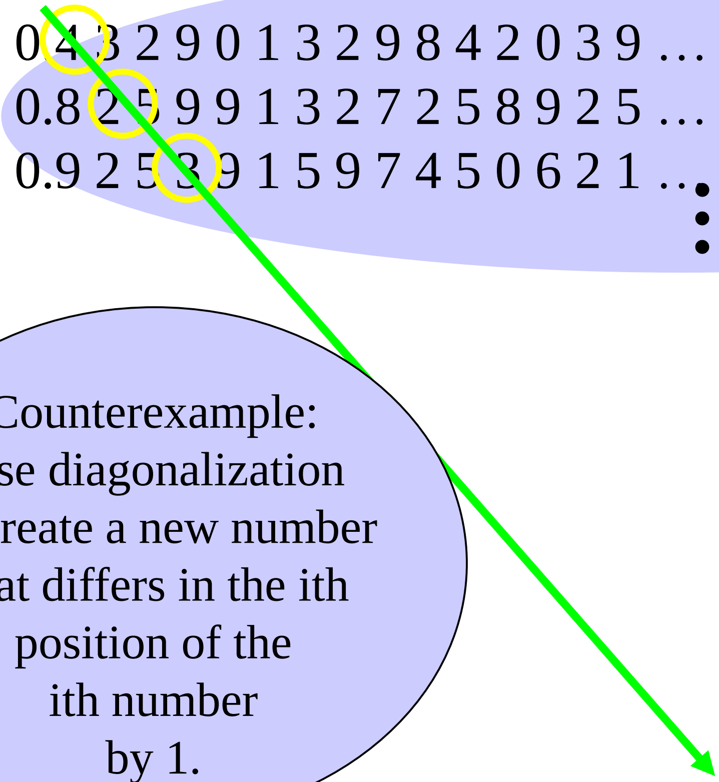
Therefore any subset of it is also countable, in particular the interval [0,1].

How many real numbers are in interval [0, 1]?

Real Numbers

- How many real numbers are in interval [0, 1]?

“Countably many! There’s part of the list!”



0.4 3 2 9 0 1 3 2 9 8 4 2 0 3 9 …
0.8 2 5 9 9 1 3 2 7 2 5 8 9 2 5 …
0.9 2 5 3 9 1 5 9 7 4 5 0 6 2 1 …
⋮

Counterexample:
Use diagonalization
to create a new number
that differs in the ith
position of the
ith number
by 1.

“Are you sure they’re all there?”

0.5 3 6 …
So we say the reals are “uncountable.”