UNIVERSITY AT ALBANY

State University of New York

Lecture 3: Basic Structures: Sets, Function, Sequences etc.

Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: clong2@albany.edu

Recap Previous Lecture

- **Mathematical induction proofs** consists of two steps:

  1) **Basis**: The proposition P(1) is true.

  2) **Inductive Step**: The implication P(n) → P(n+1), is true for all positive n.

  Therefore we conclude ∀ x P(x).

- **Strong induction** uses the basis step P(1) and inductive step P(1) and P(2) … P(n-1) → P(n)

- Based on the **well-ordering property**: Every nonempty set of nonnegative integers has a least element

Recap Previous Lecture

To prove ``$\forall n \in$ N. $P(n)$'' using WOP:

1. Define the set of *counterexamples*

   C ::= $\{n \in$ N $\mid \neg P(n)\}$

2. Assume C is not empty.

3. By WOP, have minimum element $m_0 \in C$.

4. Reach a contradiction (*somehow*)

   – usually by finding a member of C that is $< m_0$.

5. Conclude no counterexamples exist. QED

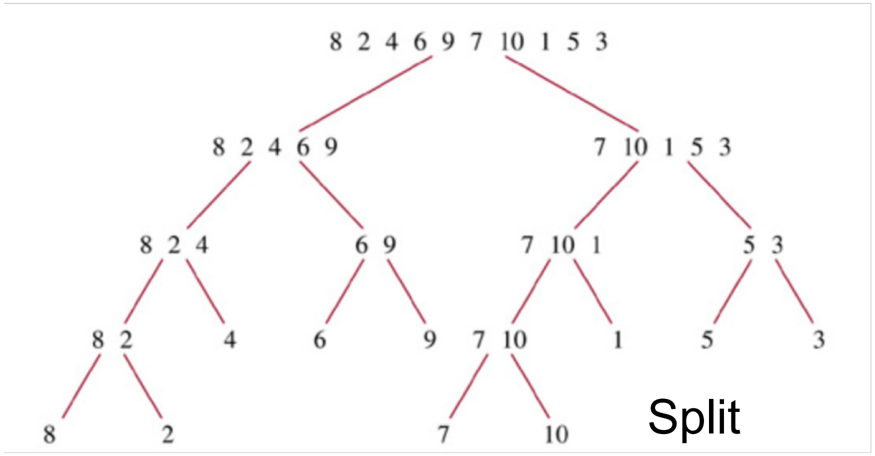
Recap Previous Lecture

- Let *R* be a recursive definition.
- Let *P* be a statement (property) about the elements defined by *R*.

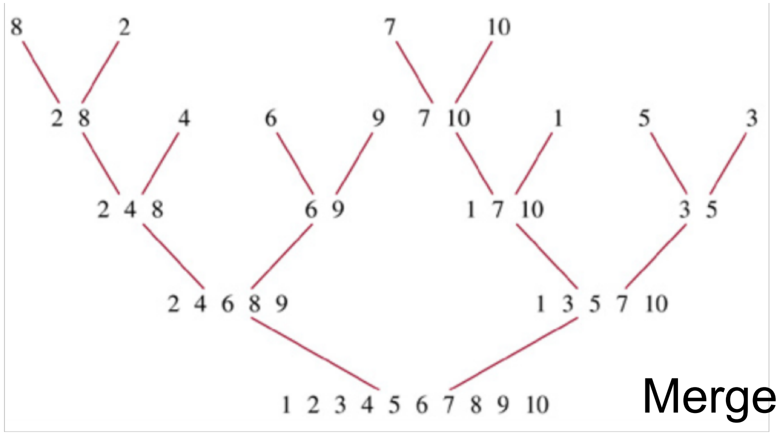
- If the following hypotheses hold:
  - P is **True** for every element $b_1,\ldots,b_m$ in the base case of the definition R.
  - For every element E constructed by the recursive definition from some elements $e_1,\ldots,e_n$: P is **True** for $e_1,\ldots,e_\mathrm{n} \Rightarrow P$ is true for E.
- Then we can conclude that:
- *P* is **True** for every element *E* defined by the recursive definition *R*.

Recap Previous Lecture

- Recursive Algorithms: by reducing it to an instance of the same problem with smaller input.
- Examples:
  - **Recursive Euclid's Algorithm**
  - Recursive Linear Search
  - Recursive Binary Search
  - Recursive Fibonacci Algorithm and iterative Fibonacci Algorithm
  - Recursive Merge Sort (Split and Merge)
  - **Modular Exponentiation**



Split



Merge

Outline

- Set
- Function
- Sequences
- Matrices

Set

Introduction (1)

- We have already implicitly dealt with sets
  - Integers ($\mathbb{Z}$), rationals ($\mathbb{Q}$), naturals ($\mathbb{N}$), reals ($\mathbb{R}$), etc.
- We will develop more fully
  - The definitions of sets
  - The properties of sets
  - The operations on sets
- **Definition**: A set is an unordered collection of (unique) objects
- Sets are fundamental discrete structures and for the basis of more complex discrete structures like graphs

Introduction (2)

- **Definition**: The objects in a set are called elements or members of a set. A set is said to contain its elements
- Notation, for a set A:
  - $x \in A$: x is an element of A   \$\in\$
  - $x \notin A$: x is not an element of A   \$\notin\$
- **Definition**: Two sets, A and B, are equal is they contain the same elements. We write A=B.
- Example:
  - $\{2,3,5,7\}=\{3,2,7,5\}$, because a set is unordered
  - Also, $\{2,3,5,7\}=\{2,2,3,5,3,7\}$ because a set contains unique elements
  - However, $\{2,3,5,7\} \neq \{2,3\}$ \$\neq\$

A set is a collection of well defined and distinct objects.

Terminology (2)

- A multi-set is a set where you specify the number of occurrences of each element: $\{m_1 \cdot a_1, m_2 \cdot a_2, \ldots, m_r \cdot a_r\}$ is a set where
  - m_1 occurs a_1 times
  - m_2 occurs a_2 times
  - …
  - m_r occurs a_r times
- In Databases, we distinguish
  - A set: elements cannot be repeated
  - A bag: elements can be repeated

Terminology (3)

- The **set-builder** notation

  $O=\{ x \mid (x\in\mathbb{Z}) \wedge (x=2k) \text{ for some } k\in Z\}$

  reads: O is the set that contains all x such that x is an integer and x is even
- A set is defined in **intension** when you give its set-builder notation

  $O=\{ x \mid (x\in\mathbb{Z}) \wedge (0\leq x\leq 8) \wedge (x=2k) \text{ for some } k \in Z \}$
- A set is defined in **extension** when you enumerate all the elements:

  $O=\{0,2,4,6,8\}$

More Terminology and Notation (1)

- A set that has no elements is called the **empty set** or **null set** and is denoted $\emptyset$ $\emptyset$
- A set that has one element is called a **singleton set**.
  - For example: {a}, with brackets, is a singleton set
  - a, without brackets, is an element of the set {a}
- Note the subtlety in $\emptyset \neq \{\emptyset\}$
  - The left-hand side is the empty set
  - The right hand-side is a singleton set, and a set containing a set

More Terminology and Notation (2)

- **Definition**: A is said to be a **subset** of B, and we write $A \subseteq B$, if and only if every element of A is also an element of B $\subseteq$
- That is, we have the equivalence:

$$A \subseteq B \Leftrightarrow \forall x\ (x \in A \Rightarrow x \in B)$$

- **Definition**: A set A that is a subset of a set B is called a **proper subset** if $A \neq B$.
- That is there is an element $x \in B$ such that $x \notin A$
- We write: $A \subset B$, A B
- In LaTex: $\subset$, $\subsetneq$

Proving Equivalence (1)

- You may be asked to show that a set is
  - a subset of,
  - proper subset of, or
  - equal to another set.
- To prove that A is a subset of B, use the equivalence discussed earlier $A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$
  - To prove that $A \subseteq B$ it is enough to show that for an arbitrary (nonspecific) element x, $x \in A$ implies that x is also in B.
  - Any proof method can be used.
- To prove that A is a proper subset of B, you must prove
  - A is a subset of B **and**
  - $\exists x\ (x \in B) \wedge (x \notin A)$

Proving Equivalence (2)

- Finally to show that two sets are equal, it is sufficient to show independently (much like a biconditional) that
  - $A \subseteq B$ and
  - $B \subseteq A$
- Logically speaking, you must show the following quantified statements:

  $$(\forall x\ (x \in A \Rightarrow x \in B)) \wedge (\forall x\ (x \in B \Rightarrow x \in A))$$

  we will see an example later..

Power Set

- **Definition**: The power set of a set S, denoted P(S), is the set of all subsets of S.
- Examples
  - Let A={a,b,c}, P(A)={∅,{a},{b},{c},{a,b},{b,c},{a,c},{a,b,c}}
  - Let A={{a,b},c}, P(A)={∅,{{a,b}},{c},{{a,b},c}}
- Note: the empty set ∅ and the set itself are always elements of the power set.
- The power set is a fundamental combinatorial object useful when considering all possible combinations of elements of a set
- **Fact**: Let S be a set such that |S|=n, then

$$|P(S)| = 2^n$$

Tuples (1)

- Sometimes we need to consider ordered collections of objects
- **Definition**: The ordered n-tuple (a_1,a_2,…,a_n) is the ordered collection with the element a_i being the i-th element for i=1,2,…,n
- Two ordered n-tuples (a_1,a_2,…,a_n) and (b_1,b_2,…,b_n) are equal iff for every i=1,2,…,n we have a_i=b_i (a_1,a_2,…,a_n)
- A 2-tuple (n=2) is called an ordered pair

Cartesian Product (1)

- **Definition**: Let A and B be two sets. The Cartesian product of A and B, denoted AxB, is the set of all ordered pairs (a,b) where a$\in$A and b$\in$B

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

- The Cartesian product is also known as the cross product
- **Definition**: A subset of a Cartesian product, R $\subseteq$ AxB is called a relation. We will talk more about relations in the next set of slides
- Note: AxB $\neq$ BxA unless A=$\emptyset$ or B=$\emptyset$ or A=B. Find a counter example to prove this.

Cartesian Product (2)

- Cartesian Products can be generalized for any n-tuple
- **Definition**: The Cartesian product of n sets, $A_1, A_2, \ldots, A_n$, denoted $A_1 \times A_2 \times \ldots \times A_n$, is

$$A_1 \times A_2 \times \ldots \times A_n = \{ (a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i=1,2,\ldots,n\}$$

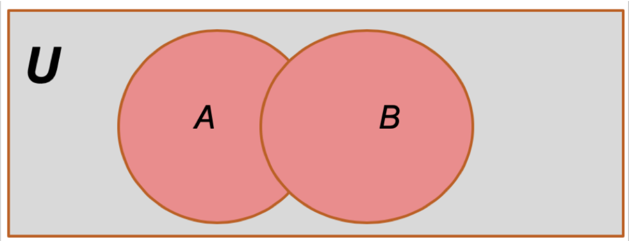
Notation with Quantifiers

- Whenever we wrote $\exists x P(x)$ or $\forall x P(x)$, we specified the universe of discourse using explicit English language
- Now we can simplify things using set notation!
- Example
  - $\forall\ x \in \mathbb{R}\ (x^2 \geq 0)$
  - $\exists\ x \in \mathbb{Z}\ (x^2 = 1)$
  - Also mixing quantifiers:

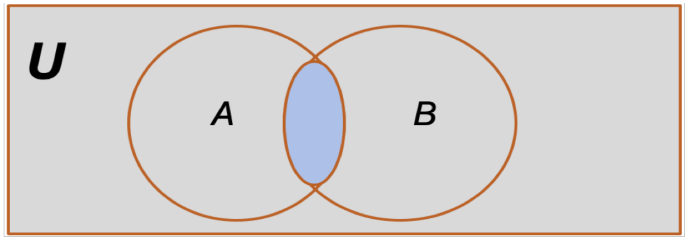
$$\forall a,b,c \in \mathbb{R}\ \exists\ x \in \mathbb{C}\ (ax^2+bx+c=0)$$

Set Operations

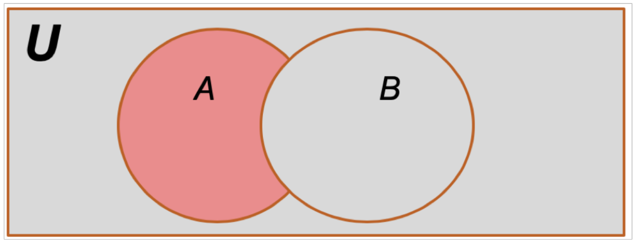
- Similarly, set operators exist and act on two sets to give us new sets
  - Union $\cup$ and intersection $\cap$
  - Set difference $\setminus$
  - Set complement $\overline{S}$



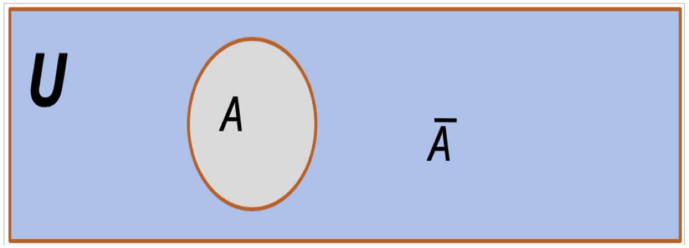
$A \cup B = \{ x \mid (a \in A) \vee (b \in B) \}$



$A \cap B = \{ x \mid (a \in A) \wedge (b \in B) \}$



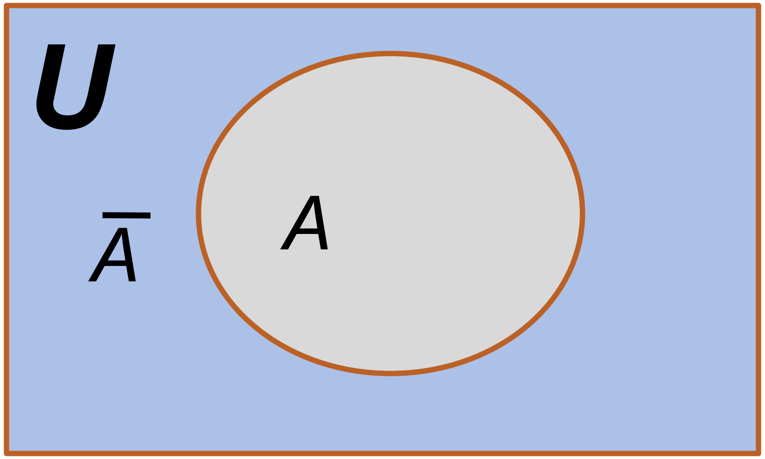
$A - B$

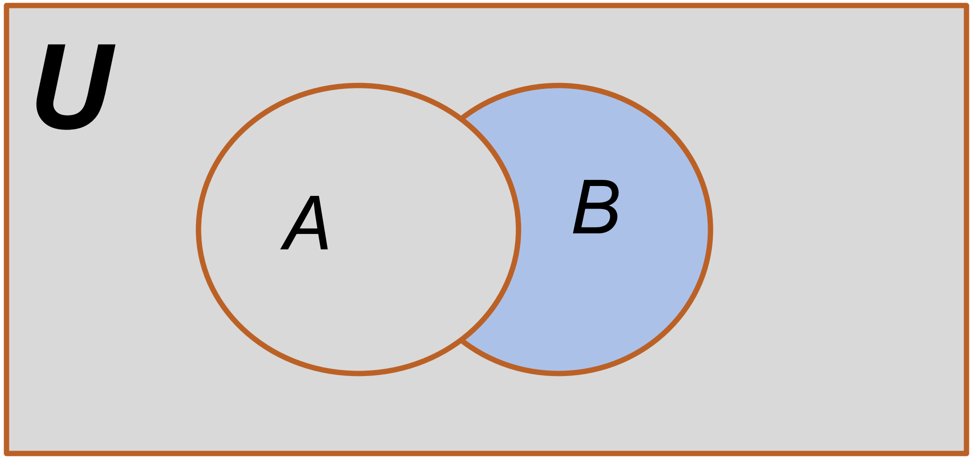


$\overline{A} = A^C = \{x \mid x \notin A\}$

Set Complement: Absolute & Relative

- Given the Universe U, and A,B $\subset$ U.
- The (absolute) complement of A is A=U\A
- The (relative) complement of A in B is B\A





Generalized Union

- **Definition**: The union of a collection of sets is the set that contains those elements that are members of at least one set in the collection

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$$

LaTeX: $\Bigcup_{i=1}^{n}A_i=A_1\cup A_2 \cup\ldots\cup A_n$

Generalized Intersection

- **Definition**: The intersection of a collection of sets is the set that contains those elements that are members of every set in the collection

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

LaTex: $\Bigcap_{i=1}^{n}A_i=A_1\cap A_2 \cap\ldots\cap A_n$

Computer Representation of Sets (1)

- There really aren’t ways to represent infinite sets by a computer since a computer has a finite amount of memory
- If we assume that the universal set U is finite, then we can easily and effectively represent sets by bit vectors
- Specifically, we force an ordering on the objects, say:

$$U=\{a_1, a_2,\ldots,a_n\}$$

- For a set $A \subseteq U$, a bit vector can be defined as, for $i=1,2,\ldots,n$
  - $b_i=0$ if $a_i \notin A$
  - $b_i=1$ if $a_i \in A$

Computer Representation of Sets (2)

- Examples
  - Let U={0,1,2,3,4,5,6,7} and A={0,1,6,7}
  - The bit vector representing A is: 1100 0011
  - How is the empty set represented?
  - How is U represented?
- Set operations become trivial when sets are represented by bit vectors
  - Union is obtained by making the bit-wise OR
  - Intersection is obtained by making the bit-wise AND

Computer Representation of Sets (3)

- Let U={0,1,2,3,4,5,6,7}, A={0,1,6,7}, B={0,4,5}
- What is the bit-vector representation of B?
- Compute, bit-wise, the bit-vector representation of A∩B
- Compute, bit-wise, the bit-vector representation of A∪B
- What sets do these bit vectors represent?

Programming Question

- Using bit vector, we can represent sets of cardinality equal to the size of the vector
- What if we want to represent an arbitrary sized set in a computer (i.e., that we do not know a priori the size of the set)?
- What data structure could we use?

How to Compare Infinities?

Cardinality

- "The number of elements in a set."
- Let A be a set.

a. If $A = \varnothing$ (the empty set), then the cardinality of A is 0.

b. If A has exactly n elements, n a natural number, then the cardinality of A is n. The set A is a ***finite*** *set*

c. Otherwise, A is an ***infinite*** *set*.

Cardinality Notations

- The cardinality of a set A is denoted by $|A|$.

a. If $A = \varnothing$, then $|A| = 0$.

b. If A has exactly n elements, then $|A| = n$.

c. If A is an infinite set, then $|A| = \infty$.

Examples

- $A = \{2, 3, 5, 7, 11, 13, 17, 19\}$; $|A| = 8$
- $A = N$ (natural numbers); $|N| = \infty$
- $A = Q$ (rational numbers); $|Q| = \infty$
- $A = \{2n \mid n$ is an integer$\}$; $|A| = \infty$

  (the set of even integers)

Equal Cardinality

DEFINITION:

- Let A and B be sets. Then, $|A| = |B|$ if and only if there is a one-to-one correspondence between the elements of A and the elements of B.

- If there is a one-to-one function (*i.e.*, an **injection**) from A to B, the cardinality of A is less than or the same as the cardinality of B and we write $|A| \leq |B|$.

- When $|A| \leq |B|$ and A and B have different cardinality, we say that the cardinality of A is less than the cardinality of B and write $|A| < |B|$.

Example

1. $A = \{1, 2, 3, 4, 5\}$

   $B = \{a, e, i, o, u\}$

   $1 \rightarrow a,\ 2 \rightarrow e,\ 3 \rightarrow i,\ 4 \rightarrow o,\ 5 \rightarrow u; \quad |B| = 5$

Example

- 2. $A = N$ (the natural numbers)

  $B = \{2n \mid n$ is a natural number$\}$ (the even natural numbers)

  $n \rightarrow 2n$ is a one-to one correspondence between A and B. Therefore, $|A| = |B|$; $|B| = \infty$.

Example

- 3. $A = N$ (the natural numbers)

  $C = \{2n - 1 \mid n$ is a natural number$\}$ (the odd natural numbers)

  $n \rightarrow 2n - 1$ is a one-to one correspondence between A and C. Therefore, $|A| = |C|$; $|C| = \infty$.

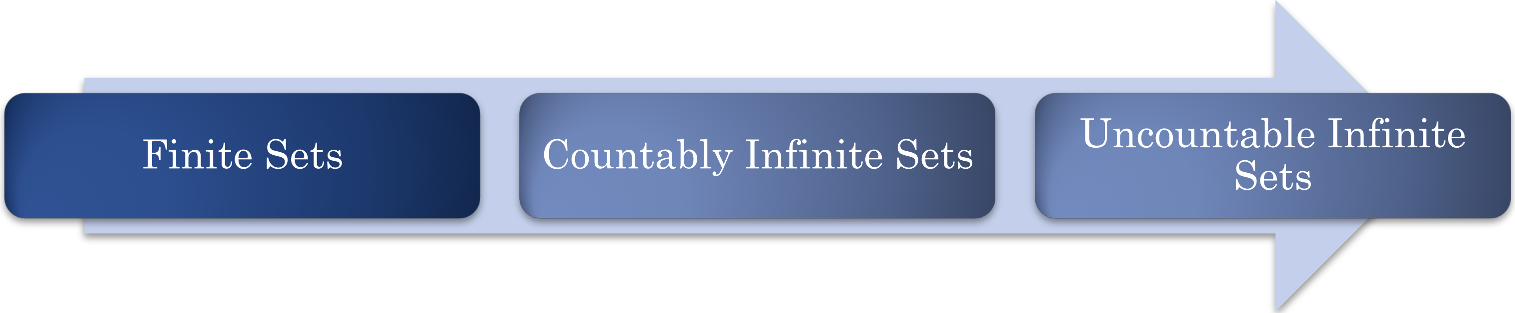
Countable Sets

DEFINITIONS:

- 1. A set *S* is *finite* if there is a one-to-one correspondence between it and the set {1, 2, 3, . . ., *n*} for some natural number *n.*
- 2. A set *S* is *countably infinite* if there is a one-to-one correspondence between it and the natural numbers *N.*
- *3.* A set *S* is *countable* if it is either finite or countably infinite.
- 4. A set *S* is *uncountable* if it is not countable.

Levels of the Infinity

- A set that is either finite or has the **same cardinality** as the set of **natural numbers** (or $\mathbf{Z}^+$) is called **countable**.
- A set that is not countable is **uncountable**.
- The set of real numbers **R** is an uncountable set.
- When an infinite set is countable (**countably infinite**) its cardinality is $\aleph_0$ or "aleph null"(where $\aleph$ is aleph, the 1st letter of the Hebrew alphabet).



Showing That a Set is Countable

- An infinite set is countable if and only if it is possible to list the elements of the set in a sequence (indexed by the positive integers).
- The reason for this is that a one-to-one correspondence ***f*** from the set of positive integers to a set *S* can be expressed in terms of a sequence
  - $a_1, a_2, \ldots, a_n, \ldots$
  - where $a_1 = f(1)$, $a_2 = f(2), \ldots, a_n = f(n), \ldots$

Example

- 1. $A = \{1, 2, 3, 4, 5, 6, 7\}$,

  $\Omega = \{a, b, c, d, . . . x, y, z\}$ are finite sets;

  $|A| = 7, \ |\Omega| = 26$.

- 2. N (the natural numbers), Z (the integers), and Q (the rational numbers) are countably infinite sets; that is,

  $|Q| = |Z| = |N|.$

- 3. I (the irrational numbers) and $\Re$ (the real numbers) are uncountable sets; that is

  $|I| > |N|$ and $|\Re| > |N|.$

Some Facts

1. A set S is finite if and only if for any proper subset $A \subset S$, $|A| < |S|$; that is, "proper subsets of a finite set have fewer elements."

2. Suppose that A and B are infinite sets and $A \subseteq B$. If B is countably infinite then A is countably infinite and $|A| = |B|$.

3. Every subset of a countable set is countable.

4. If A and B are countable sets, then $A \cup B$ is a countable set.

Cardinality in Practice

- **Problem:** Prove that Cartesian product of two countable sets is a countable set.
- **Solution:**
- Let *A* and *B* are countable sets. Then *A* × *B* is a set of ordered pairs <*a*, *b*> such that $a \in A$ and $b \in B$.
- If we group all pairs that have the same first element ($\forall a \in A \rightarrow \{a\} \times B$) then there is a bijective function for each group from *B* to the group. As *B* is countable set then each group is a countable set too.
- Number of such groups is equal to the number of elements of *A*, which is countable set. Hence countable sequence of the countable sets is a countable set, as desired.
- **At home:** Prove that **N** x **N** is countable.

Cardinality in Practice

- **Problem:** Show that the set of finite strings (words) *W* over an alphabet *A* = {0, 1} is countably infinite.
- **Solution**:

1. It is easy to define a bijective function from **N** to *A*.
2. Let's group all words by the lengths starting from 1 letter.
3. All words in a group could be ordered in "a dictionary" order.
4. Ordering implies a bijection from **N** to a set, *i.e.* makes a set countable.
5. Countable sequence of countable sets is a countable set.

At home: Show that the set of finite strings (words) *W* over any finite alphabet *A* is countably infinite.

If the Set of C programs Countable?

- **Problem**: Show that the set of all C programs is countable.

Solution: Let's consider a C code as a one string constructed from the characters which can appear in a C program. Then see above.

Cardinality in Use

- The idea of the cardinality of sets is used to compare finite, countable infinite and uncountable infinite sets.
- One of the most important theorems of the theory of sets says that the set and the power set of this set may not have equal cardinality.
- The theory may result in paradoxes in practice:
  - A barber follows the rule to shave everybody in the town who does not shave himself.
  - Should he shave himself?
- Suppose *x* is a set of the sets that are not elements of itself. Would be *x* an element of *x*:
  - If $\forall y \in x \Leftrightarrow x \notin x$, then $\exists\ y = x$, such that $x \in x \Leftrightarrow x \notin x$.
-

Function

Introduction

- You have already encountered function
  - $f(x,y) = x+y$
  - $f(x) = x$
  - $f(x) = \sin(x)$
- Here we will study functions defined on discrete domains and ranges
- We will generalize functions to mappings
- We may not always be able to write function in a ‘neat way’ as above

Definition: Function

- **Definition**: A function f from a set A to a set B is an assignment of exactly one element of B to each element of A.
- We write *f*(a)=b if b is the unique element of B assigned by the function f to the element a $\in$ A.
- If *f* is a function from A to B, we write

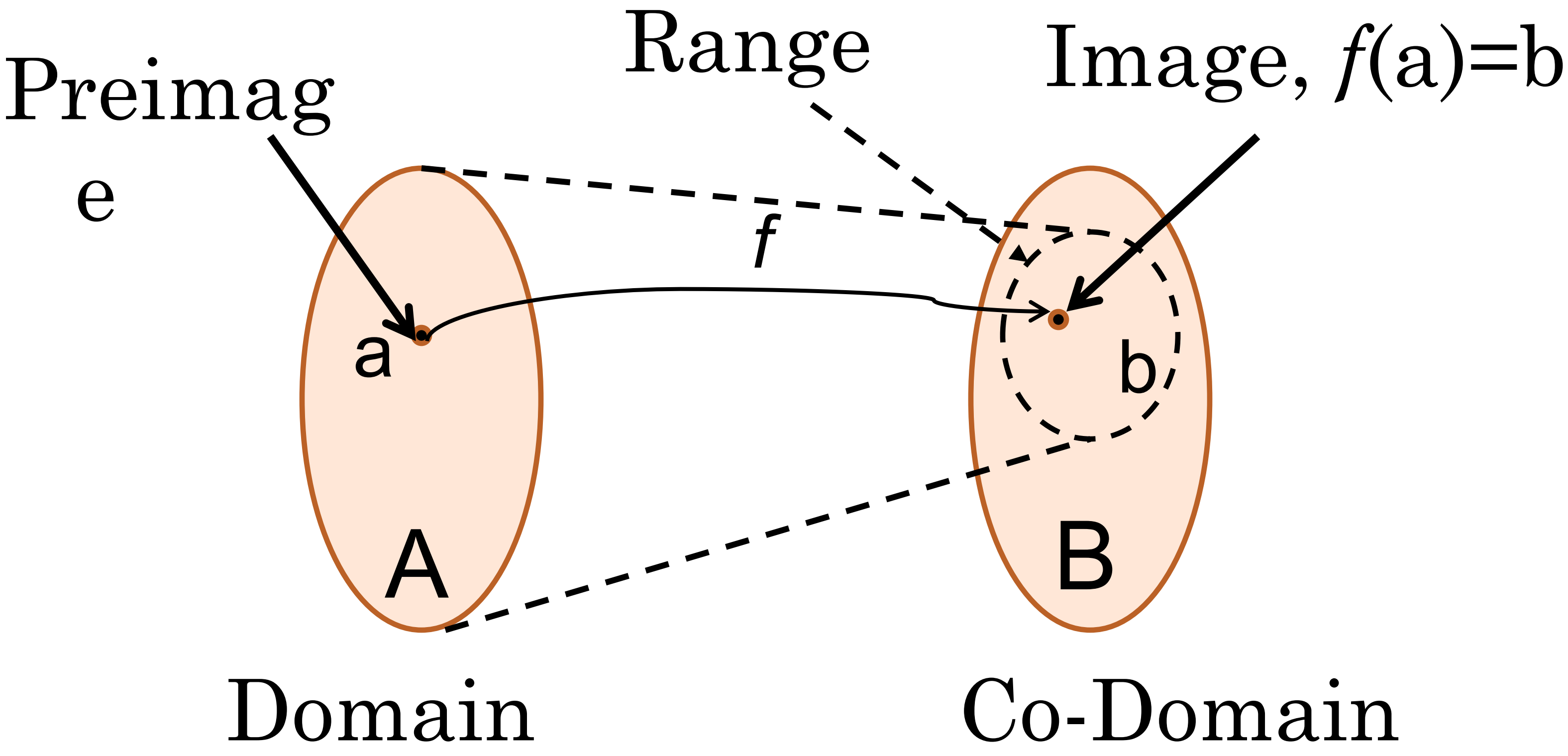
  $$f: A \rightarrow B$$

  This can be read as '*f* maps A to B'
- Note the subtlety
  - Each and every element of A has a single mapping
  - Each element of B may be mapped to by several elements in A or not at all

Terminology

- Let *f*: A → B and *f*(a)=b. Then we use the following terminology:
  - A is the domain of *f*, denoted dom(*f*)
  - B is the co-domain of *f*
  - b is the image of a
  - a is the preimage (antecedent) of b
  - The range of f is the set of all images of elements of A, denoted rng(*f*)

Function: Visualization



A function, f: A → B

More Definitions (1)

- **Definition**: Let f_1 and f_2 be two functions from a set A to $\mathbb{R}$. Then f_1+f_2 and f_1f_2 are also function from A to R defined by:
  - $(f_1+f_2)(x) = f_1(x) + f_2(x)$
  - $f_1f_2(x)= f_1(x)f_2(x)$
- Example: Let $f_1(x)=x^4+2x^2+1$ and $f_2(x)=2-x^2$
  - $(f_1+f_2)(x) = x^4+2x^2+1+2-x^2 = x^4+x^2+3$
  - $f_1f_2(x) = (x^4+2x^2+1)(2-x^2)= -x^6+3x^2+2$

More Definitions (2)

- **Definition**: Let f: A→ B and S $\subseteq$A. The image of the set S is the subset of B that consists of all the images of the elements of S. We denote the image of S by f(S), so that

$$f(S)=\{ f(s) \mid \forall\ s \in S \}$$

- Note there that the image of S is a set and not an element.

More Definitions (3)

- **Definition**: A function *f* whose domain and codomain are subsets of the set of real numbers ($\mathbb{R}$) is called
  - strictly increasing if $f(x)<f(y)$ whenever $x<y$ and x and y are in the domain of *f*.
  - strictly decreasing if $f(x)>f(y)$ whenever $x<y$ and x and y are in the domain of *f*.
- A function that is increasing or decreasing is said to be monotonic

Definition: Injection

- **Definition**: A function *f* is said to be one-to-one or injective (or an injection) if

  $\forall$ x and y in in the domain of *f*, $f(x)=f(y) \Rightarrow x=y$

- Intuitively, an injection simply means that each element in the range has at most one preimage (antecedent)
- It is useful to think of the contrapositive of this definition

$$x \neq y \;\Rightarrow\; f(x) \neq f(y)$$

Definition: Surjection

- **Definition**: A function *f*: A→B is called onto or surjective (or an surjection) if

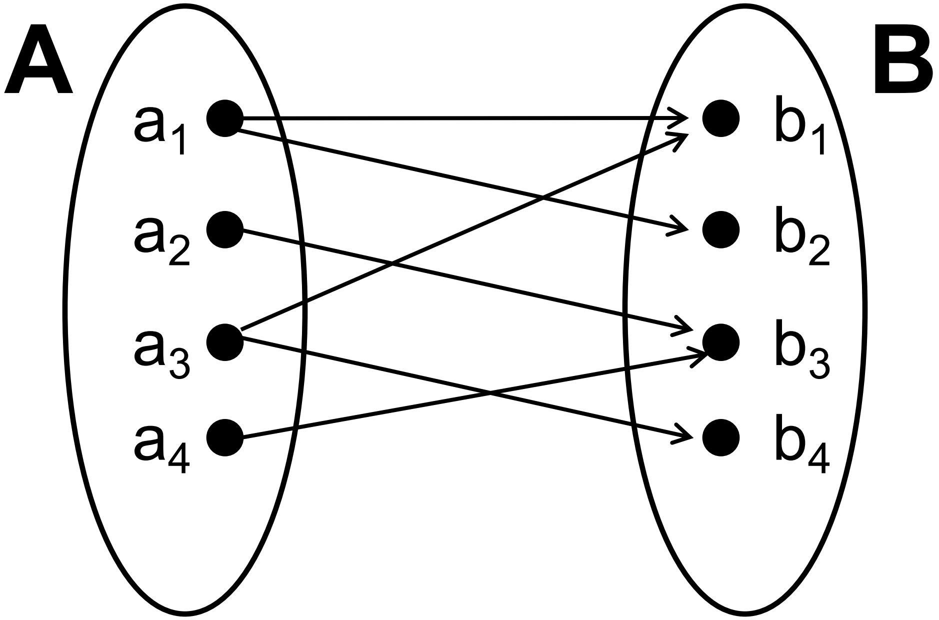
$$\forall\ b \in B,\ \exists\ a \in A \text{ with } f(a)=b$$

- Intuitively, a surjection means that every element in the codomain is mapped into (i.e., it is an image, has an antecedent)
- Thus, the range is the same as the codomain

Definition: Bijection

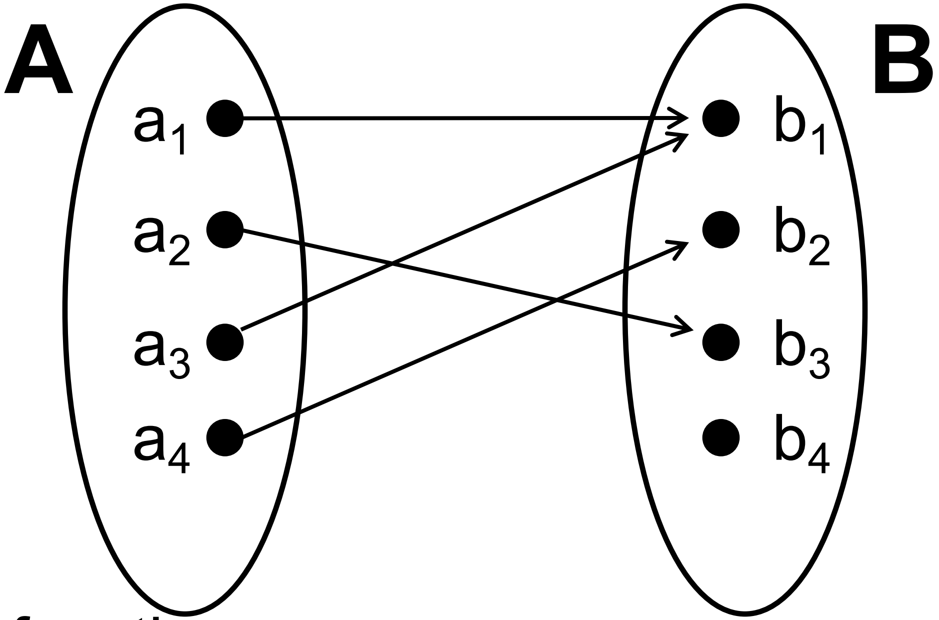
- **Definition**: A function *f* is a one-to-one correspondence (or a bijection), if is both one-to-one (injective) and onto (surjective)
- One-to-one correspondences are important because they endow a function with an inverse.
- They also allow us to have a concept cardinality for infinite sets
- Let's look at a few examples to develop a feel for these definitions…

Functions: Example 1



- Is this a function? Why?
- No, because each of a_1, a_2 has two images

Functions: Example 2

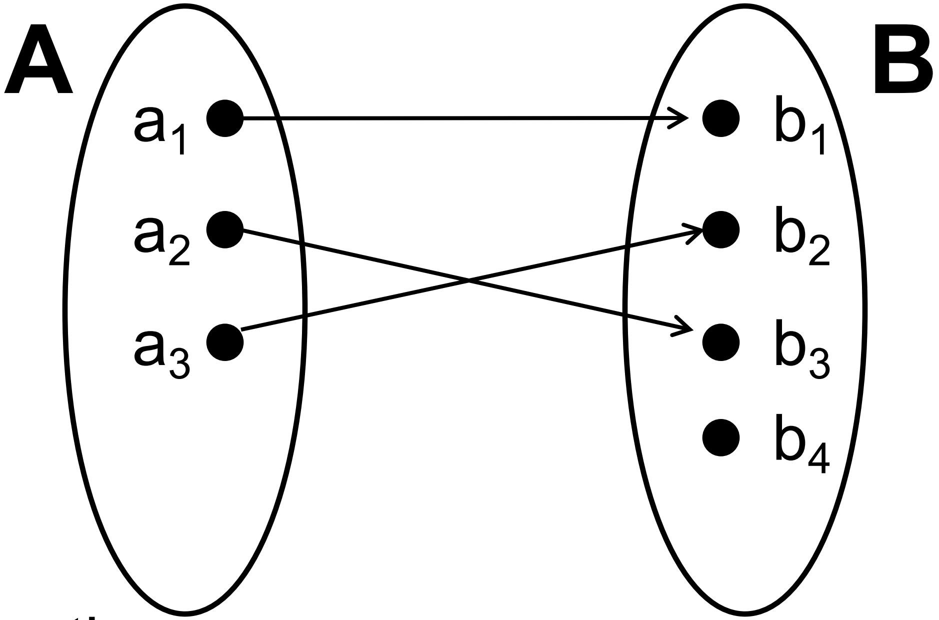


- Is this a function
  - One-to-one (injective)? Why?
  - Onto (surjective)? Why?

No, b_1 has 2 preimages

No, b_4 has no preimage

Functions: Example 3

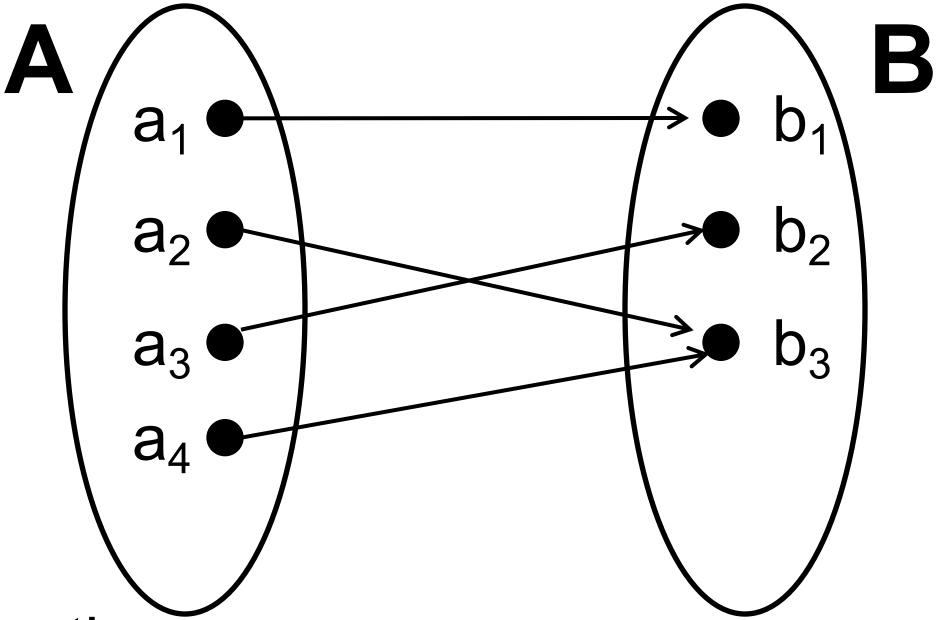


- Is this a function
  - One-to-one (injective)? Why?
  - Onto (surjective)? Why?

Yes, no b_i has 2 preimages

No, b_4 has no preimage

Functions: Example 4

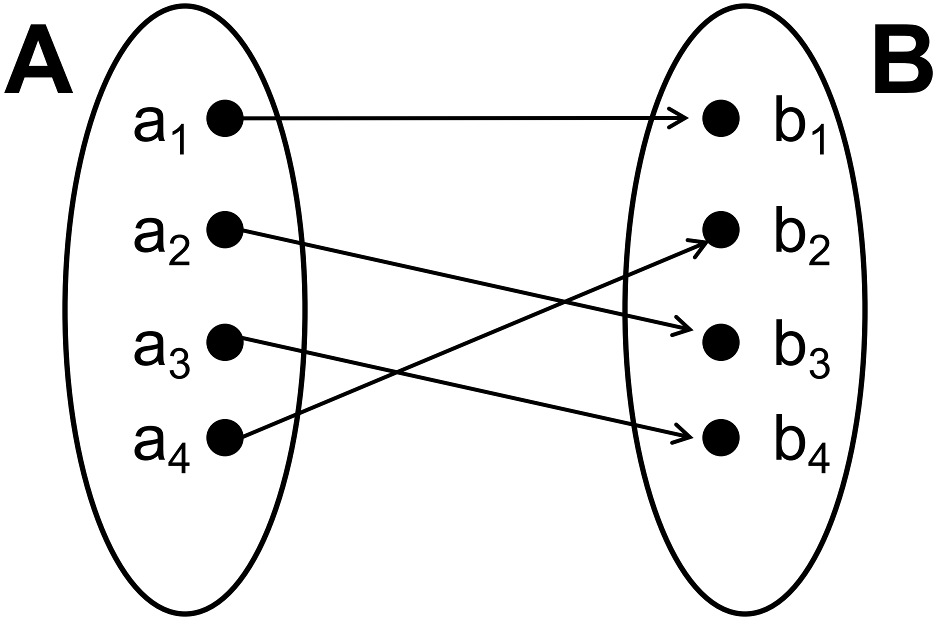


- Is this a function
  - One-to-one (injective)? Why?
  - Onto (surjective)? Why?

No, b_3 has 2 preimages

Yes, every b_i has a preimage

Functions: Example 5



- Is this a function
  - One-to-one (injective)?
  - Onto (surjective)?

Thus, it is a bijection or a one-to-one correspondence

Exercice 1

- Let $f:\mathbb{Z}\rightarrow\mathbb{Z}$ be defined by

$$f(x)=2x-3$$

- What is the domain, codomain, range of f?
- Is f one-to-one (injective)?
- Is f onto (surjective)?
- Clearly, dom(f)=$\mathbb{Z}$. To see what the range is, note that:

  $b\in$ rng(f) $\Leftrightarrow$ $b=2a-3$, with $a\in\mathbb{Z}$

  $\Leftrightarrow$ $b=2(a-2)+1$

  $\Leftrightarrow$ b is odd

Exercise 1 (cont'd)

- Thus, the range is the set of all odd integers
- Since the range and the codomain are different (i.e., rng(*f*) $\neq \mathbb{Z}$), we can conclude that *f* is not onto (surjective)
- However, *f* is one-to-one injective. Using simple algebra, we have:

$$f(x_1) = f(x_2) \Rightarrow 2x_1-3 = 2x_2-3 \Rightarrow x_1 = x_2 \quad \text{QED}$$

Exercise 2

- Let *f* be as before

  $$f(x)=2x-3$$

  but now we define $f:\mathbb{N}\to\mathbb{N}$
- What is the domain and range of *f*?
- Is *f* onto (surjective)?
- Is *f* one-to-one (injective)?

- By changing the domain and codomain of *f*, *f* is not even a function anymore. Indeed, $f(1)=2\cdot1-3=-1\notin\mathbb{N}$

Exercice 3

- Let f:$\mathbb{Z}\rightarrow\mathbb{Z}$ be defined by

$$f(x) = x^2 - 5x + 5$$

- Is this function
  - One-to-one?
  - Onto?

Exercice 3: Answer

- It is not one-to-one (injective)

$f(x_1)=f(x_2) \Rightarrow x_1^2-5x_1+5=x_2^2 - 5x_2+5 \Rightarrow x_1^2 - 5x_1 = x_2^2 - 5x_2$

$\Rightarrow x_1^2 - x_2^2 = 5x_1 - 5x_2 \Rightarrow (x_1 - x_2)(x_1 + x_2) = 5(x_1 - x_2)$

$\Rightarrow (x_1 + x_2) = 5$

Many $x_1,x_2 \in \mathbb{Z}$ satisfy this equality. There are thus an infinite number of solutions. In particular, $f(2)=f(3)=-1$

- It is also not onto (surjective).

The function is a parabola with a global minimum at (5/2,-5/4). Therefore, the function fails to map to any integer less than -1

- What would happen if we changed the domain/codomain?

Exercice 4

- Let $f:\mathbb{Z}\rightarrow\mathbb{Z}$ be defined by

$$f(x) = 2x^2 + 7x$$

- Is this function
  - One-to-one (injective)?
  - Onto (surjective)?
- Again, this is a parabola, it cannot be onto (where is the global minimum?)

Exercice 4: Answer

- However, it is one-to-one! Indeed:

$f(x_1)=f(x_2) \Rightarrow 2x_1^2+7x_1=2x_2^2 + 7x_2 \Rightarrow 2x_1^2 - 2x_2^2 = 7x_2 - 7x_1$

$\Rightarrow 2(x_1 - x_2)(x_1 + x_2) = 7(x_2 - x_1) \Rightarrow 2(x_1 + x_2) = -7 \Rightarrow (x_1 + x_2) = -7$

$\Rightarrow (x_1 + x_2) = -7/2$

But -7/2 $\notin$ Z. Therefore it must be the case that $x_1 = x_2$.

It follows that *f* is a one-to-one function.
QED

Exercise 5

- Let f:$\mathbb{Z}\rightarrow\mathbb{Z}$ be defined by

$$f(x) = 3x^3 – x$$

- Is this function
  - One-to-one (injective)?
  - Onto (surjective)?

Exercice 5: *f* is one-to-one

- To check if *f* is one-to-one, again we suppose that for $x_1,x_2 \in \mathbb{Z}$ we have $f(x_1)=f(x_2)$

  $f(x_1)=f(x_2) \Rightarrow 3x_1^3-x_1=3x_2^3-x_2$

  $\Rightarrow 3x_1^3 - 3x_2^3 = x_1 - x_2$

  $\Rightarrow 3 (x_1 - x_2)(x_1^2 +x_1x_2+x_2^2)= (x_1 - x_2)$

  $\Rightarrow (x_1^2 +x_1x_2+x_2^2)= 1/3$

  which is impossible because $x_1,x_2 \in \mathbb{Z}$

  thus, *f* is one-to-one

Exercice 5: *f* is not onto

- Consider the counter example *f*(a)=1
- If this were true, we would have

  $3a^3 – a=1 \Rightarrow a(3a^2 – 1)=1$ where a and $(3a^2 – 1) \in \mathbb{Z}$
- The only time we can have the product of two integers equal to 1 is when they are both equal to 1 or -1
- Neither 1 nor -1 satisfy the above equality
  - Thus, we have identified $1 \in \mathbb{Z}$ that does not have an antecedent and *f* is not onto (surjective)

Inverse Functions (1)

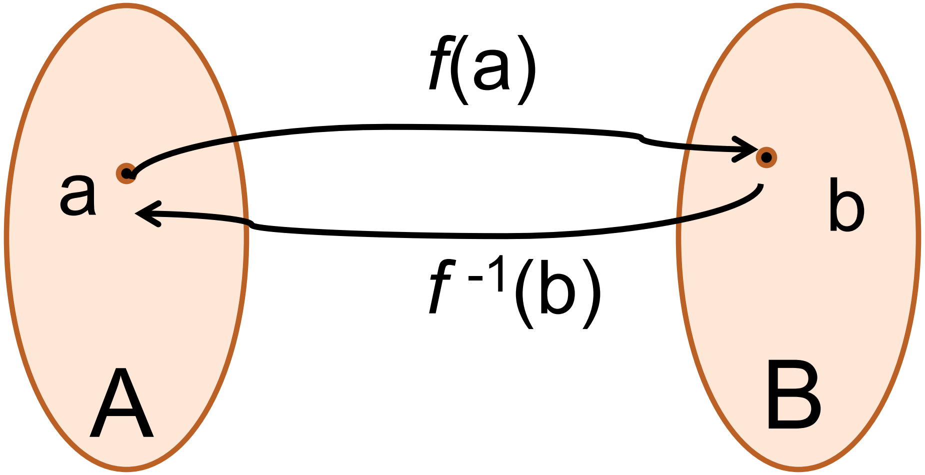
- **Definition**: Let f: A→B be a bijection. The <u>inverse</u> function of f is the function that assigns to an element b∈B the unique element a∈A such that f(a)=b
- The inverse function is denote f^{-1}.
- When f is a bijection, its inverse exists and

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

Inverse Functions (2)

- Note that by definition, a function can have an inverse if and only if it is a bijection. Thus, we say that a bijection is <u>invertible</u>
- Why must a function be bijective to have an inverse?
  - Consider the case where f is not one-to-one (not injective). This means that some element $b \in B$ has more than one antecedent in A, say a_1 and a_2. How can we define an inverse? Does $f^{-1}(b)=a_1$ or a_2?
  - Consider the case where f is not onto (not surjective). This means that there is some element $b \in B$ that does not have any preimage $a \in A$. What is then $f^{-1}(b)$?

Inverse Functions: Representation



Domai

Co-Domain

n A function and its inverse

Inverse Functions Example

- Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = 2x - 3$$

- What is f^{-1}?

1. We must verify that f is invertible, that is, is a bijection. We prove that is one-to-one (injective) and onto (surjective). It is.
2. To find the inverse, we use the substitution
   - Let $f^{-1}(y)=x$
   - And y=2x-3, which we solve for x. Clearly, x= (y+3)/2
   - So, $f^{-1}(y)= (y+3)/2$

Function Composition (1)

- The value of functions can be used as the input to other functions
- **Definition**: Let g:A→B and f:B →C. The <u>composition</u> of the functions f and g is

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

- $f \circ g$ is read as ‘*f* circle *g*’, or ‘*f* composed with *g*’, ‘*f* following *g*’, or just ‘*f* of *g*’
- In LaTeX: $\circ$

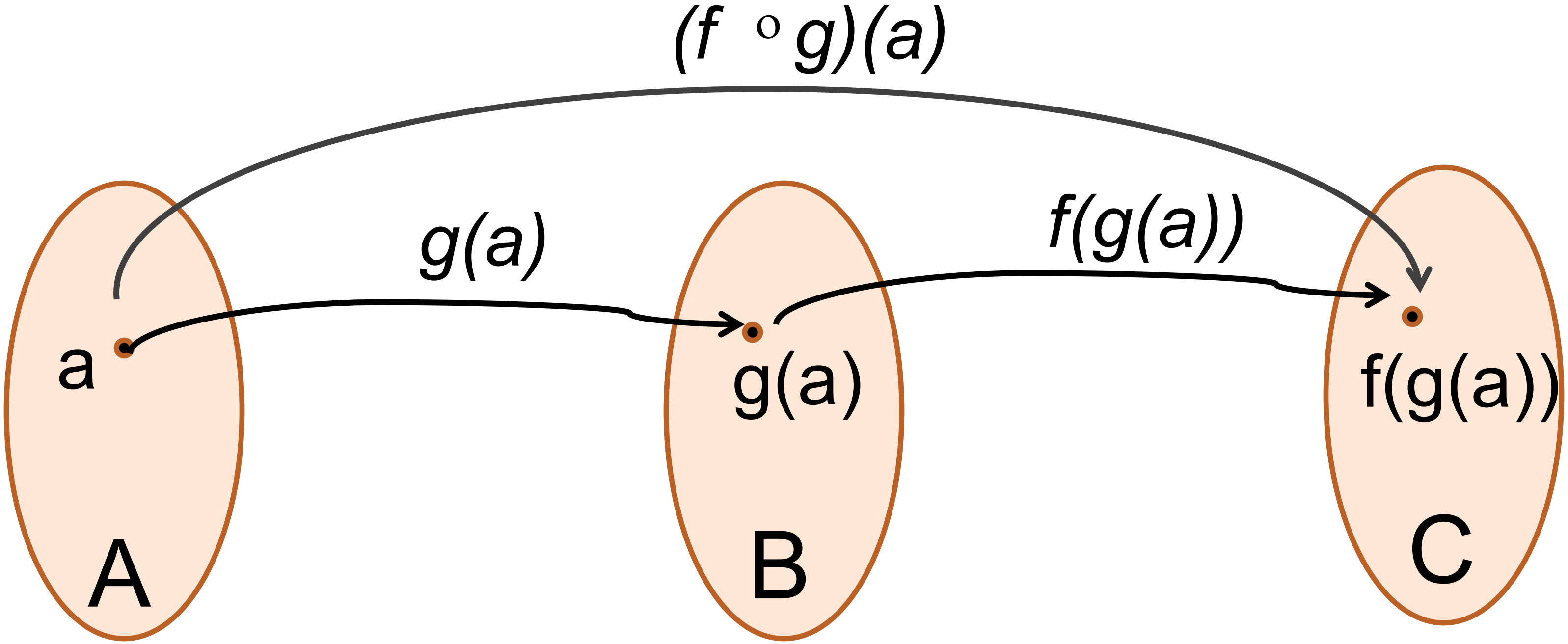
Function Composition (2)

- Because $(f \circ g)(x)=f(g(x))$, the composition $f \circ g$ cannot be defined unless the range of g is a subset of the domain of f

$$f \circ g \text{ is defined } \Leftrightarrow \text{rng}(g) \subseteq \text{dom}(f)$$

- The order in which you apply a function matters: you go from the inner most to the outer most
- It follows that $f \circ g$ is in general not the same as $g \circ f$

Composition: Graphical Representation



The composition of two functions

Composition Example

- Let f, g be two functions on $\mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = 2x - 3$$
$$g(x) = x^2 + 1$$

- What are $f \circ g$ and $g \circ f$?
- We note that
  - f is bijective, thus dom(f)=rng(f)= codomain(f)= $\mathbb{R}$
  - For g, dom(g)= $\mathbb{R}$ but rng(g)=$\{x \in \mathbb{R} \mid x \geq 1\} \subseteq \mathbb{R}^+$
  - Since rng(g)=$\{x \in \mathbb{R} \mid x \geq 1\} \subseteq \mathbb{R}^+ \subseteq$ dom(f) $= \mathbb{R}$, $f \circ g$ is defined
  - Since rng(f)= $\mathbb{R} \subseteq$ dom(g) $= \mathbb{R}$, $g \circ f$ is defined

Composition Example (cont')

- Given $f(x) = 2x – 3$ and $g(x) = x^2 + 1$
- $(f \circ g)(x) = f(g(x)) = f(x^2+1) = 2(x^2+1)-3$
  $= 2x^2 - 1$
- $(g \circ f)(x) = g(f(x)) = g(2x-3) = (2x-3)^2 +1$
  $= 4x^2 - 12x + 10$

Function Equality

- Although it is intuitive, we formally define what it means for two functions to be equal
- **Lemma**: Two functions *f* and *g* are equal if and only
  - $\mathrm{dom}(f) = \mathrm{dom}(g)$
  - $\forall\ a \in \mathrm{dom}(f)\ \ (f(a) = g(a))$

Associativity

- The composition of function is not commutative ($f \circ g \neq g \circ f$), it is associative
- **Lemma**: The composition of functions is an associative operation, that is

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

Important Functions: Identity

- **Definition**: The identity function on a set A is the function

$$\iota: A \rightarrow A$$

ι

defined by $\iota(a)=a$ for all $a \in A$.

- One can view the identity function as a composition of a function and its inverse:

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

- Moreover, the composition of any function *f* with the identity function is itself *f*:

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

Inverses and Identity

- The identity function, along with the composition operation, gives us another characterization of inverses when a function has an inverse
- **Theorem**: The functions f: A→B and g: B→A are inverses if and only if

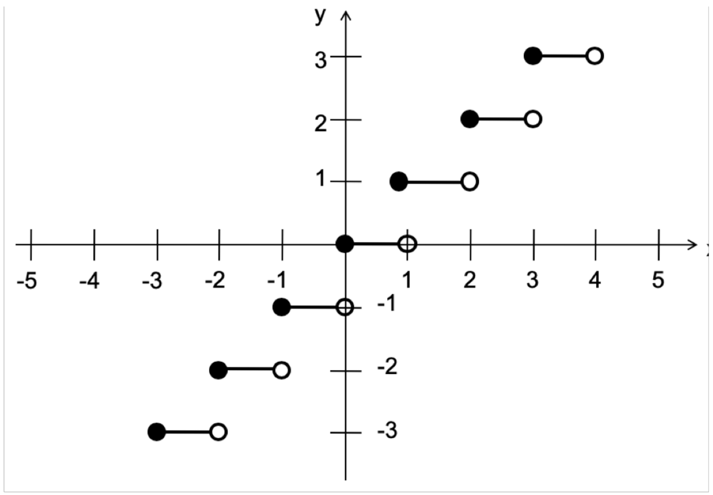
$$(g \circ f) = \iota_A \text{ and } (f \circ g) = \iota_B$$

where the ι_A and ι_B are the identity functions on sets A and B. That is,

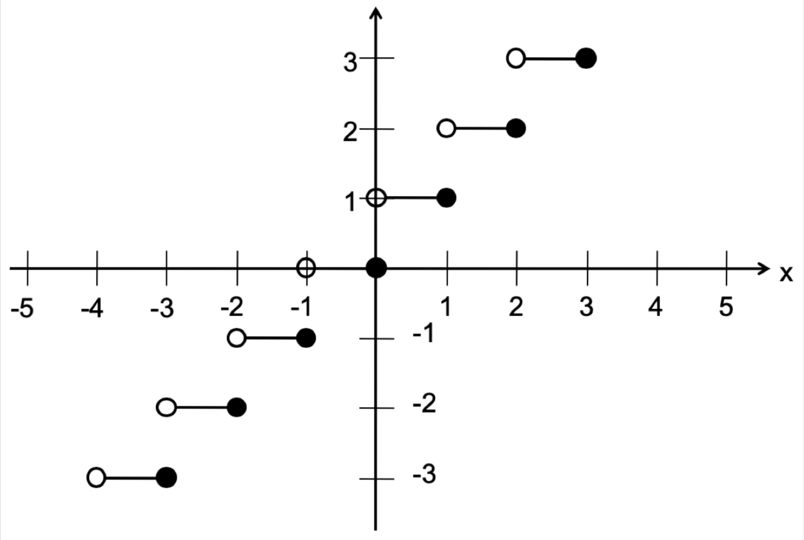
$$\forall a \in A, b \in B \; (\, (g(f(a)) = a) \wedge (f(g(b)) = b) \,)$$

Important Functions

- Floor function, denoted ⌊x⌋
- Ceiling function, denoted ⌈x⌉
- Factorial function, denoted n!



Floor function

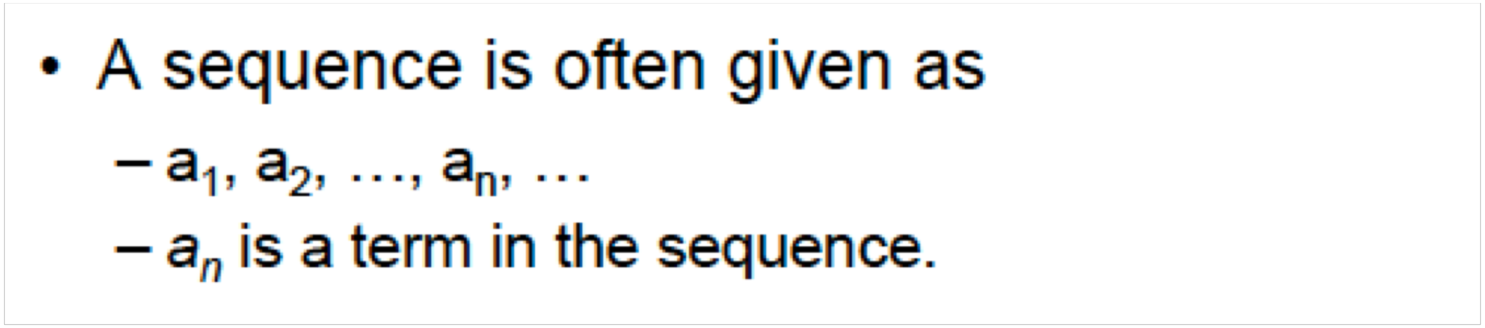


Ceiling function

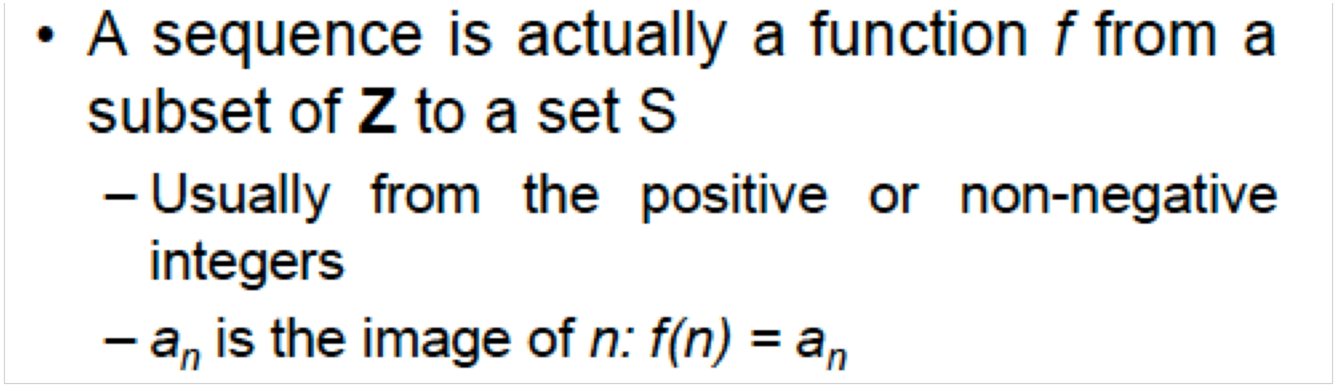
Sequences

Sequence

A sequence is an ordered list of elements.

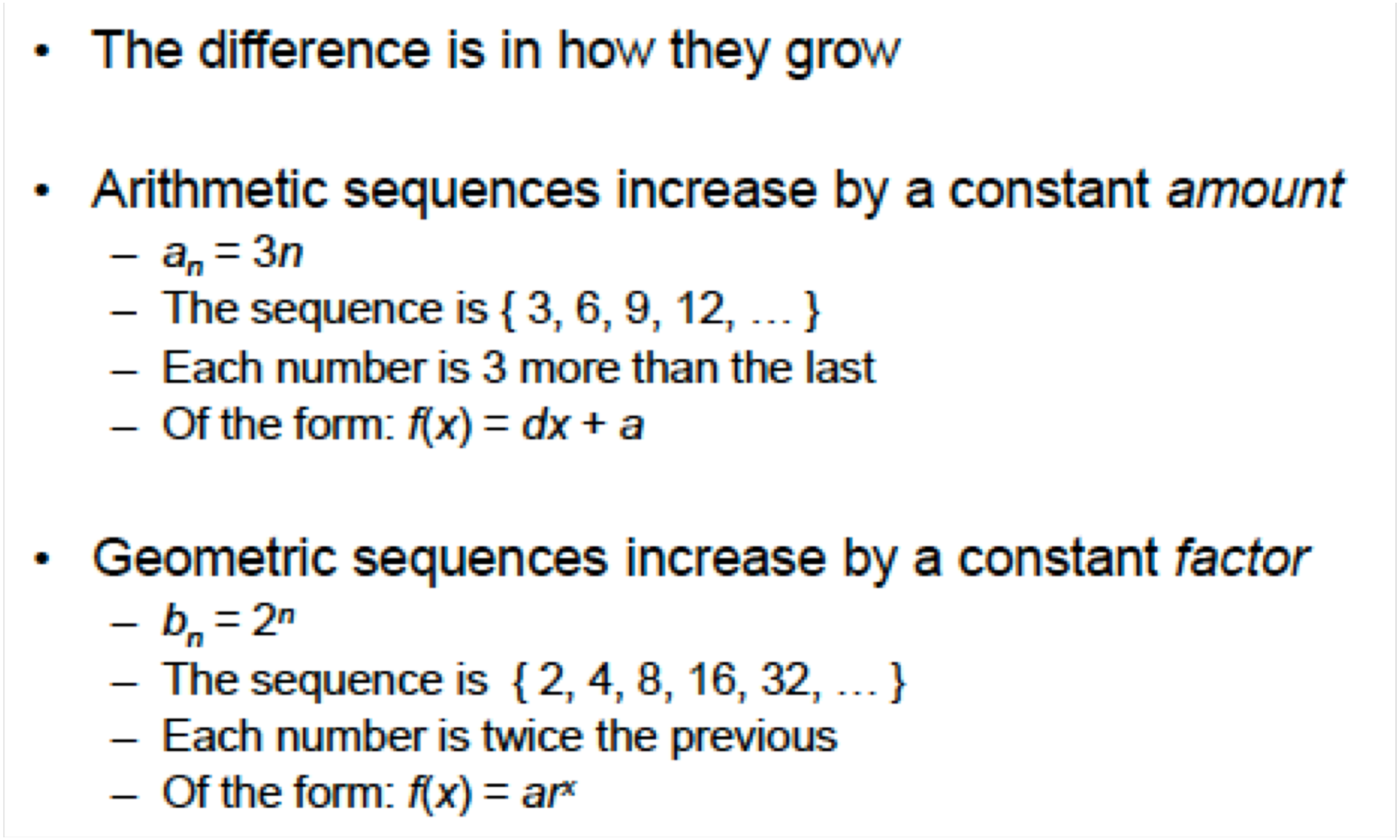


- A sequence is often given as
  - $a_1, a_2, \ldots, a_n, \ldots$
  - a_n is a term in the sequence.



- A sequence is actually a function *f* from a subset of **Z** to a set S
  - Usually from the positive or non-negative integers
  - a_n is the image of n: $f(n) = a_n$

Examples of Sequence

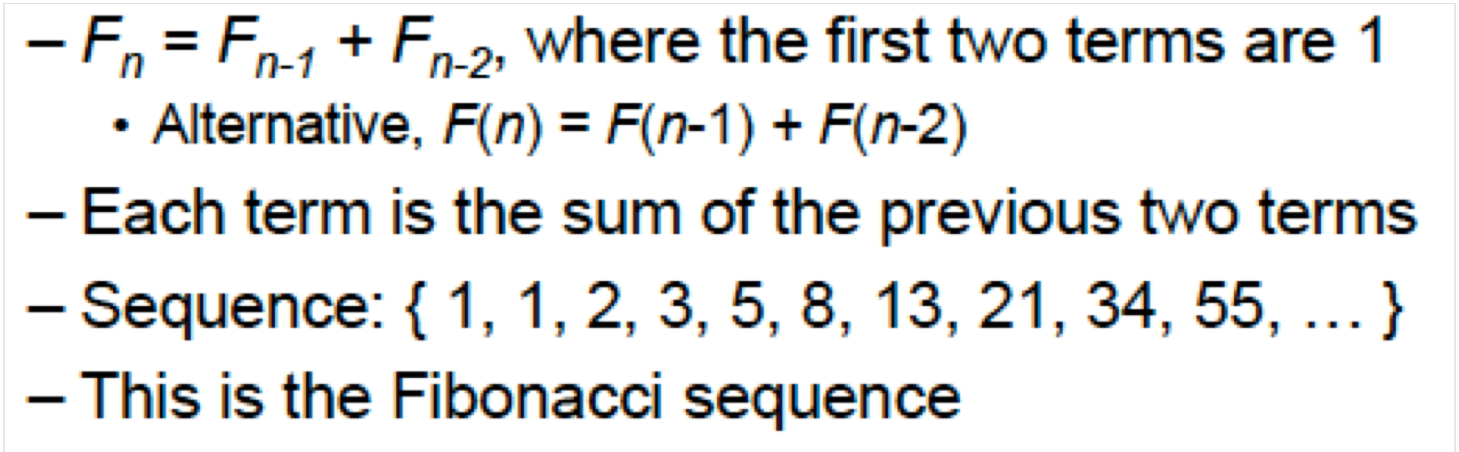


- The difference is in how they grow
- Arithmetic sequences increase by a constant *amount*
  - $a_n = 3n$
  - The sequence is { 3, 6, 9, 12, … }
  - Each number is 3 more than the last
  - Of the form: $f(x) = dx + a$
- Geometric sequences increase by a constant *factor*
  - $b_n = 2^n$
  - The sequence is { 2, 4, 8, 16, 32, … }
  - Each number is twice the previous
  - Of the form: $f(x) = ar^x$

Examples of Sequence

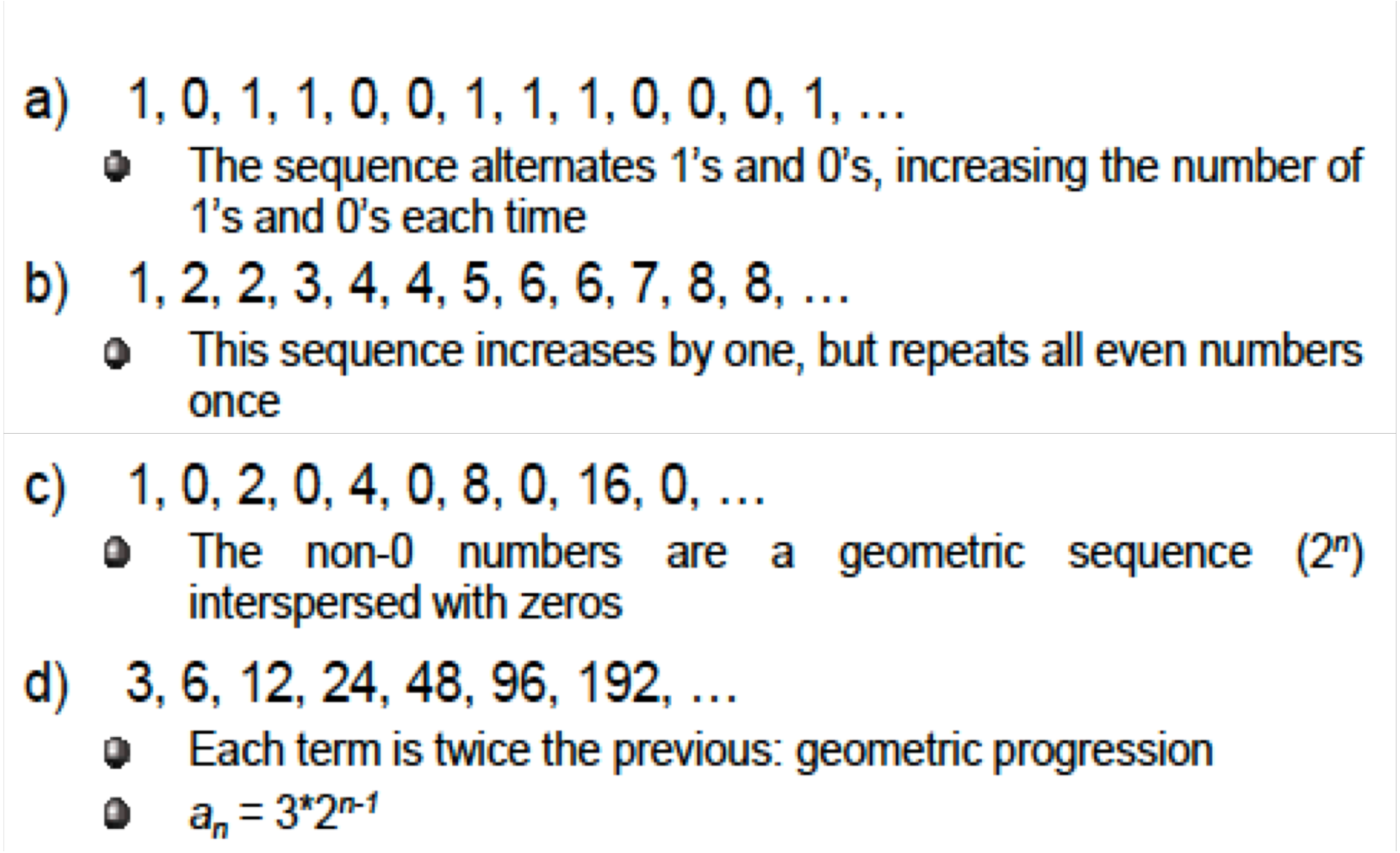
Not all sequences are arithmetic or geometric sequences.

An example is Fibonacci sequence



- $F_n = F_{n-1} + F_{n-2}$, where the first two terms are 1
  - Alternative, $F(n) = F(n\text{-}1) + F(n\text{-}2)$
- Each term is the sum of the previous two terms
- Sequence: { 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, … }
- This is the Fibonacci sequence

Sequence Formula



a) 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, …

- The sequence alternates 1's and 0's, increasing the number of 1's and 0's each time

b) 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, …

- This sequence increases by one, but repeats all even numbers once

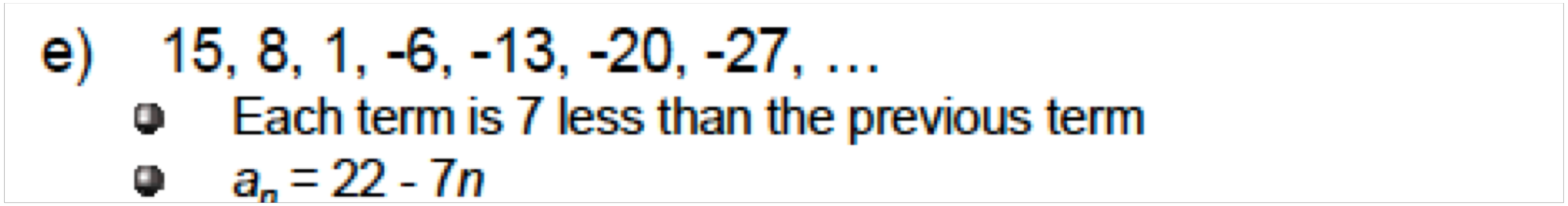
c) 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, …

- The non-0 numbers are a geometric sequence (2^n) interspersed with zeros

d) 3, 6, 12, 24, 48, 96, 192, …

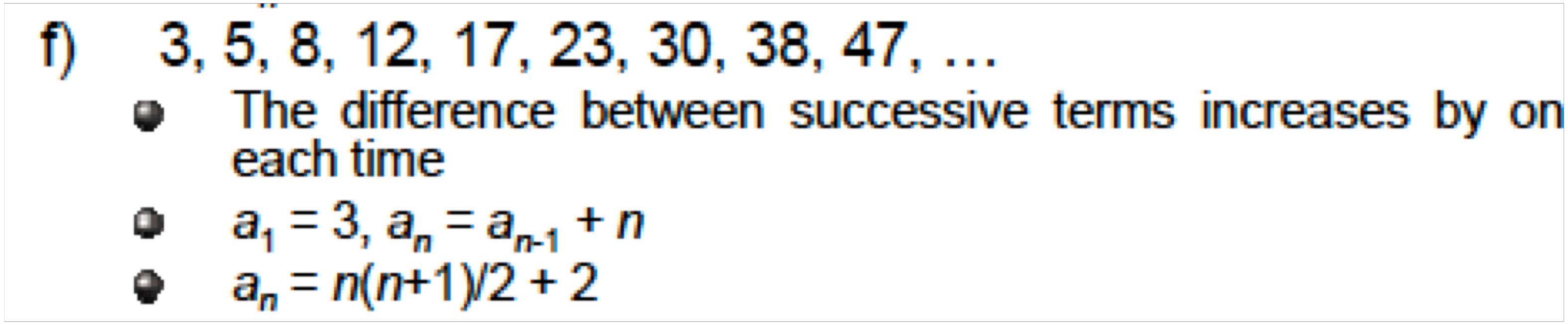
- Each term is twice the previous: geometric progression
- $a_n = 3*2^{n-1}$

Sequence Formula



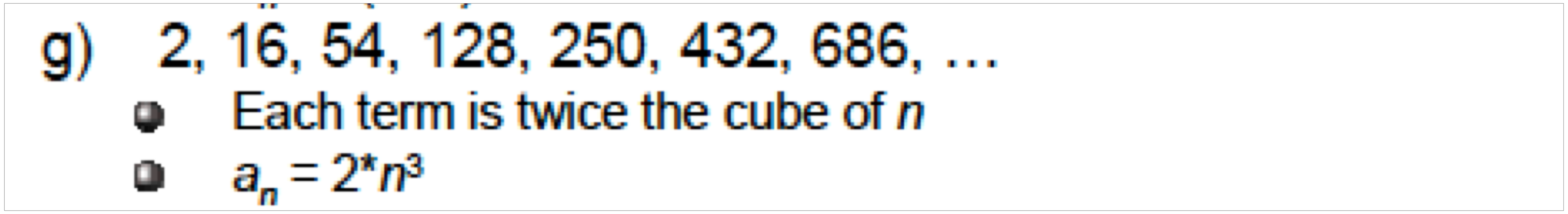
e) 15, 8, 1, -6, -13, -20, -27, …

- Each term is 7 less than the previous term
- $a_n = 22 - 7n$



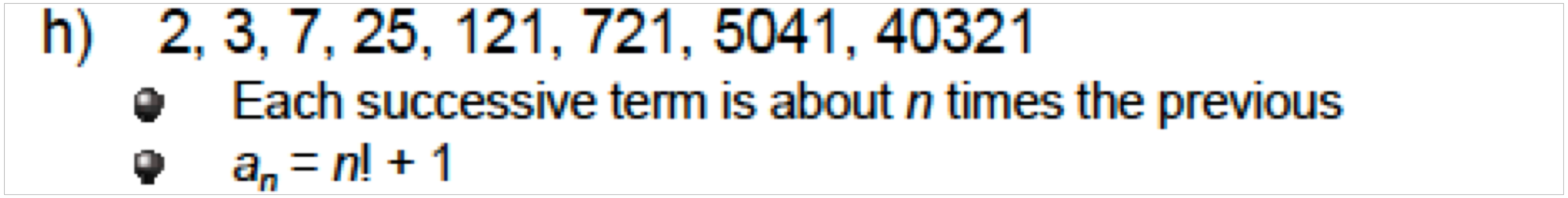
f) 3, 5, 8, 12, 17, 23, 30, 38, 47, …

- The difference between successive terms increases by on each time
- $a_1 = 3$, $a_n = a_{n-1} + n$
- $a_n = n(n+1)/2 + 2$



g) 2, 16, 54, 128, 250, 432, 686, …

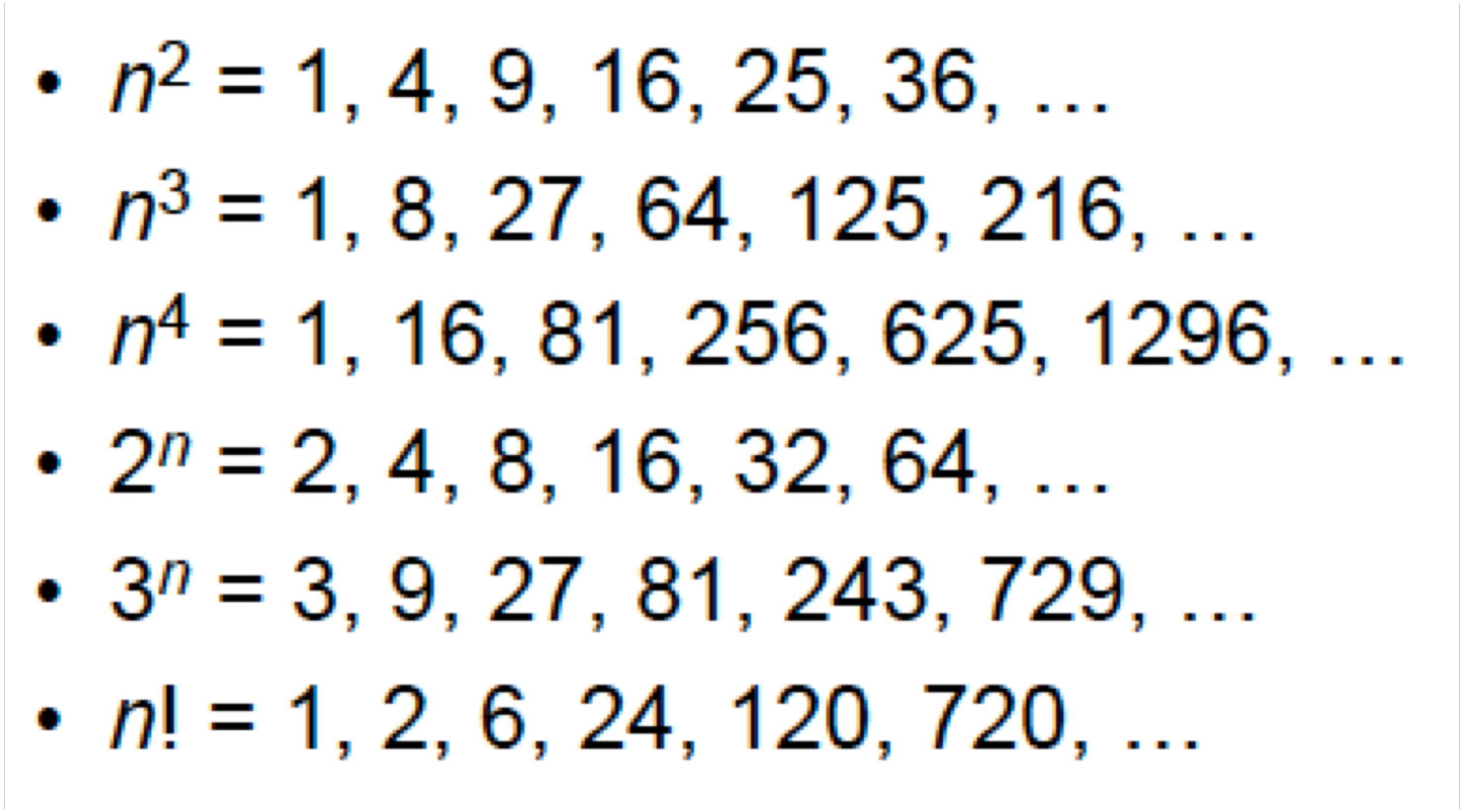
- Each term is twice the cube of *n*
- $a_n = 2^*n^3$



h) 2, 3, 7, 25, 121, 721, 5041, 40321

- Each successive term is about *n* times the previous
- $a_n = n! + 1$

Some useful sequences



- $n^2 = 1, 4, 9, 16, 25, 36, \ldots$
- $n^3 = 1, 8, 27, 64, 125, 216, \ldots$
- $n^4 = 1, 16, 81, 256, 625, 1296, \ldots$
- $2^n = 2, 4, 8, 16, 32, 64, \ldots$
- $3^n = 3, 9, 27, 81, 243, 729, \ldots$
- $n! = 1, 2, 6, 24, 120, 720, \ldots$

Sequences: Example 2

- The sequence: $\{h_n\}_{n=1}^{\infty}$ = 1/n

  is known as the **harmonic** sequence
- The sequence is simply:

  1, 1/2, 1/3, 1/4, 1/5, …
- This sequence is particularly interesting because its summation is divergent:

$$\sum_{n=1}^{\infty} (1/n) = \infty$$

Sequences: Example 1

- Consider the sequence

$$\{(1 + 1/n)^n\}_{n=1}^{\infty}$$

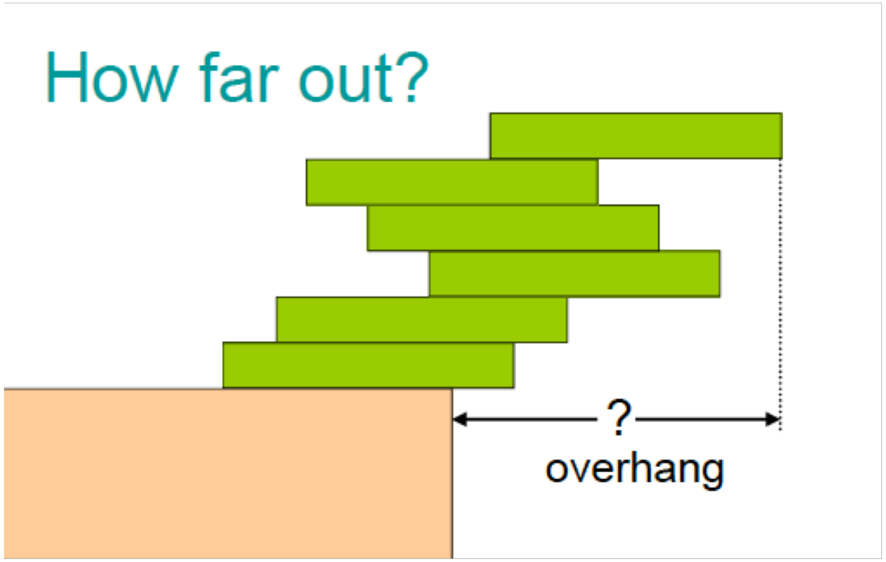
- The terms of the sequence are:

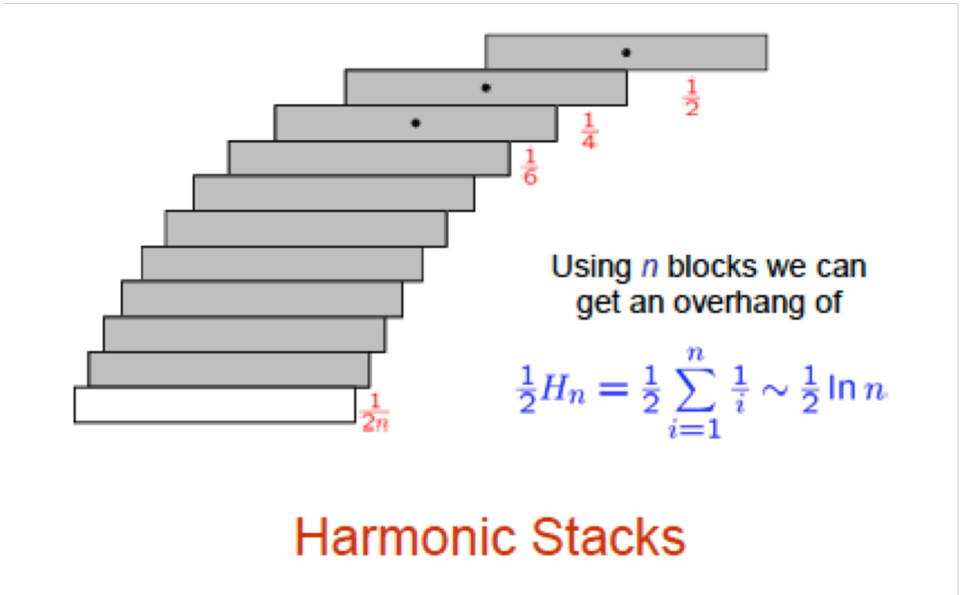
$$a_1 = (1 + 1/1)^1 = 2.00000$$
$$a_2 = (1 + 1/2)^2 = 2.25000$$
$$a_3 = (1 + 1/3)^3 = 2.37037$$
$$a_4 = (1 + 1/4)^4 = 2.44140$$
$$a_5 = (1 + 1/5)^5 = 2.48832$$

- What is this sequence?

- The sequence corresponds to $\lim_{n\to\infty}\{(1 + 1/n)^n\}_{n=1}^{\infty}$ = e = 2.71828..

Book stacking example




$\frac{1}{2}$
$\frac{1}{4}$
$\frac{1}{6}$
$\frac{1}{2n}$
Using n blocks we can get an overhang of
$\frac{1}{2}H_n = \frac{1}{2}\sum_{i=1}^{n}\frac{1}{i} \sim \frac{1}{2}\ln n$
Harmonic Stacks

Progressions: Geometric

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

$$a, aq^2, aq^3, \dots, aq^n, \dots$$

Where:

  - $a \in \mathbb{R}$ is called the initial term
  - $q \in \mathbb{R}$ is called the common ratio

- A geometric progression is a discrete analogue of the exponential function

$$f(x) = aq^x$$

Geometric Progressions: Examples

- A common geometric progression in Computer Science is:

  $$\{a_n\}= 1/2^n$$

  with a=1 and q=1/2

- Give the initial term and the common ratio of
  - $\{b_n\}$ with $b_n= (-1)^n$
  - $\{c_n\}$ with $c_n= 2(5)^n$
  - $\{d_n\}$ with $d_n= 6(1/3)^n$

Progressions: Arithmetic

- **Definition**: An arithmetric progression is a sequence of the form

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

  Where:

  - $a \in \mathbb{R}$ is called the initial term
  - $d \in \mathbb{R}$ is called the common difference

- An arithmetic progression is a discrete analogue of the linear function

  $$f(x) = dx+a$$

Arithmetic Progressions: Examples

- Give the initial term and the common difference of
  - $\{s_n\}$ with $s_n = -1 + 4n$
  - $\{t_n\}$ with $s_n = 7 - 3n$

Summations

- You should be by now familiar with the summation notation:

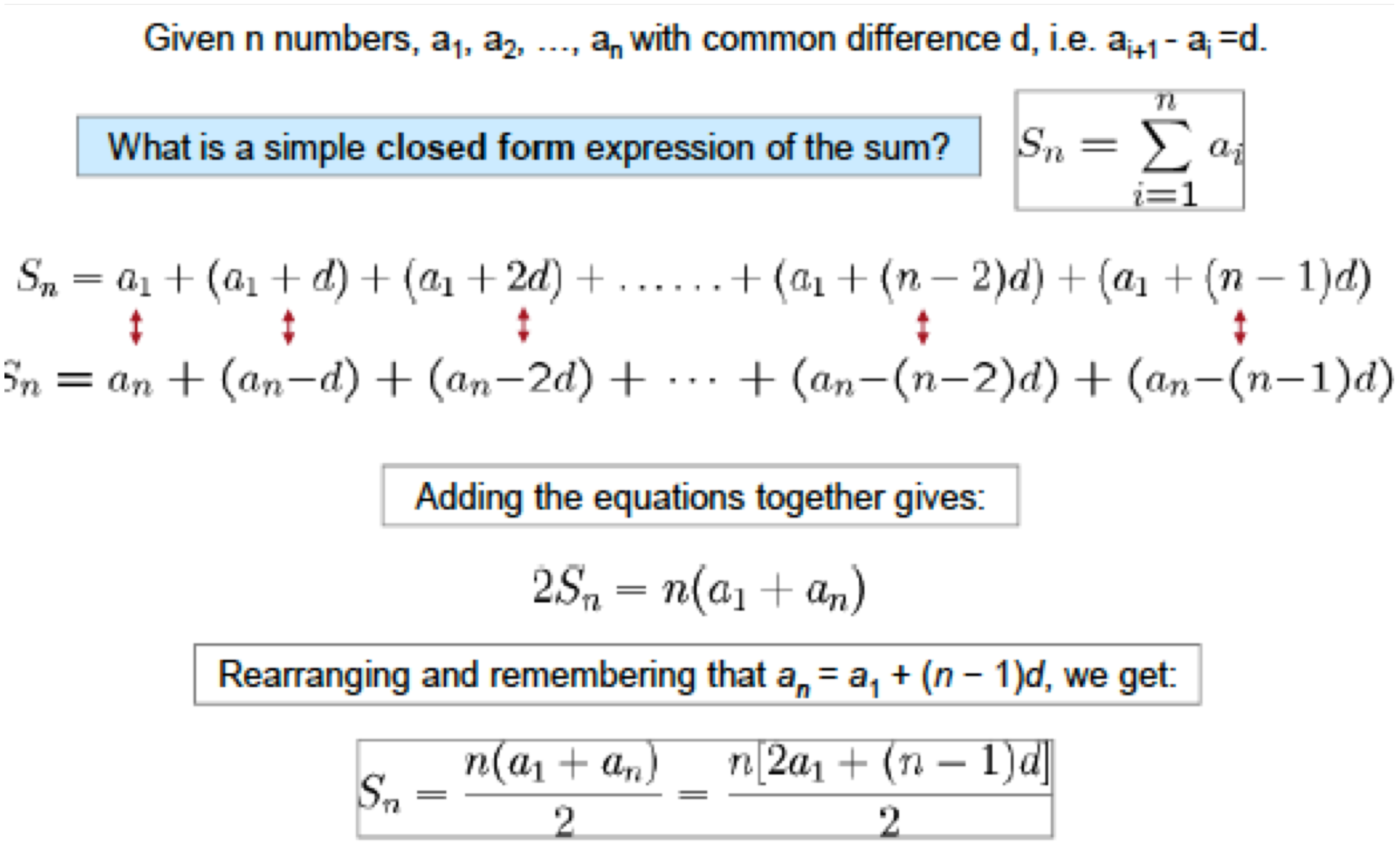
  $$\sum_{i=m}^{n} a_i \;=\; a_m + a_{m+1} + \dots + a_{n-1} + a_n$$

  Here

  - i is the index of the summation
  - m is the lower limit
  - n is the upper limit
- Often times, it is useful to change the lower/upper limits, which can be done in a straightforward manner (although we must be very careful):

  $$\sum_{i=1}^{n} a_i = \sum_{i=0}^{n-1} a_{i+1}$$

Sum of arithmetic series



Given n numbers, a_1, a_2, …, a_n with common difference d, i.e. $a_{i+1} - a_i = d$.

What is a simple closed form expression of the sum?

$$S_n = \sum_{i=1}^{n} a_i$$

$$S_n = a_1 + (a_1 + d) + (a_1 + 2d) + \ldots\ldots + (a_1 + (n-2)d) + (a_1 + (n-1)d)$$

$$\updownarrow \qquad \updownarrow \qquad \updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$S_n = a_n + (a_n - d) + (a_n - 2d) + \cdots + (a_n - (n-2)d) + (a_n - (n-1)d)$$

Adding the equations together gives:

$$2S_n = n(a_1 + a_n)$$

Rearranging and remembering that $a_n = a_1 + (n - 1)d$, we get:

$$\boxed{S_n = \frac{n(a_1 + a_n)}{2} = \frac{n[2a_1 + (n-1)d]}{2}}$$

Summation

- You should be by now familiar with the summation notation:

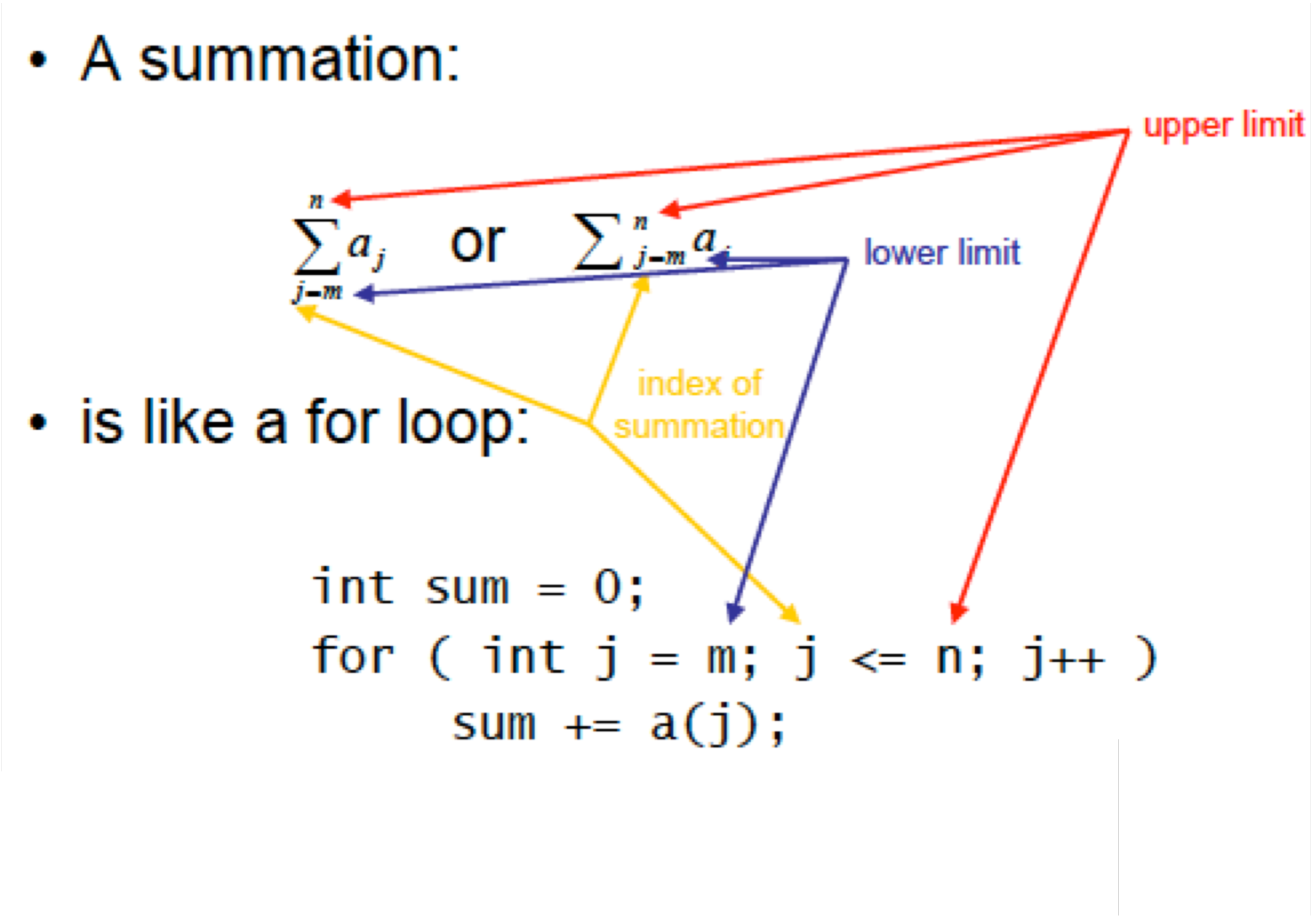
  $$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \ldots + a_{n-1} + a_n$$

  Here

  - i is the index of the summation
  - m is the lower limit
  - n is the upper limit
- Often times, it is useful to change the lower/upper limits, which can be done in a straightforward manner (although we must be very careful):

  $$\sum_{i=1}^{n} a_i = \sum_{i=0}^{n-1} a_{i+1}$$

Summation



- A summation:

$$\sum_{j-m}^{n} a_j \quad \text{or} \quad \sum\nolimits_{j-m}^{n} a_j$$

upper limit

lower limit

index of summation

- is like a for loop:

```
int sum = 0;
for ( int j = m; j <= n; j++ )
      sum += a(j);
```

Summation of Geometric Sequence

With 5 terms of the general geometric sequence, we have

$$S_5 = a + ar + ar^2 + ar^3 + ar^4$$

TRICK Multiply by *r:*

$$rS_5 = ar + ar^2 + ar^3 + ar^4 + ar^5$$

Subtracting the expressions gives

$$\begin{aligned} S_5 - rS_5 = {} & a + ar + ar^2 + ar^3 + ar^4 \\ - & \underline{ar + ar^2 + ar^3 + ar^4 + ar^5} \end{aligned}$$

Move the lower row 1 place to the right and subtract

Summation of Geometric Sequence

With 5 terms of the general geometric sequence, we have

$$S_5 = a + ar + ar^2 + ar^3 + ar^4$$

TRICK Multiply by *r:*

$$rS_5 = ar + ar^2 + ar^3 + ar^4 + ar^5$$

Subtracting the expressions gives

$$\begin{aligned} S_5 - rS_5 = \; & a + ar + ar^2 + ar^3 + ar^4 \\ - \; & \underline{ar + ar^2 + ar^3 + ar^4 + ar^5} \end{aligned}$$

$$S_5 - rS_5 = a - ar^5$$

Summation of Geometric Sequence

So, $$S_5 - rS_5 = a - ar^5$$

Take out the common factors

$$S_5(1-r) = a(1 - r^5)$$

and divide by (1 – *r*)

$$\Rightarrow \qquad S_5 = \frac{a(1 - r^5)}{1-r}$$

Similarly, for *n* terms we get

$$S_n = \frac{a(1 - r^n)}{1-r}$$

Summation of Geometric Sequence

The formula

$$S_n = \frac{a(1 - r^n)}{1 - r}$$

gives a negative denominator if $r > 1$

Instead, we can use

$$S_n = \frac{a(r^n - 1)}{r - 1}$$

Example

Find the sum of the first 20 terms of the geometric series, leaving your answer in index form $2 - 6 + 18 - 54 + \;.\;\;.\;\;.$

Solution: $a = 2, \quad r = \frac{\overset{-3}{\cancel{-6}}}{\underset{1}{\cancel{2}}} = -3$

$$S_n = \frac{a(1 - r^n)}{1 - r} \Rightarrow S_{20} = \frac{2\left(1 - (-3)^{20}\right)}{1 - (-3)}$$

We'll simplify this answer without using a calculator

Example

$$\Rightarrow \quad S_{20} = \frac{2\left(1-(-3)^{20}\right)}{1-(-3)}$$

There are 20 minus signs here and 1 more outside the bracket!

$$= \frac{\overset{1}{\cancel{2}}\left(1-3^{20}\right)}{\cancel{4}\;{}_{2}}$$

$$= \frac{1-3^{20}}{2}$$

Series

- When we take the sum of a sequence, we get a series
- We have already seen a closed form for geometric series
- Some other useful closed forms include the following:
  - $\sum_{i=k}^{u} 1$ = u-k+1, for k≤u
  - $\sum_{i=k}^{u} i$ = n(n+1)/2
  - $\sum_{i=1}^{n} i^2$ = n(n+1)(2n+1)/6
  - $\sum_{i=1}^{n} i^k \approx$ n^{k+1}/(k+1)

Infinite Series

- Although we will mostly deal with finite series (i.e., an upper limit of n for fixed integer), inifinite series are also useful
- Consider the following geometric series:
  - $\Sigma_{n=0}(1/2^n) = 1 + 1/2 + 1/4 + 1/8 +$ … converges to 2
  - $\Sigma_{n=0}(2^n) = 1 + 2 + 4 + 8 +$ … does not converge
- However note: $\Sigma_{n=0} (2^n) = 2^{n+1} – 1$ (a=1, q=2)

Can you evaluate this?

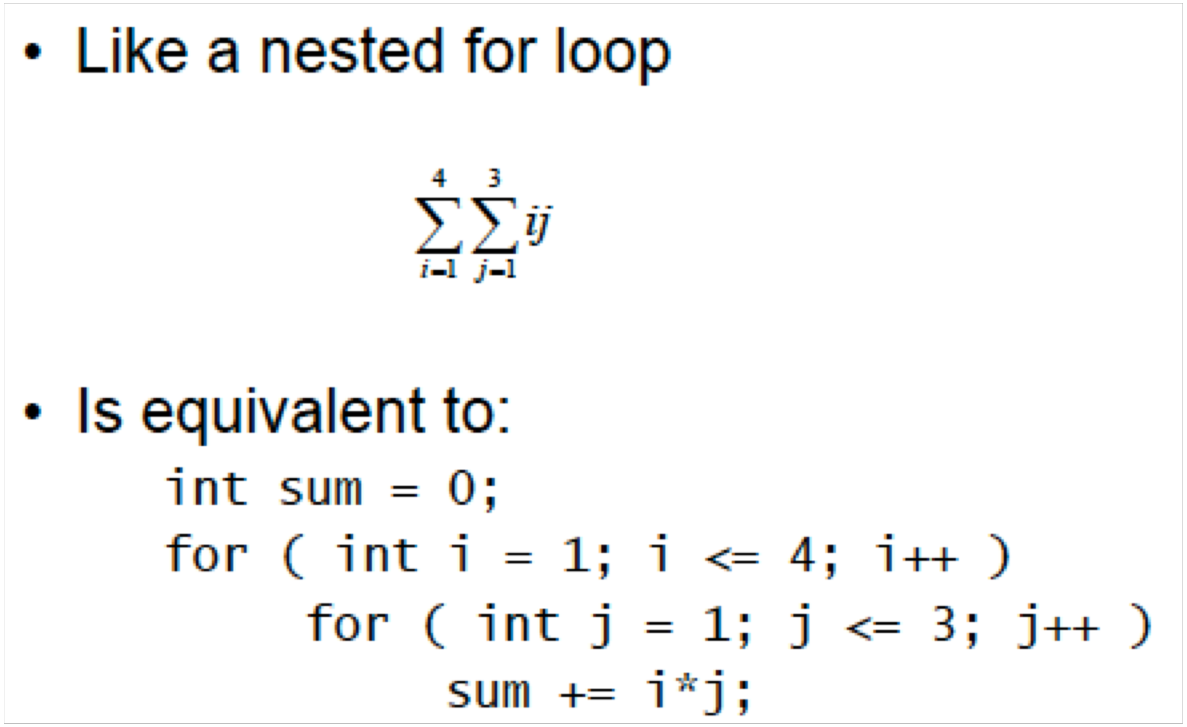
$$\sum_{i=1}^{n} \frac{1}{k(k+1)}$$

Here is the trick. Note that

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

Does it help?

Double Summation



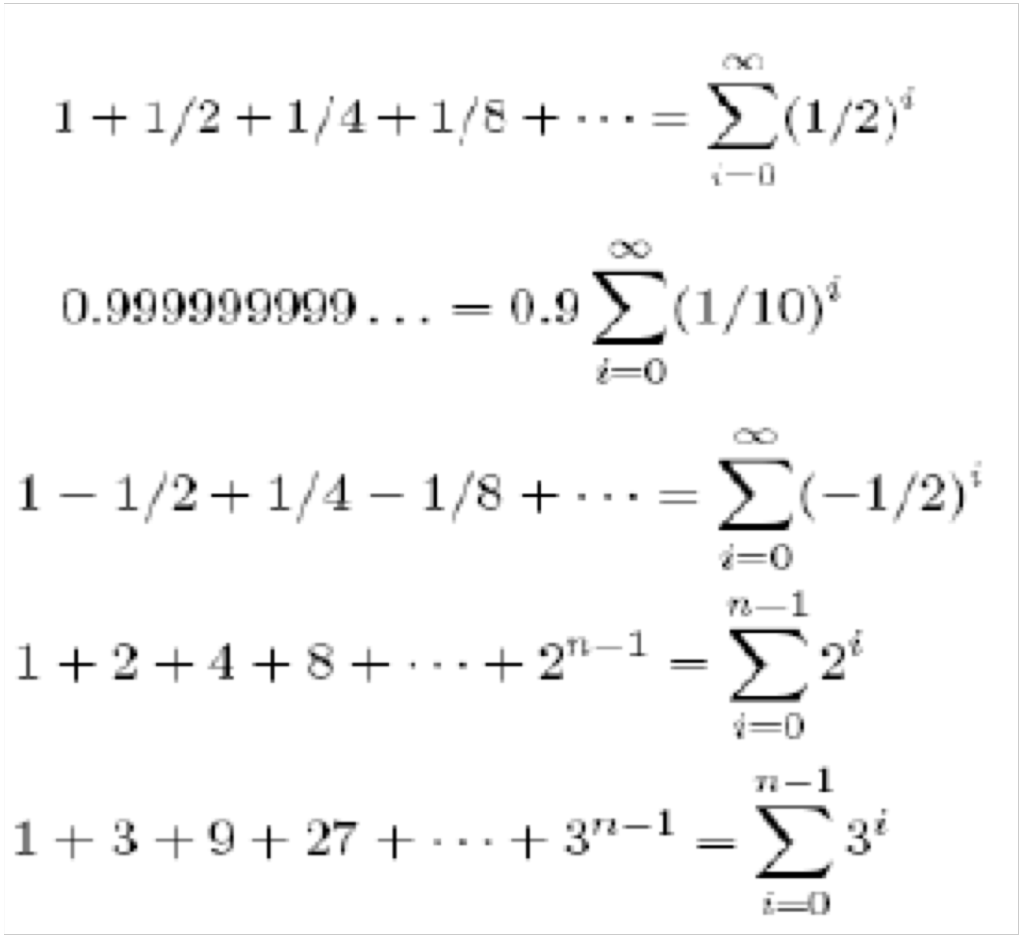
- Like a nested for loop

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij$$

- Is equivalent to:

```
int sum = 0;
for ( int i = 1; i <= 4; i++ )
      for ( int j = 1; j <= 3; j++ )
            sum += i*j;
```

Solve the following



$$1 + 1/2 + 1/4 + 1/8 + \cdots = \sum_{i=0}^{\infty} (1/2)^i$$

$$0.999999999\ldots = 0.9 \sum_{i=0}^{\infty} (1/10)^i$$

$$1 - 1/2 + 1/4 - 1/8 + \cdots = \sum_{i=0}^{\infty} (-1/2)^i$$

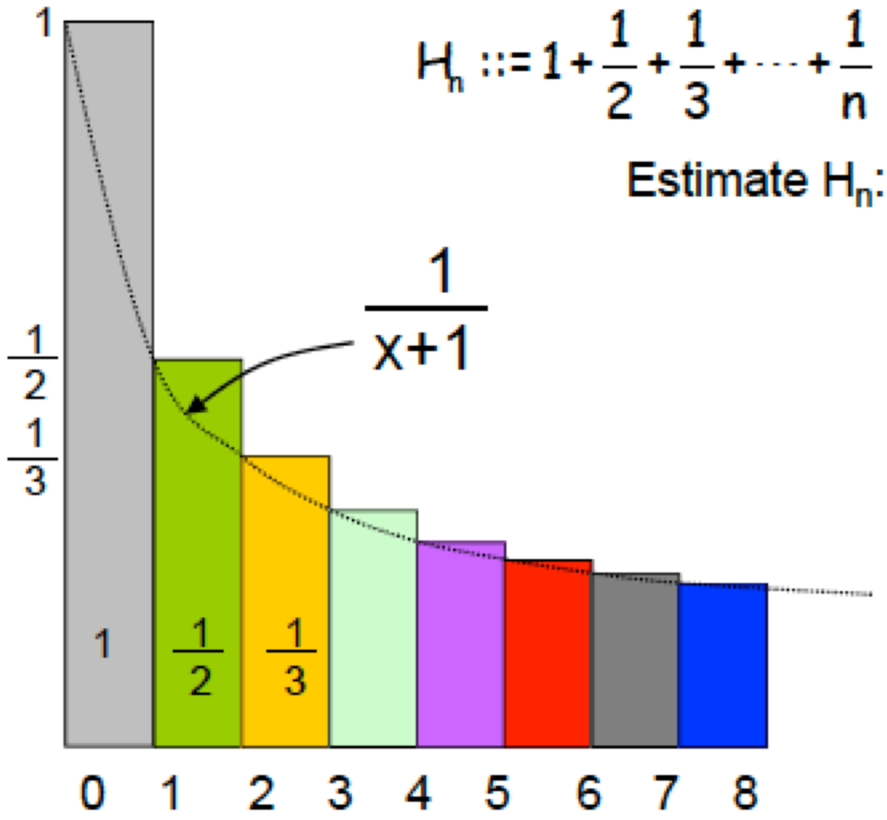
$$1 + 2 + 4 + 8 + \cdots + 2^{n-1} = \sum_{i=0}^{n-1} 2^i$$

$$1 + 3 + 9 + 27 + \cdots + 3^{n-1} = \sum_{i=0}^{n-1} 3^i$$

Sum of harmonic series

$$H_n ::= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

Estimate H_n:



$$\int_0^n \frac{1}{x+1}\,dx \le 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

$$\int_1^{n+1} \frac{1}{x}\,dx \le H_n$$

$$\ln(n+1) \le H_n$$

Products

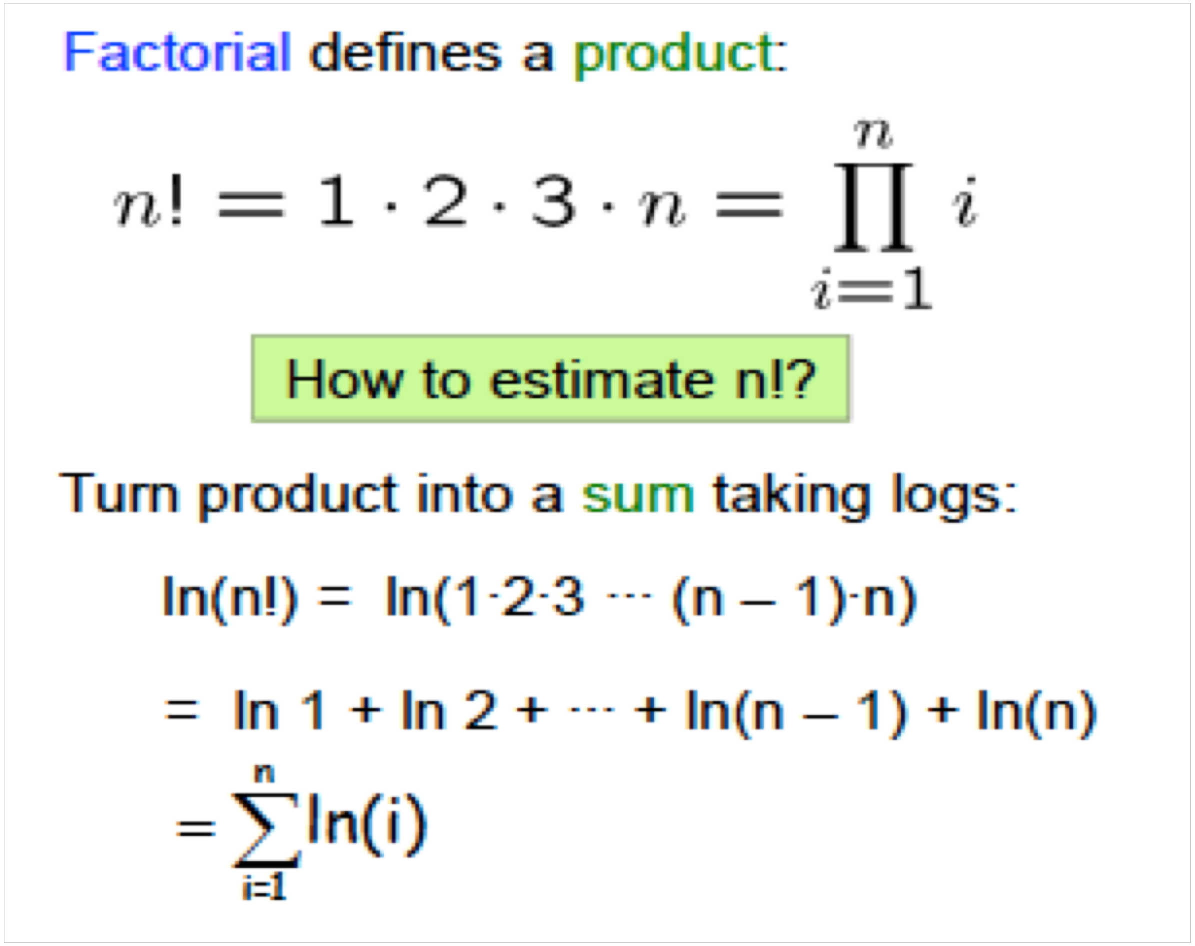
$$\prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdots a_n$$

$$\prod_{k=1}^{5} k^2$$

$$\prod_{k=1}^{n} \frac{k}{k+1}$$

$$\prod_{k=1}^{n} 2^k$$

Dealing with Products



Factorial defines a product:

$$n! = 1 \cdot 2 \cdot 3 \cdot n = \prod_{i=1}^{n} i$$

How to estimate n!?

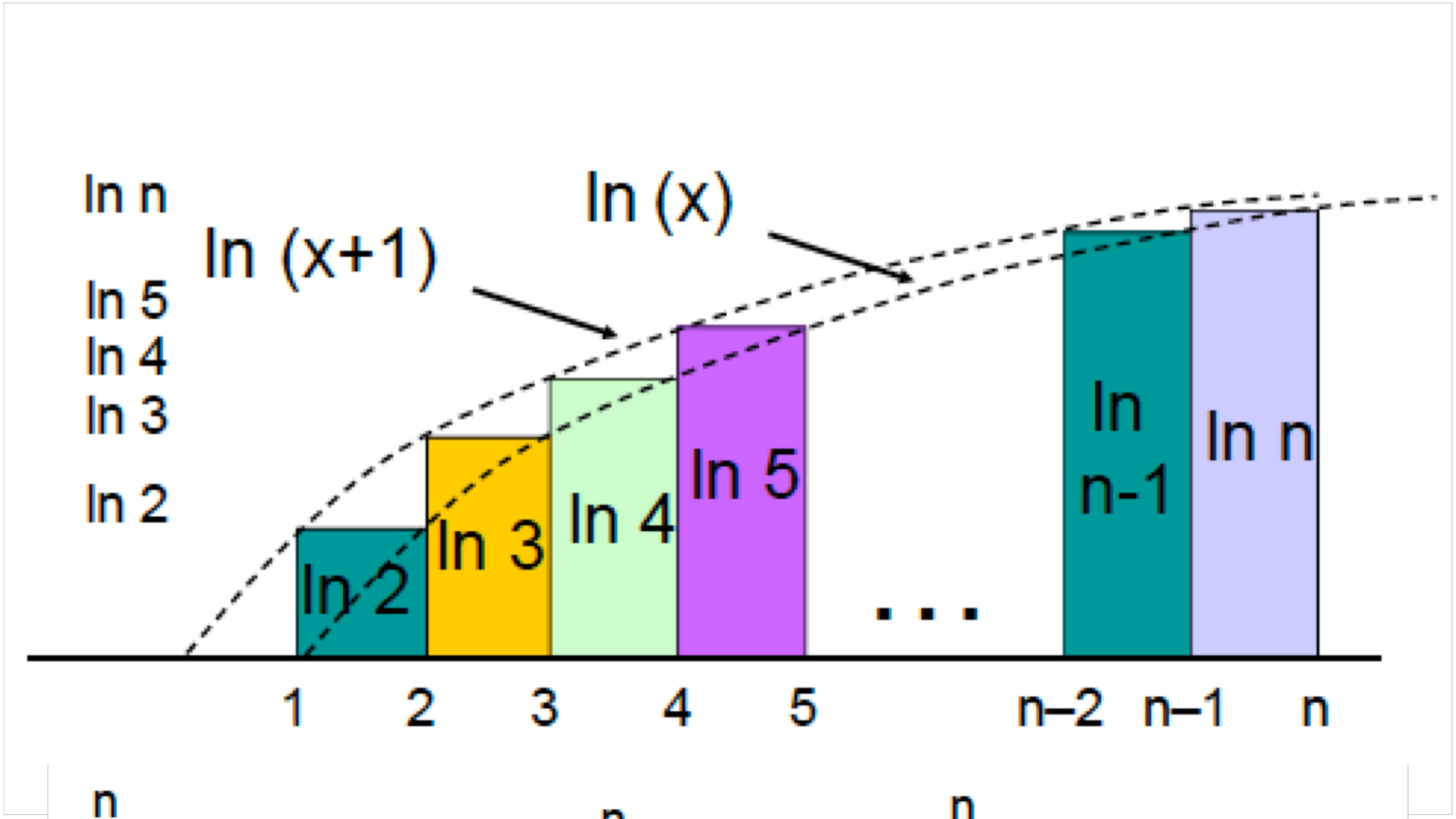
Turn product into a sum taking logs:

$$\ln(n!) = \ln(1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n)$$

$$= \ln 1 + \ln 2 + \cdots + \ln(n-1) + \ln(n)$$

$$= \sum_{i=1}^{n} \ln(i)$$

Factorial



$$\int_{1}^{n} \ln(x)\,dx \leq \sum_{i=1}^{n} \ln(i) \leq \int_{0}^{n} \ln(x+1)dx$$

Factorial

$$\int_{1}^{n} \ln(x)\, dx \leq \sum_{i=1}^{n} \ln(i) \leq \int_{0}^{n} \ln\,(x+1)dx$$

Reminder: $\int \ln x\, dx = x \ln\left(\frac{x}{e}\right)$

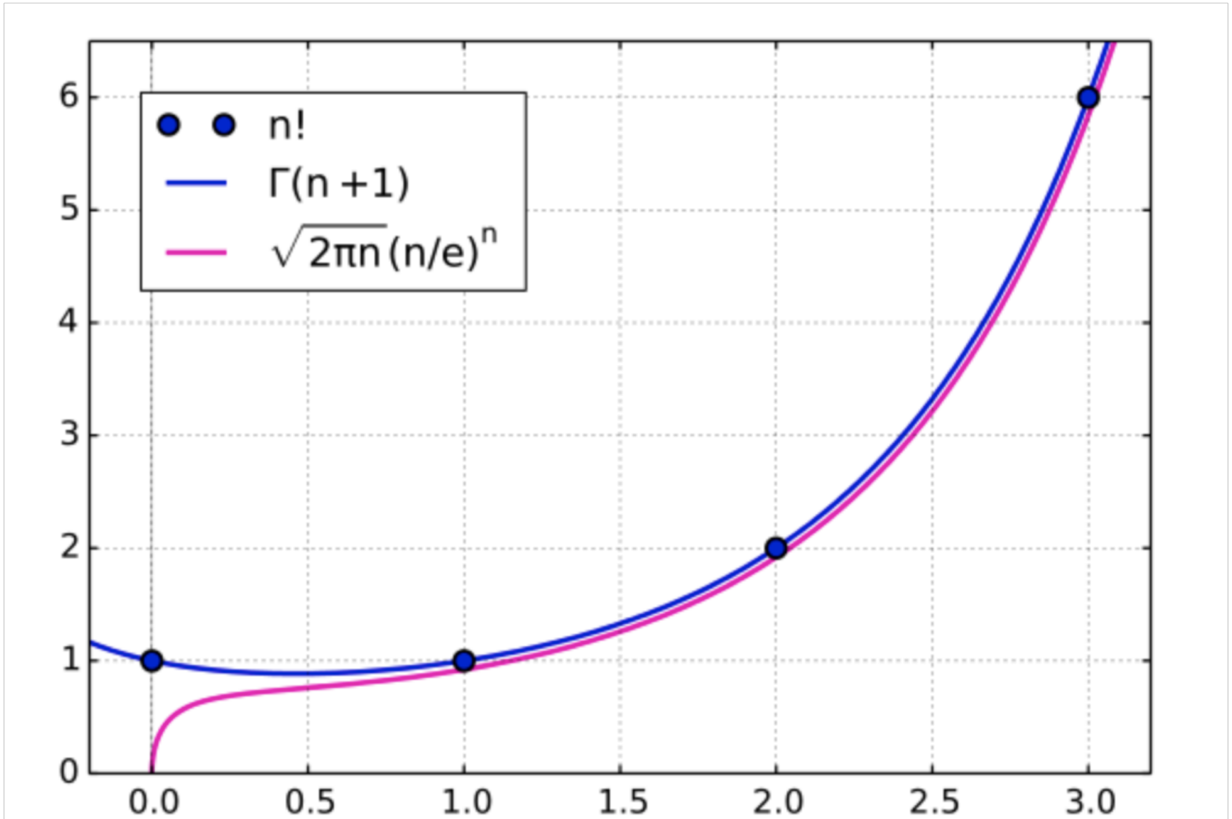
$$n \ln(n/e) +1 \leq \sum \ln(i) \leq (n+1) \ln((n+1)/e) +1$$

so guess: $\sum_{i=1}^{n} \ln(i) \approx \left(n+\frac{1}{2}\right)\ln\left(\frac{n}{e}\right)$

Stirling’s formula

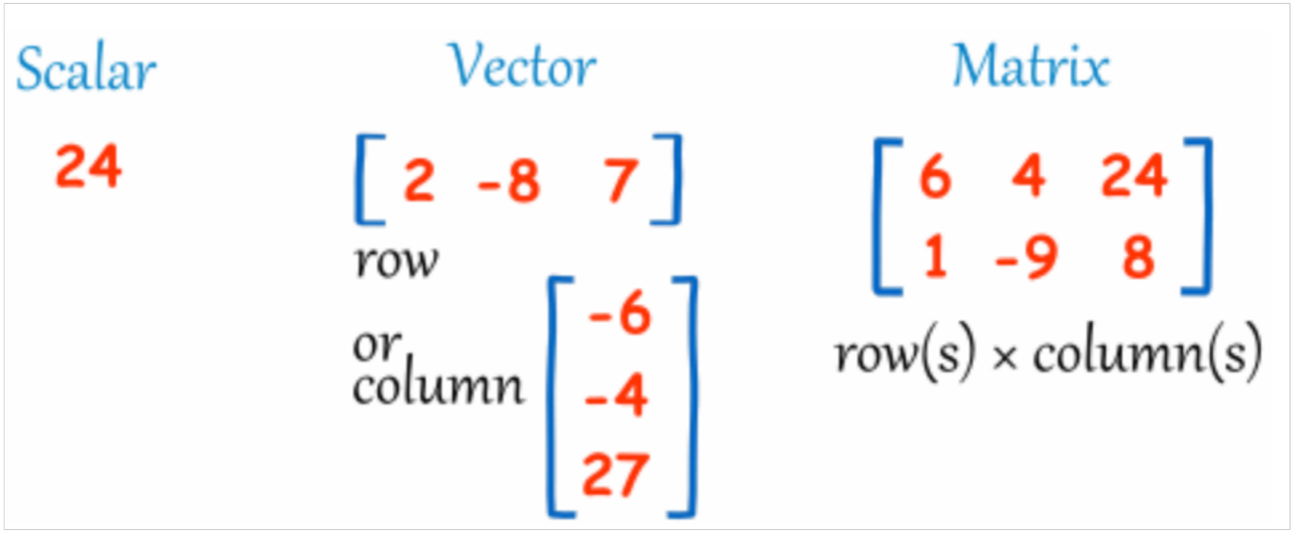
$$\sum_{i=1}^{n} \ln(i) \approx \left(n+\frac{1}{2}\right)\ln\left(\frac{n}{e}\right)$$

exponentiating: $$n! \approx \sqrt{n/e}\left(\frac{n}{e}\right)^{n}$$



Matrices

Introduction

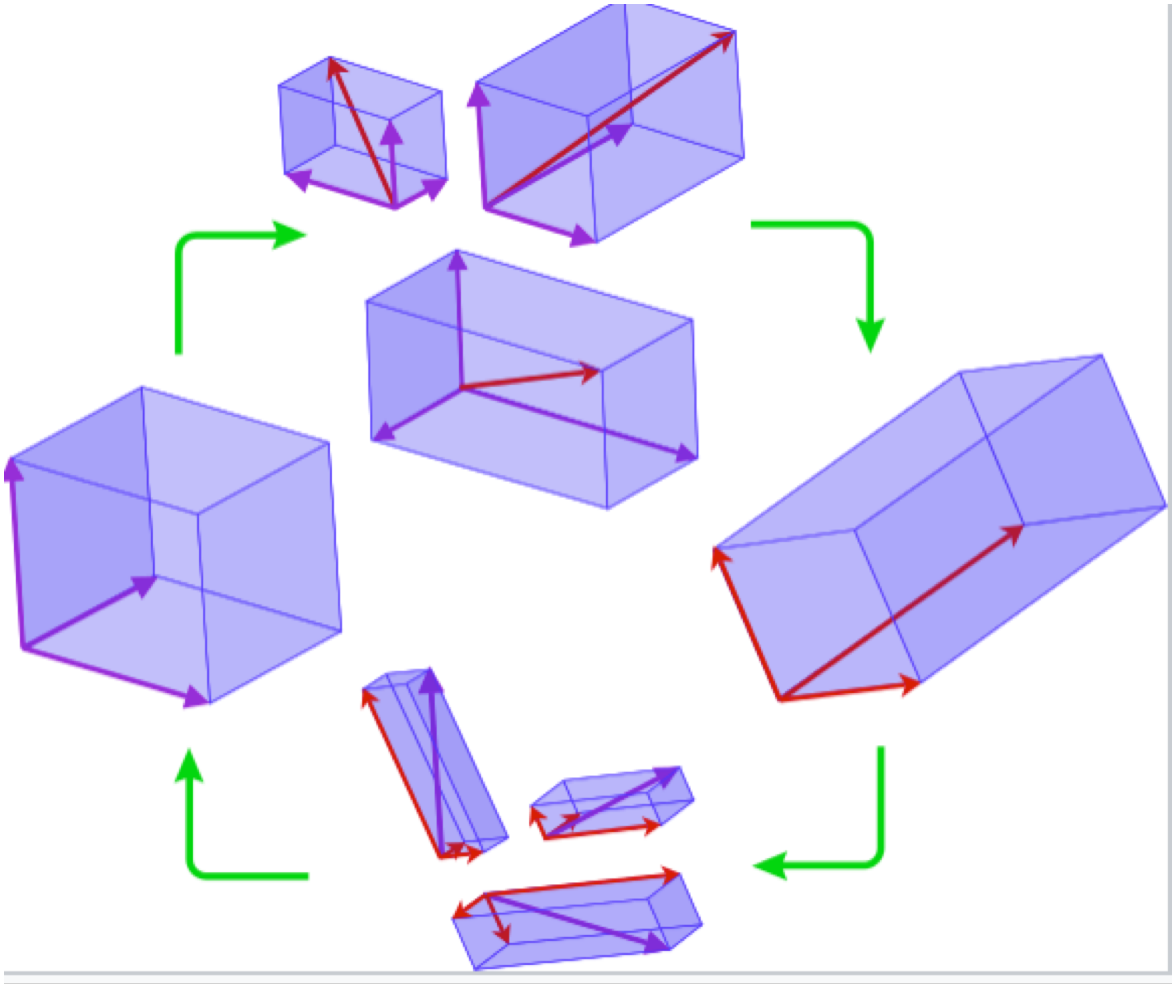


- Scalars: A single number
- Vector: A 1D array of numbers, where each element is identified by an single index
- Matrix: A 2D array of numbers

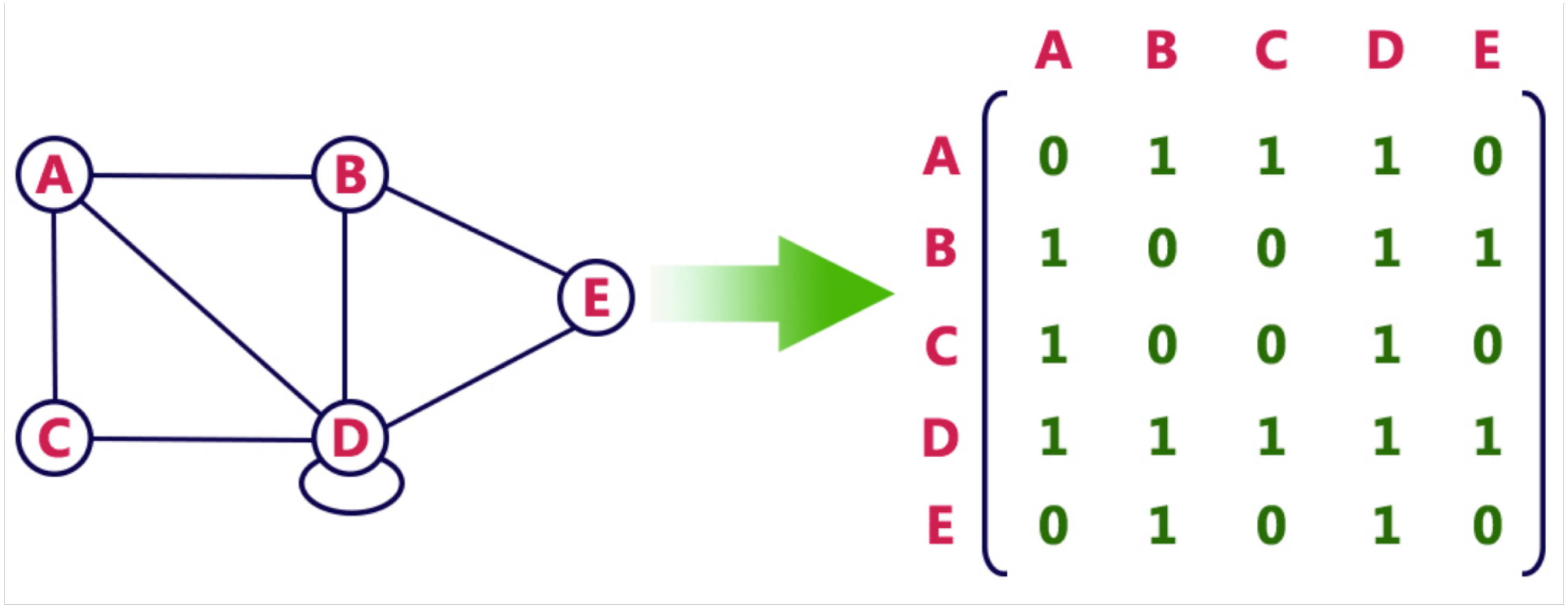
Matrix

- Matrices are useful discrete structures that can be used in many ways. For example, they are used to:
  - describe certain types of functions known as linear transformations.
  - Express which vertices of a graph are connected by edges.

Linear transformation



Matrix: a graph are connected by edges



$$
\begin{array}{c|ccccc|}
 & A & B & C & D & E \\
\hline
A & 0 & 1 & 1 & 1 & 0 \\
B & 1 & 0 & 0 & 1 & 1 \\
C & 1 & 0 & 0 & 1 & 0 \\
D & 1 & 1 & 1 & 1 & 1 \\
E & 0 & 1 & 0 & 1 & 0
\end{array}
$$

Matrix

Definition: A *matrix* is a rectangular array of numbers. A matrix with *m* rows and *n* columns is called an $m \times n$ matrix.

- The plural of matrix is *matrices*.
- A matrix with the same number of rows as columns is called *square*.
- Two matrices are *equal* if they have the same number of rows and the same number of columns and the corresponding entries in every position are equal.

3×2 matrix

3 by 2 matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$$

Notation

- Let *m* and *n* be positive integers and let

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & & . \\ . & . & & . \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

- The *i*-th row of **A** is the $1\times n$ matrix [a_{i1}, a_{i2}, …, a_{in}]. The *j*-th column of **A** is the $m\times 1$ *matrix:*

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ . \\ . \\ a_{mj} \end{bmatrix}$$

- The (*i*,*j*)-th *element* or *entry* of **A** is the element a_{ij}. We can use **A** = [a_{ij}] to denote the matrix with its (*i*,*j*)-th element equal to a_{ij}.

Types of Matrices

$$\begin{bmatrix} 1 & 1 & 1 \\ 9 & 9 & 0 \\ 6 & 6 & 1 \end{bmatrix}$$

square matrix

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 3 & 3 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & 7 \\ 7 & -7 \\ 7 & 6 \end{bmatrix}$$

rectangle matrix

$$\begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 9 \end{bmatrix}$$

diagonal matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

unit or identity matrix

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Null (zero) matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 5 & 2 & 3 \end{bmatrix}$$

lower triangular matrix

$$\begin{bmatrix} 1 & 7 & 4 & 4 \\ 0 & 1 & 7 & 4 \\ 0 & 0 & 7 & 8 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

upper triangular matrix

$$\begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}$$

scalar matrix

Matrix addition

Defintion: Let $\mathrm{A} = [\mathrm{a}_{\mathrm{ij}}]$ and $\mathrm{B} = [\mathrm{b}_{\mathrm{ij}}]$ be $m \times n$ matrices. The sum of **A** and **B**, denoted by **A + B**, is the $m \times n$ matrix that has $a_{\mathrm{ij}} + b_{\mathrm{ij}}$ as its (i,j)-th element. In other words, **A + B** = $[a_{ij} + b_{ij}]$.

Example:

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}$$

Note that matrices of different sizes can not be added.

Matrix multiplication

Definition: Let **A** be an *n*×*k* matrix and **B** be a *k* × *n* matrix. The *product* of **A** and **B**, denoted by **AB**, is the *m*×*n* matrix that has its (*i*,*j*)-th element equal to the sum of the products of the corresponding elments from the *i*-th row of **A** and the *j*-th column of **B**. In other words, if **AB** = $[c_{ij}]$ then $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{kj}b_{2j}$.

Example:

$$\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{bmatrix}$$

The product of two matrices is undefined when the number of columns in the first matrix is not the same as the number of rows in the second.

Illustration of matrix multiplication

- The Product of **A** = [a_{ij}] and **B** = [b_{ij}]

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1k} \\ a_{21} & a_{22} & \ldots & a_{2k} \\ . & . & & . \\ . & . & & . \\ a_{i1} & a_{i2} & \ldots & a_{ik} \\ . & . & & . \\ . & . & & . \\ a_{m1} & a_{m2} & \ldots & a_{mk} \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} b_{11} & a_{12} & \ldots & b_{1j} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2j} & \ldots & b_{2n} \\ . & . & & . & & \\ . & . & & . & & \\ b_{k1} & b_{k2} & \ldots & b_{kj} & \ldots & b_{kn} \end{bmatrix}$$

$$\mathbf{AB} = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ . & . & & . \\ . & . & c_{ij} & . \\ . & . & & . \\ c_{m1} & c_{m2} & \ldots & c_{mn} \end{bmatrix}$$

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj}$$

Matrix multiplication is not commutative

Example: Let

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Does **AB** = **BA**?

Solution:

$$\mathbf{AB} = \begin{bmatrix} 2 & 2 \\ 5 & 3 \end{bmatrix} \qquad \mathbf{BA} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$$

AB ≠ **BA**

Identity matrix and powers of matrices

Definition: The *identity matrix of order n* is the n x n matrix $\mathbf{I}_n = [\delta_{ij}]$, where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$.

$$\mathbf{I_n} = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ . & . & & . \\ . & . & . & . \\ . & . & & . \\ 0 & 0 & \ldots & 1 \end{bmatrix}$$

$\mathbf{AI}_n = \mathbf{I}_m\mathrm{A} = \mathbf{A}$, when $\mathbf{A}$ is an $m \times n$ matrix

Powers of square matrices can be defined. When A is an $n \times n$ matrix, we have:

$$\mathbf{A}^0 = \mathbf{I}_n \qquad \mathbf{A}^r = \mathbf{AAA} \cdots \mathbf{A}$$

Transposes of matrices

Definition: Let **A** = $[a_{ij}]$ be an $m \times n$ matrix. The *transpose* of **A**, denoted by $\mathbf{A}^{\mathrm{T}}$,is the $n \times m$ matrix obtained by interchanging the rows and columns of **A**.

If $\mathbf{A}^{\mathrm{T}} = [b_{ij}]$, then $\mathrm{b}_{\mathrm{ij}} = \mathrm{a}_{\mathrm{ji}}$ for $i = 1,2,\ldots,n$ and $j = 1,2, \ldots,m$.

The transpose of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ is the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$.

Transposes of matrices

Definition: A square matrix **A** is called symmetric if **A** = **A**^{T}. Thus **A** = $[a_{ij}]$ is symmetric if $a_{ij} = a_{ji}$ for i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$.

$$\text{The matrix } \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \text{ is square.}$$

Square matrices do not change when their rows and columns are interchanged.

Zero-one matrices

Definition: A matrix all of whose entries are either 0 or 1 is called a *zero-one matrix*

Algorithms operating on discrete structures represented by zero-one matrices are based on Boolean arithmetic defined by the following Boolean operations:

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{if } b_1 = b_2 = 1 \\ 0 & \text{otherwise} \end{cases} \qquad b_1 \vee b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

Zero-one matrices

Definition: Let **A** = $[a_{ij}]$ and **B** = $[b_{ij}]$ be an $m \times n$ zero-one matrices.

- The *join* of **A** and **B** is the zero-one matrix with (i,j)-th entry $a_{\mathrm{ij}} \vee b_{\mathrm{ij}}$. The *join* of **A** and **B** is denoted by **A** ∨ **B**.
- The meet of of **A** and **B** is the zero-one matrix with (i,j)-th entry $a_{\mathrm{ij}} \wedge b_{\mathrm{ij}}$. The *meet* of **A** and **B** is denoted by **A** ∧ **B**.

Joins and meets of zero-one matrices

Example: Find the join and meet of the zero-one matrices

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Solution:

The join of **A** and **B** is

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The meet of **A** and **B** is

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Boolean product of zero-one matrices

Definition: Let **A** = [a_{ij}] be an $m \times k$ zero-one matrix and **B** = [b_{ij}] be a $k \times n$ zero-one matrix. The *Boolean product* of **A** and **B**, denoted by **A** ⊙ **B**, is the $m\times n$ zero-one matrix with(i,j)-th entry

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \ldots \vee (a_{ik} \wedge b_{kj}).$$

Example: Find the Boolean product of **A** and **B**, where

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Boolean product of zero-one matrices

Solution: The Boolean product **A** ⊙ **B** is given by

$$\mathbf{A} \odot \mathbf{B} = \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Boolean product of zero-one matrices

Definition: Let **A** be a square zero-one matrix and let *r* be a positive integer. The *r*-th Boolean power of **A** is the Boolean product of *r* factors of **A**, denoted by $\mathbf{A}^{[r]}$. Hence,

$$\mathbf{A}^{[r]} = \underbrace{\mathbf{A} \odot \mathbf{A} \odot \ldots \odot \mathbf{A}}_{r \text{ times}}.$$

We define $\mathbf{A}^{[r]}$ to be $\mathbf{I}_n$.

(The Boolean product is well defined because the Boolean product of matrices is associative.)

Boolean product of zero-one matrices

Example: Let $\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$

Find $\mathbf{A}^n$ for all positive integers n.

Solution:

$$\mathbf{A}^{[2]} = \mathbf{A} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{A}^{[3]} = \mathbf{A}^{[2]} \odot \mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\mathbf{A}^{[4]} = \mathbf{A}^{[3]} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\mathbf{A}^{[5]} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \mathbf{A}^{[\mathbf{n}]} = \mathbf{A}^{\mathbf{5}} \quad \text{for all positive integers } n \text{ with } n \geq 5.$$

Next class

- Topic: Algorithm, Growth Function and Complexity
- Pre-class reading: Chap 3