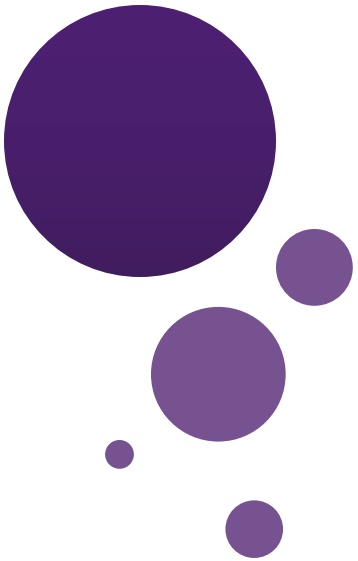


Lecture 15: Review for Midterm Exam 1

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

About the Midterm Exam 1

- The 1st Midterm Exam will be taken on Mar 8, 2019 at the LC 25 from 11:30 AM to 12:25 PM.
- It will cover Chap 1 to Chap 3.
- Note that this is a close book and close note exam.
- The necessary cheat sheet such as the equivalence laws will be provided.

Problem	Points	Scores
Problem 1: True or False	20	
Problem 2: True Table and Logical Equivalence	20	
Problem 3: Predicatives and Quantifiers	20	
Problem 4: Set, Sequences and Summation	20	
Problem 5: Functions	20	

(used in 2018 Fall semester)

About Midterm Exam 1

Figure 1: Logical equivalences.

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

$$p \to q \equiv \neg p \vee q$$
$$p \to q \equiv \neg q \to \neg p$$
$$p \vee q \equiv \neg p \to q$$
$$p \wedge q \equiv \neg(p \to \neg q)$$
$$\neg(p \to q) \equiv p \wedge \neg q$$
$$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$$
$$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$$
$$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$$
$$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$$

(a) Involving conditional statements.

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$
$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$
$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$
$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

(b) Involving biconditional statements.

Outlines

- Propositional and Logical Logic
- Rules of Inference, and Proofs
- Sets, Functions, Sequences and Matrices
- Algorithm, Growth Functions and Complexity
- Sample Problems in Tests

Outlines

- **Propositional and Logical Logic**
- Rules of Inference, and Proofs
- Sets, Functions, Sequences and Matrices
- Algorithm, Growth Functions and Complexity
- Sample Problems in Tests

Truth Tables

- Truth tables are used to show/define the relationships between the truth values of
  - the individual propositions and
  - the compound propositions based on them

p	*q*	*p*∧*q*	*p*∨*q*	*p*⊕*q*	*P->q*	*P<->q*
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Quantifiers

Statement	True when …	False when …
$\forall x\, P(x)$	$P(x)$ is true for every x	There is an x for which $P(x)$ is false
$\exists x\, P(x)$	There is an x for which $P(x)$ is true	$P(x)$ is false for every x

Statement	True when …	False when …
$\forall x \forall y\, P(x,y)$	$P(x,y)$ is true for every pair x,y	There is at least one *pair* x,y for which $P(x,y)$ is false
$\forall x \exists y\, P(x,y)$	For every x, there is a y for which $P(x,y)$ is true	There is an x for which $P(x,y)$ is false for every y
$\exists x \forall y\, P(x,y)$	There is an x for which $P(x,y)$ is true for every y	For every x, there is a y for which $P(x,y)$ is false
$\exists x \exists y P(x,y)$	There is at least one pair x,y for which $P(x,y)$ is true	$P(x,y)$ is false for every pair x,y

Logical Equivalences: Cheat Sheet

Identities (Equivalences)	Name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation laws

Logical Equivalences Involving Conditional Statements.
$p \rightarrow q \equiv \neg p \vee q$
$p \rightarrow q \equiv \neg q \rightarrow \neg p$
$p \vee q \equiv \neg p \rightarrow q$
$p \wedge q \equiv \neg(p \rightarrow \neg q)$
$\neg(p \rightarrow q) \equiv p \wedge \neg q$
$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Outlines

- Propositional and Logical Logic
- **Rules of Inference, and Proofs**
- Sets, Functions, Sequences and Matrices
- Algorithm, Growth Functions and Complexity
- Sample Problems in Tests

Rules of Inference

- Modus ponens: $(p \land (p \rightarrow q)) \rightarrow q$
- Addition: $p \rightarrow (p \lor q)$
- Simplification: $(p \land q) \rightarrow p$
- Conjunction: $((p) \land (q)) \rightarrow (p \land q)$
- Modus Tollens: $(\neg q \land (p \rightarrow q)) \rightarrow \neg p$
- Contrapositive: $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$
- Hypothetical Syllogism: $((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$
- Disjunctive Syllogism: $((p \lor q) \land \neg p) \rightarrow q$
- Resolution: $((p \lor q) \land (\neg p \lor r)) \rightarrow (q \lor r)$

Trivial Proofs

- Trivial Proof: Conclusion holds without using the premise.
- A trivial proof can be given when the conclusion is shown to be (always) true.
- That is, if q is true, then $p \rightarrow q$ is true

- **Example** It is easy to see:

$(x+1)^2 - 2x$

$= (x^2 + 2x + 1) - 2x$

$= x^2 + 1$

$\geq x^2$

Vacuous Proofs

- If the premise p is false
- Then the implication $p \rightarrow q$ is always true
- A vacuous proof is a proof that relies on the fact that no element in the universe of discourse satisfies the premise (thus the statement exists in vacuum in the UoD).
- Example:
  - If x is a prime number divisible by 16, then $x^2 < 0$
- No prime number is divisible by 16, thus this statement is true (counter-intuitive as it may be)

Direct Proofs

- Most of the proofs we have seen so far are direct proofs
- In a direct proof
  - You assume the hypothesis p, and
  - Give a direct series (sequence) of implications
  - Using the rules of inference
  - As well as other results (proved independently)
  - To show that the conclusion q holds.

Proof by Contrapositive

- Recall that $(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$
- This is the basis for the proof by contraposition
  - You assume that the conclusion is false, then
  - Give a series of implications to show that
  - Such an assumption implies that the premise is false
- **Example**
  - Prove that if $x^3 < 0$ then $x < 0$
  - The contrapositive is "if $x \geq 0$ then $x^3 \geq 0$"
  - Proof:
    1. If $x=0 \rightarrow x^3=0 \geq 0$
    2. If $x>0 \rightarrow x^2>0 \rightarrow x^3>0$ QED

Proof by Contradiction

- To prove a statement p is true
  - you may assume that it is false
  - And then proceed to show that such an assumption leads a contradiction with a known result
- In terms of logic, you show that
  - for a known result r,
  - $(\neg p \rightarrow (r \wedge \neg r))$ is true
  - Which yields a contradiction c = $(r \wedge \neg r)$ cannot hold
- Example: $\sqrt{2}$ is an irrational number

Proof by Contradiction: Example

- Let p be the proposition '$\sqrt{2}$ is an irrational number'
- Assume $\neg p$ holds, and show that it yields a contradiction
- $\sqrt{2}$ is rational

$\rightarrow \sqrt{2} = a/b$, a, b $\in \mathbb{R}$ and a, b have no common factor (proposition r) — *Definition of rational numbers*

$\rightarrow 2 = a^2/b^2$ — *Squarring the equation*

$\rightarrow (2b^2 = a^2) \rightarrow (a^2$ is even$) \rightarrow (a = 2c)$ — *Algebra*

$\rightarrow (2b^2 = 4c^2) \rightarrow (b^2 = 2c^2) \rightarrow (b^2$ is even$) \rightarrow (b$ is even) — *Algebra*

$\rightarrow$ (a, b are even) $\rightarrow$ (a, b have a common factor 2) $\rightarrow \neg r$

$\rightarrow (\neg p \rightarrow (r \wedge \neg r))$, which is a contradiction

So, ($\neg p$ is false) $\rightarrow$ (p is true), which means $\sqrt{2}$ is irrational

Proof by Cases

- Sometimes it is easier to prove a theorem by
  - Breaking it down into cases and
  - Proving each one separately
- Example:
  - Let $n \in \mathbb{Z}$. Prove that $9n^2+3n-2$ is even

Proof by Cases: Example

- Observe that $9n^2+3n-2=(3n+2)(3n-1)$
- n is an integer $\rightarrow$(3n+2)(3n-1) is the product of two integers
- **Case 1**: Assume 3n+2 is even

  $\rightarrow$ $9n^2+3n-2$ is trivially even because it is the product of two integers, one of which is even
- **Case 2**: Assume 3n+2 is odd

  $\rightarrow$ 3n+2-3 is even $\rightarrow$ 3n-1 is even $\rightarrow$ $9n^2+3n-2$ is even because one of its factors is even □

Existence Proofs

- A **constructive existence proof** asserts a theorem by providing a specific, concrete example of a statement
  - Such a proof only proves a statement of the form $\exists x P(x)$ for some predicate P.
  - It does not prove the statement for all such x
- A **nonconstructive existence proof** also shows a statement of the form $\exists x P(x)$, but is does not necessarily need to give a specific example x.
  - Such a proof usually proceeds by contradiction:
    - Assume that $\neg\exists x P(x) \equiv \forall x \neg P(x)$ holds
    - Then get a contradiction

Uniqueness Proofs

- A **uniqueness proof** is used to show that a certain element (specific or not) has a certain property.
- Such a proof usually has two parts
  1. A proof of existence: $\exists x P(x)$
  2. A proof of uniqueness: if $x \neq y$ then $\neg P(y)$)
- Together we have the following:

$$\exists x \, (\, P(x) \wedge (\forall y \, (x \neq y \rightarrow \neg P(y) \,) \,)$$

Counter Examples

- Sometimes you are asked to disprove a statement
- In such a situation you are actually trying to prove the negation of the statement
- With statements of the form $\forall x\ P(x)$, it suffices to give a counter example
  - because the existence of an element x for which $\neg P(x)$ holds proves that $\exists x\ \neg P(x)$
  - which is the negation of $\forall x\ P(x)$

Counter Examples: Example

- Example: Disprove n^2+n+1 is a prime number for all $n \geq 1$
- A simple counterexample is n=4.
- In fact: for n=4, we have

  $n^2+n+1 = 4^2+4+1$

  $= 16+4+1$

  $= 21 = 3 \times 7$, which is clearly not prime QED

Outlines

- Propositional and Logical Logic
- Rules of Inference, and Proofs
- **Sets, Functions, Sequences and Matrices**
- Algorithm, Growth Functions and Complexity
- Sample Problems in Tests

Set

- **Definition**: A set is an unordered collection of (unique) objects
- 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:

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

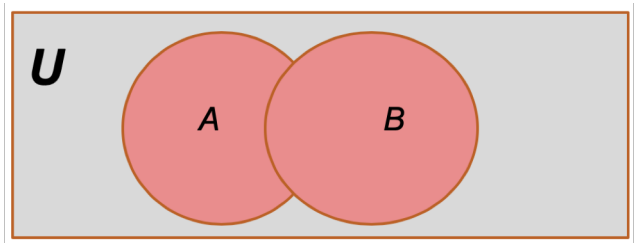
Power Set

- **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

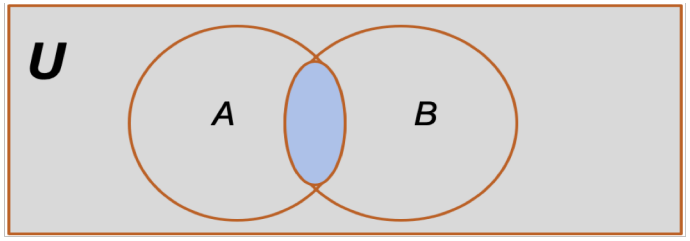
$$|P(S)| = 2^n$$

Set Operations

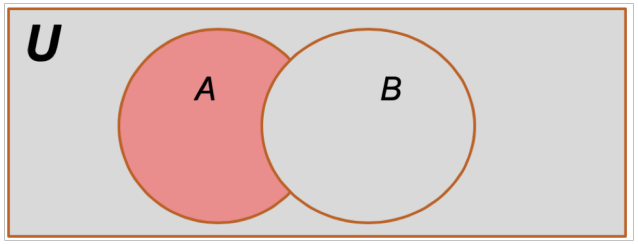
- Similarly, set operators exist and act on two sets to give us new sets
  - Union $\cup$ and intersection $\cap$
  - Set difference $\setminus$
  - Set complement $\overline{S}$



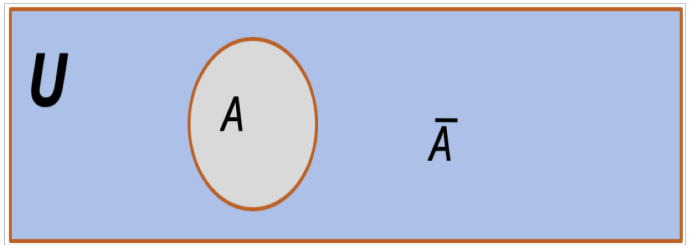
$A \cup B = \{ x \mid (a \in A) \vee (b \in B) \}$



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



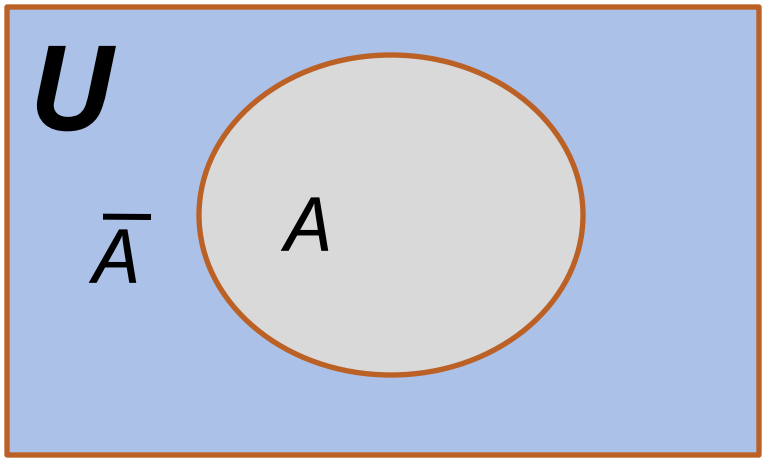
$A - B$

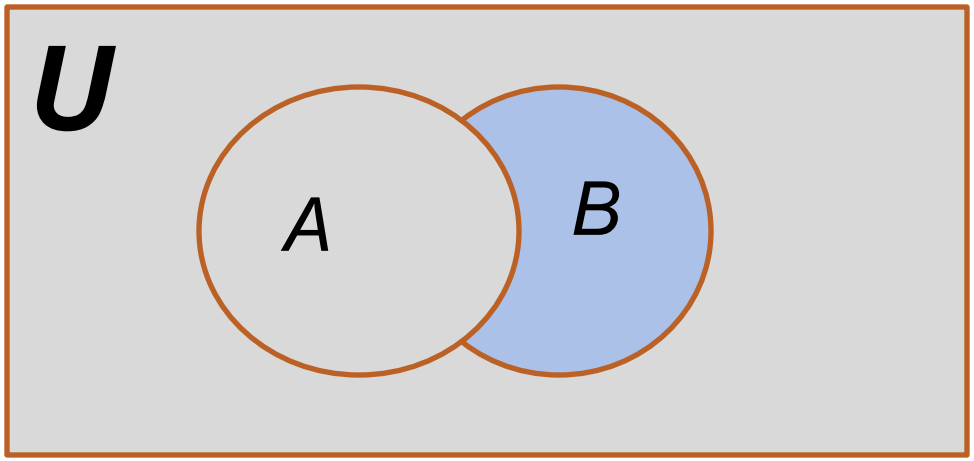


$\overline{A} = A^C = \{x \mid x \notin A\}$

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





Cartesian Product

- **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 $b \in B$

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

- The Cartesian product is also known as the cross product
- 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

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

Computer Representation of Sets

- 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 $a_i \in A$

Cardinality

- 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 $|A| = \infty$.

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 $a_1 = f(1), a_2 = f(2), \ldots, a_n = f(n), \ldots$

Some Facts

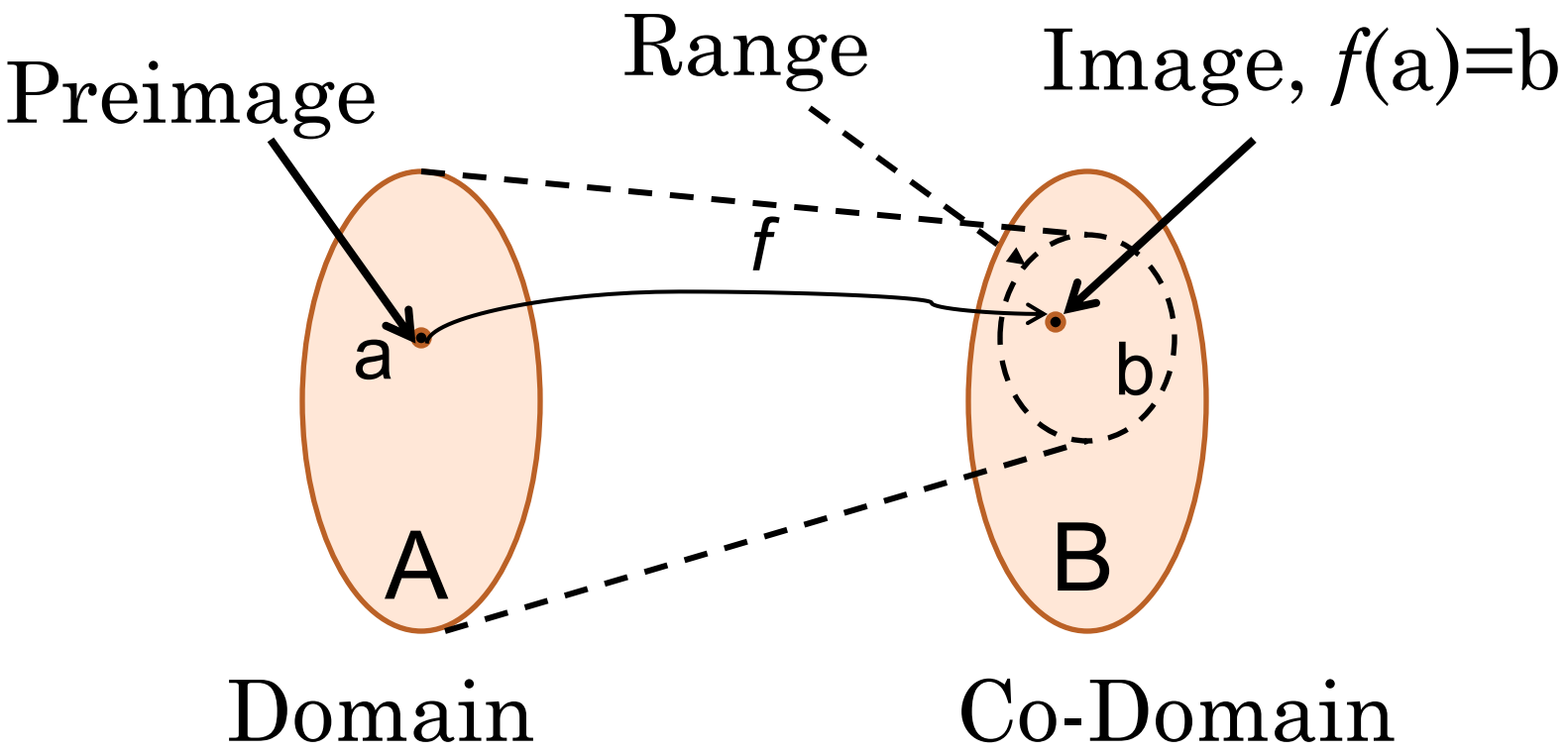
1. A set S is finite if and only if for any proper subset $A \subset S$, $|A| < |S|$; that is, "proper subsets of a finite set have fewer elements."

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.

Function



A function, f: A $\rightarrow$ B

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$\rightarrow$B is called <u>onto</u> or <u>surjective</u> (or an surjection) if

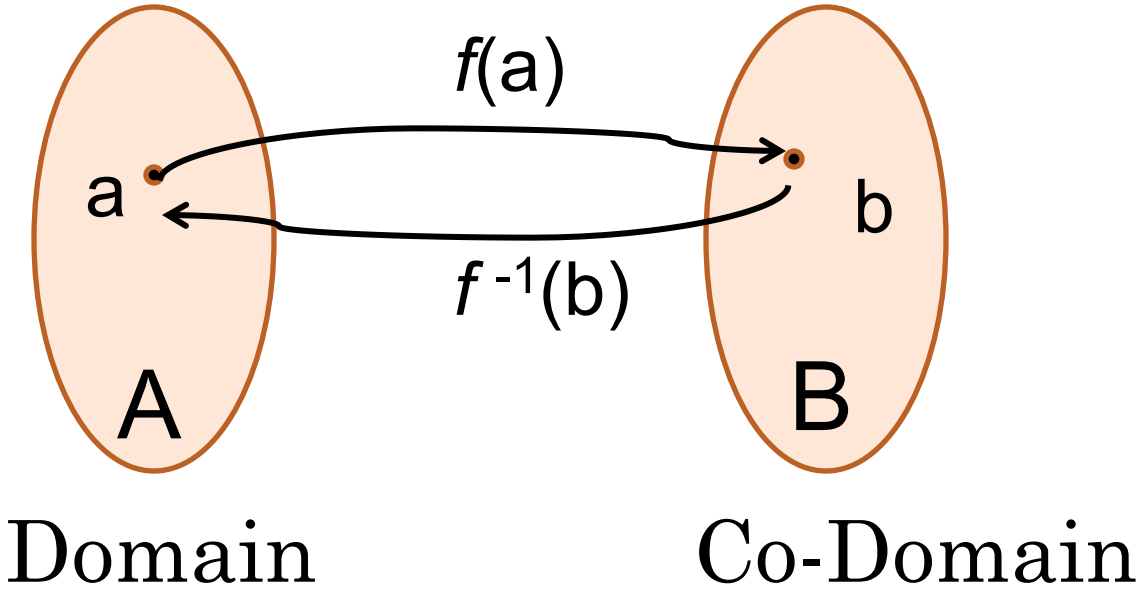
$$\forall\ b \in B, \exists\ a \in A \text{ with } f(a)=b$$

- 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

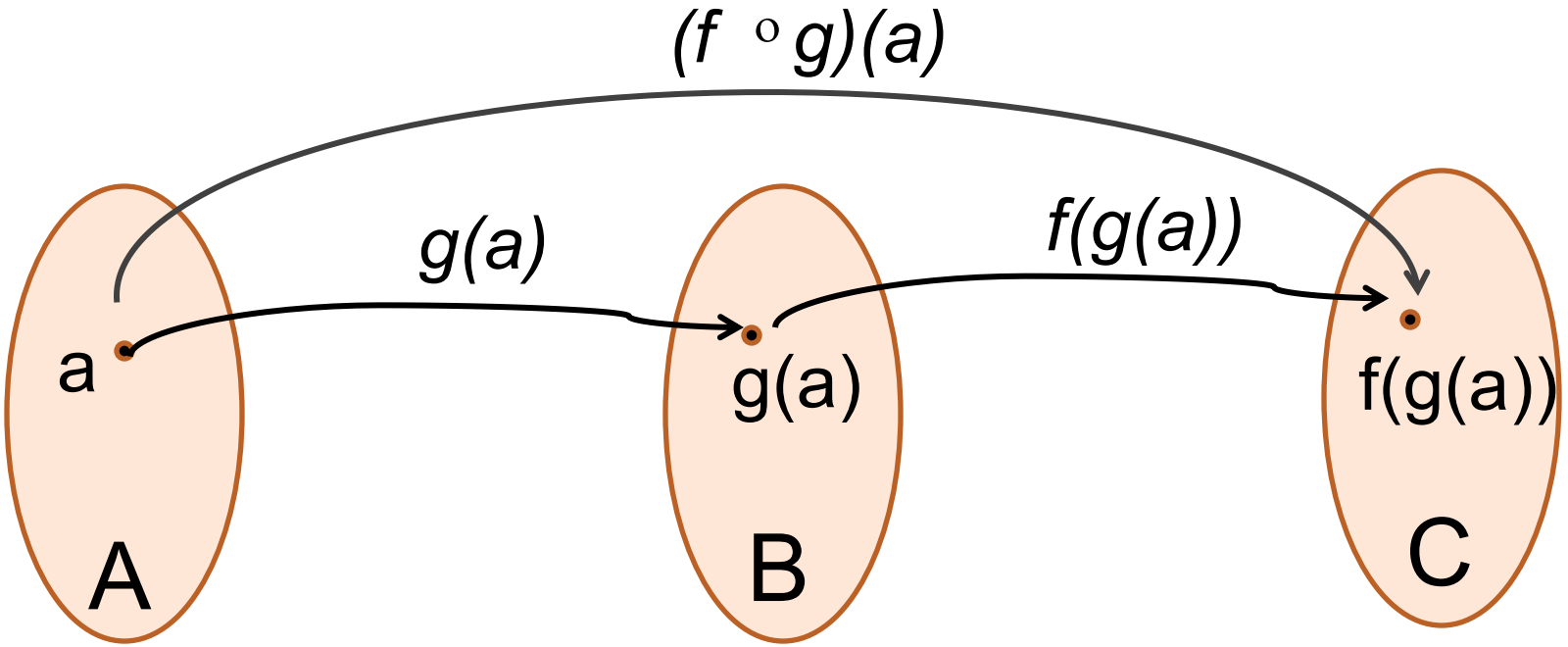
- **Definition**: A function *f* is a one-to-one correspondence (or a bijection), if is both one-to-one (injective) and onto (surjective)
- One-to-one correspondences are important because they endow a function with an inverse.
- They also allow us to have a concept cardinality for infinite sets
- Let's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

Inverse Functions: Representation



A function and its inverse

Composition: Graphical Representation



The composition of two functions

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: $f(x) = ar^x$

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

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

Sum of arithmetic series

$$S = \frac{n\left(a_1 + a_n\right)}{2}$$

$$\begin{cases} S = \text{Sum} \\ n = \text{Number of Terms} \\ a_1 = \text{First Term} \\ a_n = \text{Last Term} \end{cases}$$

$$S = \frac{n\left(a_1 + a_1 + \left(n-1\right)d\right)}{2}$$

$$S = \frac{n\left(2a_1 + \left(n-1\right)d\right)}{2}$$

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?

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:

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

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

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

Zero-one matrices

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

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

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 $\mathbf{A} = [a_{ij}]$ be an $m \times k$ zero-one matrix and $\mathbf{B} = [b_{ij}]$ be a $k \times n$ zero-one matrix. The *Boolean product* of **A** and **B**, denoted by $\mathbf{A} \odot \mathbf{B}$, 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 $\mathbf{A} \odot \mathbf{B}$ 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:

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

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

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

Outlines

- Propositional and Logical Logic
- Rules of Inference, and Proofs
- Sets, Functions, Sequences and Matrices
- **Algorithm, Growth Functions and Complexity**
- Sample Problems in Tests

Algorithms

- When presented a problem, e.g., given a sequence of integers, find the larges one
- Construct a model that translates the problem into a mathematical context
  - Discrete structures in such models include sets, sequences, functions, graphs, relations, etc.
- A method is needed that will solve the problem (using a sequence of steps)
- **Algorithm**: a sequence of steps

Algorithm

- **Algorithm**: a finite set of precise instructions for performing a computation or for solving a problem

- Some problems have no solution.
- Some people know solution for some problem.
- Some solutions for some problems could be described as a sequence of instructions.
- Some sequences of instructions are **algorithms**.

Big-*O* Notation

- Let *f* and *g* be functions from the set of integers or the set of real numbers to the set of real numbers. We say that *f*(*x*) is *O*(*g*(*x*)) if there are constants *C* and *k* such that

$$|f(x)| \leq C|g(x)|$$

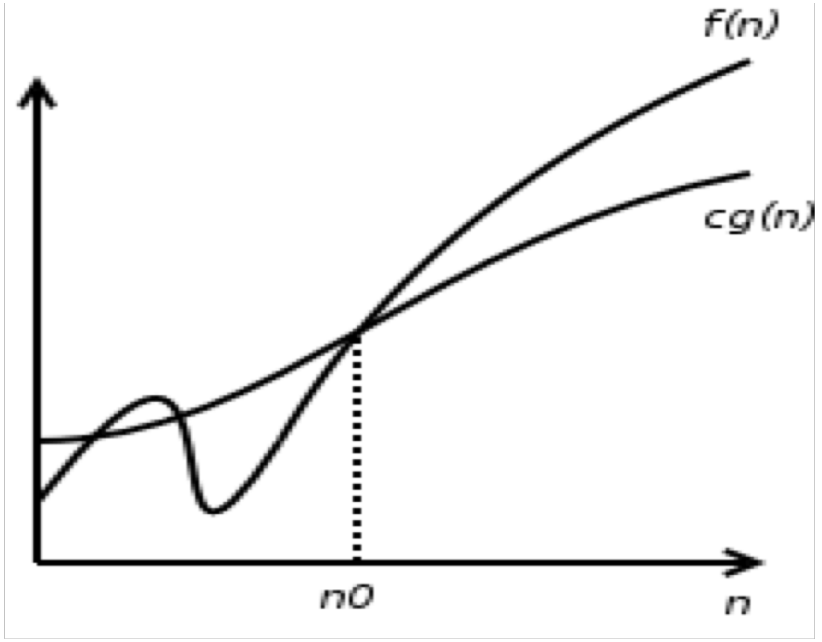
  whenever $x > k$.
- This is read as "*f*(*x*) is big oh of *g*(*x*)" or "*g* asymptotically dominates *f*."
- The constants C and k are called **witnesses** to the relationship *f*(*x*) is *O*(*g*(*x*)). Only one pair of witnesses is needed.

Big-Omega Notation

- Let *f* and *g* be functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $\Omega(g(x))$
- if there are constants *C* and *k* such that $|f(x)| \geq C|g(x)|$
- when $x > k$.
- We say that "*f*(*x*) is big-Omega of *g*(*x*)."

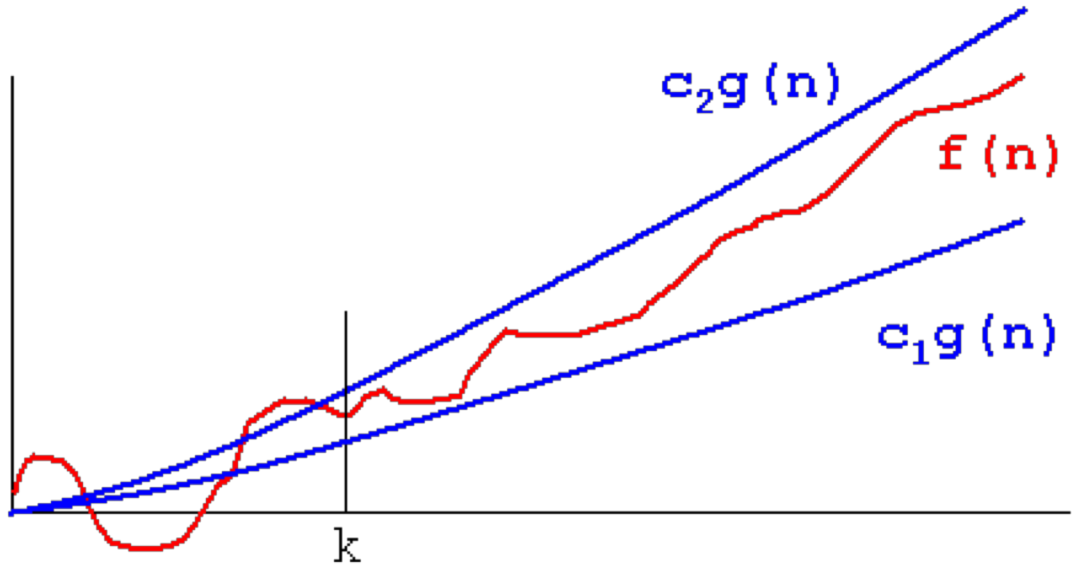
Big-Omega Notation

- Big-*O* gives an upper bound on the growth of a function, while Big-Omega gives a lower bound. Big-Omega tells us that a function grows at least as fast as another.
- $f(x)$ is $\Omega(g(x))$ if and only if $g(x)$ is $O(f(x))$. This follows from the definitions.



Big-Theta Notation

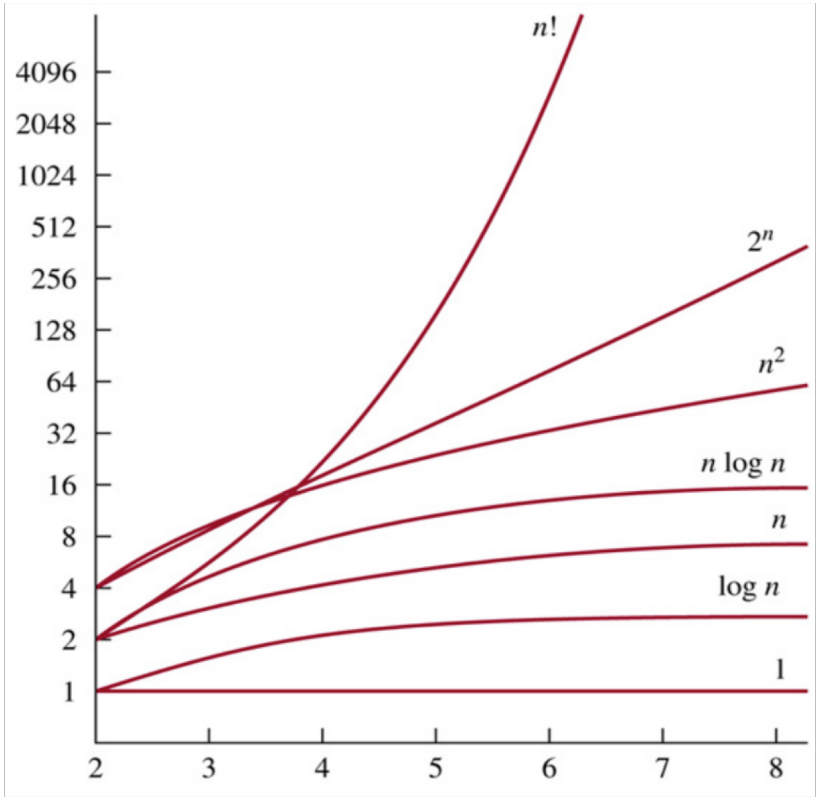
- Let *f* and *g* be functions from the set of integers or the set of real numbers to the set of real numbers. The function $f(x)$ is $\Theta(g(x))$ if $f(x)$ is $O(g(x))$ and $f(x)$ is $\Omega(g(x))$



Comparison of Complexities

- Important complexity classes:

$$O(1) \subseteq O(\log n) \subseteq O(n) \subseteq O(n \log n) \subseteq O(n^2) \subseteq O(c^n) \subseteq O(n!)$$



A Display of the Growth of Functions Commonly Used in Big-O Estimates

Outlines

- Propositional and Logical Logic
- Rules of Inference, and Proofs
- Sets, Functions, Sequences and Matrices
- Algorithm, Growth Functions and Complexity
- **Sample Problems in Tests**

True/False Problem Examples

Problem 1: True or False (20 points)

(1) The sentences "x + 2 = 11." and "Do not pass go." are propositions.
- ○ True ○ False

(2) $1 + 1 = 3$ if and only if monkeys can fly.
- ○ True ○ False

(3) For integer variable m and n, the true value of $\exists n \forall m(nm = m)$ is True.
- ○ True ○ False

(4) $\emptyset$ is an element in the set $\{\emptyset\}$.
- ○ True ○ False

(5) $\emptyset$ is a subset in the set $\{\emptyset\}$.
- ○ True ○ False

(6) If A and B are sets, then $A - B$ is equivalent to $B - A$.
- ○ True ○ False

(7) The function $f(x) = 2x - 3$ is a one-to-one (injective) and onto (surjective) function from interger numbers **Z** to **Z**.
- ○ True ○ False

(8) The function $f(x) = 2x - 3$ is a one-to-one (injective) and onto (surjective) function from natural numbers **N** to **N**.
- ○ True ○ False

(9) The set $C = \{2n - 1 \mid n \text{ is a natural number}\}$ (the odd natural numbers) is countably infinite.
- ○ True ○ False

(10) Let **A** and **B** are two arbitrary 2×2 matrix. $\mathbf{AB} = \mathbf{BA}$.
- ○ True ○ False

(1) False

(2) p : $1+1=3$, is False
q : monkeys can fly, is False
$p \leftrightarrow q$: True

(3) $\exists n \forall m \ (nm = m)$: If $n = 1$ (say)
for $\forall m \in Z$, $(1)(m) = m$.
which is True.
∴ There exist at least one n, i.e., $n = 1$,
for which all the values of m satisfies
$(nm = m)$ condition.
∴ Answer = True

(4) True

(5) True

(6) False

(7) True

(8) False ; $y = 2x - 3 \Rightarrow x = \frac{y+3}{2}$ ⇒ if $y \in N$ (for all) but $x \notin N$.
∴ Not onto function.

(9) True

(10) False

Problem Example

Problem 2: True Table and Logical Equivalence (20 points)

(1) [8 points] Use a truth table to verify the first De Morgan law $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

(2) [12 points] Show that $\neg p \rightarrow (q \rightarrow r)$ and $q \rightarrow (p \vee r)$ are logically equivalent.

(1) Verify $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

p	q	¬p	¬q	p ∧ q	¬(p ∧ q)	¬p ∨ ¬q
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

Since the truth values of ¬(p ∧ q) and ¬p ∨ ¬q is the same for the same combinations of p and q, they are logically equivalent.

(2) $\neg p \rightarrow (q \rightarrow r) \equiv q \rightarrow (p \vee r)$

Show if it is logically equivalent.

p	q	r	¬p	q → r	¬p → (q → r)	(p ∨ r)	q → (p ∨ r)
T	T	T	F	T	T	T	T
T	T	F	F	F	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	F	F
F	F	T	T	T	T	T	T
F	F	F	T	T	T	F	T

Since the truth values of ¬p → (q → r) and q → (p ∨ r) are the same for the same combinations of p and q, they are logically equivalent.

You should know how to prove logical equivalence using the known equivalence laws provided in the cheat sheet.

Problem Example

Problem 3: Predicatives and Quantifiers (20 points)

Let $Q(x)$ be the statement "$x+1 > 2x$." If the domain consists of all integers, what are these truth values for the following statements and why? Explain your solution with details.

(1) $Q(0)$, $Q(-1)$, and $Q(1)$.
(2) $\exists x Q(x)$
(3) $\forall x Q(x)$
(4) $\exists x \neg Q(x)$
(5) $\forall x \neg Q(x)$.

Problem: 3

$Q(x)$: $x+1 > 2x$ (Domain is Integers)

(1) $Q(0)$: $0+1 > 2(0) \Rightarrow 1 > 0$
which is true
$\therefore$ $Q(0)$ is True

$Q(-1)$: $-1+1 > 2(-1) \Rightarrow 0 > -2$,
which is true
$\therefore$ $Q(-1)$ is True

$Q(1)$: $1+1 > 2(1) \Rightarrow 2 > 2$,
which is false
$\therefore$ $Q(1)$ is False

(2) $\exists x Q(x)$: This statement is true, when we have at least one value of x such that $Q(x)$ is True.
Let's have, $x = 0$,
$Q(0)$: $0+1 > 2(0) \Rightarrow 1 > 0$, which is True
$\therefore$ $\exists x Q(x)$ is True

(3) $\forall x Q(x)$: This statement is true, when all the values of x satisfies $Q(x)$ else it is false.
Let's have $x = 1$
$Q(1)$: $1+1 > 2(1) \Rightarrow 2 > 2$, which is false.
$\therefore$ when $x = 1$, $Q(x)$ gives false value.
$\therefore$ $\forall x Q(x)$ is False

(4) $\exists x \neg Q(x)$: This statement is true, when there exist any one x such that $Q(x)$ is False.
Let's have $x = 1$.
$Q(1)$: $2 > 2$, which is false.
$\therefore$ $\exists x \neg Q(x)$ is True

(5) $\forall x \neg Q(x)$: This statement is True, when $Q(x)$ gives false value for all values of x. Else, it is a False statement.
Let $x = 1$, $Q(0)$: True.
$\therefore$ $\forall x \neg Q(x)$ is False

Problem Example

Problem 4: Set, Sequences and Summation (20 points)

(1) **[4 points]** Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{0, 3, 6\}$. Find $A \vee B$, $A \wedge B$, $A - B$ and $B - A$.

(2) **[6 points]** For each of these lists of integers, provide a simple formula or rule that generates the terms of an integer sequence that begins with the given list. Assuming that your formula or rule is correct, determine the next three terms of the sequence.

[a] $15, 8, 1, -6, -13, -20, -27, \ldots$

[b] $3, 6, 12, 24, 48, 96, 192, \ldots$

(3) **[10 points]** Compute the sum $\sum_{j=1}^{20}(1 + 3j + (-1)^j)$.

Problem 4:

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

$B = \{0, 3, 6\}$

$A \cap B = \{3\}$

$A \cup B = \{0, 1, 2, 3, 4, 5, 6\}$

$A - B = \{1, 2, 4, 5\}$

$B - A = \{0, 6\}$

(2)

(a) $15, 8, 1, -6, -13, -20, -27, \ldots$

As the difference between any two adjacent numbers is same, it produces an arithmetic sequence whose nth term is defined by formula,

$a_n = a_1 + (n-1)d$ where,

a_1 = value of first term

d = difference.

→ Here $a_1 = 15$ and $d = 8 - 15 = (-7)$

$\therefore a_n = 15 + (n-1)(-7)$

$= 15 - 7n + 7$

$\boxed{a_n = 22 - 7n}$, $n \geq 1$.

Given sequence is: $15, 8, 1, -6, -13, -20, -27, \ldots$

Here, the difference between 2 adjacent numbers is -7.

∴ The term after $-27 = -27 - 7 = -34$

the term after $-34 = -34 - 7 = -41$

the term after $-41 = -41 - 7 = -48$

∴ $\boxed{-34, -41, -48}$ are the next 3 terms of the given sequence.

(b) Given sequence: $3, 6, 12, 24, 48, 96, 192, \ldots$

Since the ratio between two adjacent numbers is same, this sequence is a geometric sequence with $a_1 = 3$ and $r(\text{ratio}) = \frac{6}{3} = 2$.

∴ nth term of G.P is given by,

$a_n = a_1 r^{n-1}$

$\therefore \boxed{a_n = (3)(2)^{n-1}}$, $n \geq 1$

Here, the sequence is: $3, 6, 12, 24, 48, 96, 192, \ldots$ with ratio $= 2$,

The term after $192 = 192 \times 2 = 384$

the term after $384 = 384 \times 2 = 768$

the term after $768 = 768 \times 2 = 1536$

∴ 384, 768 and 1536 are the next 3 terms in the sequence.

(3) $\sum_{j=1}^{20}\left(1 + 3j + (-1)^j\right)$

$= \sum_{j=1}^{20} 1 + \sum_{j=1}^{20}(3j) + \sum_{j=1}^{20}(-1)^j$

$= 20 + 3\frac{(20)(20+1)}{2} + \{(-1)^1 + (-1)^2 + (-1)^3 + (-1)^4 + \cdots + (-1)^{19} + (-1)^{20}\}$

$\left[\because \sum_{j=1}^{n} 1 = n \text{ and } \sum_{j=1}^{n} j = \frac{n(n+1)}{2}\right]$

$= 20 + (30)(21) + 0$

$= 20 + 630$

$= 650$

$\therefore \boxed{\sum_{j=1}^{20}\left(1 + 3j + (-1)^j\right) = 650}$

Problem Example

Problem 5: functions (20 points)

(a) **[10 points]** Show the function $f(x) = x^3 + 1$ is a bijection from **R** to **R**.

(b) **[10 points]** Find $f \circ g$ and $g \circ f$, where $f(x) = x^2 + 1$ and $g(x) = x + 2$, are functions from **R** to **R**.

Problem 5 :

(1) Show that the function, $f(x) = x^3 + 1$ is bijection from $R \to R$.

→ For a function to be bijection, it has to be one-to-one as well as onto function.

→ To prove a function to be one-to-one, let us assume $f(x_1) = f(x_2)$ and if we get $x_1 = x_2$, then the function is one-to-one else not.

$\Rightarrow$ If $f(x_1) = f(x_2) \Rightarrow x_1^3 + 1 = x_2^3 + 1$

$\Rightarrow x_1^3 = x_2^3$

$\Rightarrow x_1 = x_2$

∴ This function is one-to-one.

→ To prove a function to be an onto function, let us assume $f(x) = Y$.

$\Rightarrow x^3 + 1 = Y$

$\Rightarrow x^3 = Y - 1$

$\Rightarrow x = \sqrt[3]{Y-1}$

∴ $\forall Y \in R \Rightarrow \sqrt[3]{Y-1} \in R \Rightarrow x \in R$.

Thus, every value of Y in codomain, there is a value of x in domain corresponding to it.

Thus, this function is onto function.

→ Since this function is both one-to-one function as well as an onto function, it is a bijection function

(2) $f : R \to R$, $f(x) = x^2 + 1$

$g : R \to R$, $g(x) = x + 2$

$fog(x) = f(g(x)) = f(x+2) = (x+2)^2 + 1$

$= x^2 + 4x + 5$

$gof(x) = g(f(x)) = g(x^2+1) = (x^2+1) + 2$

$= x^2 + 3$

Next class

- Topic: Integers and Division
- Pre-class reading: Chap 4.1