# Mathematics Review I
# (Basic Terminology)

- Unlike other CS courses, this course is a MATH course...
- We will look at a lot of definitions, theorems and proofs
- This lecture: reviews basic math notation and terminology
  - Set, Sequence, Function, Graph, String...
- Also, common proof techniques
  - By construction, induction, contradiction

# Set

- A set is a group of items
- One way to describe a set:  list every item in the group inside { }
  - E.g., { 12, 24, 5 } is a set with three items
- When the items in the set has trend:  use ...
  - E.g., { 1, 2, 3, 4, ... }  means the set of natural numbers
- Or, state the rule
  - E.g., { n | n = $m^2$ for some positive integer m } means the set { 1, 4, 9, 16, 25, ... }
- A set with no items is an empty set denoted by { } or $\emptyset$

# Set

- The order of describing a set does not matter
  - $\{ 12, 24, 5 \} = \{ 5, 24, 12 \}$

- Repetition of items does not matter too
  - $\{ 5, 5, 5, 1 \} = \{ 1, 5 \}$

- Membership symbol $\in$
  - $5 \in \{ 12, 24, 5 \}$   $7 \notin \{ 12, 24, 5 \}$

- How many items are in each of the following set?
  - { 3, 4, 5, ..., 10 }
  - { 2, 3, 3, 4, 4, 2, 1 }
  - { 2, {2}, {{1,2,3,4,5,6}} }
  - $\emptyset$
  - {$\emptyset$}

# Set

Given two sets A and B

- we say $A \subseteq B$ (read as A is a subset of B) if every item in A also appears in B
  - E.g., A = the set of primes, B = the set of integers

- we say $A \subsetneq B$ (read as A is a proper subset of B) if $A \subseteq B$ but $A \neq B$

Warning: Don't be confused with $\in$ and $\subseteq$

  - Let A = { 1, 2, 3 }. Is $\emptyset \in A$? Is $\emptyset \subseteq A$?

# Union, Intersection, Complement

Given two sets A and B
- A ∪ B (read as the union of A and B) is the set obtained by combining all elements of A and B in a single set
  - E.g., A = { 1, 2, 4 }  B = { 2, 5 }
    A ∪ B = { 1, 2, 4, 5 }
- A ∩ B (read as the intersection of A and B) is the set of common items of A and B
  - In the above example, A ∩ B = { 2 }
- $\overline{A}$ (read as the complement of A) is the set of items under consideration not in A

# Set

- The **power set** of A is the set of all subsets of A, denoted by $2^A$
  - E.g., A = { 0, 1 }
    $$2^A = \{ \{\}, \{0\}, \{1\}, \{0,1\} \}$$
  - How many items in the above power set of A?
- If A has n items, how many items does its power set contain? Why?

# Sequence

- A sequence of items is a list of these items in some order
- One way to describe a sequence: list the items inside ( )
  - ( 5, 12, 24 )
- Order of items inside ( ) matters
  - ( 5, 12, 24 ) ≠ ( 12, 5, 24 )
- Repetition also matters
  - ( 5, 12, 24 ) ≠ ( 5, 12, 12, 24 )
- Finite sequences are also called tuples
  - ( 5, 12, 24 ) is a 3-tuple
  - ( 5, 12, 12, 24 ) is a 4-tuple

# Sequence

Given two sets A and B

- The **Cartesian product** of A and B, denoted by A x B, is the set of all possible 2-tuples with the first item from A and the second item from B
  - E.g., $A = \{1, 2\}$ and $B = \{x, y, z\}$
  $A \times B = \{ (1,x), (1,y), (1,z), (2,x), (2,y), (2,z) \}$

- The Cartesian product of k sets, $A_1, A_2, ..., A_k$, denoted by $A_1 \times A_2 \times \cdots \times A_k$, is the set of all possible k-tuples with the $i^{th}$ item from $A_i$

# Functions

- A function takes an input and produces an output
- If f is a function, which gives an output b when input is a, we write

$$f(a) = b$$

- For a particular function f, the set of all possible input is called f's domain
- The outputs of a function come from a set called f's range

# Functions

- To describe the property of a function that it has domain D and range R, we write

$$f : D \rightarrow R$$

- E.g., The function add (to add two numbers) will have an input of two integers, and output of an integer
  - We write: add: $Z \times Z \rightarrow Z$

# Strings

- An alphabet = a set of characters
  - E.g., The English Alphabet = {A,B,C,...,Z}
- A string = a sequence of characters
- A string *over* an alphabet $\Sigma$
  - A sequence of characters, with each character coming from $\Sigma$
- The length of a string w, denoted by |w|, is the number of characters in w
- The empty string (written as $\varepsilon$) is a string of length 0

# Strings

Let $w = w_1 w_2 \ldots w_n$ be a string of length $n$

- A **substring** of w is a **consecutive** subsequence of w (that is, $w_i w_{i+1} \ldots w_j$ for some $i \leq j$)

- The **reverse** of w, denoted by $w^R$, is the string $w_n \ldots w_2 w_1$

- A set of strings is called a **language**

# PROOF TECHNIQUES

# We look at

- Proof by contradiction

- Proof by construction

- Proof by induction

- 

- But we may use some other also..

- For eg., Proof by counter example to disprove a statement…

# By Contradiction

- One common way to prove a theorem is to assume that the theorem is false, and then show that this assumption leads to an obviously false consequence (also called a contradiction)

- This type of reasoning is used frequently in everyday life, as shown in the following example

# By Contradiction

- Jack sees Jill, who just comes in from outdoor
- Jill looks completely dry
- Jack knows that it is not raining
- Jack's proof:
  - If it *were* raining (the assumption that the statement is false), Jill will be wet.
  - The consequence is: "Jill is wet" AND "Jill is dry", which is obviously false
  - Therefore, it must not be raining

# By Contradiction [Example 1]

- Let us define a number is rational if it can be expressed as p/q where p and q are integers; if it cannot, then the number is called irrational

- E.g.,
  - 0.5 is rational because 0.5 = 1/ 2
  - 2.375 is rational because 2.375 = 2375 / 1000

# By Contradiction

- Theorem: $\sqrt{2}$ (the square-root of 2) is irrational.

- How to prove?

- First thing is …

    Assume that $\sqrt{2}$ is rational

# By Contradiction

- Proof: Assume that $\sqrt{2}$ is rational. Then, it can be written as p/q for some positive integers p and q.

- In fact, we can further restrict that p and q does not have common factor.
  - If D is a common factor of p and q, we use p' = p/D and q' = q/D so that p'/q' = p/q = $\sqrt{2}$ and there is no common factor between p' and q'

- Then, we have $p^2/q^2 = 2$, or $2q^2 = p^2$.

# By Contradiction

- Since $2q^2$ is an even number, $p^2$ is also an even number

  - This implies that p is an even number (why?)

- So, $p = 2r$ for some integer r

- $2q^2 = p^2 = (2r)^2 = 4r^2$

  - This implies $2r^2 = q^2$

- So, q is an even number

- Something wrong happens... (what is it?)

# By Contradiction

- We now have: "p and q does not have common factor" AND "p and q have common factor"

  - This is a contradiction

- Thus, the assumption is wrong, so that $\sqrt{2}$ is irrational

# By Contradiction [Example 2]

- Theorem (Pigeonhole principle): A total of $n+1$ balls are put into $n$ boxes. At least one box containing 2 or more balls.

- Proof: Assume "at least one box containing 2 or more balls" is false
    - That is, each has at most 1 or fewer ball

    Consequence: total number of balls $\leq n$

    Thus, there is a contradiction (what is that?)

# Proof By Construction

- Many theorem states that a particular type of object exists

- One way to prove is to find a way to construct one such object

- This technique is called proof by construction

- Theorem: There exists a rational number p which can be expressed as $q^r$, with q and r both irrational.

- How to prove?
  - Find p, q, r satisfying the above condition

- What is the irrational number we just learnt? Can we make use of it?

# By Construction

- What is the following value?
  $$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$$

- If $\sqrt{2}^{\sqrt{2}}$ is rational, then $q = r = \sqrt{2}$ gives the desired answer

- Otherwise, $q = \sqrt{2}^{\sqrt{2}}$ and $r = \sqrt{2}$ gives the desired answer

# By Induction

- Normally used to show that all elements in an infinite set have a specified property

- The proof consists of proving two things:  The basis, and the inductive step

- Mathematical induction proves that we can climb as high as we like on a ladder, by proving that we can climb onto the bottom rung (the **basis**) and that from each rung we can climb up to the next one (the **inductive step**).

# We consider only enumerable or countable sets with a least element [well ordered sets]

1. The **base case**: prove that the statement holds for the first natural number $n$. Usually, $n = 0$ or $n = 1$;

   - rarely, but sometimes conveniently, the base value of $n$ may be taken as a larger number, or even as a negative number (the statement only holds at and above that threshold).

2. The **step case** or **inductive step**: assume the statement holds for some natural number $n$, and prove that then the statement holds for $n + 1$.

# By Induction [Example 1]

- Let F(k) be a sequence defined as follows:
- $F(1) = 1$
- $F(2) = 1$
- for all $k \geq 3$, $F(k) = F(k-1) + F(k-2)$
- Theorem: For all $n \geq 1$,

$$F(1)+F(2) + \ldots + F(n) = F(n+2) - 1$$

# By Induction

- Let P(k) means "the theorem is true when n = k"
- Basis:  To show P(1) is true.
  - F(1) = 1,  F(3) = F(1) + F(2) = 2
  - Thus, F(1) = F(3) – 1
  - Thus, P(1) is true
- Inductive Step:  To show for $k \geq 1$, P(k)$\rightarrow$P(k+1)
  - P(k) is true means:  F(1) + F(2) + ... + F(k) = F(k+2) – 1
  - Then, we have

$$F(1) + F(2) + ... + F(k+1)$$
$$= (F(k+2) – 1) + F(k+1)$$
$$= F(k+3) – 1$$

  - Thus, P(k+1) is true if P(k) is true

# Variants

- There can be many other types of basis and inductive step, as long as by proving both of them, they can cover all the cases
- For example, to show P is true for all k > 1, we can show
  - Basis: P(1) is true, P(2) is true
  - Inductive step: P(k) → P(k+2)

# Variants

- **Complete (strong) induction:** (in contrast to which the basic form of induction is sometimes known as **weak induction**) makes the inductive step easier to prove by using a stronger hypothesis: one proves the statement $P(m + 1)$ under the assumption that $P(n)$ holds for all $n,\ n \leq m$.

# Example: forming dollar amounts by coins

- Assume an infinite supply of 4 and 5 dollar coins.
- Prove that any whole amount of dollars greater than 12 can be formed by a combination of such coins.
- In more precise terms, we wish to show that for any amount $n \geq 12$ there exist natural numbers $a$ and $b$ such that $n = 4a + 5b$, where 0 is included as a natural number.
- The statement to be shown true is thus:

$$S(n): \quad n \geq 12 \Rightarrow \exists\, a, b \in \mathbb{N}.\ \ n = 4a + 5b$$

**Base case**: Show that $S(k)$ holds for $k = 12, 13, 14, 15$.

$$4 \cdot 3 + 5 \cdot 0 = 12$$
$$4 \cdot 2 + 5 \cdot 1 = 13$$
$$4 \cdot 1 + 5 \cdot 2 = 14$$
$$4 \cdot 0 + 5 \cdot 3 = 15$$

The base case holds.

Induction step:
For $j = 12, 13, \dots, 15, \dots, k$ we assume that the theorem is true.

For $j = k + 1$, we show that the theorem is true.

Since for $j = k, k - 1, k - 2, k - 3$ the theorem is true (why?).
So, $k - 3 = 4a + 5b$, for some nonnegative integers $a$ and $b$.
Since $k + 1 = (k - 3) + 4$,
we have, $k + 1 = 4a + 5b + 4 = 4(a + 1) + 5b$.          Q.E.D.

- The following is not a valid proof by induction!

# By Induction?

- CLAIM: In any set of h horses, all horses are of the same color.

- PROOF: By induction. Let P(k) means "the claim is true when h = k"

- Basis: P(1) is true, because in any set of 1 horse, all horses clearly are the same color.

# By Induction?

- Inductive step:
  - Assume P(k) is true.
  - Then we take any set of k+1 horses.
  - Remove one of them. Then, the remaining horses are of the same color (because P(k) is true).
  - Put back the removed horse into the set, and remove another horse
  - In this new set, all horses are of same color (because P(k) is true).
  - Therefore, all horses are of the same color!
- What's wrong?

# More on Pigeonhole Principle

- Theorem: For any graph with more than two vertices, there exists two vertices whose degree are the same.

- How to prove?

# For connected graphs

First, suppose that $G$ is a connected finite simple graph with $n$ vertices. Then every vertex in $G$ has degree between 1 and $n-1$ (the degree of a given vertex cannot be zero since $G$ is connected, and is at most $n-1$ since $G$ is simple). Since there are $n$ vertices in $G$ with degree between 1 and $n-1$, the pigeon hole principle lets us conclude that there is some integer $k$ between 1 and $n-1$ such that two or more vertices have degree $k$.

# For arbitrary graphs

Now, suppose $G$ is an arbitrary finite simple graph (not necessarily connected). If $G$ has any connected component consisting of two or more vertices, the above argument shows that that component contains two vertices with the same degree, and therefore $G$ does as well. On the other hand, if $G$ has no connected components with more than one vertex, then every vertex in $G$ has degree zero, and so there are multiple vertices in $G$ with the same degree. $\square$

- As we go, we see various proofs.
- Proofs has to be formal.
- You can not scribble something and expect the examiner to interpret the answer !!

- As we go, w

- Proofs has

- You can not                    nd expect the
  examiner to                    !!

Your TA should not become like this !

# General Advise

- Use standard vocabulary, simple notation, and techniques described in the class.

- Most numeric questions are toy problems, whose answer can be obtained by common sense (often simple trial and error method is enough).

- You **have to** use the method(s) described in the **classwork** or in the **text books**. Otherwise you may not get marks.