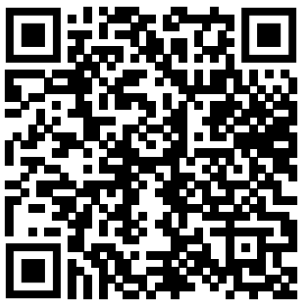


Forewords

Hi, I'm Chee Xiang, also known as Pallon. I have created this help sheet for my own study, and it is the treasure and culmination of my efforts. However, for some reason, I have decided to share this help sheet with other students, including you. One of the main reasons is that I hope it can help you in your studies. Another fun reason is to observe how my little help sheet can spread throughout our community. You can think of it as me performing a Breadth-First Search (BFS) with myself as the root node, trying to find the maximum depth.

I'm sure it will also be fun to keep a record of who is in our community. Therefore, I have created a contributor list that records those who have progressively contributed to the improvement of this help sheet (of course, it starts with only me). If you're bored or interested, you can also check their LinkedIn profiles (if they have provided them) to connect with them. You can find the contributor list here:

<https://docs.google.com/spreadsheets/d/1r2SgdThPMcMoWAEyFPwaqrq1CjQ87ZfKuwDy0lADPJM/edit#gid=0>



Feel free to click on this link to provide me with feedback on this help sheet:

<https://docs.google.com/forms/d/1taARJqNnGrxbzEunaVD6IhviVO5hTVbMv6D66nSnaJw/edit>



Lastly, please note that this help sheet is not perfect, and it could contain errors or undergo changes in versions, despite all the contributors and me doing our best to maintain its correctness. The latest version of the help sheet can be retrieved at <https://github.com/PallonCX/CS1231S-Helpsheet>. Please use it at your own risk.

Wishing you all the best in your studies!

Lecture 1: Speaking Mathematically

Important Sets:

\mathbb{N} - Natural numbers (includes 0) | \mathbb{Z} - Integers | \mathbb{Q} - Rational numbers | \mathbb{R} - Real numbers [$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$]

Superscripts (Top) & Subscripts (Bottom):

\mathbb{Z}^+ : Positive integers | \mathbb{R}^- : Negative real numbers | $\mathbb{Z}_{\geq 12}$: Integers greater than or equal to 12 (0 is neither – or +)

Terminology:

Definition:

A precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true.

Axiom / Postulate:

A statement that is assumed to be true without proof.

Theorem:

A mathematical statement that is proved using rigorous mathematical reasoning.

Lemma:

A small theorem.

Corollary:

A result that is a simple deduction from a theorem.

Conjecture:

A statement believed to be true, but for which there is no proof (yet).

Basic Properties of Integers [Lecture #1 Slides #26] $\forall x, y, z \in \mathbb{Z}$:

Closure under + and \times : $x + y \in \mathbb{Z}$ and $xy \in \mathbb{Z}$

Commutativity: $x + y = y + x$ and $xy = yx$

Associativity: $x + y + z = (x + y) + z = x + (y + z)$ and $xyz = (xy)z = x(yz)$.

Distributivity: $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.

Trichotomy: Exactly one of the following is true: $x = y$, or $x < y$, or $x > y$.

Definition: **Even and Odd integers** [Lecture #1 Slides #27]:

If n is an integer, then

n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.

n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$.

Assumption 1 [Lecture #1 Slides #27]:

Every integer is even or odd, but not both.

Definition: **Divisibility** [Lecture #1 Slides #32]:

If $n, d \in \mathbb{Z}$ and $d \neq 0$: $d \mid n \Leftrightarrow \exists k \in \mathbb{Z}$ such that $n = dk$.

Thus, “ n is a multiple of d ”, or “ d is a factor of n ”, or “ d is a divisor of n ” or “ d divides n ”.

$a \mid b$ is a statement, which is evaluated to true or false. It is not a numerical value.

Irrationality of $\sqrt{2}$ [Theorem 4.7.1 (5th: 4.8.1)]: $\sqrt{2}$ is irrational.

Definition: **Rational and irrational numbers** [Lecture #1 Slides #37]:

r is rational $\Leftrightarrow \exists a, b \in \mathbb{Z}$ s.t. $r = \frac{a}{b}$ and $b \neq 0$.

A real number that is not rational is irrational.

Definition: **Fraction in lowest term** [Lecture #1 Slides #37]:

A quotient of two integers with a nonzero denominator is also commonly known as a fraction. A fraction a/b (where $b \neq 0$) is said to be in lowest terms if the largest integer that divides both a and b is 1.

Assumption 2 [Lecture #1 Slides #37]:

Every rational can be reduced to a fraction in its lowest term.

[Proposition 4.6.4 (5th: 4.7.4)]: For all integers n , if n^2 is even then n is even.

Made by Tan Chee Xiang (Pallon)

Version 1.0

Tutorial #1 Question #10: Let n be an integer. Then n^2 is odd if and only if n is odd.

Definition: **Colorful** (Only for CS1231S) [Lecture #1 Slides #44]:

An integer n is said to be colorful if there exists some integer k such that $n = 3k$.

General pattern of proof:

Example #1: Prove that the product of two consecutive odd numbers is always odd.

Justification.
(Important!)

Some tips:

1. Write the draft proof by

(1) Start of the proof: Let

(2) End of the proof: Thus (Conclusion)

2. Continue the remaining parts with logical arguments, definitions or properties

Numbering and indentation.

1. Let a and b be the two consecutive odd numbers.
 - 1.1 Without loss of generality*, assume that $a < b$, hence $b = a + 2$.
 - 1.2 Now, $a = 2k + 1$ (by definition of odd numbers)
 - 1.3 Similarly, $b = a + 2 = 2k + 3$.
 - 1.4 Therefore, $ab = (2k + 1)(2k + 3) = (4k^2 + 6k) + (2k + 3) = 4k^2 + 8k + 3 = 2(2k^2 + 4k + 1) + 1$ (by basic algebra)
 - 1.5 Let $m = (2k^2 + 4k + 1)$ which is an integer (by closure of integers under \times and $+$).
 - 1.6 Then $ab = 2m + 1$, which is odd (by definition of odd numbers).
2. Therefore, the product of two consecutive odd numbers is always odd.

"Without loss of generality" may be abbreviated to **WLOG**. This is used before an assumption in a proof which narrows the premise to some special case, and implies that the proof for that case can be easily applied to all other cases.

28

Proofs:

Type of Proof	Pattern	Usage
Proof by construction (Direct proof)	1. Let / Consider 2. Note that (The thing let above have some property) 3. Also, (With the property, we can conclude that)	-When a specific value with some properties is required to suffice the proof -To proof existential statement (Find a specific value or give directions to find)
Disproof by counter example	1. Let 2. Therefore, (With the property of the thing let above, the statement is not true)	-To show a statement is false (Often for universal statement) -One counter-example is sufficient
Proof by exhaustion / Proof by cases / Proof by brute force	1. Let (Specific values from cases, such as 0, 1) 1.1 (Show that everything let above suffice the statement) 2. Therefore, (Conclude)	-Number of cases is finite
Proof by deduction (Direct proof)	1. Let (An abstract value, such as n, k) 1.1 (Show that the thing let above suffice the statement) 2. Therefore, (Conclude)	-Number of cases is infinite -General problem
Proof by contradiction (Indirect proof)	1. Suppose not, that is, (The negation of the statement) 1.1 (Show that we can deduce something that contradicts the assumption) 2. Therefore, the assumption that (The negation of the statement) is false. 3. Hence (The statement we want to prove)	-The statement to prove is absence of form -Direct proof is difficult
Proof by contraposition	1. Contrapositive statement: (The contraposition of statement) 2. (Prove the contrapositive statement) 3. Hence, (The original statement is true)	-Conditional statement that is hard to prove in the original direction
Proof by Mathematical Induction	1. Let $P(n) \equiv \dots$ (Set up predicate.) 2. Basis step: ... 3. Assume $P(k)$ is true for some k (Inductive Hypothesis) 4. Inductive step: (Start from $k + 1$, and use	

	inductive hypothesis to support the proof) 5. Therefore, (Conclude statement)	
--	--	--

Lecture 2: The Logic of Compound Statements (aka Propositional Logic)

Definition: **Statement** Definition 2.1.1:

A statement (or proposition) is a sentence that is true or false, but not both.

Definition: **Negation** Definition 2.1.2:

If p is a statement variable, the negation of p is “not p ” or “it is not the case that p ” and is denoted $\sim p$.

Definition: **Conjunction** Definition 2.1.3:

If p and q are statement variables, the conjunction of p and q is “ p and q ”, denoted $p \wedge q$.

Definition: **Disjunction** Definition 2.1.4:

If p and q are statement variables, the disjunction of p and q is “ p or q ”, denoted $p \vee q$.

Definition: **Statement Form / Propositional Form** Definition 2.1.5:

A statement form (or propositional form) is an expression made up of statement variables and logical connectives that becomes a statement when actual statements are substituted for the component statement variables.

Definition: **Logical Equivalence** Definition 2.1.6:

Two statement forms are called logically equivalent if, and only if, they have identical truth values for each possible substitution of statements for their statement variables. The logical equivalence of statement forms P and Q is denoted by $P \equiv Q$.

*To show logical equivalence: Show that truth table have identical truth values

*To show non-equivalence:

(1) Truth table method: Show that truth table have at least one row where truth values differ

(2) Counter-example method: Find a counter example such that one is true another is false.

Definition: **Tautology** Definition 2.1.7:

A tautology is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a tautological statement.

Definition: **Contradiction** Definition 2.1.8:

A contradiction is a statement form that is always false regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a contradiction is a contradictory statement.

Logical Equivalence Theorem 2.1.1: *Just quote the law name

Given any statement variables p , q and r , a tautology **true** and a contradiction **false**:

1	Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2	Associative laws	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$p \vee q \vee r \equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$
3	Distributive laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4	Identity laws	$p \wedge \text{true} \equiv p$	$p \vee \text{false} \equiv p$
5	Negation laws	$p \vee \sim p \equiv \text{true}$	$p \wedge \sim p \equiv \text{false}$
6	Double negative law	$\sim(\sim p) \equiv p$	
7	Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
8	Universal bound laws	$p \vee \text{true} \equiv \text{true}$	$p \wedge \text{false} \equiv \text{false}$
9	De Morgan's laws	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10	Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11	Negation of true and false	$\sim \text{true} \equiv \text{false}$	$\sim \text{false} \equiv \text{true}$

*Implication law: $p \rightarrow q \equiv \sim p \vee q$

*Variant absorption laws: $p \wedge (\sim p \vee q) \equiv p \wedge q$ or $p \vee (\sim p \wedge q) \equiv p \vee q$

Made by Tan Chee Xiang (Pallon)

Version 1.0

Definition: **Conditional** Definition 2.2.1:

If p and q are statement variables, the conditional of q by p is “if p then q ” or “ p implies q ”, denoted $p \rightarrow q$. It is false when p is true and q is false; otherwise it is true. We called p the hypothesis (or antecedent) of the conditional and q the conclusion (or consequent).

* A conditional statement that is true when its hypothesis is false is often called vacuously true or true by default.

Definition: **Contrapositive** Definition 2.2.2:

The contrapositive of $p \rightarrow q$ is $\sim q \rightarrow \sim p$.

Definition: **Converse** Definition 2.2.3:

The converse of $p \rightarrow q$ is $q \rightarrow p$.

Definition: **Inverse** Definition 2.2.4:

The inverse of $p \rightarrow q$ is $\sim p \rightarrow \sim q$.

*Note that:

(1) Conditional statement \equiv Its contrapositive | (2) Its converse \equiv its inverse | (3) Statement $\not\equiv$ Converse (Normally)

Definition: **Only if** Definition 2.2.5:

“ p only if q ” means “if not q then not p ” or “ $\sim q \rightarrow \sim p$ ”. Or, equivalently, “if p then q ” or “ $p \rightarrow q$ ”.

Definition: **Biconditional** Definition 2.2.6:

Given statement variables p and q , the biconditional of p and q is “ p if, and only if, q ” and is denoted $p \leftrightarrow q$. It is true if both p and q have the same truth values and is false if p and q have opposite truth values. The words if and only if are sometimes abbreviated iff.

* $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Definition: **Necessary and Sufficient Conditions** Definition 2.2.7:

If r and s are statements, “ r is a sufficient condition for s ” means “if r then s ” or “ $r \rightarrow s$ ”,

“ r is a necessary condition for s ” means “if not r then not s ” or “if s then r ” or “ $s \rightarrow r$ ”.

* r is a necessary and sufficient condition for s means “ r if and only if s ” or “ $r \leftrightarrow s$ ”.

Logical connectives	Not / Negation: \sim		If-then / Implies: \rightarrow			If and only if: \leftrightarrow			And: \wedge *We use “but” in English sometimes			Or: \vee			Exclusiv e-or (Special)
Truth tables	p	$\sim p$	p	q	$p \rightarrow q$	p	q	$p \leftrightarrow q$	p	q	$p \wedge q$	p	q	$p \vee q$	$(p \vee q) \wedge \sim (p \wedge q)$
	T	F	T	T	T	T	T	T	T	T	T	T	T	T	
			T	F	F	T	F	F	T	F	F	T	F	T	
	F	T	F	T	T	F	T	F	F	T	F	F	T	T	
			F	F	T	F	F	T	F	F	F	F	F	F	
Order or operation	Performed first		Coequal (Performed last)						Coequal (After negation) *Use parentheses to disambiguate						-

Definition: **Argument** Definition 2.3.1:

An argument (argument form) is a sequence of statements (statement forms). All statements in an argument (argument form), except for the final one, are called premises (or assumptions or hypothesis). The final statement (statement form) is called the conclusion. The symbol \bullet , which is read “therefore”, is normally placed just before the conclusion. To say that an argument form is valid means that no matter what particular statements are substituted for the statement variables in its premises, if the resulting premises are all true, then the conclusion is also true.

*Testing validity of argument form (Critical row method):

(1) Identify premises and conclusion

Made by Tan Chee Xiang (Pallon)

Version 1.0

(2) Construct truth table

(3) Find critical row (All premises are true), if conclusion in every critical row is true, then the argument form is valid

* **Tutorial #1 Additional Notes** Testing validity of argument form:

Given an argument:

p_1

p_2

:

p_k

$\therefore q$

where p_1, p_2, \dots, p_k are the k premises and q the conclusion, we can say that "the argument is valid if and only if $(p_1 \wedge p_2 \wedge \dots \wedge p_k) \rightarrow q$ is a tautology".

Term: **Syllogism** **Lecture #2 Slides #57**:

An argument form consisting of two premises and a conclusion.

Term: **Rule of inference** **Lecture #2 Slides #61**:

A form of argument that is valid.

*Just quote the rule name

Rule of inference		Rule of inference	
Modus Ponens	$p \rightarrow q$ p $\bullet q$	Elimination	$p \vee q$ $\sim q$ $\bullet p$
Modus Tollens	$p \rightarrow q$ $\sim q$ $\bullet \sim p$	Transitivity	$p \rightarrow q$ $q \rightarrow r$ $\bullet p \rightarrow r$
Generalization	p $\bullet p \vee q$	Proof by Division Into Cases	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\bullet r$
Specialization	$p \wedge q$ $\bullet p$	Contradiction Rule	$\sim p \rightarrow \text{false}$ $\bullet p$
Conjunction	p q $\bullet p \wedge q$		

Term: **Fallacy** **Lecture #2 Slides #69**:

An error in reasoning that results in an invalid argument.

*Three common fallacies:

(1) Using ambiguous premises (2) Circular reasoning (Assume the conclusion) (3) Jumping to a conclusion

*Example:

Converse error / Fallacy of affirming the consequence	Inverse error	Valid argument with a false premise (Logical problem in premise)
$p \rightarrow q$ q $\bullet p$	$p \rightarrow q$ $\sim p$ $\bullet \sim q$	

Definition: **Sound and Unsound Arguments** **Definition 2.3.2**:

An argument is called sound if, and only if, it is valid and all its premises are true. An argument that is not sound is called unsound.

Some common questions:

- (1) Which of the following statements is/are logically equivalent to ... ?
 - (i) Try to transform the option into the given statement
 - (ii) Substitute the statement variables with true and false
- (2) What is/are the missing premise(s) to make the following argument valid?
 - (i) Try to transform the conclusion into a form that is the conjunction of all premises

Common questions:

- (1) Simplify proposition – Change “implies” to “and” and “or”, remember to use \equiv
- (2) Mastermind –
 - (i) If 3 colour is correct, we can deduct the 4th colour is among those which's not inside.
 - (ii) If those who have the 4th colour are all in the sequence, then only one among them have correct colour
 - (iii) Once get all the correct colour, refer to sequence which have only sink without hit to know some position
 - (iv) Lastly, use the answer to check all (Optional)

Lecture 3: The Logic of Quantified Statements (aka Predicate Logic)

Definition: **Predicate** Definition 3.1.1:

A predicate is a sentence that contains a finite number of predicate variables and becomes a statement when specific values are substituted for the variables. The domain of a predicate variable is the set of all values that may be substituted in place of the variable.

*Ways to change predicate into statement:

- (1) Assign specific values to all predicate variables
- (2) Add quantifiers

Definition: **Truth set** Definition 3.1.2:

If $P(x)$ is a predicate and x has domain D , the truth set is the set of all elements of D that make $P(x)$ true when they are substituted for x . The truth set of $P(x)$ is denoted $\{x \in D \mid P(x)\}$.

* In set theory, the symbol \mid is used to mean “such that”.

* Sometimes we can narrow the domain to truth set in quantified statements.

Symbol: **Universal quantifier** / \forall denotes “for all” (or “for any”, “for every”, “for each”)

Definition: **Universal Statement** Definition 3.1.3:

Let $Q(x)$ be a predicate and D the domain of x . A universal statement is a statement of the form “ $\forall x \in D, Q(x)$ ” (May omit commas). It is defined to be true iff $Q(x)$ is true for every x in D . It is defined to be false iff $Q(x)$ is false for at least one x in D . A value for x for which $Q(x)$ is false is called a counterexample.

*To check the truth and falsity:

- (1) True: Method of exhaustion (Try every value in the domain) / Prove
- (2) False: Find a counterexample

*Vacuous truth:

In general, a statement of the form $\forall x \in D (P(x) \rightarrow Q(x))$ is called vacuously true or true by default if, and only if, $P(x)$ is false for every x in D .

As a special case, $\forall a \in X, P(a)$ is vacuously true if X is an empty set.

* Usually in the form $\forall x (P(x) \rightarrow Q(x))$, not $\forall x (P(x) \wedge Q(x))$

Symbol: **Existential quantifier** / \exists denotes “there exists”, “there is a”, “we can find a”, “there is at least one”, “for some”, and “for at least one”.

* The words “such that” or “s.t.” are inserted just before the predicate. (May omit)

* $\exists!$ is used to denote “there exists a unique” or “there is one and only one”.

Definition: **Existential Statement** Definition 3.1.4:

Let $Q(x)$ be a predicate and D the domain of x . An existential statement is a statement of the form “ $\exists x \in D$ such that $Q(x)$ ”. It is defined to be true iff $Q(x)$ is true for at least one x in D . It is defined to be false iff $Q(x)$ is false for all x in D .

*To check the truth and falsity:

- (1) True: Find an example
- (2) False: Prove

* Usually in the form $\exists x (P(x) \wedge Q(x))$, not $\exists x (P(x) \rightarrow Q(x))$

Negation of a Universal Statement Theorem 3.2.1:

$\sim(\forall x \in D, P(x)) \equiv \exists x \in D$ such that $\sim P(x)$

Negation of an Existential Statement Theorem 3.2.2:

$\sim(\exists x \in D$ such that $P(x)) \equiv \forall x \in D, \sim P(x)$

Relation among \forall, \exists, \wedge , and \vee Lecture #3 Slides #35:

$\forall x \in D, Q(x) \equiv Q(x_1) \wedge Q(x_2) \wedge \dots \wedge Q(x_n)$

$\exists x \in D, Q(x) \equiv Q(x_1) \vee Q(x_2) \vee \dots \vee Q(x_n)$

Definition: **Contrapositive, converse, inverse** Definition 3.2.1:

Consider a statement of the form: $\forall x \in D (P(x) \rightarrow Q(x))$. Its contrapositive is: $\forall x \in D (\sim Q(x) \rightarrow \sim P(x))$. Its converse is: $\forall x \in D (Q(x) \rightarrow P(x))$. Its inverse is: $\forall x \in D (\sim P(x) \rightarrow \sim Q(x))$.

*It follows that $\forall x \in D (P(x) \rightarrow Q(x)) \equiv \forall x \in D (\sim Q(x) \rightarrow \sim P(x))$ and $\forall x \in D (P(x) \rightarrow Q(x)) \not\equiv \forall x \in D (Q(x) \rightarrow P(x))$

Definition: **Necessary and Sufficient conditions, Only if** Definition 3.2.2:

" $\forall x, r(x)$ is a sufficient condition for $s(x)$ " means " $\forall x (r(x) \rightarrow s(x))$ ". "

$\forall x, r(x)$ is a necessary condition for $s(x)$ " means " $\forall x (\sim r(x) \rightarrow \sim s(x))$ " or, equivalently, " $\forall x (s(x) \rightarrow r(x))$ ".

" $\forall x, r(x)$ only if $s(x)$ " means " $\forall x (\sim s(x) \rightarrow \sim r(x))$ " or, equivalently, " $\forall x (r(x) \rightarrow s(x))$ ".

Negations of Multiply-Quantified Statements Lecture #3 Slides #57:

$\sim(\forall x \in D, \exists y \in E \text{ such that } P(x, y)) \equiv \exists x \in D \text{ such that } \forall y \in E, \sim P(x, y)$

$\sim(\exists x \in D \text{ such that } \forall y \in E, P(x, y)) \equiv \forall x \in D, \exists y \in E \text{ such that } \sim P(x, y)$

*Basically change the \forall to \exists and \exists to \forall , and negates any predicate.

Order of Quantifier Lecture #3 Slides #61:

In a statement containing both \forall and \exists , changing the order of the quantifiers usually changes the meaning of the statement. However, if one quantifier immediately follows another quantifier of the same type, then the order of the quantifiers does not affect the meaning.

Definition: **Valid Argument Form** Definition 3.4.1:

No matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true.

Universal Modus Ponens	Universal Modus Tollens	Converse Error (Quantified Form)	Inverse Error (Quantified Form)	Universal Transitivity
$\forall x (P(x) \rightarrow Q(x)).$ $P(a)$ for a particular a . • $Q(a).$	$\forall x (P(x) \rightarrow Q(x)).$ $\sim Q(a)$ for a particular a . • $\sim P(a).$	$\forall x (P(x) \rightarrow Q(x)).$ $Q(a)$ for a particular a . • $P(a).$	$\forall x (P(x) \rightarrow Q(x)).$ $\sim P(a)$ for a particular a . • $\sim Q(a).$	$\forall x (P(x) \rightarrow Q(x)).$ $\forall x (Q(x) \rightarrow R(x)).$ • $\forall x (P(x) \rightarrow R(x)).$

Rule of Inference for quantified statements	Name
$\forall x \in D P(x)$ $\therefore P(a)$ if $a \in D$	Universal instantiation
$P(a)$ for every $a \in D$ $\therefore \forall x \in D P(x)$	Universal generalization
$\exists x \in D P(x)$ $\therefore P(a)$ for some $a \in D$	Existential instantiation
$P(a)$ for some $a \in D$ $\therefore \exists x \in D P(x)$	Existential generalization

Tutorial #2 Question #3:

- (a) Integers are closed under division. (Disproved)
- (b) Rational numbers are closed under addition. (Proved by deduction)
- (c) Rational number are closed under division. (Disproved)

Tutorial #2 Question #7: $\forall x \in \mathbb{R} ((x^2 > x) \rightarrow (x < 0) \vee (x > 1))$. (Proof by deduction)

Made by Tan Chee Xiang (Pallon)

Version 1.0

Tutorial #2 Question #10: If n is a product of two positive integers a and b , then $a \leq n^{1/2}$ or $b \leq n^{1/2}$ (Proof by contraposition / contradiction)

Lecture 4: Methods of Proof

Definition: **Prime and Composite** [Lecture #4 Slides #6]:

n is prime: $(n > 1) \wedge \forall r, s \in \mathbb{Z}^+, (n = rs \rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$.

n is prime: $(n > 1) \wedge (\forall r, s \in \mathbb{Z} ((r > 1) \wedge (s > 1) \rightarrow rs \neq n))$.

n is composite: $\exists r, s \in \mathbb{Z}^+ (n = rs \wedge (1 < r < n) \wedge (1 < s < n))$.

Definition: **Prime** [Lecture #4 Slides #7]:

n is prime: $(x \neq 1) \wedge \forall y, z (x = yz \rightarrow ((y = x) \vee (z = 1)))$

Proving Existential Statement	Constructive Proof
Disproving Universal Statement	Counterexample (For conditional statement, find a value in domain for which the hypothesis is true but the conclusion is false.)
Proving Universal Statement	(Finite) Method of exhaustion (Infinite) Generalizing from the generic particular (To show that every element of a set satisfies a certain property, suppose x is a particular but arbitrarily chosen element of the set, and show that x satisfies the property.)

[Theorem 4.2.1 (5th: 4.3.1)]: Every integer is a rational number. (Constructive Proof)

[Theorem 4.2.2 (5th: 4.3.2)]: The sum of any two rational numbers is rational. (Constructive Proof)

[Corollary 4.2.3 (5th: 4.2.3)]: The double of a rational number is rational.

A Positive Divisor of a Positive Integer [Theorem 4.3.1 (5th: 4.4.1)]:

For all positive integers a and b , if $a \mid b$, then $a \leq b$. (Constructive Proof)

Divisors of 1 [Theorem 4.3.2 (5th: 4.4.2)]:

The only divisors of 1 are 1 and -1. (Proof by division into cases)

Transitivity of Divisibility [Theorem 4.3.3 (5th: 4.4.3)]:

For all integers a , b and c , if $a \mid b$ and $b \mid c$, then $a \mid c$. (Constructive Proof)

[Theorem 4.6.1 (5th: 4.7.1)]: There is no greatest integer. (Proof by contradiction)

[Proposition 4.6.4 (5th: 4.7.4)]: For all integers n , if n^2 is even then n is even. (Proof by contraposition)

Lecture 5: Set Theory

Definition: **Set** [Lecture #5 Slides #6]:

Set is a unordered collection of objects. The objects are called members or elements of the set. Order and duplicate do not matter, which means an element is only counted once regardless of the number of duplicate in the set.

Definition: **Membership of a Set (Notation: \in)** [Lecture #5 Slides #7]:

If S is a set, the notation $x \in S$ means that x is an element of S . ($x \notin S$ means x is not an element of S .)

Definition: **Cardinality of a Set (Notation: $|S|$)** [Lecture #5 Slides #7]:

The cardinality of a set S , denoted as $|S|$, is the size of the set, that is, the number of elements in S .

Term: **Set-Roster Notation** [Lecture #5 Slides #6]:

A set may be specified by writing all of its elements between braces. Examples: $\{1, 2, 3\}$, $\{1, 2, 3, \dots, 100\}$, $\{1, 2, 3, \dots\}$. (The symbol \dots is called an ellipsis and is read “and so forth”.)

Term: **Set-Builder Notation** [Lecture #5 Slides #11]:

Let U be a set and $P(x)$ be a predicate over U . Then the set of all elements $x \in U$ such that $P(x)$ is true is denoted $\{x \in U : P(x)\}$ or $\{x \in U \mid P(x)\}$ which is read as “the set of all x in U such that $P(x)$ (is true)”.

*An object z is an element of the set $S = \{x \in U : P(x)\}$ only if $z \in U$ and $P(z)$ is true.

Term: **Replacement Notation** [Lecture #5 Slides #12]:

Let A be a set and $t(x)$ be a term in a variable x . Then the set of all objects of the form $t(x)$ where x ranges over the elements of A is denoted $\{t(x) : x \in A\}$ or $\{t(x) \mid x \in A\}$ which is read as “the set of all $t(x)$ where $x \in A$ ”.

* An object z is an element of $S = \{t(x) : x \in A\}$ only if there is an $x \in A$ such that $t(x) = z$.

Definition: **Subset** [Lecture #5 Slides #13]:

$A \subseteq B$ iff $\forall x (x \in A \Rightarrow x \in B)$. “ A is a subset of B ” is same meaning as “ A is contained in B ”. We may also write $B \supseteq A$ which reads as “ B contains A ” or “ B includes A ”.

* $A \not\subseteq B \Leftrightarrow \exists x (x \in A \wedge x \notin B)$.

Definition: **Proper Subset** [Lecture #5 Slides #13]:

$A \subset B$, iff $A \subseteq B$ and $A \neq B$. In this case, we may say that the inclusion of A in B is proper or strict.

Definition: **Empty Set** [Lecture #5 Slides #14]:

A set with no element is an empty set, denoted as \emptyset or $\{\}$.

Theorem 6.2.4: An empty set is a subset of every set, i.e. $\emptyset \subseteq A$ for all sets A .

Definition: **Singleton** [Lecture #5 Slides #14]:

A set with exactly one element is called a singleton.

Definition: **Ordered Pair** [Lecture #5 Slides #16]:

An ordered pair is an expression of the form (x, y) . Two ordered pairs (a, b) and (c, d) are equal iff $a = c$ and $b = d$.

Symbolically: $(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d)$.

Definition: **Cartesian Product** [Lecture #5 Slides #17]:

Given sets A and B , the Cartesian product of A and B , denoted $A \times B$ and read “ A cross B ”, is the set of all ordered pairs (a, b) where a is in A and b is in B . Symbolically: $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.

Definition: **Set equality** [Lecture #5 Slides #19]:

Given sets A and B , A equals B , written $A = B$ iff every element of A is in B and every element of B is in A .

Symbolically: $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$ or $A = B \Leftrightarrow \forall x (x \in A \Leftrightarrow x \in B)$ [Lecture #5 Slides #21]

*To prove set equality:

[S1] Let sets X and Y be given. To prove $X = Y$: [S2] (\subseteq) Prove that $X \subseteq Y$. (Take any element of X , prove it's in Y)

[S3] (\supseteq) Prove that $Y \subseteq X$ (or $X \supseteq Y$). [S4] From (2) and (3), conclude that $X = Y$.

Term: **Universal set** [Lecture #5 Slides #24]:

In a certain situation within some context, all sets being considered as a specific sets, for example sets of real numbers, thus the sets of real numbers would be called universal set or a universe of discourse for the discussion.

Definition: **Union, intersection, difference and complement** [Lecture #5 Slides #25]:

Let A and B be subsets of a universal set U .

The union of A and B , denoted $A \cup B$, is the set of all elements that are in at least one of A or B .

$$A \cup B = \{x \in U : x \in A \vee x \in B\}$$

The intersection of A and B , denoted $A \cap B$, is the set of all elements that are common to both A and B .

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}$$

The difference of B minus A (or relative complement of A in B), denoted $B - A$, or $B \setminus A$, is the set of all elements that are in B and not A . $B \setminus A = \{x \in U : x \in B \wedge x \notin A\}$

The complement of A , denoted \bar{A} , is the set of all elements in U that are not in A . (Note: Epp uses the notation A^c .)
 $\bar{A} = \{x \in U \mid x \notin A\}$.

*Sometimes U is omitted in the definition

$$*\bar{X} = U \setminus X \text{ [Lecture #5 Slides #26]}$$

Notation: **Interval of real numbers** [Lecture #5 Slides #27]:

Given real numbers a and b with $a \leq b$:

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}, [a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}, (a, b] = \{x \in \mathbb{R} : a < x \leq b\}, [a, b) = \{x \in \mathbb{R} : a \leq x < b\}.$$

The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:

$$(a, \infty) = \{x \in \mathbb{R} : x > a\}, [a, \infty) = \{x \in \mathbb{R} : x \geq a\}, (-\infty, b) = \{x \in \mathbb{R} : x < b\}, (-\infty, b] = \{x \in \mathbb{R} : x \leq b\}.$$

Definition: **Union & Intersection for more than two sets** [Lecture #5 Slides #28]:

$$\bigcup_{i=0}^n A_i = A_0 \cup A_1 \cup \dots \cup A_n$$

$$\bigcap_{i=0}^n A_i = A_0 \cap A_1 \cap \dots \cap A_n$$

Definition: **Disjoint** [Lecture #5 Slides #29]:

Two sets are disjoint iff they have no elements in common. Symbolically: A and B are disjoint iff $A \cap B = \emptyset$.

Definition: **Mutually disjoint** [Lecture #5 Slides #29]:

Sets A_1, A_2, A_3, \dots are **mutually disjoint** (or **pairwise disjoint** or **nonoverlapping**) iff no two sets A_i and A_j with distinct subscripts have any elements in common, i.e. for all $i, j = 1, 2, 3, \dots$, $A_i \cap A_j = \emptyset$ whenever $i \neq j$.

Definition: **Partition**:

[Lecture #5 Slides #29] Division of set into nonoverlapping (or disjoint) pieces.

[Lecture #5 Slides #30] If A is called a union of mutually disjoint subsets A_1, A_2, A_3 , and A_4 , then the collection of sets $\{A_1, A_2, A_3, A_4\}$ is said to be a partition of A .

The Quotient-Remainder Theorem [Theorem 4.4.1]:

Given any integer n and positive integer d , there exist unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.

*Usage: By the quotient-remainder theorem, every integer n can be written in exactly one of the three forms: $n = 3k$, or $n = 3k + 1$, or $n = 3k + 2$ for some integer k .

Definition: **Power set** [Lecture #5 Slides #33]:

Given a set A , the power set of A , denoted $\mathcal{P}(A)$, is the set of all subsets of A .

[Theorem 6.3.1]: Suppose A is a finite set with n elements, then $\mathcal{P}(A)$ has 2^n elements. In other words, $|\mathcal{P}(A)| = 2^{|A|}$.
(Proof by mathematical induction)

• Definition

Unions and Intersections of an Indexed Collection of Sets

Given sets A_0, A_1, A_2, \dots that are subsets of a universal set U and given a nonnegative integer n ,

$$\bigcup_{i=0}^n A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \dots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one nonnegative integer } i\}$$

$$\bigcap_{i=0}^n A_i = \{x \in U \mid x \in A_i \text{ for all } i = 0, 1, 2, \dots, n\}$$

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all nonnegative integers } i\}.$$

Definition: **Ordered n -tuples** [Lecture #5 Slides #36]:

Let $n \in \mathbb{Z}^+$ and let x_1, x_2, \dots, x_n be (not necessarily distinct) elements. An **ordered n -tuple** is an expression of the form (x_1, x_2, \dots, x_n) . An **ordered pair** is an ordered 2-tuple; an **ordered triple** is an ordered 3-tuple. Equality of two ordered n -tuples: $(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n) \Leftrightarrow x_1 = y_1, x_2 = y_2, \dots, x_n = y_n$.

Definition: **Cartesian product** [Lecture #5 Slides #36]:

Given sets A_1, A_2, \dots, A_n , the **Cartesian product** of A_1, A_2, \dots, A_n , denoted $A_1 \times A_2 \times \dots \times A_n$, is the set of all ordered n -tuples (a_1, a_2, \dots, a_n) where $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$. $A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \dots \wedge a_n \in A_n\}$. If A is a set, then $A^n = A \times A \times \dots \times A$ (n many A 's).

Some Subset Relations [Theorem 6.2.1]:

Inclusion of Intersection: For all sets A and B , (a) $A \cap B \subseteq A$ (b) $A \cap B \subseteq B$

Inclusion in Union: For all sets A and B , (a) $A \subseteq A \cup B$ (b) $B \subseteq A \cup B$

Transitive Property of Subsets: For all sets A, B and C , $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$.

Procedural Versions of Set Definitions [Lecture #5 Slides #40]:

Let X and Y be subsets of a universal set U and suppose a and b are elements of U .

(1) $a \in X \cup Y \Leftrightarrow a \in X \vee a \in Y$ (2) $a \in X \cap Y \Leftrightarrow a \in X \wedge a \in Y$ (3) $a \in X - Y \Leftrightarrow a \in X \wedge a \notin Y$

(4) $a \in \bar{X} \Leftrightarrow a \notin X$ (5) $(a, b) \in X \times Y \Leftrightarrow a \in X \wedge b \in Y$

Set Identities [Theorem 6.2.2]: *Just quote law name

Let all sets referred to below be subsets of a universal set U .

1. **Commutative Laws**: For all sets A and B ,
(a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$.
2. **Associative Laws**: For all sets A, B and C ,
(a) $(A \cup B) \cup C = A \cup (B \cup C)$ and (b) $(A \cap B) \cap C = A \cap (B \cap C)$.
3. **Distributive Laws**: For all sets A, B and C ,
(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. **Identity Laws**: For all sets A ,
(a) $A \cup \emptyset = A$ and (b) $A \cap U = A$.
5. **Complement Laws**: For all sets A ,
(a) $A \cup \bar{A} = U$ and (b) $A \cap \bar{A} = \emptyset$.
6. **Double Complement Law**: For all sets A ,
 $\bar{\bar{A}} = A$.

7. **Idempotent Laws**: For all sets A ,
(a) $A \cup A = A$ and (b) $A \cap A = A$.
8. **Universal Bound Laws**: For all sets A ,
(a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$.
9. **De Morgan's Laws**: For all sets A and B ,
(a) $\overline{A \cup B} = \bar{A} \cap \bar{B}$ and (b) $\overline{A \cap B} = \bar{A} \cup \bar{B}$.
10. **Absorption Laws**: For all sets A and B ,
(a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$.
11. **Complements of U and \emptyset** :
(a) $\bar{U} = \emptyset$ and (b) $\bar{\emptyset} = U$.
12. **Set Difference Law**: For all sets A and B ,
 $A \setminus B = A \cap \bar{B}$.

Tutorial #3 Question #5: For all sets A, B, C , $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Tutorial #3 Question #6: For all sets A, B, C , $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

Tutorial #3 Question #8: Let A and B be set. $A \subseteq B$ if and only if $A \cup B = B$.

Assignment #1 Question #6:

- (a) $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$. (Proved)
- (b) $(A \cup B = A \cup C) \Rightarrow B = C$. (Disproved)
- (c) $(A \cap B = A \cap C) \Rightarrow B = C$. (Disproved)
- (d) $(A \cup B = A \cup C) \wedge (A \cap B = A \cap C) \Rightarrow B = C$. (Proved)

Assignment #2 Question #4: $A = (A \setminus B) \cup (A \cap B)$.

Common questions:

1. Find power set – Just list out, can check by number of element
2. Prove set equality – Noted does the question mention set operation (also called element method, which is the definition of sets and some propositional logic) or set identities
3. Find partition – Non-empty subsets + Mutually disjoint + Every element in exactly one of the component

Made by Tan Chee Xiang (Pallon)

Version 1.0

Lecture 6: Relations

Definition: **Relation** [Lecture #6 Slides #6]:

Let A and B be sets. A (binary) relation from A to B is a subset of $A \times B$. Given an ordered pair (x, y) in $A \times B$, x is related to y by R , or x is R -related to y , written $x R y$, iff $(x, y) \in R$.

* $x R y$ means $(x, y) \in R$, $x \not R y$ means $(x, y) \notin R$

Definition: **Domain, Co-domain, Range** [Lecture #6 Slides #9]:

Let A and B be sets and R be a relation from A to B . The domain of R , $Dom(R)$, is the set $\{a \in A : a R b \text{ for some } b \in B\}$. The co-domain of R , $coDom(R)$, is the set B . The range of R , $Range(R)$, is the set $\{b \in B : a R b \text{ for some } a \in A\}$.

Definition: **Inverse of a Relation** [Lecture #6 Slides #12]:

Let R be a relation from A to B . The **inverse relation** R^{-1} from B to A is: $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$.

* $\forall x \in A, \forall y \in B ((y, x) \in R^{-1} \Leftrightarrow (x, y) \in R)$

Definition: **Relation on a Set** [Lecture #6 Slides #12]:

A relation on a set A is a relation from A to A . In other words, a relation on a set A is a subset of $A \times A$ (A^2).

* In general, we may write A^n for $A \times \dots \times A$ (n times).

Definition: **Composition of Relations** [Lecture #6 Slides #16]:

Let A, B and C be sets. Let $R \subseteq A \times B$ be a relation. Let $S \subseteq B \times C$ be a relation. The composition of R with S , denoted $S \circ R$, is the relation from A to C such that: $\forall x \in A, \forall z \in C (x S \circ R z \Leftrightarrow (\exists y \in B (x R y \wedge y S z)))$

* There is a "path" from x to z via some intermediate element $y \in B$ in the arrow diagram.

Proposition: **Composition is Associative** [Lecture #6 Slides #18] [Tutorial #4 Question #6]:

Let A, B, C, D be sets. Let $R \subseteq A \times B$, $S \subseteq B \times C$ and $T \subseteq C \times D$ be relations. $T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$

Proposition: **Inverse of Composition** [Lecture #6 Slides #18]:

Let A, B and C be sets. Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be relations. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Definition: **n -ary Relation** [Lecture #6 Slides #19]:

Given n sets A_1, A_2, \dots, A_n , an **n -ary relation** R on $A_1 \times A_2 \times \dots \times A_n$ is a subset of $A_1 \times A_2 \times \dots \times A_n$. The special cases of 2-ary, 3-ary and 4-ary relations are called **binary**, **ternary** and **quaternary relations** respectively.

Definition: **Reflexivity, Symmetry, Transitivity** [Lecture #6 Slides #19]:

Let R be a relation on a set A .

R is **reflexive** iff $\forall x \in A (x R x)$. *Prove: Let a and prove $a R a$. *If A has n elements, R has at least n elements

R is **symmetric** iff $\forall x, y \in A (x R y \Rightarrow y R x)$. *Prove: Let $a R b$ and prove $b R a$.

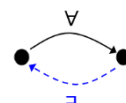
R is **transitive** iff $\forall x, y, z \in A (x R y \wedge y R z \Rightarrow x R z)$. *Prove: Let $a R b$ and $b R c$, then prove $a R c$.

*Properties of a relation, not properties of members of the set.

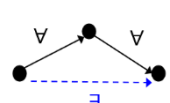
Reflexive



Symmetric



Transitive



Definition: **Transitive Closure** [Lecture #6 Slides #31]:

Let A be a set and R a relation on A . The **transitive closure** of R is the relation R^t on A that satisfies the following three properties: (1) R^t is transitive. (2) $R \subseteq R^t$. (3) If S is any other transitive relation that contains R , then $R^t \subseteq S$.

*The relation obtained by adding the least number of ordered pairs to ensure transitivity is called the transitive closure of the relation.

Definition: **Partition** [Lecture #6 Slides #35]:

C is a **partition** of a set A if the following hold:

(1) C is a set of which all elements are non-empty subsets of A , i.e., $\emptyset \neq S \subseteq A$ for all $S \in C$.

(2) Every element of A is in exactly one element of C , i.e., $\forall x \in A \exists S \in C (x \in S)$ and $\forall x \in A \exists S_1, S_2 \in C (x \in S_1 \wedge x \in S_2 \Rightarrow S_1 = S_2)$.

*Shorter definition: A partition of set A is a set C of non-empty subsets of A such that $\forall x \in A \exists ! S \in C (x \in S)$.

*[Lecture #6 Slides #34] A partition of a set A is a finite or infinite collection of nonempty, mutually disjoint subsets whose union is A .

*Elements of a partition are called **components** of the partition.

Made by Tan Chee Xiang (Pallon)

Version 1.0

Definition: **Relation Induced by a Partition** [Lecture #6 Slides #38]:

Given a partition C of a set A , the relation R induced by the partition is defined on A as follows: $\forall x, y \in A, xRy \Leftrightarrow \exists$ a component S of C s.t. $x, y \in S$.

Relation Induced by a Partition [Theorem 8.3.1]:

Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.

Definition: **Equivalence Relation (Symbol \sim)** [Lecture #6 Slides #40]:

Let A be a set and R a relation on A . R is an **equivalence relation** iff R is reflexive, symmetric and transitive.

Definition: **Equivalence Class** [Lecture #6 Slides #43]:

Suppose A is a set and \sim is an equivalence relation on A . For each $a \in A$, the **equivalence class** of a , denoted $[a]$ and called the **class of a** for short, is the set of all elements $x \in A$ s.t. a is \sim -related to x . $[a]_{\sim} = \{x \in A : a \sim x\}$

Equivalence Classes [Lemma Rel.1]:

Let \sim be an equivalence relation on a set A . The following are equivalent for all $x, y \in A$.

(i) $x \sim y$ (ii) $[x] = [y]$ (iii) $[x] \cap [y] \neq \emptyset$.

The Partition Induced by an Equivalence Relation [Theorem 8.3.4]:

If A is a set and R is an equivalence relation on A , then the distinct equivalence classes of R form a partition of A ; that is, the union of the equivalence classes is all of A , and the intersection of any two distinct classes is empty.

Definition: **Congruence** [Lecture #6 Slides #53]:

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a is congruent to b modulo n iff $a - b = nk$ for some $k \in \mathbb{Z}$. In other words, $n \mid (a - b)$. In this case, we write $a \equiv b \pmod{n}$.

Proposition: [Lecture #6 Slides #54]:

Congruence-mod n is an equivalence relation on \mathbb{Z} for every $n \in \mathbb{Z}^+$.

*It will form n distinct equivalence classes.

Definition: **Set of equivalence classes** [Lecture #6 Slides #56]:

Let A be a set and \sim be an equivalence relation on A . Denote by A/\sim the set of all equivalence classes with respect to \sim , i.e., $A/\sim = \{[x]_{\sim} : x \in A\}$. We may read A/\sim as “the quotient of A by \sim ”.

*Which is the partition induced by equivalence relation.

Equivalence classes form a partition [Theorem Rel.2]:

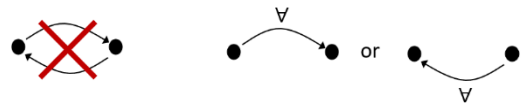
Let \sim be an equivalence relation on a set A . Then A/\sim is a partition of A .

Definition: **Antisymmetry** [Lecture #6 Slides #63]:

Let R be a relation on a set A . R is **antisymmetric** iff $\forall x, y \in A (xRy \wedge yRx \Rightarrow x = y)$.

* R is **not antisymmetric** iff $\exists x, y \in A (xRy \wedge yRx \wedge x \neq y)$.

*Different with not symmetric



Definition: **Partial Order Relation (Symbol \leq (Curly less than or equal to))** [Lecture #6 Slides #68]:

Let R be a relation on a set A . Then R is a partial order relation (or simply partial order) iff R is reflexive, antisymmetric and transitive.

*May view as a set of tasks

Definition: **Partially Ordered Set** [Lecture #6 Slides #68]:

A set A is called a partially ordered set (or poset) with respect to a partial order relation R on A , denoted by (A, R) .

Definition: **Comparability** [Lecture #6 Slides #79]:

Suppose \leq is a partial order relation on a set A . Elements a and b of A are said to be comparable iff either $a \leq b$ or $b \leq a$. Otherwise, a and b are noncomparable.

Definition: **Maximal, minimal, largest, smallest** [Lecture #6 Slides #80]:

Let a set A be partially ordered with respect to a relation \leq and $c \in A$.

(1) c is a maximal element of A iff $\forall x \in A$, either $x \leq c$, or x and c are not comparable. Alternatively, c is a maximal element of A iff $\forall x \in A (c \leq x \Rightarrow c = x)$.

(2) c is a minimal element of A iff $\forall x \in A$, either $c \leq x$, or x and c are not comparable. Alternatively, c is a minimal element of A iff $\forall x \in A (x \leq c \Rightarrow c = x)$. (Nothing is below)

(3) c is the largest element / greatest element / maximum of A iff $\forall x \in A (x \leq c)$.

(4) c is the smallest element / least element / minimum of A iff $\forall x \in A (c \leq x)$. (Everything is above)

Proposition: **A smallest element is minimal / A largest element is maximal.** [Lecture #6 Slides #83]:

Consider a partial order \leq on a set A . Any smallest element is minimal and any largest element is maximal.

Definition: **Total Order Relations** [Lecture #6 Slides #86]:

If R is a partial order relation on a set A , and for any two elements x and y in A , either $x R y$ or $y R x$, then R is a total order relation (or simply total order) on A . R is a total order iff R is a partial order and $\forall x, y \in A (x R y \vee y R x)$.

*Hasse diagram of total order is one single line (chain)

Definition: **Linearization of a partial order** [Lecture #6 Slides #87]:

Let \leq be a partial order on a set A . A **linearization** of \leq is a total order \leq^* on A such that $\forall x, y \in A (x \leq y \Rightarrow x \leq^* y)$.

*Linearization of a total order is the total order itself.

*If two elements are not comparable, their order can be interchangeable as long as does not violate the conditions.

Kahn's Algorithm (1962)

Input: A finite set A and a partial order \leq on A .

1. Set $A_0 := A$ and $i := 0$.
2. Repeat until $A_i = \emptyset$
 - 2.1. find a minimal element c_i of A_i wrt \leq
 - 2.2. set $A_{i+1} = A_i \setminus \{c_i\}$
 - 2.3. set $i := i + 1$

Output: A linearization \leq^* of \leq defined by setting, for all indices i, j ,
 $c_i \leq^* c_j \Leftrightarrow i \leq j$.

Definition: **Well-Ordered Set** [Lecture #6 Slides #91]:

Let \leq be a total order on a set A . A is **well-ordered** iff every non-empty subset of A contains a smallest element.

Symbolically, $\forall S \in \mathcal{P}(A), S \neq \emptyset \Rightarrow (\exists x \in S \forall y \in S (x \leq y))$

[Tutorial #4 Question #2]: The following are logically equivalent:

(1) R is symmetric, i.e. $\forall x, y \in A (x R y \Rightarrow y R x)$. (2) $\forall x, y \in A (x R y \Leftrightarrow y R x)$ (3) $R = R^{-1}$

[Tutorial #4 Question #9]:

(a) if $x \in S \in \mathcal{C}$, then $[x] = S$. (b) $A / \sim = \mathcal{C}$.

Definition: **Reflexive closure** [Tutorial #5 Question #5]:

Let A be a set and R a relation on A . It is the smallest relation on A that is reflexive and contains R as a subset.

Definition: **Asymmetry** [Tutorial #5 Question #6]:

$\forall x, y \in A (x R y \Rightarrow y \not R x)$.

[Tutorial #5 Question #6]: Every asymmetric relation is antisymmetric. (asymmetry property forces the antisymmetry property to be vacuously true.)

[Tutorial #5 Question #7]: Consider a set A and a total order \leq on A . Show that all minimal elements are smallest.

Definition: **Comparable, compatible** [Tutorial #5 Question #8]:

We say a, b are comparable iff $a \leq b$ or $b \leq a$. We say a, b are compatible iff there exists $c \in A$ such that $a \leq c$ and $b \leq c$.

[Tutorial #5 Question #10]: In all partially ordered sets, any two comparable elements are compatible.

Common questions:

1. Find relation – Use definition of relation, definition of inverse relation, definition of composition of relations
2. Find equivalence class – Use definition of equivalence class, definition of \sim
3. Proof equivalence – Proof Reflexivity, Symmetry, Transitivity

Made by Tan Chee Xiang (Pallon)

Version 1.0

Type of relation	Type	Irreflexive	Reflexive	Symmetric	Antisymmetric	Asymmetric	Transitive	Antitransitive
Equal Relation on \mathbb{Q}	Equivalence	No	Yes	Yes	Yes	No	Yes	No
Congruence-mod n	Equivalence	No	Yes	Yes	No	No	Yes	No
Relation Induced by a Partition	Equivalence	No	Yes	Yes	No	No	Yes	No
Cardinality	Equivalence	No	Yes	Yes	No	No	Yes	No
Divisibility (For all positive integers)	Partial order (Not total order)	No	Yes	No	Yes	No	Yes	No
Divisibility (For all integers)		No	Yes	No	No	No	Yes	No
Less than or equal to (For natural numbers or any lower bounded set)	Partial order (Total order) (Well-ordered)	No	Yes	No	Yes	No	Yes	No
Less than or equal to (For any non-lower bounded set)	Partial order (Total order) (Not well-ordered)	No	Yes	No	Yes	No	Yes	No
Less than (Rational numbers)		Yes	No	No	Yes	Yes	Yes	No
Subset	Partial order (Not total order)	No	Yes	No	Yes	No	Yes	No
Proper Subset		Yes	No	No	Yes	Yes	Yes	No
Empty relation (on empty set)	Equivalence & partial order (Total order) (Well-ordered)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Empty relation (on non-empty set)		Yes	No	Yes	Yes	Yes	Yes	Yes

Arrow diagram	Directed graph	Hasse Diagrams
Represent the elements of A as points in one region and the elements of B as points in another region. For each	Instead of representing A as two separate sets of points, represent A	For all <u>distinct</u> $x, y, m \in A$: If $x \preccurlyeq y$ and no $m \in A$ is such that $x \preccurlyeq m \preccurlyeq y$, then x is placed below y

Made by Tan Chee Xiang (Pallon)

Version 1.0

$x \in A$ and $y \in B$, draw an arrow from x to y iff xRy .	<u>only once</u> , and draw an arrow from each point of A to its related point. If a point is related to itself, a loop is drawn that extends out from the point and goes back to it.	with a line joining them, else no line joins x and y .
For relation on two different sets	For relation on a set	For relation on a set (Partial order)

Lecture 7: Functions

Definition: **Function** [Lecture #7 Slides #7]:

A function f from a set X to a set Y , denoted $f: X \rightarrow Y$, is a relation satisfying the following properties:

(1) $\forall x \in X \exists y \in Y (x, y) \in f$.

(2) $\forall x \in X \forall y_1, y_2 \in Y ((x, y_1) \in f \wedge (x, y_2) \in f) \rightarrow y_1 = y_2$. (That is, the y in (1) is unique.)

*Alternatively: $\forall x \in X \exists! y \in Y (x, y) \in f$.

*Informally: A function from X to Y is an assignment to each element of X exactly one element of Y . Every element in X relates to exactly one element in Y .

*Arrow diagram for finite sets function:

(1) Every element of X has an arrow coming out of it.

(2) No element of X has two arrows coming out of it that point to two different elements of Y .

Definition: **Argument, image, preimage, input, output** [Lecture #7 Slides #11]:

Let $f: X \rightarrow Y$ be a function. We write $f(x) = y$ iff $(x, y) \in f$. We say that “ f sends/maps x to y ” and we may also write $x \xrightarrow{f} y$ or $f: x \mapsto y$. Also, x is called the **argument** of f . $f(x)$ is read “ f of x ”, or “the **output** of f for the **input** x ”, or “the value of f at x ”, or “the **image** of x under f ”. If $f(x) = y$, then x is a **preimage** of y .

*To summarise: x is argument or input (of f) and preimage (of y). $f(x)$ is the output (of f for x) and image (of x under f)

Definition: **Setwise image and preimage** [Lecture #7 Slides #12]:

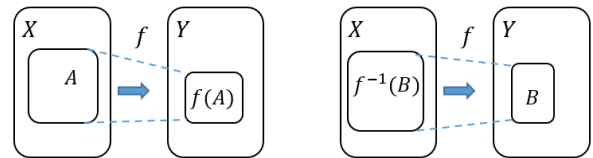
Let $f: X \rightarrow Y$ be a function from set X to set Y .

If $A \subseteq X$, then let $f(A) = \{f(x) : x \in A\}$.

If $B \subseteq Y$, then let $f^{-1}(B) = \{x \in X : f(x) \in B\}$

We call $f(A)$ the **(setwise) image** of A , and $f^{-1}(B)$ the **(setwise) preimage** of B under f .

*Setwise preimage needs not be a function



Definition: **Domain, co-domain, range** [Lecture #7 Slides #16]:

Let $f: X \rightarrow Y$ be a function. X is the domain of f and Y the co-domain of f . The range of f is the (setwise) image of X under f : $\{y \in Y : y = f(x) \text{ for some } x \in X\}$.

* $\text{Range} \subseteq \text{Co-domain}$

Definition: **Sequence** [Lecture #7 Slides #18]:

A **sequence** a_0, a_1, a_2, \dots can be represented by a function a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geq 0}$. *In this sense, any function whose domain is $\mathbb{Z}_{\geq m}$ for some $m \in \mathbb{Z}$ represents a sequence.

Definition: **Fibonacci Sequence** [Lecture #7 Slides #19]:

The **Fibonacci sequence** F_0, F_1, F_2, \dots is defined by setting, for each $n \in \mathbb{Z}_{\geq 0}$, $F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$. *Fibonacci sequence: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

Definition: **String** [Lecture #7 Slides #20]:

Let A be a finite set with at least one element. A **string** or a word over A is an expression of the form $a_0 a_1 a_2 \dots a_{l-1}$ (finite sequence) where $l \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, a_2, \dots, a_{l-1} \in A$. The elements of A are called **characters** of the string.

Here l is called the **length** of the string. The **empty string / null string** ε is the string of length 0. Let A^* denote the set of all strings over A .

Equality of Sequences [Lecture #7 Slides #21]:

Given two sequences a_0, a_1, a_2, \dots and b_0, b_1, b_2, \dots defined by the functions $a(n) = a_n$ and $b(n) = b_n$ respectively for every $n \in \mathbb{Z}_{\geq 0}$, we say that the two sequences are equal if and only if $a(n) = b(n)$ for every $n \in \mathbb{Z}_{\geq 0}$.

Equality of Strings [Lecture #7 Slides #21]:

Given two strings $s_1 = a_0 a_1 a_2 \dots a_{l-1}$ and $s_2 = b_0 b_1 b_2 \dots b_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$, we say that $s_1 = s_2$ if and only if $a_i = b_i$ for all $i \in \{0, 1, 2, \dots, l-1\}$.

Function Equality [Theorem 7.1.1]:

Two functions $f: A \rightarrow B$ and $g: C \rightarrow D$ are equal, i.e. $f = g$, iff (i) $A = C$ and $B = D$, and (ii) $f(x) = g(x) \forall x \in A$.

Definition: Injection (one-to-one function) [Lecture #7 Slides #25]:

A function $f: X \rightarrow Y$ is **injective** (or **one-to-one**) iff $\forall x_1, x_2 \in X (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$. or, equivalently (contrapositive), $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. An injective function is called an **injection**.

*Informally: Every element of X has a unique image in Y such that no other element of X has the same image.

*Every element of Y has at most one preimage.

*A function $f: X \rightarrow Y$ is **not injective** iff $\exists x_1, x_2 \in X (f(x_1) = f(x_2) \wedge x_1 \neq x_2)$.

*To prove:

(1) Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. (2) Show $x_1 = x_2$.

Definition: Surjection (onto function) [Lecture #7 Slides #27]:

A function $f: X \rightarrow Y$ is **surjective** (or **onto**) iff $\forall y \in Y \exists x \in X (y = f(x))$. Every element in the co-domain has a preimage. So, range = co-domain. A surjective function is called a **surjection**.

*Every element of Y has at least one preimage.

*A function $f: X \rightarrow Y$ is **not surjective** iff $\exists y \in Y \forall x \in X (y \neq f(x))$.

*To prove:

(1) Let $y \in Y$. (2) Show $y = f(x)$.

Definition: Bijection (one-to-one correspondence) [Lecture #7 Slides #27]:

A function $f: X \rightarrow Y$ is **bijective** iff f is injective and surjective, i.e. $\forall y \in Y \exists! x \in X (y = f(x))$. A bijective function is called a **bijection** or **one-to-one correspondence**.

*Every element of Y has exactly one preimage.

Definition: Inverse function [Lecture #7 Slides #31]:

Let $f: X \rightarrow Y$. Then $g: Y \rightarrow X$ is an **inverse** of f iff $\forall x \in X \forall y \in Y (y = f(x) \Leftrightarrow x = g(y))$. We denote the inverse of f as f^{-1} .

Proposition: Uniqueness of inverses [Lecture #7 Slides #34]:

If g_1 and g_2 are inverses of $f: X \rightarrow Y$, then $g_1 = g_2$.

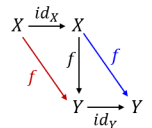
[Theorem 7.2.3]: If $f: X \rightarrow Y$ is a bijection, then $f^{-1}: Y \rightarrow X$ is also a bijection. In other words, $f: X \rightarrow Y$ is bijective iff f has an inverse.

Definition: Composition of Functions [Lecture #7 Slides #39]:

Let $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ be functions. Define a new function $g \circ f: X \rightarrow Z$ as follows: $(g \circ f)(x) = g(f(x)) \forall x \in X$. where $g \circ f$ is read “ g circle f ” and $g(f(x))$ is read “ g of f of x ”. The function $g \circ f$ is called the **composition** of f and g .

Definition: Identity function [Lecture #7 Slides #41]:

The identity function on a set X , id_X , is the function from X to X defined by $id_X(x) = x$ for all $x \in X$.



Composition with an Identity Function [Theorem 7.3.1]: Let $f: X \rightarrow Y$. $f \circ id_X = f$ and $id_Y \circ f = f$.

Composition of a Function with Its Inverse [Theorem 7.3.2]: Let $f: X \rightarrow Y$. $f^{-1} \circ f = id_X$ and $f \circ f^{-1} = id_Y$.

Theorem: Associativity of Function Composition [Lecture #7 Slides #47]:

Let $f: A \rightarrow B$, $g: B \rightarrow C$ and $h: C \rightarrow D$. Then $(h \circ g) \circ f = h \circ (g \circ f)$. Function composition is associative.

*Because a function is a relation.

***Noncommutativity of Function Composition** [Lecture #7 Slides #48]: $(g \circ f)(x) \neq (f \circ g)(x)$

Composition of Injections [Theorem 7.3.3]: If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both injective, then $g \circ f$ is injective.

Composition of Surjections [Theorem 7.3.4]: If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both surjective, then $g \circ f$ is surjective.

Notation: Lecture #7 Slides #54:

The quotient \mathbb{Z}/\sim_n where \sim_n is the congruence-mod- n relation on \mathbb{Z} , is denoted \mathbb{Z}_n .

Definition: **Addition and Multiplication on \mathbb{Z}_n** Lecture #7 Slides #56:

Define addition $+$ and multiplication \cdot on \mathbb{Z}_n as follows: whenever $[x], [y] \in \mathbb{Z}_n$, $[x] + [y] = [x + y]$ and $[x] \cdot [y] = [x \cdot y]$

Proposition: **Addition on \mathbb{Z}_n is well defined** Lecture #7 Slides #57:

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$, $[x_1] = [x_2]$ and $[y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2]$.

*To prove addition well defined:

- (1) Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
- (2) Then $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$ by the definition of congruence. (Or other setting)
- (3) ...
- (4) So $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$. (Or other setting)
- (5) Therefore, $[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$.

Proposition: **Multiplication on \mathbb{Z}_n is well defined** Lecture #7 Slides #58:

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$, $[x_1] = [x_2]$ and $[y_1] = [y_2] \Rightarrow [x_1] \cdot [y_1] = [x_2] \cdot [y_2]$.

*To prove addition well defined:

- (1) Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
- (2) Then $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$ by the definition of congruence. (Or other setting)
- (3) ...
- (4) So $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{n}$. (Or other setting)
- (5) Therefore, $[x_1] \cdot [y_1] = [x_1 \cdot y_1] = [x_2 \cdot y_2] = [x_2] \cdot [y_2]$

Tutorial #6 Question #6: Let $f: B \rightarrow C$. If function g with domain C such that $g \circ f$ is injective, f is injective.

Tutorial #6 Question #7: Let $f: B \rightarrow C$. If function e with codomain B such that $f \circ e$ is surjective, f is surjective.

Tutorial #6 Question #9: Let $f: A \rightarrow B$ be a function. Let $X \subseteq A$ and $Y \subseteq B$. $X \subseteq f^{-1}(f(X))$. $f(f^{-1}(Y)) \subseteq Y$.

Function (Generally, may have specific case)	Injective	Surjective	Bijjective
Linear function (On unbounded domain and codomain)	Yes	Yes	Yes
Quadratic function (On unbounded domain and codomain)	No	No	No

Common question:

1. Determine whether a relation is a function: Proof by the two condition of function or disproof by counterexample
2. Determine whether a function is bijection: Proof injective and surjective or Theorem 7.2.3: If $f: X \rightarrow Y$ is a bijection, then $f^{-1}: Y \rightarrow X$ is also a bijection. In other words, $f: X \rightarrow Y$ is bijective iff f has an inverse.
3. Len(): Careful that the argument is element or set
4. Determine whether a function has inverse: Theorem 7.2.3: If $f: X \rightarrow Y$ is a bijection, then $f^{-1}: Y \rightarrow X$ is also a bijection. In other words, $f: X \rightarrow Y$ is bijective iff f has an inverse.
5. Determine well-defined: Proof $[x_1] * [y_1] = [x_2] * [y_2]$ by Lemma Rel.1.

Lecture 8: Mathematical Induction

Definition: **Sequence and Terms** [Lecture #8 Slides #5]:

A **sequence** is an ordered set with members called **terms**. Usually, the terms are numbers. A sequence may have infinite terms.

*General form: $a_m, a_{m+1}, a_{m+2}, \dots, a_n$ where $m \leq n$. The k in a_k is called a **subscript** or **index**.

*Infinite sequence: $a_m, a_{m+1}, a_{m+2}, \dots$

*An explicit formula for a sequence is a rule that shows how the values of a_k depend on k .

Definition: **Summation** [Lecture #8 Slides #7]:

If m and n are integers, $m \leq n$, the symbol $\sum_{k=m}^n a_k$ is the **sum** of all the terms $a_m, a_{m+1}, a_{m+2}, \dots, a_n$. We say that $a_m + a_{m+1} + a_{m+2} + \dots + a_n$ is the **expanded form** of the sum, and we write $\sum_{k=m}^n a_k = a_m + a_{m+1} + a_{m+2} + \dots + a_n$. We call k the **index** of the summation, m the **lower limit** of the summation and n the **upper limit** of the summation.

*Summation can be expressed using recursive definition. If m is any integer, then $\sum_{k=m}^m a_k = a_m$ and

$\sum_{k=m}^n a_k = \left(\sum_{k=m}^{n-1} a_k\right) + a_n$ for all integers $n > m$.

*An empty sum (eg: $\sum_{k=m}^n a_k$ where $m > n$) is equal to the additive identity 0.

*Some sums can be transformed into telescoping sums, which then can be rewritten as a simple expression.

*The index is dummy variable.

Definition: **Product** [Lecture #8 Slides #11]:

If m and n are integers, $m \leq n$, the symbol $\prod_{k=m}^n a_k$ is the **product** of all the terms $a_m, a_{m+1}, a_{m+2}, \dots, a_n$. We write $\prod_{k=m}^n a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \dots \cdot a_n$.

*Recursive definition for the product notation: If m is any integer, then $\prod_{k=m}^m a_k = a_m$ and $\prod_{k=m}^n a_k = \left(\prod_{k=m}^{n-1} a_k\right) \cdot a_n$ for all integers $n > m$.

*An empty product (eg: $\prod_{k=m}^n a_k$ where $m > n$) is equal to the multiplicative identity 1.

Properties of Summations and Products [Theorem 5.1.1]:

If $a_m, a_{m+1}, a_{m+2}, \dots$ and $b_m, b_{m+1}, b_{m+2}, \dots$ are sequences of real numbers and c is any real number, then the following equations hold for any integer $n \geq m$:

(1) $\sum_{k=m}^n a_k + \sum_{k=m}^n b_k = \sum_{k=m}^n (a_k + b_k)$ (Proof by mathematical induction)

(2) $c \cdot \sum_{k=m}^n a_k = \sum_{k=m}^n c \cdot a_k$ (generalized distributive law)

(3) $\left(\prod_{k=m}^n a_k\right) \cdot \left(\prod_{k=m}^n b_k\right) = \prod_{k=m}^n (a_k \cdot b_k)$

Definition: **Arithmetic Sequence** [Lecture #8 Slides #18]:

A sequence a_0, a_1, a_2, \dots is called an **arithmetic sequence** (or **arithmetic progression**) iff there is a constant d such that $a_k = a_{k-1} + d$ for all integers $k \geq 1$. It follows that, $a_n = a_0 + dn$ for all integers $n \geq 0$.

* d is the common difference, a_0 the initial value.

*Summing an arithmetic sequence of n terms: $\sum_{k=0}^{n-1} a_k = \frac{n}{2}(2a_0 + (n-1)d)$

Definition: **Geometric Sequence** [Lecture #8 Slides #19]:

A sequence a_0, a_1, a_2, \dots is called a **geometric sequence** (or **geometric progression**) iff there is a constant r such that $a_k = ra_{k-1}$ for all integers $k \geq 1$. It follows that, $a_n = a_0 r^n$ for all integers $n \geq 0$.

* r is the common ratio, a_0 the initial value.

*Summing a geometric sequence of n terms ($r \neq 1$), $\sum_{k=0}^{n-1} a_k = a_0 \left(\frac{1-r^n}{1-r}\right)$

Squares	1, 4, 9, 16, 25, 36, 49, ...
Triangle numbers	1, 3, 6, 10, 15, 21, 28, ...
Fibonacci numbers:	1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...
Lazy Caterer's Sequence:	1, 2, 4, 7, 11, 16, ...

Definition: **Principle of Mathematical Induction (PMI)** [Lecture #8 Slides #24]:

Let $P(n)$ be a property that is defined for integers n , and let a be a fixed integer. Suppose the following 2 statements

Made by Tan Chee Xiang (Pallon)

Version 1.0

are true: (1) $P(a)$ is true. (2) For all integers $k \geq a$, if $P(k)$ is true then $P(k + 1)$ is true. Then the statement “for all integers $n \geq a$, $P(n)$ ” is true.

Weak (regular) induction (or 1PI)	(1) $P(a)$ holds (2) For every $k \geq a$, $P(k) \Rightarrow P(k + 1)$
Strong induction (or 2PI)	(1) $P(a)$ holds (2) For every $k \geq a$, $(P(a) \wedge P(a + 1) \wedge \dots \wedge P(k)) \Rightarrow P(k + 1)$
Strong induction (or 2PI) (variation – other variations possible)	(1) $P(a), P(a + 1), \dots, P(b)$ hold (2) For every $k \geq a$, $P(k) \Rightarrow P(k + b - a + 1)$

Sum of the First n Integers [Theorem 5.2.2 (5th: 5.2.1)]:

For all integers $n \geq 1$, $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$ (Proof by mathematical induction)

Sum of Geometric Sequence [Theorem 5.2.3 (5th: 5.2.2)]:

For any real number $r \neq 1$, and any integers $n \geq 0$, $\sum_{i=0}^n r^i = \frac{r^{n+1}-1}{r-1}$ (Proof by mathematical induction)

Definition: Closed Form [Lecture #8 Slides #27]:

If a sum with a variable number of terms is shown to be equal to a formula that does not contain either an ellipsis (...) or a summation symbol (Σ), we say that it is written in **closed form**.

Proposition 5.3.1 (5th: 5.3.2) [Lecture #8 Slides #29]:

For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3. (Proof by mathematical induction)

Proposition 5.3.2 (5th: 5.3.3) [Lecture #8 Slides #30]:

For all integers $n \geq 3$, $2n + 1 < 2^n$ (Proof by mathematical induction)

Term: Well-Ordering Principle for the Integers [Lecture #8 Slides #43]:

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element. (Proof by contradiction & MI)

Definition: Recurrence relation [Lecture #8 Slides #48]:

A **recurrence relation** for a sequence a_0, a_1, a_2, \dots is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \dots, a_{k-i}$, where i is an integer with $k - i \geq 0$. If i is a fixed integer, the **initial conditions** for such a recurrent relation specify the values of $a_0, a_1, a_2, \dots, a_{i-1}$. If i depends on k , the initial conditions specify the values of $a_0, a_1, a_2, \dots, a_m$, where m is an integer with $m \geq 0$.

*Initial condition + Recurrence relation = Recursive definition

Term: Recursive definition of a set S [Lecture #8 Slides #58]:

(Base clause) Specify that certain elements, called founders, are in S : if c is a founder, then $c \in S$.

(Recursion clause) Specify certain functions, called constructors, under which the set S is closed: if f is a constructor and $x \in S$, then $f(x) \in S$.

(Minimality clause) Membership for S can always be demonstrated by (infinitely many) successive applications of the clauses above.

Term: Structural induction over S [Lecture #8 Slides #58]:

To prove that $\forall x \in S P(x)$ is true, where each $P(x)$ is a proposition, it suffices to:

(Basis step) Show that $P(c)$ is true for every founder c ; and

(Induction step) Show that $\forall x \in S (P(x) \Rightarrow P(f(x)))$ is true for every constructor f .

In words, if all the founders satisfy a property P , and P is preserved by all constructors, then all elements of S satisfy P .

Common questions:

1. Prove closed form

2. Prove inequality: In inductive step will get $\geq = \geq$

Made by Tan Chee Xiang (Pallon)

Version 1.0

3. Proof about set: In inductive step try to take out one element and proof by divided into case
4. Proof divisibility: In inductive step, use the formula in inductive hypothesis
5. Proof something like $\forall n \in \mathbb{Z}_{\geq 8} \exists x, y \in \mathbb{N} (n = 3x + 5y)$. Use 1PI or 2PI
6. Proof fibonacci: If the question didn't specify induction, can don't use
7. Structural induction and recursive definition: To proof element exists, use base clause and recursion clause; To disproof element exist, use structural induction to find a property that the element doesn't fulfil or use recursion clause.

Lecture 9: Cardinality

Definition: **Pigeonhole Principle** [Lecture #9 Slides #6]:

Let A and B be finite sets. If there is an injection $f: A \rightarrow B$, then $|A| \leq |B|$. Contrapositive: Let $m, n \in \mathbb{Z}^+$ with $m > n$. If m pigeons are put into n pigeonholes, then there must be (at least) one pigeonhole with (at least) two pigeons.

Definition: **Dual Pigeonhole Principle** [Lecture #9 Slides #6]:

Let A and B be finite sets. If there is a surjection $f: A \rightarrow B$, then $|A| \geq |B|$. Contrapositive: Let $m, n \in \mathbb{Z}^+$ with $m < n$. If m pigeons are put into n pigeonholes, then there must be (at least) one pigeonhole with no pigeons.

Definition: **Finite set and Infinite set** [Lecture #9 Slides #9]:

Let $\mathbb{Z}_n = \{1, 2, 3, \dots, n\}$, the set of positive integers from 1 to n . A set S is said to be **finite** iff S is empty, or there exists a bijection from S to \mathbb{Z}_n for some $n \in \mathbb{Z}^+$. A set S is said to be **infinite** if it is not finite.

*We say that two finite sets whose elements can be paired by a bijection have the *same size*.

Definition: **Cardinality** [Lecture #9 Slides #10]:

The **cardinality** of a finite set S , denoted $|S|$, is (1) 0 if $S = \emptyset$, or (2) n if $f: S \rightarrow \mathbb{Z}_n$ is a bijection.

Theorem: **Equality of Cardinality of Finite Sets** [Lecture #9 Slides #10]:

Let A and B be any finite sets. $|A| = |B|$ iff there is a bijection $f: A \rightarrow B$.

Definition: **Same Cardinality (Cantor)** [Lecture #9 Slides #12]:

Given any two sets A and B . A is said to have the **same cardinality** as B , written as $|A| = |B|$, iff there is a bijection $f: A \rightarrow B$.

Theorem: **Properties of Cardinality** [Lecture #9 Slides #13]:

The cardinality relation is an equivalence relation. For all sets A, B and C :

Reflexive: $|A| = |A|$. **Symmetric:** $|A| = |B| \rightarrow |B| = |A|$. **Transitive:** $(|A| = |B|) \wedge (|B| = |C|) \rightarrow |A| = |C|$.

Definition: **Infinite Set** [Lecture #9 Slides #18] [Tutorial #8 Question #7]:

A set A is infinite iff there exists a set B such that $(B \subseteq A) \wedge (B \neq A) \wedge (|B| = |A|)$.

Definition: **Cardinal numbers** [Lecture #9 Slides #22]:

Define $\aleph_0 = |\mathbb{Z}^+|$. (Some author use \mathbb{N} instead of \mathbb{Z}^+ .) \aleph is pronounced "aleph", the first letter of the Hebrew alphabet. This is the first cardinal number.

Definition: **Countably infinite** [Lecture #9 Slides #22]:

A set S is said to be **countably infinite** (or, S has the cardinality of natural numbers) iff $|S| = \aleph_0$.

Definition: **Countable set and Uncountable set** [Lecture #9 Slides #22]:

A set is said to be **countable** iff it is finite or countably infinite. A set is said to be **uncountable** if it is not countable.

[Lecture #9 Slides #29] Theorem: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable.

Theorem: **Cartesian Product** [Lecture #9 Slides #30]:

If sets A and B are both countably infinite, then so is $A \times B$. (Proof by diagonal counting method)

Corollary: **General Cartesian Product** [Lecture #9 Slides #30]:

Given $n \geq 2$ countably infinite sets A_1, A_2, \dots, A_n , the Cartesian product $A_1 \times A_2 \times \dots \times A_n$ is also countably infinite. (Proof by mathematical induction)

Made by Tan Chee Xiang (Pallon)

Version 1.0

Theorem: **Unions** [Lecture #9 Slides #30]:

The union of countably many countable sets is countable. That is, if A_1, A_2, \dots are all countable sets, then so is $\bigcup_{i=1}^{\infty} A_i$. (Proof by diagonal counting method)

Proposition 9.1 [Lecture #9 Slides #32]:

An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \dots \in B$ in which every element of B appears exactly once.

Lemma 9.2: **Countability via Sequence** [Lecture #9 Slides #33]:

An infinite set B is countable if and only if there is a sequence b_0, b_1, b_2, \dots in which every element of B appears.

Theorem 7.4.2 (Cantor): The set of real numbers between 0 and 1, $(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$ is uncountable. (Proof by Cantor's diagonalization process / Cantor's Diagonalization Argument & Proof by contradiction)

1. Suppose $(0,1)$ is countable.
2. Since it is not finite, it is countably infinite.
3. We list the elements x_i of $(0,1)$ in a sequence as follows:

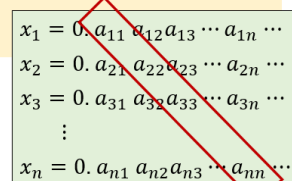
$$\begin{aligned} x_1 &= 0. a_{11} a_{12} a_{13} \dots a_{1n} \dots \\ x_2 &= 0. a_{21} a_{22} a_{23} \dots a_{2n} \dots \\ x_3 &= 0. a_{31} a_{32} a_{33} \dots a_{3n} \dots \\ &\vdots \\ x_n &= 0. a_{n1} a_{n2} a_{n3} \dots a_{nn} \dots \\ &\vdots \end{aligned}$$

where each $a_{ij} \in \{0,1,\dots,9\}$ is a digit.*

4. Now, construct a number $d = 0. d_1 d_2 d_3 \dots d_n \dots$ s.t.

$$d_n = \begin{cases} 1, & \text{if } a_{nn} \neq 1; \\ 2, & \text{if } a_{nn} = 1. \end{cases}$$

5. Note that $\forall n \in \mathbb{Z}^+, d_n \neq a_{nn}$. Thus, $d \neq x_n, \forall n \in \mathbb{Z}^+$.
6. But clearly, $d \in (0,1)$, hence a contradiction. Therefore $(0,1)$ is uncountable.



$$\begin{aligned} x_1 &= 0. a_{11} a_{12} a_{13} \dots a_{1n} \dots \\ x_2 &= 0. a_{21} a_{22} a_{23} \dots a_{2n} \dots \\ x_3 &= 0. a_{31} a_{32} a_{33} \dots a_{3n} \dots \\ &\vdots \\ x_n &= 0. a_{n1} a_{n2} a_{n3} \dots a_{nn} \dots \end{aligned}$$

Theorem 7.4.3: Any subset of any countable set is countable.

Corollary 7.4.4 (Contrapositive of Theorem 7.4.3): Any set with an uncountable subset is uncountable.

Proposition 9.3 [Lecture #9 Slides #43]: Every infinite set has a countably infinite subset.

Lemma 9.4: **Union of Countably Infinite Sets**. [Lecture #9 Slides #44]:

Let A and B be countably infinite sets. Then $A \cup B$ is countable.

Tutorial #8 Question #2: B be a countably infinite set and C a finite set. $B \cup C$ is countable.

Tutorial #8 Question #3: Suppose A_1, A_2, \dots are finite sets. Then $\bigcup_{i=1}^n A_i$ is finite for any $n \geq 2$.

Tutorial #8 Question #4: Suppose A_1, A_2, A_3, \dots are countable sets. $\bigcup_{i=1}^n A_i$ is countable for any $n \in \mathbb{Z}^+$.

Tutorial #8 Question #5: $\bigcup_{i \in \mathbb{Z}^+} A_i$ is countable.

Tutorial #8 Question #7: A set B is infinite if and only if there is $A \subsetneq B$ such that $|A| = |B|$.

Tutorial #8 Question #8: \mathbb{C} (the set of complex numbers) is uncountable.

Tutorial #8 Question #9: If A be a countably infinite set, $\mathcal{P}(A)$ is uncountable.

Assignment #2 Question #4:

(a) A and B are sets. If A is countably infinite and B is finite, then $A \setminus B$ is countably infinite.

(b) Suppose A, B and C are sets such that $A \subseteq B \subseteq C$. If A and C are countably infinite, then B is countably infinite too.

Set	Finite (Countable)	Countably infinite (Countable, infinite)	Uncountable (Infinite)
\mathbb{Z}		Yes (Proof: start in the middle and work outward)	
\mathbb{Q}^+		Yes	

$\mathbb{Z}^+ \times \mathbb{Z}^+$		Yes, $f(x, y) = \frac{(x+y-2)(x+y-1)}{2} + x$ (Diagonal counting method)	
\mathbb{R}, \mathbb{C}			Yes

Important notes for proving question in cardinality:

1. Pigeonhole Principle and Dual Pigeonhole Principle.
2. To show that a set S is finite, show $S \rightarrow \mathbb{Z}_n$ is a bijection.
3. If a set is certainly not finite (like \mathbb{Z}), if it's countable, it has to be countably infinite. (by definition of countable set)
4. To show that a set S is countably infinite, find a bijection from \mathbb{Z}^+ to \mathbb{Z} . (Start in the middle and work outward; Diagonal counting method)
5. Theorem: **Cartesian Product** [Lecture #9 Slides #30](#): If sets A and B are both countably infinite, then so is $A \times B$.
6. Corollary: **General Cartesian Product** [Lecture #9 Slides #30](#):
Given $n \geq 2$ countably infinite sets A_1, A_2, \dots, A_n , the Cartesian product $A_1 \times A_2 \times \dots \times A_n$ is also countably infinite.
7. Theorem: **Unions** [Lecture #9 Slides #30](#): The union of countably many countable sets, $\bigcup_{i=1}^{\infty} A_i$ is countable.
8. Lemma 9.2: **Countability via Sequence** [Lecture #9 Slides #33](#):
An infinite set B is countable if and only if there is a sequence b_0, b_1, b_2, \dots in which every element of B appears.
9. To show that a set S is uncountable, prove by contradiction that there *is no possibility of a bijection from that set to* \mathbb{Z}^+ . (Cantor's Diagonalization Argument)
10. [Theorem 7.4.3](#): Any subset of any countable set is countable.
11. If B be any subset of A , if A is finite then B must be finite. [Lecture #9 Slides #40](#)
- OR [Assignment #2 Question #4](#): Any subset of a finite set is finite.
12. [Corollary 7.4.4 \(Contrapositive of Theorem 7.4.3\)](#): Any set with an uncountable subset is uncountable.
13. Proposition 9.3 [Lecture #9 Slides #43](#): Every infinite set has a countably infinite subset.
14. Lemma 9.4: **Union of Countably Infinite Sets**. [Lecture #9 Slides #44](#):
Let A and B be countably infinite sets. Then $A \cup B$ is countable.

Lecture 10: Counting and Probability I

Definition: **Sample space & Event** [Lecture #10 Slides #8]:

A **sample space** is the set of all possible outcomes of a random process or experiment. An **event** is a subset of a sample space.

*A process is **random** means that when it takes place, one outcome from sample set is sure to occur, but it is impossible to predict with certainty which outcome that will be.

Notation: [Lecture #10 Slides #9]:

For a finite set A , $|A|$ denotes the number of elements in A .

Equally Likely Probability Formula [Lecture #10 Slides #9]:

If S is a finite sample space in which all outcomes are equally likely and E is an event in S , then the **probability** of E , denoted $P(E)$, is $P(E) = \text{The number of outcomes in } E / \text{The total number of outcomes in } S = |E| / |S|$

The Number of Elements in a List [Theorem 9.1.1]:

If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

The Multiplication / Product Rule [Theorem 9.2.1]:

If an operation consists of k steps and the first step can be performed in n_1 ways, the second step can be performed in n_2 ways (regardless of how the first step was performed), ... the k^{th} step can be performed in n_k ways (regardless of how the preceding steps were performed), Then the entire operation can be performed in $n_1 \times n_2 \times n_3 \times \dots \times n_k$ ways.

[Theorem 5.2.4]: Suppose A is a finite set. Then $|\mathcal{P}(A)| = 2^{|A|}$.

Principle of Sum (or the Addition Principle) [Lecture #10 Slides #31]:

If we have m ways of doing something and n ways of doing another thing and we cannot do both at the same time, then there are $m+n$ ways to choose one of these actions.

Permutations [Theorem 9.2.2]:

A **permutation** of a set of objects is an ordering of the objects in a row. The number of permutations of a set with n ($n \geq 1$) elements is $n!$. (Proved by multiplication rule)

* $0!$ is defined to be 1.

Definition: **r -permutation** [Lecture #10 Slides #36]:

An **r -permutation** of a set of n elements is an ordered selection of r elements taken from the set. The number of r -permutations of a set of n elements is denoted $P(n, r)$.

r -permutations from a set of n elements [Theorem 9.2.3]:

If n and r are integers and $1 \leq r \leq n$, then the number of r -permutations of a set of n elements is given by the formula $P(n, r) = n(n-1)(n-2) \dots (n-r+1)$ or $P(n, r) = n! / (n-r)!$

The Addition/Sum Rule [Theorem 9.3.1]:

Suppose a finite set A equals the union of k distinct mutually disjoint subsets A_1, A_2, \dots, A_k . Then $|A| = |A_1| + |A_2| + \dots + |A_k|$.

The Difference Rule [Theorem 9.3.2]:

If A is a finite set and $B \subseteq A$, then $|A \setminus B| = |A| - |B|$.

Formula for the Probability of the Complement of an Event [Lecture #10 Slides #48]:

If S is a finite sample space and A is an event in S , then $P(\bar{A}) = 1 - P(A)$

The Inclusion/Exclusion Rule for 2 or 3 Sets [Theorem 9.3.3]:

If A, B , and C are any finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$ and $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Definition: **Pigeonhole Principle (PHP)** [Lecture #10 Slides #55]:

A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain.

Definition: **Generalized Pigeonhole Principle** [Lecture #10 Slides #62]:

For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k , if $k < n/m$, then there is some $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of X .

Definition: **Generalized Pigeonhole Principle (Contrapositive Form)** [Lecture #10 Slides #65]:

For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k , if for each $y \in Y$, $f^{-1}(\{y\})$ has at most k elements, then X has at most km elements; in other words, $n \leq km$.

[Tutorial #9 Question #6]: In general, the number of circular permutations of n objects is $(n-1)!$

Common question:

1. Possibilities for tournament play - Possibility tree
2. No. of Personal Identification Numbers (PINs) / Pick card - Multiplication rule (& addition rule or difference rule sometimes)
3. No. of subset - Multiplication rule
4. No. of ways to choose people - Multiplication rule or Possibility tree
5. Permutations of the letters in a word - Permutation
6. Counting elements of a general union - Inclusion / Exclusion rule
7. Birthday problem / Last initial problem – PHP
8. Decimal expansions of fraction (*the decimal expansion of any rational number either terminates or repeats.*) – PHP
9. Student computer problem – PHP (Contrapositive)
10. Circular table problem – (S1) Put the first type of element in to permutation (S2) The space between the elements are allowed to choose and permutation *Treat empty chair as a person

Lecture 11: Counting and Probability 2

Definition: ***r*-combination** [Lecture #11 Slides #4]:

Let n and r be non-negative integers with $r \leq n$. An ***r*-combination** of a set of n elements is a subset of r of the n elements. $\binom{n}{r}$, read “ n choose r ”, denotes the number of subsets of size r (r -combinations) that can be chosen from a set of n elements.

Formula for $\binom{n}{r}$ [Theorem 9.5.1]:

The number of subsets of size r (or r -combinations) that can be chosen from a set of n elements, $\binom{n}{r}$, is given by the formula $\binom{n}{r} = \frac{P(n, r)}{r!}$ or, equivalently, $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ where n and r are non-negative integers with $r \leq n$.

Permutations with Sets of Indistinguishable Objects [Theorem 9.5.2]:

Suppose a collection consists of n objects of which n_1 are of type 1 and are indistinguishable from each other, n_2 are of type 2 and are indistinguishable from each other ... n_k are of type k and are indistinguishable from each other and suppose that $n_1 + n_2 + \dots + n_k = n$. Then the number of distinguishable permutations of the n objects is

$$\binom{n}{n_1} \binom{n-n_1}{n_2} \binom{n-n_1-n_2}{n_3} \dots \binom{n-n_1-n_2-\dots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!n_3!\dots n_k!}$$

Definition: **Multiset / *r*-Combinations with Repetition Allowed** [Lecture #11 Slides #18]:

An ***r*-combination with repetition allowed**, or **multiset of size r** , chosen from a set X of n elements is an unordered selection of elements taken from X with repetition allowed. If $X = \{x_1, x_2, \dots, x_n\}$, we write an r -combination with repetition allowed as $[x_{i_1}, x_{i_2}, \dots, x_{i_r}]$ where each x_{i_j} is in X and some of the x_{i_j} may equal each other.

Number of *r*-combinations with Repetition Allowed [Theorem 9.6.1]:

The number of r -combination with repetition allowed (multisets of size r) that can be selected from a set of n elements is: $\binom{r+n-1}{r}$ This equals the number of ways r objects can be selected from n categories of objects with repetitions allowed.

Pascal's Formula [Theorem 9.7.1]:

Let n and r be positive integers, $r \leq n$. Then $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

*Proof by (1) Algebraic proof (Using **Formula for $\binom{n}{r}$** [Theorem 9.5.1]) (2) Combinatorial proof (Consider the case of presence and absence of an element in the set)

Term: **Combinatorial Proof** [Lecture #11 Slides #27]:

A combinatorial proof (or combinatorial argument) uses counting as the basis of the proof. It includes these types of proof:

- Bijective proof. We have seen how to prove that two sets X and Y have the same cardinality by deriving a bijective function that maps each element in X to each element in Y .
- Proof by double counting. Counting the number of elements in two different ways to obtain the different expressions in the identity.

[Lecture #11 Slides #29]: $\binom{n}{r} = \binom{n}{n-r}$

[Lecture #11 Slides #31]: $k\binom{n}{k} = n\binom{n-1}{k-1}$

Number of elements in a Power Set [Theorem 6.3.1]:

If a set X has n ($n \geq 0$) elements, then $\mathcal{P}(X)$ has 2^n elements.

[Lecture #11 Slides #32]: $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = 2^n$

Made by Tan Chee Xiang (Pallon)

Version 1.0

Binomial Theorem [Theorem 9.7.2]:

Given any real numbers a and b and any non-negative integer n , $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k = a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a^1 b^{n-1} + b^n$

*In algebra a sum of two terms, such as $a + b$, is called binomial.

* $\binom{n}{r}$ is called binomial coefficient

Probability Axioms [Lecture #11 Slides #39]:

Let S be a sample space. A probability function P from the set of all events in S to the set of real numbers satisfies the following axioms: For all events A and B in S ,

(1) $0 \leq P(A) \leq 1$ (2) $P(\emptyset) = 0$ and $P(S) = 1$ (3) If A and B are disjoint events ($A \cap B = \emptyset$), then $P(A \cup B) = P(A) + P(B)$

Probability of a General Union of Two Events [Lecture #11 Slides #41]:

If A and B are any events in a sample space S , then $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Definition: Expected Value [Lecture #11 Slides #43]:

Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, a_3, \dots, a_n$ which occur with probabilities $p_1, p_2, p_3, \dots, p_n$ respectively. The **expected value** of the process is $\sum_{k=1}^n a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \dots + a_n p_n$

*It is an average value, not an actual value

Linearity of Expectation [Lecture #11 Slides #41]:

The expected value of the sum of random variables is equal to the sum of their individual expected values, regardless of whether they are independent. For random variables X_1, X_2, \dots, X_n and constants c_1, c_2, \dots, c_n , $E[\sum_{i=1}^n c_i \cdot X_i] = \sum_{i=1}^n (c_i \cdot E[X_i])$

Definition: Conditional Probability [Formula 9.9.1] [Lecture #11 Slides #53]:

Let A and B be events in a sample space S . If $P(A) \neq 0$, then the **conditional probability of B given A** , denoted $P(B|A)$, is $P(B|A) = \frac{P(A \cap B)}{P(A)}$.

[Formula 9.9.2] [Lecture #11 Slides #53]: $P(A \cap B) = P(B|A) \cdot P(A)$

[Formula 9.9.3] [Lecture #11 Slides #53]: $P(A) = \frac{P(A \cap B)}{P(B|A)}$

Bayes' Theorem [Theorem 9.9.1]:

Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, B_3, \dots, B_n$. Suppose A is an event in S , and suppose A and all the B_i have non-zero probabilities. If k is an integer with $1 \leq k \leq n$, then

$$P(B_k|A) = \frac{P(A|B_k) \cdot P(B_k)}{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + \dots + P(A|B_n) \cdot P(B_n)}$$

Definition: Independent Events [Lecture #11 Slides #73]:

If A and B are events in a sample space S , then A and B are **independent**, if and only if, $P(A \cap B) = P(A) \cdot P(B)$.

Definition: Pairwise Independent and Mutually Independent [Lecture #11 Slides #79]:

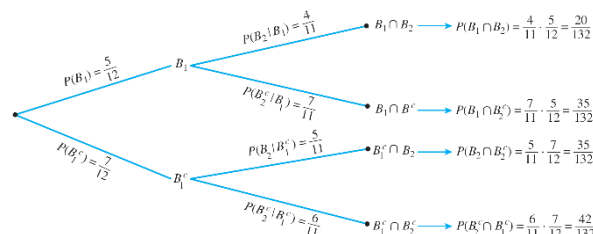
Let A, B and C be events in a sample space S . A, B and C are **pairwise independent**, if and only if, they satisfy conditions 1 – 3 below. They are **mutually independent** if, and only if, they satisfy all four conditions below.

(1) $P(A \cap B) = P(A) \cdot P(B)$ (2) $P(A \cap C) = P(A) \cdot P(C)$ (3) $P(B \cap C) = P(B) \cdot P(C)$ (4) $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

Definition: Mutually Independent [Lecture #11 Slides #80]:

Events A_1, A_2, \dots, A_n in a sample space S are **mutually independent** if, and only if, the probability of the intersection of any subset of the events is the product of the probabilities of the events in the subset. $P(A_1 \cap A_2 \cap \dots \cap A_n) = P(A_1) \cdot P(A_2) \cdot \dots \cdot P(A_n)$

*Probabilities of the form $\binom{n}{k} p^{n-k} (1-p)^k$, where $0 \leq p \leq 1$, are called **binomial probabilities**.



Common question:

1. Teams with members of two types - r-combination (sometimes with addition rule and difference rule)
2. Number of solutions for linear equation – r-combination with repetition allowed (make sure each variable is non-negative integer)
3. Expected value of dice – Normal fair dice is 3.5 (sometimes with linearity of expectation)
4. False positive – A patient **does not** have the disease, the test indicates that the patient **has** the disease.
False negative - A patient **does** have the disease, the test indicates that the patient **does not** have it.
5. Gender of children – Conditional Probability
6. Balls in urn / Disease test – Bayes' Theorem
7. Coin toss – Independent Events
8. Grid walk – Find the no. horizontal step and no. vertical step, then use **Permutations with Sets of Indistinguishable Objects** Theorem 9.5.2

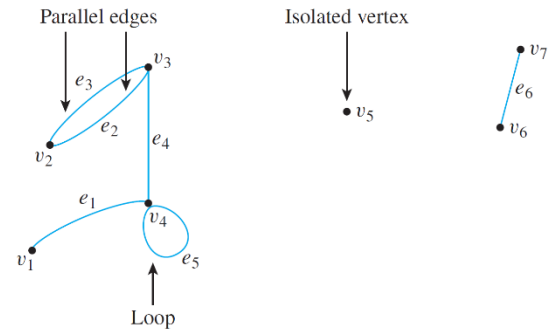
	Order Matters	Order Does Not Matter
Repetition Is Allowed	n^k	$\binom{k+n-1}{k}$
Repetition Is Not Allowed	$P(n, k)$	$\binom{n}{k}$

Lecture 12: Graphs

Definition: **Undirected Graph** [Lecture #12 Slides #7]:

An undirected **graph** G denoted by $G = (V, E)$ consists of 2 finite sets: a nonempty set V of **vertices** and a set E of **edges**, where each (undirected) edge is associated with a set consisting of either one or two vertices called its **endpoints**. An edge is said to **connect** its endpoints; two vertices that are connected by an edge are called **adjacent vertices**; and a vertex that is an endpoint of a loop is said to be **adjacent to itself**. An edge is said to be **incident on** each of its endpoints, and two edges incident on the same endpoint are called **adjacent edges**. We write $e = \{v, w\}$ for an undirected edge e incident on vertices v and w .

*If v and w are a same vertex, we write it as $\{v, v\}$



Definition: **Directed Graph** [Lecture #12 Slides #8]:

A **directed graph**, or **digraph**, G , consists of 2 finite sets: a nonempty set V of **vertices** and a set E of **directed edges**, where each (directed) edge is associated with an ordered pair of vertices called its **endpoints**. We write $e = (v, w)$ for a directed edge e from vertex v to vertex w .

Conjecture: **Four-Colour Conjecture** [Lecture #12 Slides #11]:

Four colours are sufficient to colour any map in a plane, such that regions that share a common boundary do not share the same colour.

Term: **Vertex Colouring** [Lecture #12 Slides #13]:

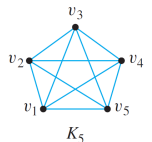
A **vertex colouring** of a graph is an assignment of colours to vertices so that no two adjacent vertices have the same colour.

Definition: **Simple Graph** [Lecture #12 Slides #19]:

A **simple graph** is an undirected graph that does not have any loops or parallel edges. (That is, there is at most one edge between each pair of distinct vertices.)

Definition: **Complete Graph** [Lecture #12 Slides #20]:

A **complete graph** on n vertices, $n > 0$, denoted K_n , is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.



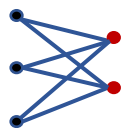
Definition: **Bipartite Graph** [Lecture #12 Slides #21]:

A **bipartite graph** (or bigraph) is a simple graph whose vertices can be divided into two disjoint sets U and V such that every edge connects a vertex in U to one in V .



Definition: **Complete Bipartite Graph** [Lecture #12 Slides #21]:

A **complete bipartite graph** is a bipartite graph on two disjoint sets U and V such that every vertex in U connects to every vertex in V . If $|U| = m$ and $|V| = n$, the complete bipartite graph is denoted as $K_{m,n}$.

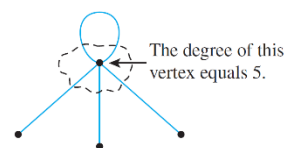


Definition: **Subgraph of a Graph** [Lecture #12 Slides #22]:

A graph H is said to be a **subgraph** of graph G if and only if every vertex in H is also a vertex in G , every edge in H is also an edge in G , and every edge in H has the same endpoints as it has in G .

Definition: **Degree of a Vertex and Total Degree of an Undirected Graph** [Lecture #12 Slides #23]:

Let G be a undirected graph and v a vertex of G . The **degree** of v , denoted $\deg(v)$, equals the number of edges that are incident on v , with an edge that is a loop counted twice. The **total degree of G** is the sum of the degrees of all the vertices of G .



The Handshake Theorem [Theorem 10.1.1]:

If G is any graph, then the sum of the degrees of all the vertices of G equals twice the number of edges of G .

Specifically, if the vertices of G are v_1, v_2, \dots, v_n , where $n \geq 0$, then, The total degree of $G = \deg(v_1) + \deg(v_2) + \dots + \deg(v_n) = 2 \times (\text{the number of edges of } G)$.

Corollary 10.1.2: The total degree of a graph is even.

Proposition 10.1.3: In any graph there are an even number of vertices of odd degree.

Definition: Indegree and outdegree of a Vertex of a Directed Graph [Lecture #12 Slides #26]:

Let $G=(V,E)$ be a directed graph and v a vertex of G . The **indegree** of v , denoted $\deg^-(v)$, is the number of directed edges that end at v . The **outdegree** of v , denoted $\deg^+(v)$, is the number of directed edges that originate from v . Note that $\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|$.

Definition: Walk, trail, path [Lecture #12 Slides #32]:

Let G be a graph, and let v and w be vertices of G . A **walk from v to w** is a finite alternating sequence of adjacent vertices and edges of G . Thus a walk has the form $v_0 e_1 v_1 e_2 \dots v_{n-1} e_n v_n$, where the v 's represent vertices, the e 's represent edges, $v_0=v$, $v_n=w$, and for all $i \in \{1, 2, \dots, n\}$, v_{i-1} and v_i are the endpoints of e_i . The number of edges, n , is the **length** of the walk. The **trivial walk** from v to v consists of the single vertex v . A **trail from v to w** is a walk from v to w that does not contain a repeated edge. A **path from v to w** is a trail that does not contain a repeated vertex.

Definition: Closed walk, circuit, cyclic [Lecture #12 Slides #33]:

A **closed walk** is a walk that starts and ends at the same vertex. A **circuit** (or **cycle**) is a closed walk of length at least 3 that does not contain a repeated edge. A **simple circuit** (or **simple cycle**) is a circuit that does not have any other repeated vertex except the first and last. An undirected graph is **cyclic** if it contains a loop or a cycle; otherwise, it is **acyclic**.

*A path is not a closed walk (It has no repeated vertex)

Definition: Connectedness [Lecture #12 Slides #35]:

Two vertices v and w of a graph $G=(V,E)$ are **connected** if and only if there is a walk from v to w . **The graph G is connected** if and only if given *any* two vertices v and w in G , there is a walk from v to w . Symbolically, G is connected iff \forall vertices $v, w \in V, \exists$ a walk from v to w .

Lemma 10.2.1: Let G be a graph. (1) If G is connected, then any two distinct vertices of G can be connected by a path. (2) If vertices v and w are part of a circuit in G and one edge is removed from the circuit, then there still exists a trail from v to w in G . (3) If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G .

Definition: Connected Component [Lecture #12 Slides #38]:

A graph H is a **connected component** of a graph G if and only if

(1) The graph H is a subgraph of G ; (2) The graph H is connected; and (3) No connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H .

Definition: Euler Circuit [Lecture #12 Slides #41]:

Let G be a graph. An **Euler circuit** for G is a circuit that contains every vertex and traverses every edge of G exactly once.

Definition: Eulerian Graph [Lecture #12 Slides #41]:

An **Eulerian graph** is a graph that contains an Euler circuit.

Theorem 10.2.2: If a graph has an Euler circuit, then every vertex of the graph has positive even degree.

Contrapositive Version of Theorem 10.2.2: If some vertex of a graph has odd degree, then the graph does not have an Euler circuit.

Theorem 10.2.3: If a graph G is connected and the degree of every vertex of G is a positive even integer, then G has an Euler circuit.

Theorem 10.2.4: A graph G has an Euler circuit if and only if G is connected and every vertex of G has positive even degree.

Definition: **Euler Trail** [Lecture #12 Slides #43]:

Let G be a graph, and let v and w be two distinct vertices of G . An **Euler trail/path from v to w** is a sequence of adjacent edges and vertices that starts at v , ends at w , passes through every vertex of G at least once, and traverses every edge of G exactly once.

*[Lecture #12 Slides #45] Adding an edge between the two vertices with odd degree will give us an Euler circuit.

Corollary 10.2.5: Let G be a graph, and let v and w be two distinct vertices of G . There is an Euler trail from v to w if and only if G is connected, v and w have odd degree, and all other vertices of G have positive even degree.

Definition: **Hamiltonian Circuit** [Lecture #12 Slides #49]:

Given a graph G , a **Hamiltonian circuit** for G is a simple circuit that includes every vertex of G . (That is, every vertex appears exactly once, except for the first and the last, which are the same.)

*Note that although an Euler circuit for a graph G must include every vertex of G , it may visit some vertices more than once and hence may not be a Hamiltonian circuit.

*On the other hand, a Hamiltonian circuit for G does not need to include all the edges of G and hence may not be an Euler circuit.

Definition: **Hamiltonian Graph** [Lecture #12 Slides #49]:

A **Hamiltonian graph** (also called **Hamilton graph**) is a graph that contains a Hamiltonian circuit.

Proposition 10.2.6: If a graph G has a Hamiltonian circuit, then G has a subgraph H with the following properties:

(1) H contains every vertex of G . (2) H is connected. (3) H has the same number of edges as vertices. (4) Every vertex of H has degree 2.

Definition: **Matrix** [Lecture #12 Slides #58]:

An $m \times n$ (read “ m by n ”) **matrix** A over a set S is a rectangular array of elements of S arranged into m rows and n columns. We write $A = (a_{ij})$.

[Lecture #12 Slides #59]: If A and B are matrices, then $A = B$ if, and only if, A and B have the same size and the corresponding entries of A and B are all equal; that is, $a_{ij} = b_{ij}$ for all $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n$.

[Lecture #12 Slides #59]: A matrix for which the numbers of rows and columns are equal is called a square matrix.

[Lecture #12 Slides #59]: If A is a square matrix of size $n \times n$, then the main diagonal of A consists of all the entries $a_{11}, a_{22}, \dots, a_{nn}$.

Definition: **Symmetric Matrix** [Lecture #12 Slides #62]:

An $n \times n$ square matrix $A = (a_{ij})$ is called **symmetric** if, and only if, $a_{ij} = a_{ji}$ for all $i, j = 1, 2, \dots, n$.

Definition: **Identity Matrix** [Lecture #12 Slides #69]:

For each positive integer n , the $n \times n$ **identity matrix**, denoted $I_n = (\delta_{ij})$ or just I (if the size of the matrix is obvious from context), is the $n \times n$ matrix in which all the entries in the main diagonal are 1's and all other entries are 0's. In other words,

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \quad \text{for all } i, j = 1, 2, \dots, n.$$

Definition: **Adjacency Matrix of a Directed Graph** [Lecture #12 Slides #61]:

Let G be a directed graph with ordered vertices v_1, v_2, \dots, v_n . The **adjacency matrix of G** is the $n \times n$ matrix $A = (a_{ij})$ over the set of non-negative integers such that a_{ij} = the number of arrows from v_i to v_j for all $i, j = 1, 2, \dots, n$.

Definition: **Adjacency Matrix of an Undirected Graph** [Lecture #12 Slides #62]:

Let G be an undirected graph with ordered vertices v_1, v_2, \dots, v_n . The **adjacency matrix of G** is the $n \times n$ matrix $A = (a_{ij})$ over the set of non-negative integers such that a_{ij} = the number of edges connecting v_i and v_j for all $i, j = 1, 2, \dots, n$.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{bmatrix}$$

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1i} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2i} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ii} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{ni} & \dots & a_{nn} \end{bmatrix}$$

2, ..., n.

*The matrix is symmetric.

Definition: **Scalar Product** [Lecture #12 Slides #63]:

Suppose that all entries in matrices **A** and **B** are real numbers. If the number of elements, n , in the i th row of **A** equals the number of elements in the j th column of **B**, then the **scalar product** or **dot product** of the i th row of **A** and the j th column of **B** is the real number obtained as follows:

$$\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{bmatrix} \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Definition: **Matrix Multiplication** [Lecture #12 Slides #64]:

Let **A** = (a_{ij}) be an $m \times k$ matrix and **B** = (b_{ij}) an $k \times n$ matrix with real entries. The (matrix) product of **A** times **B**, denoted **AB**, is that matrix (c_{ij})

defined as follows: where $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} = \sum_{r=1}^k a_{ir}b_{rj}$ for all $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n$.

*[Lecture #12 Slides #67]: Matrix multiplication is not commutative but associative.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{i1} & c_{i2} & \cdots & c_{ij} & \cdots & c_{in} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mn} \end{bmatrix}$$

Definition: **n^{th} Power of a Matrix** [Lecture #12 Slides #70]:

For any $n \times n$ matrix **A**, the **powers of A** are defined as follows:

$\mathbf{A}^0 = \mathbf{I}$ where **I** is the $n \times n$ identity matrix; $\mathbf{A}^n = \mathbf{A} \mathbf{A}^{n-1}$ for all integers $n \geq 1$

[Theorem 10.3.2]: If G is a graph with vertices v_1, v_2, \dots, v_m and **A** is the adjacency matrix of G , then for each positive integer n and for all integers $i, j = 1, 2, \dots, m$, the ij -th entry of \mathbf{A}^n = the number of walks of length n from v_i to v_j .

Definition: **Isomorphic Graph** [Lecture #12 Slides #79]:

Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs. **G is isomorphic to G'**, denoted $G \cong G'$, if and only if there exist bijections $g: V_G \rightarrow V_{G'}$ and $h: E_G \rightarrow E_{G'}$ that preserve the edge-endpoint functions of G and G' in the sense that for all $v \in V_G$ and $e \in E_G$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$.

*Alternative definition: Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs. **G is isomorphic to G'** if and only if there exists a permutation $\pi: V_G \rightarrow V_{G'}$ such that $\{u, v\} \in E_G \Leftrightarrow \{\pi(u), \pi(v)\} \in E_{G'}$.

Graph Isomorphism is an Equivalence Relation [Theorem 10.4.1]:

Let S be a set of graphs and let \cong be the relation of graph isomorphism on S . Then \cong is an equivalence relation on S .

Definition: **Planar Graph** [Lecture #12 Slides #82]:

A **planar graph** is a graph that can be drawn on a (two-dimensional) plane without edges crossing.

[Kuratowski's Theorem]: A finite graph is planar if and only if it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$.

[Euler's Formula]: For a connected planar simple graph $G = (V, E)$ with $e = |E|$ and $v = |V|$, if we let f be the number of faces or regions, then $f = e - v + 2$

Definition: **Complement of graph** [Tutorial #10 Question #10]:

If G is a simple graph, the **complement** of G , denoted \bar{G} , is obtained as follows: the vertex set of \bar{G} is identical to the vertex set of G . However, two distinct vertices v and w of \bar{G} are connected by an edge if and only if v and w are not connected by an edge in G .

Definition: **Irreflexive** [Tutorial #10 Question #11]:

$\forall a \in A, (a \not R a)$.

Definition: **Anti-symmetry** [Tutorial #10 Question #11]:

$\forall x, y (x \neq y) \Rightarrow ((x, y) \in R) \Rightarrow ((y, x) \notin R)$.

Definition: **Strict partial order** [Tutorial #10 Question #11]:

A relation is a **strict partial order** if and only if it is irreflexive, antisymmetric and transitive.

Definition: **Chain** [Tutorial #10 Question #11]:

Let $<$ be a strict partial order on a set A . A subset C of A is called a **chain** if and only if each pair of *distinct* elements in C is comparable, that is, $\forall a, b \in C (a \neq b) \Rightarrow (a < b \vee b < a)$.

Definition: **Maximal Chain** [Tutorial #10 Question #11]:

A **maximal chain** is a chain M such that $t \notin M \Rightarrow M \cup \{t\}$ is not a chain.

Common question:

1. Wedding Planner / Class Schedule / Radio Station / Traffic Signal – Vertex Colouring
2. Travelling Salesman Problem – Use Hamiltonian Circuit (Find all and compute total distance)
3. Proof about complement of graph: (Use graph to assist if have time) (S1) Assume a simple graph with n vertices (S2) Consider K_n

Lecture 13: Trees

Definition: **Tree** [Lecture #13 Slides #4]:

(The graph is assumed to be undirected here.) A **graph** is said to be **circuit-free** if and only if it has no circuits. A graph is called a **tree** if and only if it is circuit-free and connected. A **trivial tree** is a graph that consists of a single vertex. A graph is called a **forest** if and only if it is circuit-free and not connected.

[Lemma 10.5.1]: Any non-trivial tree has at least one vertex of degree 1. (Proof: Pick a vertex of tree and choose the adjacent vertex without repetition until there's no adjacent vertex. The algorithm must eventually terminate because the set of vertices of the tree T is finite and T is circuit-free.)

Definition: **Terminal vertex (leaf) and internal vertex** [Lecture #13 Slides #9]:

Let T be a tree. If T has only one or two vertices, then each is called a **terminal vertex** (or **leaf**). If T has at least three vertices, then a vertex of degree 1 in T is called a **terminal vertex** (or **leaf**), and a vertex of degree greater than 1 in T is called an **internal vertex**.

[Theorem 10.5.2]: Any tree with n vertices ($n > 0$) has $n - 1$ edges. (Proof by Mathematical Induction: In the inductive step, find a vertex with degree 1 and exclude it from the graph to use the inductive hypothesis)

[Lecture #13 Slides #12]: A non-trivial tree has at least 2 vertices of degree 1. (Prove with [Theorem 10.5.2] and **The Handshake Theorem** by contradiction)

[Lemma 10.5.3]: If G is any connected graph, C is any circuit in G , and one of the edges of C is removed from G , then the graph that remains is still connected. (Same as [Lemma 10.2.1(3)])

[Theorem 10.5.4]: If G is a connected graph with n vertices and $n - 1$ edges, then G is a tree. (Proof: Since G is connected, prove by contradiction that G is circuit-free: Use [Lemma 10.5.3] to remove edges in circuit until the subgraph is circuit-free, then by [Theorem 10.5.2] it has $n - 1$ edges)

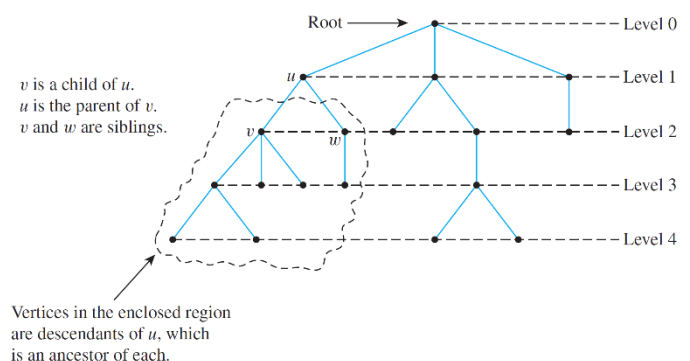
Definition: **Rooted Tree, Level, Height** [Lecture #13 Slides #19]:

A **rooted tree** is a tree in which there is one vertex that is distinguished from the others and is called the **root**. The **level** of a vertex is the number of edges along the unique path between it and the root. The **height** of a rooted tree is the maximum level of any vertex of the tree.

Definition: **Child, Parent, Sibling, Ancestor, Descendant**

[Lecture #13 Slides #19]:

Given the root or any internal vertex v of a rooted tree, the **children** of v are all those vertices that are adjacent to v and are one level farther away from the root than v . If w is a child of v , then v is called the **parent** of w , and two distinct vertices that are both children of the same parent are called **siblings**. Given two distinct vertices v and w , if v lies on the unique path between w and the root, then v is an **ancestor** of w , and w is a **descendant** of v .



Definition: **Binary Tree, Full Binary Tree** [Lecture #13 Slides #22]:

A **binary tree** is a rooted tree in which every parent has at most two children. Each child is designated either a **left child** or a **right child** (but not both), and every parent has at most one left child and one right child. A **full binary tree** is a binary tree in which each parent has exactly two children.

Definition: **Left Subtree, Right Subtree** [Lecture #13 Slides #22]:

Given any parent v in a binary tree T , if v has a left child, then the **left subtree** of v is the binary tree whose root is the left child of v , whose vertices consist of the left child of v and all its descendants, and whose edges consist of all those edges of T that connect the vertices of the left subtree. The **right subtree** of v is defined analogously.

Full Binary Tree Theorem [Theorem 10.6.1]:

If T is a full binary tree with k internal vertices, then T has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices

(leaves). (Proof: Every internal vertex has exactly two children, thus number of vertices that have a parent is $2k$, number of vertices = $2k + 1$ (root), number of terminal vertices = vertices – internal vertices)

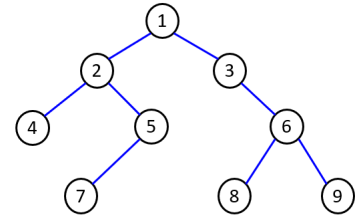
Theorem 10.6.2: For non-negative integers h , if T is any binary tree with height h and t terminal vertices (leaves), then $t \leq 2^h$. Equivalently, $\log_2 t \leq h$. (Proof by strong mathematical induction: In inductive step, assume one child and two child cases)

Term: **Tree traversal** [Lecture #13 Slides #36](#):

Tree traversal (also known as tree search) is the process of visiting each node in a tree data structure exactly once in a systematic manner. There are two types of traversal: breadth-first search (BFS) or depth-first search (DFS).

Term: **Breadth-First Search** [Lecture #13 Slides #37](#):

In breadth-first search (by E.F. Moore), it starts at the root and visits its adjacent vertices, and then moves to the next level.



Term: **Depth-first search** [Lecture #13 Slides #37](#):

- (1) Pre-order: Print – Left – Right
- (2) In-order: Left – Print – Right
- (3) Post-order: Left – Right – Print

Definition: **Spanning Tree** [Lecture #13 Slides #45](#):

A **spanning tree** for a graph G is a subgraph of G that contains every vertex of G and is a tree.

Proposition 10.7.1: (1) Every connected graph has a spanning tree. (2) Any two spanning trees for a graph have the same number of edges.

Definition: **Weighted Graph, Minimum Spanning Tree** [Lecture #13 Slides #48](#):

A **weighted graph** is a graph for which each edge has an associated positive real number **weight**. The sum of the weights of all the edges is the **total weight** of the graph. A **minimum spanning tree** for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph. If G is a weighted graph and e is an edge of G , then $w(e)$ denotes the weight of e and $w(G)$ denotes the total weight of G .

*If some edges have the same weight, more than one minimum spanning tree can occur.

Definition: **Self-complementary graph** [Tutorial #11 Definition #2](#):

A self-complementary graph is isomorphic with its complement.

Definition: **Triangle** [Tutorial #11 Definition #3](#):

A simple circuit (cycle) of length three is called a triangle.

Lemma 10.5.5: Let G be a simple, undirected graph. Then if there are two distinct paths from a vertex v to a different vertex w , then G contains a cycle (and hence G is cyclic).

Tutorial #11 Question#2: Let G be a simple graph with n vertices where every vertex has degree at least $\lfloor n/2 \rfloor$. G is connected. (Proof by contradiction)

Tutorial #11 Question#5: Let $G = (V, E)$ be a simple, undirected graph. If G is connected, then $|E| \geq |V| - 1$. (Proof by [Proposition 10.7.1](#) and [Theorem 10.5.2](#))

Tutorial #11 Question#6: Let $G = (V, E)$ be a simple, undirected graph. If G is acyclic, then $|E| \leq |V| - 1$. (Proof by assuming connected and not connected, addition rule and [Theorem 10.5.2](#))

Tutorial #11 Question#7: Let $G = (V, E)$ be a simple, undirected graph. G is a tree if and only if there is exactly one path between every pair of vertices.

Common question:

1. Find all non-isomorphic trees with n vertices

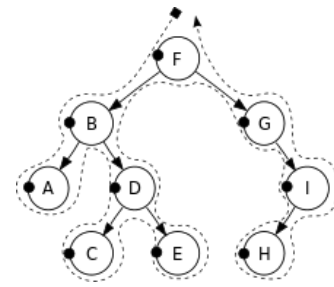
(S1) By [Theorem 10.5.2](#) any tree with n vertices has $n - 1$ edges.

(S2) By the Handshake Theorem, the tree has a total degree of $2n - 2$.

(S3) By [Lecture #13 Slides #12](#) every non-trivial tree has at least two vertices of degree 1.

(S4) The only possible combinations of degrees for the n vertices are: (Find all combination starts with 1, 1, and the order does not matter)

*Find isomorphic copies – Use Permutation



2. Tree traversal (We need at least in-order and another to get the full tree)

Pre-order	In-order	Post-order
F, B, A, D, C, E, G, I, H	A, B, C, D, E, F, G, H, I	A, C, E, D, B, H, I, G, F
(S1) The first letter is main root (F) (S2) The second letter is root of left subtree, or root of right subtree (if no left subtree)	(S1) The first letter is the “most left” element (S2) The second element is the first letter’s parent or right child	(S1) The first letter is the “most left” element (S2) The last letter is the main root (S3) The second last letter is the main root of right subtree

3. Find all spanning trees – Idea: Break the circuit

4. Find minimum spanning tree

(1) Kruskal’s algorithm: (S1) List out all edges (S2) Clear the edges and start adding from the smallest weight edge, skip those that will form a circuit. We will get $n - 1$ edges at last.

(2) Prim’s algorithm: (S1) Clear the edges, choose a vertex and it’s the starting subgraph (S2) Start adding from the smallest weight edge that connects to the existing subgraph and a vertex that is not in the subgraph. We will get $n - 1$ edges at last.

5. Draw complement graph & Self-complementary graph: A self-complementary graph exists only if the number of edges in complete graph of n vertices are even.

6. Draw binary tree: Fix the root