CS1231S Summary 24/25

Teh Xu An

Sets (Slide 1.1.3)		
$\mathbb{N}$	Set o All Natural Numbers	{0, 1, 2, 3, 4, ...}
$\mathbb{Z}$	Set of All Integers	{..., -1, 0, 1, ...}
$\mathbb{Z}^+$	Set of All Positive Integers	{1, 2, 3, 4, ...}
$\mathbb{Q}$	Set of All Rational Numbers	{..., -0.5, 0, 0.5, ...}
$\mathbb{R}$	Set of All Real Numbers	{..., -1, π, $\sqrt{2}$, 4.5, ...}
$\mathbb{C}$	Set of All Complex Numbers	{..., $-i$, 0, i, ...}

Conjunction & Disjunction / Tautology & Contradiction	
Conjunction of p and q: $(p \wedge q)$	Disjunction of p and q: $(p \vee q)$
Tautology: Always true	Contradiction: Always false

Logical Equivalence ≡	
$p \equiv q$	p & q have identical truth values ∀ (possible substitutions)

Implication Law		
Statement Type	Statement	Equivalence
Conditional	$p \to q$	$\sim p \vee q$
Negation	$\sim(p \to q)$	$p \wedge \sim q$
Converse	$q \to p$	$\sim q \vee p$
Inverse	$\sim p \to \sim q$	$p \vee \sim q$
Contrapositive	$\sim q \to \sim p$	$q \vee \sim p$

If, Only If, Biconditional	
p if q / if q then p / p is a necessary condition for q	$q \to p$
p only if q / only if q then p / p is a sufficient condition for q	$\sim q \to \sim p$ $p \to q$
p iff q / p if and only if q / p is a necessary and sufficient condition for q	$p \leftrightarrow q$ $(p \to q) \wedge (q \to p)$ $(\sim q \to \sim p) \wedge (\sim p \to \sim q)$

Order of Operations (Left to Right)				
()	~	R	∧ ∨	→ ↔

Theorem 2.1.1		
Commutative Laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative Laws	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $p \vee q \vee r \equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$	
Distributive Laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	
Identity Laws	$p \wedge true \equiv p$	$p \vee false \equiv p$
Negation Laws	$p \wedge \sim p \equiv false$	$p \vee \sim p \equiv true$
Double Negative Laws	$\sim(\sim p) \equiv p$	
Idempotent Laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal Bound Laws	$p \vee true \equiv true$	$p \wedge false \equiv false$
De Morgan's Laws	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
Absorption Laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Variant Absorption Laws (Assignment 1)	$p \vee (\sim p \wedge q) \equiv p \vee q$	$p \wedge (\sim p \vee q) \equiv p \wedge q$

Negation of T and F	$\sim true \equiv false$	$\sim false \equiv true$

Arguments (Valid and Sound)	
Valid	All premises true ∧ Conclusion true Conclusions in all critical row is true
Invalid	There is a critical row which the conclusion is false
Critical Row: All premises are true	
Sound	Valid ∧ All premises true
Unsound	Not sound ie $\sim Valid \vee$ Contradictory $Premise$
Valid & Unsound: Contradictory Premise (Vacuously True)	

Rules of Inference			
Inference	Premise 1	Premise 2	Conclusion
Modus Ponens	$p \to q$	p	$\therefore q$
Modus Tollens	$p \to q$	$\sim q$	$\therefore \sim p$
Generalisation	p q		$\therefore p \vee q$ $\therefore p \vee q$
Specialisation	$p \wedge q$ $p \wedge q$		$\therefore p$ $\therefore q$
Conjunction	p	q	$\therefore p \wedge q$
Elimination	$p \vee q$ $p \vee q$	$\sim p$ $\sim q$	$\therefore q$ $\therefore p$
Transitivity	$p \to q$	$q \to r$	$\therefore p \to r$
Contradiction	$\sim p \to false$		$\therefore p$
Proof by Division into Cases	$p \vee q$	$(p \to r) \wedge (q \to r)$	$\therefore r$

Predicate Logic	
Predicate	In the form of $P(x)$, becomes statement when x has value
Domain	Set of values that substitute x
Truth Set	$\{x \in D \mid P(x)\}$ where D is Domain of x

Universal Statements & Existential Statements	
Universal Statement	$\forall x \in D, P(x)$
Existential Statement	$\exists x \in D, P(x)$
Unique Existential Statement	$\exists! x \in D, P(x)$
Negation of Universal Statement	$\exists x \in D(\sim P(x))$
Negation of Existential Statement	$\forall x \in D(\sim P(x))$
Negation of UE Statement	$(\forall x \in D, \sim P(x)) \vee (\lvert\{x \in D, P(x)\}\rvert \geq 2)$

Rules of Inference for Quantified Statements		
Name	Premise	Conclusion
Universal Instantiation	$\forall x \in D(P(x))$	$\therefore P(a)$ if $a \in D$
Universal Generalization	$P(a)$ for every $a \in D$	$\therefore \forall x \in D(P(x))$
Existential Instantiation	$\exists x \in D(P(x))$	$\therefore P(a)$ for some $a \in D$
Existential Generalization	$P(a)$ for some $a \in D$	$\therefore \exists x \in D(P(x))$

Direct Proof & Counterexample

Proving existential statements by constructive proof.

An existential statement: $\exists x \in D(Q(x))$ is true iff $Q(x)$ is true for at least one x in D. To prove such statement, we may use constructive proofs of existence:
1) Find an x in D that makes $Q(x)$ true; or
2) Give a set of directions for finding such an x.

Disproving universal statements by counterexample.

Given a universal (conditional) statement: $\forall x \in D(P(x) \to Q(x))$. Showing this statement is false is equivalent to showing that its negation is true. The negation of the above statement is an existential statement: $\exists x \in D(P(x) \wedge \sim Q(x))$.
Find a value of x in D for which the hypothesis $P(x)$ is true but the conclusion $Q(x)$ is false. Such an x is called a counterexample.

Proving universal statements by exhaustion.

Given a universal conditional statement: $\forall x \in D\ (P(x) \to Q(x))$. When D is finite or when only a finite number of elements satisfy $P(x)$, we may prove the statement by the method of exhaustion.

Proving universal statements by generalizing from the generic particular (arbitrarily chosen element).

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.

Indirect Proof

Proof by contradiction

1) Suppose the statement to be proved, S, is false. That is, the negation of the statement, $\sim S$, is true.
2) Show that this supposition leads logically to a contradiction.
3) Conclude that the statement S is true.

Proof by contraposition (Contrapositive of $p \to q$ is $\sim q \to \sim p$)

1) Statement to be proved: $\forall x \in D(P(x) \to Q(x))$.
2) Rewrite the statement into its contrapositive form: $\forall x \in D(\sim Q(x) \to \sim P(x))$.
3) Prove the contrapositive statement by a direct proof.
   3.1) Suppose x is an (particular but arbitrarily chosen) element of D s.t. $Q(x)$ is false.
   3.2) Show that $P(x)$ is false.
4) Therefore, the original statement $\forall x \in D\ (P(x) \to Q(x))$ is true.

Proven (Methods of Proof)	
n is even	$\exists k \in \mathbb{Z}(n = 2k)$
n is odd	$\exists k \in \mathbb{Z}(n = 2k + 1)$
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 (alt)	$(n > 1) \wedge \left(\forall r, s \in \mathbb{Z}\left((r > 1) \wedge (s > 1) \to rs \neq n\right)\right)$
n is prime (alt) (Lec 4 Slide 7)	$(n \neq 1) \wedge \forall y, z \in \mathbb{Z}\left(x = yz \to \left((y = x) \vee (y = 1)\right)\right)$
n is composite	$\exists r, s \in \mathbb{Z}^+(n = rs \wedge (1 < r < n) \wedge (1 < s < n))$
n is rational	$\exists a, b \in \mathbb{Z}^+\left(n = \frac{a}{b} \wedge b \neq 0\right)$
$d \mid n\ (d, n \in Z)$	$\exists k \in \mathbb{Z}(n = dk)$

Lecture 4 Slide 16 (Example #4)	The sum of any two even integers is even.
Lecture 4 Slide 19 (Theorem 4.2.1) (5th: 4.3.1)	Every integer is a rational number.
Lecture 4 Slide 20 (Theorem 4.2.2) (5th: 4.3.2)	The sum of any two rational numbers is rational.
Lecture 4 Slide 21 (Corollary 4.2.3) (5th: 4.2.3)	The double of a rational number is rational. (Corollary: Simple deduction from theorem.)
Lecture 4 Slide 24 (Theorem 4.3.1) (5th: 4.4.1)	For all positive integers, a and b, if $a \mid b$, then $a \le b$.
Lecture 4 Slide 25 (Theorem 4.3.2) (5th: 4.4.2)	The only divisors of 1 are 1 and -1.
Lecture 4 Slide 26 (Theorem 4.3.3) (5th: 4.4.3)	For all integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.
Lecture 4 Slide 29 (Theorem 4.6.1) (5th: 4.7.1)	There is no greatest integer.
Lecture 4 Slide 32 (Proposition 4.6.4) (5th: 4.7.4)	For all integers n, if n^2 is even then n is even.
Tutorial 1 Q10	The product of any two odd integers is an odd integer.
Tutorial 1 Q11	For all integers n, n^2 is odd iff n is odd.
Tutorial 2 Q11	If n is a product of two positive integers a and b, then $a < n^{1/2}$ or $b < n^{1/2}$.
Tutorial 2 Q4	Rational numbers are closed under addition.
Tutorial 2 Q8	$\forall x \in \mathbb{R}((x^2 > x) \rightarrow (x < 0) \vee (x > 1))$

Sets			
Set-Roster Notation	{1, 2, 3, ...}		
Set-Builder Notation	$\{x \in U \mid P(x)\}$		
Replacement Notation	$\{t(x) \mid x \in A\}$		
Membership of Set ($\in$)	$x \in S$: x is an element of S		
Cardinality of Set ($\lvert S \rvert$)	$\lvert S \rvert$: Size of set S		
$A \subseteq B$	$\forall x\ (x \in A \Rightarrow x \in B)$	$A \subsetneq B$	$A \subseteq B \wedge A \neq B$
$A \nsubseteq B$	$\exists x\ (x \in A \wedge x \notin B)$	$A = B$	$\{\forall x \in A \Leftrightarrow x \in B\}$
$A \times B$	$\{(a,b) \mid a \in A \wedge b \in B\}$	$A \setminus B$	$\{x \in U \mid x \in A \wedge x \notin B\}$
$A \cup B$	$\{x \in U \mid x \in A \vee x \in B\}$	$A \cap B$	$\{x \in U \mid x \in A \wedge x \in B\}$
$\bar{A}$	$\{x \in U \mid x \notin A\}$	$\mathcal{P}(A)$	$\{S \subseteq U \mid S \subseteq A\}$
$\bigcup_{i=0}^{n} A_i$	$\{x \in U \mid x \in A_i \textit{ for at least one } i = 0,1,\dots,n\}$		
$\bigcap_{i=0}^{n} A_i$	$\{x \in U \mid x \in A_i \textit{ for all } i = 0,1,\dots,n\}$		
Lecture 5 Slide 34 (Cardinality of Power Set of a Finite Set)	Let A be a finite set where $\lvert A \rvert = n$, then $\lvert \mathcal{P}(A) \rvert = 2^n$		
Lecture 5 Slide 35 (Theorem 6.3.1)	Suppose A is a finite set with n elements, the $\mathcal{P}(A)$ has 2^n elements. In other words, $\lvert \mathcal{P}(A) \rvert = 2^{\lvert A \rvert}$.		
Equality of Ordered n-tuples, $\forall n \in \mathbb{Z}^+$ $(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n)$	$(x_1 = y_1) \wedge (x_2 = y_2) \wedge \dots \wedge (x_n = y_n)$		
Cartesian Product of Sets $A_1, A_2, \dots, A_n$ If A is a set, then	$A_1 \times A_2 \times \cdots \times A_n = \{a_1, a_2, \cdots, a_n$: $a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}$ $A^n = A \times A \times \dots \times A$ (n many A's)		
Disjoint Sets	$A \cap B = \emptyset$		

Pairwise Disjoint Sets	$A_i \cap A_j = \emptyset$ whenever $i \neq j$
Partition of Set	$\{A_1, A_2, \dots, A_n\}$ where $A_1, A_2, \dots, A_n$ are mutually disjoint subsets of A and $\bigcup_{i=0}^{n} A_i = A$

Theorem 6.2.1 (Some Subset Relations) *For all sets A, B and C			
Inclusion of Intersection	(a) $A \cap B \subseteq A$ (b) $A \cap B \subseteq B$		
Inclusion in Union	(a) $A \subseteq A \cup B$ (b) $B \subseteq A \cup B$		
Transitive Property of Subsets	$A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$		
$a \in X \cup Y$	$a \in X \vee a \in Y$	$a \in X \cap Y$	$a \in X \wedge a \in Y$
$a \in X \setminus Y$	$a \in X \wedge a \notin Y$	$a \in \bar{X}$	$a \notin X$
$(a,b) \in X \times Y$	$a \in X \wedge b \in Y$		

Theorem 6.2.2 Set Identities *For all sets A,B and C		
Commutative Laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
Identity Laws	$A \cup \emptyset = A$	$A \cap U = A$
Complement Laws	$A \cup \bar{A} = U$	$A \cap \bar{A} = \emptyset$
Double Complement Laws	$\bar{\bar{A}} = A$	
Idempotent Laws	$A \cup A = A$	$A \cap A = A$
Universal Bounds Laws	$A \cup U = U$	$A \cap \emptyset = \emptyset$
De Morgan's Laws	$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$
Absorption Laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements of U and $\emptyset$	$\bar{U} = \emptyset$	$\bar{\emptyset} = U$
Set Difference Law	$A \setminus B = A \cap \bar{B}$	

* Note that Logical Equivalence and Set Properties are similar, as they are special cases of the same general structure Boolean Algebra

Proven (Sets)	
Lecture 5 Slide 22	$\{x \in \mathbb{Z} \mid x^2 = 1\} = \{1, -1\}$
Lecture 5 Slide 31 (Theorem 4.4.1)	Quotient-Remainder Theorem $\forall n \in \mathbb{Z}, d \in \mathbb{Z}^+ (\exists!\, \mathrm{q}, \mathrm{r} \in \mathbb{Z}$ $((\mathrm{n} = \mathrm{dq} + \mathrm{r}) \wedge (0 \le \mathrm{r} < \mathrm{d})))$
Lecture 5 Slide 46	$(A \cap B) \cup (A \setminus B) = A$ for all sets A, B
Tutorial 3 Qn 3	Let $\lvert A \rvert = n$, $\lvert B \rvert = k$, then $\lvert \mathcal{P}(A \times B) \rvert = 2^{\mathrm{nk}}$
Tutorial 3 Qn 5	$A \cap B \setminus C = (A \cap B) \setminus C$
Tutorial 3 Qn 6	$A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$
Tutorial 3 Qn 7 Tutorial 3 Qn 9	$A \otimes B = (A \setminus B) \cup (B \setminus A)$ $A \otimes B = (A \cup B) \setminus (A \cap B)$
Tutorial 3 Qn 8	$A \subseteq B \Leftrightarrow A \cup B = B$

Relations	
Relation (binary) xRy "x is R-related to y"	$\forall (x,y) \in A \times B (xRy \Leftrightarrow (x,y) \in R)$ $\forall (x,y) \in A \times B (x \not R y \Leftrightarrow (x,y) \notin R)$
Domain of R: $Dom(R)$	$\{a \in A \mid aRb \textit{ for some } b \in B\}$
Co-Domain of R: $coDom(R)$	B
Range of R: $Range(R)$	$\{b \in B \mid aRb \textit{ for some } a \in A\}$
Inverse Relation: R^{-1}	$\{(y,x) \in B \times A : (x,y) \in R\}$
	$\forall x \in A, \forall y \in B((y,x) \in R^{-1} \Leftrightarrow (x,y) \in R)$
"Divides" Relations: $\mid$	$\{\forall (\mathrm{d}, \mathrm{n}) \in \mathbb{Z} \times \mathbb{Z} \mid (d \mid n \Leftrightarrow \exists k \in \mathbb{Z}(n = dk))\}$
Relation on a set A	$\forall (a_1, a_b) \in A \times A$
A^n	$A^n = A \times A \times \dots \times A$ (n times)
Composition of R with S $R \subseteq A \times B, S \subseteq B \times C$	$\forall x \in A, \forall z \in C$ $(xS \circ Rz \Leftrightarrow (\exists y \in B(xRy \wedge ySz)))$
Composition is Associative	$T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$
Inverse of Composition	$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Properties of Relations (Relation R on set A)		
Reflexive	$\forall x \in A(xRx)$	
Symmetric	$\forall x, y \in A(xRy \Rightarrow yRx)$	
Transitive	$\forall x, y, z \in A(xRy \wedge yRz \Rightarrow xRz)$	
Equivalence (~)	Reflexive, Symmetric, Transitive	
Class of a ($[a]$)	$[a]_\sim = \{x \in A \mid a \sim x\}$	$\forall x \in A(x \in [a]_\sim \Leftrightarrow a \sim x)$
Quotient of set A by ~	Set of all equivalence classes wrt ~ $A/\sim = \{[x]_\sim : x \in A\}$	
Antisymmetric	$\forall x, y \in A(xRy \wedge yRx \Rightarrow x = y)$	
~ Antisymmetric	$\exists x, y \in A(xRy \wedge yRx \wedge x \neq y)$	
Asymmetric	$\forall x, y \in A(xRy \Rightarrow y \not R x)$	
Tutorial 4 Qn 8	Every Asymmetric relation is Antisymmetric	
Partial Order	Reflexive, Antisymmetric, Transitive $((\mathbb{R}, \le), (U, \subseteq))$ $((\mathbb{Z}^+, \mid)$: Proven)	

Transitive Closure of R: R^t		
Relation obtained with least ordered pairs added to ensure transitivity in relation.		
Transitive	$R \subseteq R^t$	$\forall S \in U((S \text{ is transitive}) \wedge (R \subseteq S) \rightarrow R^t \subseteq S)$

Reflexive Closure of R (Tutorial 4 Qn 7)		
The smallest relation on A that is reflexive and contains R as a subset. $\forall x, y \in A(xSy \Leftrightarrow (x = y) \vee (xRy))$		
Reflexive	$R \subseteq S$	$\forall S' \in U((S' \text{is reflexive}) \wedge (R \subseteq S') \rightarrow S \subseteq S')$

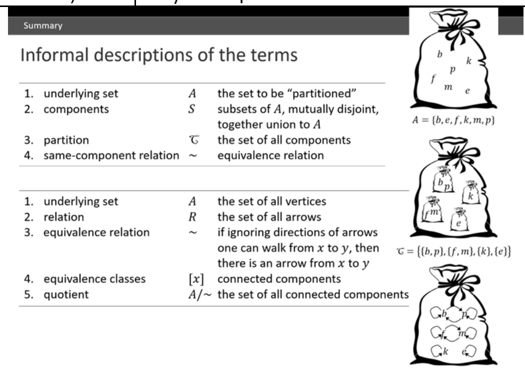
Partition of a set A	
C is a partition of a set A if the following hold: (1) C is a set of which all elements are non-empty subsets of A, i.e., $\emptyset \neq S \subseteq A$ for all $S \in$ C. (2) Every element of A is in exactly one element of C, i.e., $\forall x \in A\ \exists S \in$ C $(x \in S)$ and $\forall x \in A\ \forall S1, S2 \in$ C $(x \in S1 \wedge x \in S2 \Rightarrow S1 = S2)$.	
Partition Definition	$\forall x \in A\ \exists!\, S \in C(x \in S)$
Induced Relation by partition	$\forall x, y \in A(xRy \Leftrightarrow \exists S \in C(x, y \in S))$ R is reflexive, symmetric, and transitive (proven)

Partial Ordered Set (Poset)
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).

Lecture 6 Slide 71 (Notation $\preccurlyeq$)	Because of the special paradigmatic role played by the ≤ relation in the study of partial order relations, the symbol $\preccurlyeq$ is often used to refer to a general partial order, and the notation $x \preccurlyeq y$ is read "x is curly less than or equal to y".
Hasse Diagram	Let $\preccurlyeq$ be a partial order on a set A. A Hasse diagram of $\preccurlyeq$ satisfies the following condition for all distinct $x, y, m \in A$: If $x \preccurlyeq y$ and no $m \in A$ is such that $x \preccurlyeq m \preccurlyeq y$, then x is placed below y with a line joining them, else no line joins x and y.
x, y comparable	$(x \preccurlyeq y) \vee (y \preccurlyeq x)$
x, y noncomparable	$\sim(x \preccurlyeq y) \wedge \sim(y \preccurlyeq x)$
x, y compatible	$\exists z \in A\big((x \preccurlyeq z) \wedge (y \preccurlyeq z)\big)$
Tutorial 5 Qn 11	Any two comparable elements are compatible. Any two compatible elements are not always comparable. Eg ($\mathbb{Z}^+$,|): 2,3
Maximal Element	$\forall x \in A(c \preccurlyeq x \Rightarrow c = x)$
Minimal Element	$\forall x \in A(x \preccurlyeq c \Rightarrow c = x)$
Largest Element	$\forall x \in A(x \preccurlyeq c)$
Smallest Element	$\forall x \in A(c \preccurlyeq x)$
Largest Element = Greatest Element = Maximum Smallest Element = Least Element = Minimum	
Chain	$(C \subseteq A) \wedge \big(\forall x, y \in C(x \preccurlyeq y \vee y \preccurlyeq x)\big)$
Maximal Chain	$\text{Chain}(C) \wedge (t \notin C \Rightarrow \sim\text{Chain}(C) \cup \{t\})$
Total Order Relation	R is a partial order and $\forall x, y \in A(xRy \vee yRx)$
Linearization	Let $\preccurlyeq$ be a partial order on a set A. A linearization of $\preccurlyeq$ is a total order $\preccurlyeq *$ on A: $\forall x, y \in A(x \preccurlyeq y \Rightarrow x \preccurlyeq^* y)$
Well-Ordered Set	$\forall S \in \mathcal{P}(A), S \neq \emptyset \Rightarrow \big(\exists x \in S \forall y \in S(x \preccurlyeq y)\big)$ Ie Every non-empty subset of A has a smallest element. Eg (ℕ, ≤) is well-ordered, (ℤ, ≤) is not.

Kahn's Algorithm to finding Linearization on a partial order set
Input: A finite set A and a partial order $\preccurlyeq$ on A. 1. Set $A_0 \coloneqq A$ and $i \coloneqq 0$. 2. Repeat until $A_i = \emptyset$ 2.1. find a minimal element c_i of A_i wrt $\preccurlyeq$ 2.2. set $A_i + 1 = A_i \setminus \{c_i\}$ 2.3. set $i \coloneqq i + 1$ Output: A linearization $\preccurlyeq *$ of $\preccurlyeq$ defined by setting, for all indices i, j, $c_i \preccurlyeq * c_j \Leftrightarrow i \leq j$.

Proven (Relations)	
Tutorial 4 Qn 2	(i) R is symmetric, ie $\forall x, y \in A(xRy \Rightarrow yRx)$ (ii) $\forall x, y \in A(xRy \Leftrightarrow yRx)$ (iii) $R = R^{-1}$
Tutorial 4 Qn 5	(i) R is an equivalence relation (ii) $R^{-1} \circ R = R \circ R^{-1}$ (iii) $R \subseteq R \circ R$ (iv) $R \circ R \subseteq R$ (v) $R \circ R^{-1} = R$
Tutorial 4 Qn 6	R is an equivalence relation $\Leftrightarrow$ $R \circ R = R$
Tutorial 4 Qn 9	$S = \{(m, n) \in \mathbb{Z}^2 : m^3 + n^3\}$ $S^{-1} = S$ $S \circ S = S$ $S \circ S^{-1} = S$
Tutorial 4 Qn 10	$\forall a, b \in \mathbb{Z} \setminus \{0\}(a \sim b \Leftrightarrow ab > 0)$ ~ is an equivalence relation.
Lecture 6 Slide 27 (Example #12)	Congruence module 3 defined as: $\forall x, y \in z\big(xRy \Leftrightarrow 3 \big\| (x - y)\big)$ is reflexive, symmetric and transitive.
Lecture 6 Slide 39 (Theorem 8.3.1)	Relation Induced by a Partition is reflexive, symmetric and transitive.
Lecture 6 Slide 47 (Lemma Rel.1 Equivalence classes)	(i) $x \sim y$ equivalent $\forall x, y \in A$ (ii) $[x] = [y]$ (iii) $[x] \cap [y] \neq \emptyset$
Lecture 6 Slide 50 (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 A, and the intersection of any two distinct classes is empty.
Lecture 6 Slide 52	Congruence module n *relation*: $\forall x, y \in \mathbb{Z}\ \big(xRy \Leftrightarrow n \big\| (x - y)\big)$ iff $a \equiv b (\text{mod } n)$
Lecture 6 Slide 54 (Proposition)	Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$
Lecture 6 Slide 57 (Theorem Rel.2)	Equivalence classes for a partition. ie $A/\sim$ is a partition of A.



Lecture 6 Slide 69 (Example #20)	| is a partial order relation on $A \in \mathbb{Z}^+$
Lecture 6 Slide 83	Consider a partial order $\preccurlyeq$ on a set A. Any smallest element is minimal. Likewise, any largest element is maximal.

Functions	
Function Definition	$f: X \to Y \Leftrightarrow \forall x \in X \exists! y \in Y (x, y) \in f)$
Function Type Signature	In the form $f: (X_1, X_2, \ldots) \to (Y)$
Image, Preimage	$f: x \mapsto y \to x$ is argument of f $f(x)$,the output of f for the input x $f(x) = y, y$ *is* image of x under f/x is preimage of y
Setwise Image	$f: X \to Y \Rightarrow f: \mathcal{P}(X) \to \mathcal{P}(Y) / f(A) = \{f(x): x \in A\}$
Setwise Preimage	$f: X \to Y$ $\Rightarrow f^-1: \mathcal{P}(Y) \to \mathcal{P}(X) / f^-1(B) = \{x \in X: f(x) \in B\}$
Domain/Codomain	$f: A \to B \Rightarrow$ Domain:A,Co-Domain:B
Range	$f: A \to B \Rightarrow$ Range:$\{b \in B: b = f(a), a \in A\}$
Sequences	A sequence $a_0, a_1, a_2, \ldots$ can be represented by a function a whose domain is $Z_{\geq 0}$that satisfies $a(n) = a_n \forall n \in Z_{\geq 0}$
	$A^\infty = Seq(A) = \exists n \in Z. Z_{\geq n} \to A$
Fibonacci Sequence	$\forall n \in Z_{\geq 0}, F_0 = 0, F_1 = 2, F_{n+2} = F_{n+1} + F_n$ $\Rightarrow F_0, F_1, F_2, \ldots$
String	String over A:$a_0 a_1 \ldots a_{l-1}, l \in Z_{\geq 0}, a_0, a_1, \ldots, a_{l-1}$ $\in A$ where l is length of string, Empty String:ϵ
	$A^* = Str(A) = \exists m \in Z, I \in Z_{\geq 0}. [m, m + l) \to A$
Equality of Seq	$(a(n) = a_n) = (b(n) = b_n) \forall n \in Z_{\geq 0}$
Equality of String	$s_1 = s_2 \Leftrightarrow (a_i = b_i) \forall i \in \{0, 1, \ldots, l - 1\}$
Function Equality	$f: A \to B, g: C \to D$ then $f = g \Leftrightarrow (A = C) \wedge (B = D) \wedge \big(f(x) = g(x)\big) \forall x \in A$
Injection (1 to 1)	$\forall x_1, x_2 \in X(f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$
Surjection (Onto)	$\forall y \in Y \exists x \in X\big(y = f(x)\big)$
Bijection (Inj + Sur)	$\forall y \in Y \exists! x \in X\big(y = f(x)\big)$
Inverse	g/f^{-1}inverse of f $\Leftrightarrow$ $\forall x \in X \forall y \in Y\big(y = f(x) \Leftrightarrow x = g(y)\big)$
Uniqueness of Inverse	g_1 and g_2 are inverses of $f: X \to Y \Rightarrow g_1 = g_2$
Theorem 7.2.3	$f: X \to Y$ is bijective $\Leftrightarrow f^{-1}: Y \to X$ is bijective
	$f: X \to Y$is bijective $\Leftrightarrow f$ has an inverse
Composition of Function	$(g \circ f)(x) = g\big(f(x)\big) \forall x \in X$
Theorem 7.3.1	$id_X(x) = x, f \circ id_X = f, id_Y \circ f = f$
Theorem 7.3.2	$f^{-1} \circ f = id_X$ and $f \circ f^{-1} = id_Y$
Theorem 7.3.4	$(h \circ g) \circ f = h \circ (g \circ f)$
Lecture 7 Slide 53	Function Composition is not commutative
Theorem 7.3.3	$f: X \to Y$ and $g: Y \to Z$ inj $\Rightarrow g \circ f$ inj
Theorem 7.3.4	$f: X \to Y$ and $g: Y \to Z$ sur $\Rightarrow g \circ f$ sur
Well Defined Function	$\forall x_1, x_2 \in X, \forall f: X \to Y, x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$
Well Defined Prop wrt Eq Relation ~	$\forall x_1, x_2 \in X, \forall f: X \to Y, x_1 \sim x_2 \Rightarrow f(x_1) \sim f(x_2)$
Well Defined Prop wrt Eq Class [x]	$\forall x_1, x_2 \in X, \forall f: X \to Y, [x_1] = [x_2] \Rightarrow [f(x_1)]$ $= [f(x_2)]$
Quotient $Z/\sim_n$	$Z_n = Z/\sim_{n,\text{ where}} \sim_n$ is congruence-mod-$n$relation on Z
Addition on Z_n	$[x], [y] \in Z_n \Rightarrow [x] + [y] = [x + y]$
Multiplication on Z_n	$[x], [y] \in Z_n \Rightarrow [x] \cdot [y] = [x \cdot y]$
Lecture 7 Slide 62	Proposition: Addition on Z_n is well defined
Lecture 7 Slide 64	Proposition: Multiplication on Z_n is well defined
Sequence 2.0	$a_m, a_{m+1}, a_{m+2}, \ldots, a_n$:where k in $a_k$is called subscript of index

CS1231S Summary 24/25

Teh Xu An

Seq Explicit Form	$a_k = f(k) \forall k \in Z$
Seq Comprehension	a = [(f(k): k ∈ Z] Type Signature: $Seq(Q) = ([1, \infty) \to Q)$
Set Builder	$\{k \in U: R(x)\}: P(U)$, Where $R(x)$ is predicate/$R: U \to Bool$
Set Replacement	$\{f(k): k \in S\}: P(B)$ Where $k \in S$ and $f(k)$ is replacement/$f: S \to B$
Set Comprehension	$\{f(k_1, k_2): k_1 \in S_1, k_2 \in S_2, R(k_1, k_2)\}: P(S_3)$ $R: S_1 \times S_2 \to Bool, f: S_1 \times S_2 \to S_3$ 1 replacement, multiple generators and predicates
Summation Notation	$\sum_{k=m}^{n} a_k = \begin{cases} a_m + a_{m+1} + \cdots + a_n & m \le n \\ 0 & m > n \end{cases}$ $\sum_{k=m}^{n} a_k = (\sum_{k=m}^{n-1} a_k) + a_n$ $\sum \quad : (Int, Int, Seq(Q)) \to Q$ k:Index, m:lower limit, n:upper limit
Product Notation	$\prod_{k=m}^{n} a_k = \begin{cases} a_m \cdot a_{m+1} \cdot \ldots \cdot a_n & m \le n \\ 1 & m > n \end{cases}$ $\prod_{k=m}^{n} a_k = (\prod_{k=m}^{n-1} a_k) \cdot a_n$ $\prod \quad : (Int, Int, Seq(Q)) \to Q$
Theorem 5.1.1 Lecture 7 Slide 17	$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k+m}^{n} (a_k + b_k)$ $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$ $\prod_{k=m}^{n} a_k \cdot \prod_{k=m}^{n} b_k = \prod_{k=m}^{n} (a_k \cdot b_k)$
Lecture 7 Slide 20	$\sum_{k=m}^{n} f(k) = \sum_{i=m}^{n} f(i), \prod_{k=m}^{n} f(k) = \prod_{i=m}^{n} f(i)$
Arithmetic Seq	$a_k = a_{k-1} + d \Leftrightarrow a_n = a_0 + dn$, $\sum_{k=0}^{n-1} a_k = \frac{n}{2}(2a_0 + (n-1)d)$
Geometric Seq	$a_k = r a_{k-1}, \forall k \ge 1 \Leftrightarrow a_n = a_0 r^n, \forall n \ge 0$ $\sum_{k=0}^{n-1} a_k = a_0 \left(\frac{1-r^n}{1-r}\right), r \ne 1$
Squares Seq	$[k * k: k \in [1 \ldots]] = 1,4,9,16, \ldots$
Triangle Seq	$[tri(k): k \in [1 \ldots]] = 1,3,6,10, \ldots$ where $tri(n) = \begin{cases} 1 & n = 1 \\ n + tri(n-1) & n > 1 \end{cases}$
Fibonacci Seq	$[F(k): k \in [1 \ldots]] = 1,1,2,3, \ldots$ where $F(n) \begin{cases} 1 & n = 1 \\ 1 & n = 2 \\ F(n-1) + F(n-2) & n \ge 3 \end{cases}$
Lazy Caterer's Seq	$[cuts(k): k \in [0 \ldots]] = 1,2,4,7,11, \ldots$ where $cuts(k) = (k^2 + k + 2)/2$

Proven (Functions)	
Tutorial 6 qn 4	$f: A \to B, g: B \to C$ then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
Left Inverse	g left inv of $f \Leftrightarrow g(f(a)) = a \forall a \in A$
Left Inverse (Not Proven)	g left inv of $f \Leftrightarrow$ f is injective
Right Inverse	h right inv of $f \Leftrightarrow f(h(b)) = b \forall b \in B$
Right Inverse (Not Proven)	h right inv of $f \Leftrightarrow$ f is injective
Tutorial 6 qn 7	$g \circ f$ is inj $\Rightarrow f$ is inj
Order of Bijection Tutorial 6 qn 8	smallest $n \in Z^+ \underbrace{(f \circ f \circ \ldots \circ f)}_{n-\text{many } f} = id_A$
Tutorial 6 qn 9	$f: A \to B, X \subset A, Y \subset B \Rightarrow X \subseteq f^{-1}(f(X))$ $f: A \to B, X \subset A, Y \subset B \Rightarrow f(f^{-1}(Y)) \subseteq Y$

Mathematical Induction	
Principle of MI (PMI)	To prove that $P(n)$ is true $\forall n \in Z^+$ Basic Step: Show that $P(1)$ is true Inductive Step: Show that $P(k) \Rightarrow P(K+1) \forall k \in Z^+$
Induction Principle	$P(a) \wedge (\forall k \ge a\ (P(k) \Rightarrow P(k+1))$ $\Rightarrow \forall k \ge a\ (P(k))$
Strong MI	$(P(a) \wedge P(a+1) \wedge \ldots \wedge P(b)) \wedge$ $(\forall k \ge b, P(a) \wedge P(a+1) \wedge \ldots \wedge P(k) \Rightarrow P(k+1))$ $\Rightarrow \forall k \ge a, P(k)$
Strong Induction	$P(a) \wedge (\forall k \ge a, P(a) \wedge P(a+1) \wedge \ldots \wedge P(k) \Rightarrow P(k+1))$ $\Rightarrow \forall k \ge a, P(k)$
Strong MI Var 1	$(P(a) \wedge P(a+1) \wedge \ldots \wedge P(b))$ $(\forall k \ge a, P(k) \Rightarrow P(k+b-a+1))$ $\Rightarrow \forall k \ge a, P(k)$
Strong MI Var 2	$(P(a) \wedge P(a+1) \wedge \ldots \wedge P(b))$ $(\forall k \ge b \exists i, a \ge i \ge k, P(i) \Rightarrow P(k+1))$ $\Rightarrow \forall k \ge a, P(k)$
Well Ordering Principle for Integers	Every nonempty subset of $Z_{\ge 0}$ has a smallest element
Recurrence Relation for Seq	$a_0, a_1, \ldots$ where a_k is affected by some of $a_0, a_1, \ldots a_{k-1}$
Recursive Definition of set S	I. Base/Founder: certain element(s) $c \in S$ II. Recursion/Constructor: $x \in S \Rightarrow f(x) \in S$ III. Restriction/Minimality: Membership for S can always be demonstrated by (finitely many) successive applications of the clauses above $S ::= c_1 \| c_2 \| \ldots \| f_1(S) \| f_2(S) \| \ldots$ where c_i are founders and f_i are constructors
Structural Induction over set S	Base: $\forall$ founder $c(P(c))$ Induction: $\forall x \in S(P(x) \Rightarrow P(f(x)), \forall$ constructor f Conclusion: $\forall x \in S(P(x))$
Recursive Defined Set of Strings	$S = \{c\_1, \ldots, c\_n\}, Str(S) ::= \epsilon \| c\ (Str(S)\ (c \in S))$
Recursive Definition of Parentheses	I. Base/Founder: () is in P II. Recursion/Constructor: $\begin{cases} (E) \in P & E \in P\ (a) \\ EF \in P & E, F \in P\ (b) \end{cases}$ III. Restriction/Minimality: No other configs are in P except those derived from above
Structural Induction on Nat	$Nat ::= 0 \| 1 + Nat$ $(P(0) \wedge \forall k \ge 0, P(k) \Rightarrow P(k+1)) \Rightarrow \forall k \ge 0, P(k)$
Structural Induction on Str(A)	$Str(A) ::= \epsilon \| A.Str(A)$ $(P(\epsilon) \wedge \forall a \in A, s \in Str(A), P(s) \Rightarrow P(a.s))$ $\Rightarrow \forall s \in Str(A), P(s)$

Proven (Mathematical Induction)	
Proposition 5.3.1	$\forall n \ge 0, 3 \| 2^{2n} - 1$
Proposition 5.3.2	$\forall n \ge 3, 2n + 1 \le 2^n$
Sum of Geometric Sequence (Theorem 5.2.3)	$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}, \forall n \ge 0$
Transitivity of Divisibility (Theorem 4.3.3)	$\forall a, b, c \in Z(a \| b \wedge b \| c \Rightarrow a \| c)$

Lecture 8 Slide 47	Any integers >1 is divisible by a prime number
Lecture 8 Slide 49	Any whole amount of ≥ $12 can be formed by a combination of $4 and $5 coins
Lecture 8 Slide 50	$\forall n \in Z_{\ge 12}(\exists a, b \in N(n = 4a + 5b))$
Well Ordering Principle for Integers Examples (Lecture 8 Slide 54/55)	R^+:No smallest but principle refers to only Z^+ $\{n \in N: n^2 \le n\}$:No smallest but principle does not include non-empty set $\{n \in N: n = 46 - 7k, k \in Z\}$:4 is smallest
Lecture 8 Slide 64	(())() is in P (1) By I, () $\in P$ (2) By (1) and IIa, (()) $\in P$ (3) By (2),(1), and IIb,(())() $\in P$
Recursive Definition of $Z_{\ge 0}$	I: Base: $0 \in Z_{\ge 0}$ II: Recursive: $x \in Z_{\ge 0} \Rightarrow x + 1 \in Z_{\ge 0}$ III: Restriction: Membership for $Z_{\ge 0}$ can always be demonstrated by successive applications of the clauses above
Recursive Definition of $2Z$	I: Base: $0 \in 2Z$ II: Recursion: $x \in 2Z \Rightarrow x - 2, x + 2 \in 2Z$ III: Restriction: Membership for $2Z$ can always be demonstrated by successive applications of the clauses above
Tutorial 7 Qn 1	$\forall n \in Z^+, \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$
Tutorial 7 Qn 2	$\forall n \in Z^+, \sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1)$
Tutorial 7 Qn 4	$\forall n \in Z^+, 2^{n+2} \| (a^{2^n} - 1), a \in \{2z + 1: z \in Z\}$
Tutorial 7 Qn 5	$\forall n \in Z_{\ge 8} \exists x, y \in N(n = 3x + 5y)$
Tutorial 7 Qn 6	$\forall n \in Z^+ \exists l \in Z^+ \exists i_1, i_2, \ldots, i_l \in N$ $(i_1 < i_2 < \cdots < i_l \wedge n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_l})$ Ie Every positive int can be written as a sum of distinct non-negative integer powers of 2
Tutorial 7 Qn 7	Let $a_0, a_1, a_2, \ldots$ be seq where $a_0 = 0, a_1 = 2, a_2 = 7, \forall n \in N(a_{n+3} = a_{n+2} + a_{n+1} + a_n)$ Then $\forall n \in N(a_n < 3^n)$
Tutorial 7 Qn 8	Fib Seq: $F(0) = 0, F(1) = 1$, $\forall n \in Z^+ F(n+1) = F(n) + F(n+1)$ Let $P(a, b) \equiv F(a + b) =$ $(F(a+1) \times F(b) + F(a) \times F(b-1)) \forall a \in Z_{\ge 0}, b \in Z^+$ Then $\forall b \in N, \forall n \in Z^+(P(n-1, b) \wedge P(n, b) \Rightarrow P(n+1, b))$
Tutorial 7 Qn 9	Recursive definition of set H of Hamming Numbers: $1 \in H, n \in H \Rightarrow 2n, 3n, 5n \in H$ Canonical representation: $P(n) \equiv \exists! i \exists! j \exists! k(i, j, k \in Z_{\ge 0} \wedge n = 2^i 3^j 5^k)$

Cardinality	
Pigeonhole Principle	$\exists f: A \to B\ injective \Rightarrow \|A\| \le \|B\|$ Contrapositive: $m, n \in Z^+, m > n, m$ pigeons, n pigeonholes, then $\exists \ge 1$ pigeonhole with ≥ 2 pigeons
Dual Pigeonhole Principle	$\exists f: A \to B\ surjective \Rightarrow \|A\| \ge \|B\|$ Contrapositive: $m, n \in Z^+, m < n, m$ pigeons, n pigeonholes, then $\exists \ge 1$ pigeonhole with 0 pigeons

General Pigeonhole Principle	$\forall f: X \to Y, \forall k \in Z^+ (k < \lvert X\rvert/\lvert Y\rvert$ $\Rightarrow \exists y \in Y(y = f(x)$ for $\ge k+1$ distinct $x \in X))$ Contrapositive: $\forall f: X \to Y, \forall k \in Z^+$ $(\forall y \in Y, \lvert f^{-1}(\{y\})\rvert$ at most $k \Rightarrow \lvert X\rvert \le k\lvert Y\rvert)$
Equality of Cardinality	Same Cardinality (Cantor) $\lvert A\rvert = \lvert B\rvert$ $\lvert A\rvert = \lvert B\rvert \Leftrightarrow \exists f: A \to B\ Bijection$
Finite Definition	S is finite $\Leftrightarrow (S = \emptyset) \lor (\exists f: S \to Z_n\ Bijection, n \in Z^+)$ where $Z_n = \{1,2,\dots,n\}$
Cardinality of S	$\lvert S\rvert = \begin{cases} 0 & S = \emptyset \\ n & \exists f: S \to Z_n\ Bijection \end{cases}$
Properties of Cardinality (Theorem 7.4.1)	The same-cardinality relation is an equivalence relation Reflexive: $\lvert A\rvert = \lvert A\rvert$ Symmetric: $\lvert A\rvert = \lvert B\rvert \Rightarrow \lvert B\rvert = \lvert A\rvert$ Transitive: $(\lvert A\rvert = \lvert B\rvert) \land (\lvert B\rvert = \lvert C\rvert \Rightarrow \lvert A\rvert = \lvert C\rvert)$
Theorem Cardinality 1	Any subset of a finite set is finite $A \subseteq B, finite(B) \Rightarrow finite(A)$ Contrapositive: Any set with an infinite subset is infinite $A \subseteq B, infinite(A) \Rightarrow infinite(A)$
Countably Infinite	$CountablyInfinite(A) \Leftrightarrow \lvert A\rvert = \lvert Z^+\rvert/\lvert N\rvert/\lvert Z_{\ge 0}\rvert = \aleph_0$
Countable	$Countable(A) \Leftrightarrow finite(A) \lor CountablyInfinite(A)$
Proposition 9.1	Infinite set B is countable $\Leftrightarrow \exists$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 Infinite set B is countable $\Leftrightarrow \exists$a sequence $b_0, b_1, b_2, \dots \in B$ in which every element of B appears
Theorem 7.4.2 (cantor)	$(0,1) = \{x \in R \mid 0 < x < 1\}$ is uncountable
Theorem 7.4.3	Any subset of any countable set is countable
Corollary 7.4.4	Any set with an uncountable subset is uncountable
Proposition 9.3	Every infinite set has a countable infinite subset
Lemma 9.4	Union of 2 countably infinite sets is countable

Proven (Cardinality)	
Lecture 9 Slide 17	$\lvert 2Z\rvert = \lvert Z\rvert$
Lecture 9 Slide 24	$\lvert Z\rvert = \lvert Z^+\rvert, f(n) = \begin{cases} n/2 & Even(n) \\ -(n-1)/2 & Odd(n) \end{cases}, f: Z^+ \to Z$
Lecture 9 Slide 27	$\lvert Q^+\rvert = \lvert Z^+\rvert \Rightarrow countable(Q^+)$
Lecture 9 Slide 30 Theorem	$\lvert Z^+ \times Z^+\rvert = \lvert Z^+\rvert \Rightarrow countable(Z^+ \times Z^+)$ $f(x,y) = \frac{(x+y-2)(x+y-1)}{2} + x$
Theorem (Cartesian Product)	$CountablyInfinite(A) \land CountablyInfinite(B)$ $\Rightarrow CountablyInfinite(A \times B)$
Corollary (General Cartesian Product)	$n \in Z_{\ge 2}, \forall i \in N_{\le n} CountablyInfinite(A_i)$ $\Rightarrow CountablyInfinite(A_0 \times A_1 \times \dots \times A_{n-1})$
Theorem (Unions) Lecture 9 Slide 32	$\forall A_n, n \in Z^+ Countable(A) \Rightarrow Countable(\bigcup_{i=1}^{\infty} A_i)$
Lecture 9 Slide 46	$\lvert R\rvert = \lvert (0,1)\rvert$
Tutorial 8 Qn 2	$CountablyInfinite(B) \land finite(C)$ $\Rightarrow countable(B \cup C)$
Tutorial 8 Qn 3a	$\forall n \in Z^+, finite(A_n) \Rightarrow finite(\bigcup_{i=1}^{n} A_i)$
Tutorial 8 Qn 3b	$\forall n \in Z^+, finite(A_n) \Rightarrow$ infinite$(\bigcup_{i=1}^{\infty} A_i)$
Tutorial 8 Qn 4a	$\forall n \in Z^+, countable(A_n) \Rightarrow countable(\bigcup_{i=1}^{n} A_i)$
Tutorial 8 Qn 5	$\forall n \in Z^+, countable(A_n) \Rightarrow countable(\bigcup_{i=1}^{\infty} A_i)$

Tutorial 8 Qn 6	$(infinite(X) \land finite(Y)) \Rightarrow \exists f: X \cup Y \to X$ bijection
Tutorial 8 Qn 7	$CountableInfinite(A) \Rightarrow uncountable((\mathcal{P})(A))$
Tutorial 8 Qn 8	$R\ reflexive\ on\ A \Rightarrow \lvert A\rvert \le \lvert R\rvert$

Counting and Probability	
Sample Space	Set of all possible outcomes of a random process
Event	A subset of a sample space
$\lvert A\rvert$	For a finite set A, $\lvert A\rvert$ denotes the number of elements in A
Equally Likely Probability	$P(E) = \frac{\text{Number of outcomes in E}}{\text{Total number of outcomes in S}} = \frac{\lvert E\rvert}{\lvert S\rvert}$
Probability Axioms	1. $0 \le P(A) \le 1$ 2. $P(\emptyset) = 0$ and $P(S) = 1$ 3. $(A \cap B = \emptyset) \Rightarrow P(A \cup B) = P(A) + P(B)$
General Union of Two Events	$P(A \cup B) = P(A) + P(B) - P(A \cap B)$
Theorem 9.1.1	$m, n \in Z, m \le n$ there are $n - m + 1$ integers from m to n inclusive
Possibility Tree	Possible outcomes are represented by distinct paths from “root” (the start) to “leaf” (a terminal point) in a tree
Multiplication/ Product Rule Theorem 9.2.1	Suppose an event with k steps, $n_i$ways for i^{th} step, then there are $\prod_{i=1}^{k} n_i$ ways for the event to happen
Theorem 5.2.4	Suppose A is a finite set. Then $\lvert \mathcal{P}(A)\rvert = 2^{\lvert A\rvert}$
Theorem 9.2.2	Number of Permutations of a set with n elements is $n!$
Theorem 9.2.3	$P(n,r) = {}_nP_r = P_r^n = n(n-1)\dots(n-r+1) = \frac{n!}{(n-r)!}$
Addition/Sum Rule Theorem 9.3.1	Partitions A_1, A_2, A_k of A, $\lvert A\rvert = \lvert A_1\rvert + \lvert A_2\rvert + \dots + \lvert A_k\rvert$
Difference Rule Theorem 9.3.2	A is finite set and $B \subseteq A$, then $\lvert A \backslash B\rvert = \lvert A\rvert - \lvert B\rvert$
Probability of Complement	$P(\bar{A}) = 1 - P(A)$
Theorem 9.3.3	$\lvert A \cup B\rvert = \lvert A\rvert + \lvert B\rvert - \lvert A \cap B\rvert$ $\lvert A \cup B \cup C\rvert = \lvert A\rvert + \lvert B\rvert + \lvert C\rvert - \lvert A \cap B\rvert - \lvert A \cap C\rvert - \lvert B \cap C\rvert + \lvert A \cap B \cap C\rvert$
Theorem 9.5.1 r-combination	$\binom{n}{k} = C(n,r) = {}_nC_r = C_{n,r} = {}^nC_r = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}$, where $r \le n, r, n \in Z_{\ge 0}$
Theorem 9.5.2	For a collection of n objects of k types where $\forall i \in \{1,\dots,k\}$ n_i are indistinguishable from each other $\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\dots\binom{n-n_1-n_2-\dots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!\dots n_k!}$
Multiset	$[x_{i_1}, x_{i_2}, \dots x_{i_r}]$ where each x_{i_j} is in $X = x_1, x_2, \dots, x_n$ and some of x_{i_j} may equal each other
r-combination with repetition	Consider each x_i as their category, then select position of separators ie $[1,3,4] \equiv$ "x||x|x", $[2,4,4] \equiv$ "|x||xx" r-combination with n types $= \binom{r+n-1}{r}$

General Formulas	Ordered	Unordered
With Repetition	n^k	$\binom{k+n-1}{k}$
No Repetition	$P(n,k)$	$\binom{n}{k}$

Pascal’s Formula Theorem 9.7.1	$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

Lecture 11 Slide 30	For $0 \le k \le n, \binom{n}{k} = \binom{n}{n-k}$
Lecture 11 Slide 31	For $0 \le k \le n, k\binom{n}{k} = n\binom{n-1}{k-1}$
Lecture 11 Slide 33	$\sum_{k=0}^{n} \binom{n}{k} = \lvert \mathcal{P}(S)\rvert = 2^n$
Binomial Theorem	$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$, where $\binom{n}{r}$ is binomial coefficient
Expected Value	$\sum_{k=1}^{n} a_k p_k = a_1p_1 + a_2p_2 + \dots + a_np_n$, For when the possible outcomes are $a_1, a_2, \dots, a_n$ with probabilities $p_1, p_2, \dots, p_n respectively$
Linearity of Expectation	$E[X+Y] = E[X] + E[Y]$ or $E\left[\sum_{i=1}^{n} c_i \cdot X_i\right] = \sum_{i=1}^{n} (c_i \cdot E[X_i])$ Regardless of whether they are independent
Conditional Probability Theorem 9.9.1	$P(B \mid A) = \frac{P(A \cap B)}{P(A)}$
Theorem 9.9.2	$P(A \cap B) = P(B \mid A) \cdot P(A)$
Theorem 9.9.3	$P(A) = \frac{P(A \cap B)}{P(B \mid A)}$
Bayes’ Theorem	$P(B_k \mid A) = \frac{P(A \mid B_k) \cdot P(B_k)}{\sum_{i=1}^{n} (P(A \mid B_i) \cdot P(B_i))}$
Independent Events Lecture 11 Slide 72	Events A and B are independent $\Leftrightarrow$ $P(A \mid B) = P(A), P(B \mid A) = P(B), P(A \cap B) = P(A)P(B)$
Pairwise/ Mutually Independent	Pairwise Independent : 1 to 3, Mutually Independent: All 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. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$
Mutually Independent	$P(A_1 \cap A_2 \cap \dots \cap A_n) = P(A_1) \cdot P(A_2) \cdot \dots \cdot P(A_n)$
Binomial Probabilities	$P(X = x) = \binom{n}{x} p^{n-x} (1-p)^x$, where $0 \le p \le 1$

Proven (Countability and Probability)	
Tutorial 10 Qn 6	Let $\lvert A\rvert = n$, let each relation in $\mathcal{P}(A \times A)$ is equally likely to be chosen Prob of Reflexive Relation: $\frac{2^{n^2-n}}{2^{n^2}} = \frac{1}{2^n}$ Prob of Symmetric Relation: $\frac{2^{\frac{n^2+n}{2}}}{2^{n^2}} = \frac{1}{2^{\frac{n^2-n}{2}}}$

Graph	
Edge	$e = \{v,w\}/(v,w)$ where e is incident on endpoints v, w
Undirected Edge	$e = \{v,w\}$ for undirected edge e from vector v to vector w
Directed Edge	$e = (v,w)$ for directed edge e from vector v to vector w
Adjacent Vertices	$\exists e = \{v,w\}/(v,w) \Rightarrow v, w$ are adjacent vertices $\exists e = \{v,v\}/(v,v) \Rightarrow v$ is adjacent to itself, e: loop

Undirected Graph	$G = (V, E)$, where V is set of vertices and E is a set of undirected edges
Directed Graph	$G = (V, E)$, where V is set of vertices and E is a set of directed edges
Vertex Colouring	Assignment of colours to vertices so that no two adjacent vertices have the same colour
Map Colouring Lecture 12 Slide 11	Four Colour Conjecture: 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
Simple Graph	Undirected graph with no loops or parallel edges
Complete Graph	A complete graph on n vertices, $n > 0$, denoted K_n, is simple graph with n vertices and exactly one edge connecting each pair of distinct vertices
Graph Complement	$\bar{G} = (V, \bar{E})$ is such that $\bar{E} = \{\{v, w\} \in V \times V : \{v, w\} \notin E\}$
Graph Self-Complement	Graph is isomorphic with its complement ie $G \cong \bar{G}$
Bipartite Graph	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
Complete Bipartite Graph	A Bipartite graph on two disjoint sets U and V such that every vertex in U connects to every vertex in V If $\lvert U\rvert = m, \lvert V\rvert = n$, the complete bipartite graph is denoted as $K_{m,n}$
Subgraph	H subgraph of $G \Leftrightarrow \forall v \in V_H (v \in V_G), \forall e \in E_H (e \in E_G)$
Degree	$deg(v) =$ Number of e incident to v, loop counts twice
Total Degree	$TotalDeg(G) = \sum_{i=1}^{n} deg(v_i), V_G = \{v_1, v_2, \ldots, v_n\}$
Theorem 10.1.1	Handshake Theorem: $TotalDeg(G) = 2 \times \lvert E_G\rvert$
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
Indegree	$deg^-(v)$ is number of e that end at v
Outdegree	$deg^+(v)$ is number of e that originate at v
In/Outdegree relationship	$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = \lvert E\rvert$
Walk from v to w	Has the form: $v_0 e_1 v_1 e_2 \ldots v_{n-1} e_n v_n$ where $v_0 = v, v_n = w$, length of walk $= n$ Trivial walk from v to v: v
Trail from v to w	A walk from v to w does not contain a repeated edge
Path from v to w	A trail that does not contain a repeated vertex
Closed walk	A walk that starts and ends at the same vertex
Circuit	A closed walk of length at least 3 vertex and is a trail
Simple Circuit	A circuit that has no repeated vertex but first and last
Cyclic/Acyclic	An undirected graph is cyclic if it contains a loop or a cycle, acyclic otherwise
Connectedness	Two vertices are connected iff there is a walk between Graph is connected iff $\forall v, w \in V \exists$ a walk from v to w
Lemma 10.2.1	If G is connected, any 2 vertices of G can be connected by a path. 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

	If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G
Connected Component	1. H is a subgraph of G 2. H is connected 3. No connected subgraph of G has H as subgraph and contains vertices or edges not in H
Euler Circuit	Circuit that contains every vertex and traverses every edges exactly once
Eulerian Graph	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: If come vertex of a graph has odd degree, then the graph does not have an Euler circuit
Theorem 10.2.3	If a graph is connected and the degree of every vertex is a positive even integer, then it has an Euler Circuit
Theorem 10.2.4	A graph has an Euler Circuit iff it is connected and every vertex has positive even degree.
Euler Trail	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.
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.
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.
Hamiltonian Circuit	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.)
Hamiltonian Graph	A Hamiltonian graph (also called Hamilton graph) is a graph that contains a Hamiltonian circuit.
Proposition 10.2.6	Property of Hamiltonian graph H in G 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
Adjacency Matrix	$A = (a_{ij})$ where $a_{ij} =$ Number of arrows from $v_{i \text{ to }} v_j \forall i, j \in \{1, 2, \ldots, \lvert V\rvert\}$ Note that Adj Mat for undirected graph is symmetric ie $a_{ji} = a_{ij}$
Identity Matrix	$I_n = (\delta_{ij}), \delta_{ij} = \begin{cases} 1, & i = j \\ 0 & i \neq j \end{cases} \forall i, j = 1, 2, \ldots, n$
Powers of Matrix	$A^0 = I, A^n = AA^{n-1} \forall n \geq 1$
Theorem 10.3.2	If G is a graph with vertices $v_1, v_2, \ldots, v_m$ and A is the Adj Mat of G then $\forall n \in Z^+, \forall i, j = 1, 2, \ldots, m$ $\Rightarrow$ The ij-th entry of A^n $=$ the number of walks of length n from $v_{i \text{ to }} v_j$
Isomorphic Graph	$G \cong G' \Leftrightarrow \exists$ bijection $g: V_G \to V_{G'}$ and $h: E_G \to E_{G'}$ such that $\forall v \in V_G, e \in E_G$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$

Isomorphic Graph for Simple Graphs	G and G' are simple graphs $G \cong G' \Leftrightarrow \exists \pi: V_G \to V_{G'}$ such that $\{u, v\} \in E_G \Leftrightarrow \{\pi(u), \pi(v)\} \in E_{G'}$
Theorem 10.4.2	$\cong$, Graph Isomorphism is an Equivalence Relation
Planar Graph	A graph that can be drawn on a plane without edges crossing
Kuratowski's Theorem	A finite graph is planar iff 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 $G = (V, E)$, Letting f be the number of face, then $f = \lvert E\rvert - \lvert V\rvert + 2$
Triangle	A simple circuit of length 3

Proven (Graphs)	
Tutorial 10 Qn 12	For any simple graph with 6 vertices, it or its complementary graph will contain a triangle
Tutorial 11 Qn 4	Let $G = (V, E)$ be a simple undirected graph, then G is connected $\Rightarrow \lvert E\rvert \geq \lvert V\rvert - 1$
Tutorial 11 Qn 5	Let $G = (V, E)$ be a simple undirected graph, then G is acyclic $\Rightarrow \lvert E\rvert \leq \lvert V\rvert - 1$

Trees	
Circuit-free	Graph has no circuits
Tree	Simple graph that is circuit-free and connected
Trivial Tree	Tree with 1 vertex
Forest	Simple graph that is circuit-free and not connected
Lemma 10.5.1	Any non-trivial tree has at least one vertex of degree 1
Terminal Vertex	Vertex of degree 0 or 1 in a tree
Internal Vertex	Vertex of degree greater that 1 in a tree
Theorem 10.5.2	Any tree with n vertices$(n > 0)$ has $n - 1$ edges $T = (V, E)$ is a tree $\Rightarrow \lvert E\rvert = \lvert V\rvert - 1$
Lecture 13 Slide 12	A non-trivial tree has at least 2 vertices of degree 1
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
Theorem 10.5.4	If G is a connected graph with n vertices and $n -$ 1 edges, then G is a tree
Theorem 10.5.5	If G is a simple undirect graph, and there are two distinct paths from a vertex v to a different vertex w, then G contains a cycle
Rooted Tree	A tree in which there is one vertex that is distinguished from the others and is called the root.
Level of Vertex in Rooted Tree	The level of a vertex is the number of edges along the unique path between it and the root
Height of Rooted Tree	The height of a rooted tree is the maximum level of any vertex of the tree.
Child	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.
Parent	If w is a child of v, then v is called the parent of w,

Siblings	two distinct vertices that are both children of the same parent are called siblings.
Ascendent / Descendent	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.
Binary Tree	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.
Full Binary Tree	A full binary tree is a binary tree in which each parent has exactly two children.
Left/Right Subtree	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.
Theorem 10.6.1	T is full binary tree with k internal vertices $\Rightarrow T$ has $2k+1$ vertices and $k+1$ leaves
Theorem 10.6.2	$\forall h \in N, T$ is a binary tree with height h and t leaves $\Rightarrow t \leq 2^h, log_2 t \leq h$
Binary Tree Traversal	The process of visiting each node in a tree data structure exactly once in a systematic manner.
Breadth-First Search	Starts at the root and visits its adjacent vertices, and then moves to the next level.
Depth-First Search	Traverse subtrees by recursively calling itself
Pre-Order	In the form: RT_LT_R
In-Order	In the form: T_LRT_R
Post-Order	In the form: T_LT_RR
Spanning Tree	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	Every connected graph has a spanning tree. Any two spanning trees for a graph have the same number of edges.
Weighted Graph	A weighted graph is a graph for which each edge has an associated positive real number weight. $w(e)$ denotes the weight of e
Total Weight of Graph	The sum of the weights of all the edges, denoted by $w(G)$
Minimum Spanning Tree	A spanning tree that has the least possible total weight compared to all other spanning trees for the graph.
Kruskal's Algorithm for MST	Input: G [a connected weighted graph with n vertices] Algorithm: 1. Initialize T to have all the vertices of G and no edges. 2. Let E be the set of all edges of G, and let m = 0. 3. While (m < n – 1) 3a. Find an edge e in E of least weight. 3b. Delete e from E. 3c. If addition of e to the edge set of T does not produce a circuit, then add e to the edge set of T and set m = m + 1 End while Output: T [T is a minimum spanning tree for G]
Prim's Algorithm for MST	Input: G [a connected weighted graph with n vertices] Algorithm: 1. Pick a vertex v of G and let T be the graph with this vertex only. 2. Let V be the set of all vertices of G except v. 3. For i = 1 to n – 1 3a. Find an edge e of G such that (1) e connects T to one of the vertices in V, and (2) e has the least weight of all edges connecting T to a vertex in V. Let w be the endpoint of e that is in V. 3b. Add e and w to the edge and vertex sets of T, and delete w from V. Output: T [T is a minimum spanning tree for G]

Proven (Trees)	
Tutorial 11 Qn 6	Let $G = (V, E)$ be a simple undirected graph, then G is a tree $\Leftrightarrow$ There is exactly one path between every pair of vertices
Catalan's Number Sequence	A convolution recurrence $C_{n+2} = C_0C_n + C_1C_{n-1} + C_2C_{n-2} + \cdots C_kC_{n-k} + C_nC_0$ $C_n = \frac{1}{n+1}\binom{2n}{n} = 1,2,5,14,42,132$