CS1231S Mid Term Cheat Sheet

Ch-1 : Speaking Mathematically.

- In CS1231S, $\mathbb{N}$ includes 0.
- 0 is neither positive nor negative
- Theorem 4.4.6 : Triangle Inequality : $|x+y| \leq |x|+|y|$ for any $x, y \in \mathbb{R}$
- Theorem / Lemma 4.4.4 : for any $r \in \mathbb{R}$, $-|r| \leq r \leq |r|$
- Basic Properties of Integers

  Closure, Commutativity, Associativity, Distributivity, Trichotomy

  Trichotomy: Exactly one of the following is true: $x < y$, $x = y$ or $x > y$
- Even: An integer n is even if and only if n = twice some integer
- Odd: An integer n is odd if and only if $n = 2k+1$ for some $k \in \mathbb{Z}$
- 0 is even.
- You may assume that every integer is even or odd, but not both. (#1)
- Divisibility: If n and d are integers and $d \neq 0$,

  $d \mid n \iff \exists k \in \mathbb{Z}$ such that $n = dk$
- Rational No: A real number r is rational, iff it can be expressed as a quotient of 2 integers with a non-zero denominator.

  r is rational $\iff \exists a, b \in \mathbb{Z}$ s.t. $r = \frac{a}{b}$ and $b \neq 0$
- A number (real) that is not rational is irrational.
- A fraction $\frac{a}{b}$ $(b \neq 0)$ is said to be in lowest terms if the largest integer that divides both a and b is 1.
- You may assume that every rational can be reduced to a fraction in its lowest term (#2)
- Proposition 4.6.4 : For all integers n, if n^2 is even then n is even
- Theorem 4.7.1 : $\sqrt{2}$ is irrational
- Types of proofs : Direct proof, proof by construction, disproof by counterexample, proof by exhaustion, proof by contradiction, proof by contraposition

Ch-2: Propositional Logic

- A statement is a sentence that is true or false, but not both.

eg. $p \leftrightarrow q$ (p, q: statement variables) is not a statement because it is true for some values of p, q and false for others.

eg. $x+1 = 10$ not a statement. The truth value depends on x.

- Symbols: $\sim, \wedge, \vee, \rightarrow, \leftrightarrow, \equiv$
- $p \oplus q$ (or) p XOR q is defined as $(p \vee q) \wedge \sim(p \wedge q)$ (Exclusive OR)
- To show logical equivalence : (1) Truth table method
  (2) Algebraic method.

To disprove logical equivalence : (1) Truth table
(2) Counter example

- Tautology: Always true, regardless of the truth values of the individual statements substituted for its statement variables.
- Contradiction: Always false.
- Theorem 2.1.1

(1) Commutative Laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
(2) Associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
(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	$p \wedge \sim p \equiv \text{false}$	$p \vee \sim p \equiv \text{true}$
(6) Double Negative law	$\sim(\sim p) \equiv p$	
(7) Idempotent law	$p \wedge p \equiv p$	$p \vee p \equiv p$
(8) Universal Bound Law	$p \wedge \text{false} \equiv \text{false}$	$p \vee \text{true} \equiv \text{true}$
(9) De Morgan's Law	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
(10) Absorption Law	$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$
(11) Negation of true/false	$\sim \text{true} \equiv \text{false}$	$\sim \text{false} \equiv \text{true}$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Implication Law: $p \rightarrow q \equiv \sim p \vee q$

Note: $\sim(p \rightarrow q) \equiv \sim(\sim p \vee q) \equiv \sim(\sim p) \wedge \sim q$
$\equiv p \wedge \sim q$

↳ vacuously true / true by default

• Order of operations : $\sim$ (Highest priority)

$\wedge, \vee$ (co-equal in order)

$\rightarrow, \leftrightarrow$ (lowest priority)

eg. $p \vee q \wedge r$: Ambiguous expression!

Must use parantheses to distinguish $(p \vee q) \wedge r$ and $p \vee (q \wedge r)$

• Statement : $p \rightarrow q$ } logically equivalent

Contrapositive : $\sim q \rightarrow \sim p$ } logically equivalent

Converse : $q \rightarrow p$ } logically equivalent

Inverse : $\sim p \rightarrow \sim q$ } logically equivalent

No relation! cannot make any general conclusion.

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

• p only if q $\equiv \sim q \rightarrow \sim p \equiv p \rightarrow q$ (q is a necessary condition for p)

• p if q $\equiv q \rightarrow p$ (q is a sufficient condition for p)

$\therefore$ q is a necessary and sufficient condition for p $\equiv p \leftrightarrow q$

• An argument form is valid iff whenever statements are substituted that make all the premises true, the conclusion is also true.

To check validity, construct truth table showing truth values of all the premises and the conclusion. A row of the truth table in which all the premises are true is called a critical row.

(i) If $\exists$ critical row in which conclusion is false $\Rightarrow$ Argument form invalid.

(ii) If conclusion is true in every critical row $\Rightarrow$ Argument form valid.

• Another way to check validity : show that $(p_1 \wedge p_2 \wedge \cdots p_n) \rightarrow K$ is a tautology. (or just suppose the hypothesis & prove the conclusion)

p_1
p_2 } premises
$\vdots$
K → conclusion

• Syllogism: An argument form consisting of 2 premises and a conclusion.

• Modus ponens (Affirming the antecedent)

$p \rightarrow q$

p

$\therefore q$

Modus Tollens (Denying the consequent)

$p \rightarrow q$

$\sim q$

$\therefore \sim p$

First premise : Major , Second premise : Minor

- Other rules of Inference.

① Generalisation:	p	q
	$\therefore p \vee q$	$\therefore p \vee q$
② Specialisation: ("In particular")	$p \wedge q$	$p \wedge q$
	$\therefore p$	$\therefore q$
③ Elimination:	$p \vee q$	$p \vee q$
	$\sim q$	$\sim p$
	$\therefore p$	$\therefore q$

④ Transitivity:
$p \to q$
$q \to r$
$\therefore p \to r$
} Chain of implication

⑤ Proof by Division into cases:
$p \vee q$ — You know that p or q is true.
$p \to r$ — In either case, r must follow.
$q \to r$ — Therefore in general, r is true.
$\therefore r$

- Fallacies: Converse error : $q \to p \not\equiv p \to q$
  Inverse error : $\sim p \to \sim q \not\equiv p \to q$
- eg. If J.S. is a Singaporean, then he is a badminton player
  J.S. is a Singaporean
  $\therefore$ J.S. is a badminton player

The above argument form is valid (Modus ponens). But its major premise is false, and so is its conclusion.

- An argument is called sound iff it is valid (Argument form) and all its premises are true (Argument content).

- Contradiction Rule: $\sim p \to$ false
  $\therefore p$

Ch-3: Predicate Logic

- 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 by $\{x \in D \mid P(x)\}$
- Another way to obtain statements ~~for~~ from predicates is to add quantifiers. eg. $\forall p,\ p^2+1 \geq 0$ is a statement.
- Negation of $\forall$ is $\exists$ and vice versa
  eg. $\forall x\ \exists y\ (P(x) \rightarrow Q(x,y))$. Its negation is,
  $\exists x\ \forall y\ (P(x) \wedge \sim Q(x,y))$
- The statement $\forall x \in D\ (P(x) \rightarrow Q(x))$ is vacuously true or true by default if, and only if, $P(x)$ is false for every $x \in D$.
- Order of quantifiers matters when they are different ie, $\forall x\ \exists y (P(x) \wedge Q(y))$ is different from $\exists x\ \forall y\ (P(x) \wedge Q(y))$
- Universal instantiation: $\forall x \in D\ (P(x))$
  - $P(a)$ if $a \in D$
- Universal generalisation: $P(a)$ for every $a \in D$
  - $\forall x \in D (P(x))$

(The order is the order in which you pick the fixed values ∴ It matters)

- Existential instantiation: $\exists x \in D (P(x))$
  - $P(a)$ for some $a \in D$
- Existential generalisation: $P(a)$ for some $a \in D$
  - $\exists x \in D\ (P(x))$

eg. Nobody except John Loves Mary
: $Loves(John, Mary) \wedge \forall x\ (x \neq John \rightarrow \sim Loves(x, Mary))$

eg.

- n is prime: $\forall r, s \in \mathbb{Z}^+$, if $n = rs$ then either $(r=1$ and $s=n)$ or $(r=n$ and $s=1)$
- n is composite if $\exists r, s \in \mathbb{Z}^+$ s.t. $n = rs$ and $1 < r < n$ and $1 < s < n$

Note: Both prime and composite are only defined for $n > 1$ and $n \in \mathbb{Z}$
∴ 1 is neither prime nor composite

eg. $\forall x\ \exists y\ (Loves(x,y))$: You (∀) give me any person (x), I (∃) will find at least 1 person s.t. Loves (x,y)

∀ : Other person can choose any value (y), ∃ : Your job to find.

AZONE

- Proving Universal statements by 'Generalising from the generic particular'
  To show that every element in 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: Every integer is a rational number
- Theorem 4.2.2: The sum of any 2 rational no.s is rational
- Theorem 4.3.1 For all positive integers a and b, if $a|b$ then $a \leq b$
- Theorem 4.3.1 The only divisors of 1 are 1 and -1
- Theorem 4.3.3 For all integers a, b, c: if $a|b$ and $b|c$ then $a|c$
  (Transitivity of divisibility)
- Theorem 4.6.1: There is no greatest integer
- Proposition 4.6.4: For all integers n, if n^2 is even then n is even

Ch-5: Sets

- A set is an unordered collection of objects
  We use 'inclusion' for subset ie, A includes B
- In CS1231S, we use 'contains' for the membership relation, not subset.
- Roster Notation: $\{x_1, x_2 \cdots x_n\}$ or $\{x_1, x_2 \ldots\}$
- Set-builder notation: $\{x \in U \mid P(x)\}$ (Set of all $x \in U$ that make $P(x)$ true)
- Replacement notation: $\{t(x) : x \in A\}$ (Transform all $x \in A$ to $t(x)$)
- $A = B \iff \forall x (x \in A \iff x \in B)$ (Order and Repitition do not matter)
- Theorem 5.1.17: There exists a unique set with no element ie,
  → There is a set with no element (existence part: ≥ 1)
  → For all sets A, B, if both A and B have no element $A = B$ (Uniqueness: ≤ 1)
- $A \subseteq B \iff \forall x (x \in A \rightarrow x \in B) \equiv B \supseteq A$ (B 'includes' A)
- $A \subsetneq B \iff A \subseteq B \wedge A \neq B$ ie, A is a proper subset of B (strict inclusion)
- Power set of A: $P(A)$ → Set of all subsets of A
- If $|A| = n$, $|P(A)| = 2^n$, where $|\ |$ represents cardinality of a set.
  No. of distinct elements of set
- Sets of size 1 are called singletons
- Cartesian Product of $A \times B$ is defined as $\{(x, y) : x \in A \text{ and } y \in B\}$
- If A is a set, then $A^n = \underbrace{A \times A \times \cdots A}_{n\text{-many } A\text{'s}}$
- $|A \times B| = |A| \times |B|$

- Union : $A \cup B = \{x : x \in A \vee x \in B\}$
- Intersection : $A \cap B = \{x : x \in A \wedge x \in B\}$
- Complement : $A \setminus B = \{x : x \in A \wedge x \notin B\}$ (Complement of B in A)
- $\overline{B} = B^c = U \setminus B$ (where U is the universal set)
- Set Identities : Theorem 5.3.5

Identity law	$A \cup \emptyset = A$	$A \cap U = A$
Universal bound law	$A \cup U = U$	$A \cap \emptyset = \emptyset$
Idempotent law	$A \cup A = A$	$A \cap A = A$
Double complement law	$\overline{(\overline{A})} = A$	
Commutative law	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative law	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive law	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Absorption law	$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$
Complement law	$A \cup \overline{A} = U$	$A \cap \overline{A} = \emptyset$
Set difference law	$A \setminus B = A \cap \overline{B}$	
Top and Bottom laws	$\overline{\emptyset} = U$	$\overline{U} = \emptyset$
De Morgan's Laws	$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$	$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

- Use Truth table / Set Identities / element method to prove set equality.
- Two sets A, B are disjoint iff $A \cap B = \emptyset$
- Sets $A_1, A_2 \ldots A_n$ are pairwise disjoint or mutually disjoint iff $A_i \cap A_j = \emptyset$ for all distinct $i, j \in \{1, 2, \ldots n\}$
- Theorem 5.3.12
  (i) For disjoint sets A and B, $|A \cup B| = |A| + |B|$
  (ii) For pairwise disjoint sets $A_1, A_2 \ldots A_n$, $|A_1 \cup A_2 \cup \ldots A_n| = |A_1| + |A_2| + \ldots |A_n|$
- Theorem 5.3.13 (Inclusion-Exclusion Principle) : For all sets (finite) A and B, $|A \cup B| = |A| + |B| - |A \cap B|$

($|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$) → Note part of theorem
↳ Cannot use directly.

Ch-6 : Equivalence Relations.

- Call $\mathcal{C}$ a partition of set A iff
  (i) $\mathcal{C}$ is a set of which all elements are non-empty subsets of A.
  (ii) Every element of A is in exactly one element of $\mathcal{C}$

In other words, a set of mutually disjoint non-empty subsets of A whose union is A, is called a partition of A.

- Elements of a partition are called components of the partition.
  eg. $A = \{1,2,3\}$. One partition of set A is $\{\{1\},\{2,3\}\}$
- No. of partitions of set of size n : $B_n \rightarrow$ Bell number
  $B_0 = B_1 = 1$ and $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$

ie, 1, 1, 2, 5, 15, 52 . . .
B_0 B_1 B_2 B_3 B_4 B_5

- A relation from A to B is a subset of $A \times B$
  (No. of relations : $2^{|A||B|}$)
- A (binary) relation on a set A is a relation from A to A.
- Let A be a set and R be a relation on A
  (i) R is reflexive iff $\forall x \in A\,(xRx)$ (reflexive relation $\supseteq$ Identity Relation)
  (ii) R is symmetric iff $\forall x,y \in A\,(xRy \Rightarrow yRx)$
  (iii) R is transitive iff $\forall x,y,z \in A\,(xRy \wedge yRz \Rightarrow xRz)$

If R is reflexive, symmetric and transitive then it is an equivalence relation

- Proposition 6.2.16: Let $\mathcal{C}$ be a partition of set A. Denote by $\sim_{\mathcal{C}}$ the 'same-component relation' with respect to $\mathcal{C}$ ie, for all $x,y \in A$,
  $x \sim_{\mathcal{C}} y \Leftrightarrow$ x is in the same component of $\mathcal{C}$ as y
  $\Leftrightarrow x,y \in S$ for some $S \in \mathcal{C}$. It is an equivalence relation
- Congruence : 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 $k \in \mathbb{Z}$. Then, we write
  $a \equiv b \pmod n$

Note: $a \equiv b \pmod n \Leftrightarrow n \mid (a-b)$ [a and b leave the same remainder when divided by n]

- Proposition 6.3.4: Congruence-mod-n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$

• Equivalence classes: Let $\sim$ be an equivalence relation on set A. For each $x \in A$, the equivalence class of x with respect to $\sim$, denoted by $[x]_\sim$, is defined by $[x]_\sim = \{y \in A : x \sim y\}$
(ie, $[x]_\sim$ is the set of all elements of A that are $\sim$-related to x)

* • Lemma 6.4.4: Let $\sim$ be an equivalence relation on set A. TFAE for all $x, y \in A$: (i) $x \sim y$ (ii) $[x] = [y]$ (iii) $[x] \cap [y] \neq \emptyset$
(Equivalence classes are either equal or disjoint, ie, if you can prove that their intersection is non-empty, then they are the same class)

• 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 $\sim$ ie,
$A/\sim = \{[x]_\sim : x \in A\}$ → The quotient of A by $\sim$

• Theorem 6.4.9: Let $\sim$ be an equivalence relation on set A.
Then $A/\sim$ is a partition of A.

Ch-7: Modular Arithmetic and Partial orders.

• Another definition of partition $\mathcal{C}$: $\forall x \in A\ \exists! S \in \mathcal{C}\ (x \in S)$ $(\wedge \forall S \in \mathcal{C}(S \neq \emptyset))$

• Partition of A is a subset of the power set of A.

• A representative of an equivalence class is an element of the equivalence class

• The quotient $\mathbb{Z}/\sim_n$ where $\sim_n$ is the congruence-mod-n relation on $\mathbb{Z}$ is denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. Define addition and multiplication on $\mathbb{Z}_n$ as follows: whenever $[x], [y] \in \mathbb{Z}_n$, $[x] + [y] = [x+y]$ $[x] \cdot [y] = [x \cdot y]$ (Proposition 7.1.15 (They are well-defined for $\mathbb{Z}_n$))

These are well-defined iff they are equal for any representative we choose.
eg. If $[x_1] = [x_2]$ and $[y_1] = [y_2]$ but $[x_1] + [y_1] \neq [x_2] + [y_2]$ then addition is not well-defined.

eg. To show that $\cdot$ is well-defined for some quotient ($\mathbb{Z}/\sim$), we must show that whenever $[x_1], [x_2], [y_1], [y_2] \in \mathbb{Z}/\sim$
$[x_1] = [x_2] \wedge [y_1] = [y_2] \Rightarrow [x_1] \cdot [y_1] = [x_2] \cdot [y_2]$

To show that $+$ or $\cdot$ is not well-defined, 1 counterexample suffices.

- Let A, B be sets. A function or a map from A to B is an assignment to each element of A exactly one element of B. We write '$f: A \to B$'
Let $x \in A$. Then $f(x)$ denotes the element of B that f assigns x to.
We call $f(x)$ the image of x under f. If $y = f(x)$ then we say that f maps x to y, ie, $f: x \mapsto y$.
Here, A is the domain of f, and B is called the codomain of f.
- To show a function is not well-defined, we can show either of the following
(i) Some element of the domain is not assigned a value in the codomain.
eg. $f: \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{1}{x}$. Not well-defined $\because f(0) \notin \mathbb{R}$

(ii) Some element of the domain is assigned multiple values in the codomain
eg. $f: \mathbb{Z} \to \mathbb{Z}$, $f(x) = \pm x$ ($f(1) = 1$ and $f(1) = -1$)

- A relation R is antisymmetric iff $\forall x, y (xRy \wedge yRx \Rightarrow x = y)$
- Partial order and Total order
→ R is a (non-strict) partial order if R is reflexive, antisymmetric, transitive.
→ R is a (non-strict) total order if R is a partial order and
$\forall x, y \in A (xRy \vee yRx)$
(x and y are comparable)
(Any 2 elements must be comparable)
Hasse Diagram is always linear.
∴ A Total order is always a partial order
→ We say that the ordered pair (A, R) is a partially ordered set, or a poset, if R is a partial order on A.

eg:

- We use $\preccurlyeq$ to denote a partial order. Then, we write $x \prec y$ for $x \preccurlyeq y \wedge x \neq y$
- Let $\preccurlyeq$ be a partial order on set A. A Hasse diagram of $\preccurlyeq$ satisfies the following condition for all $x, y \in A$:
if $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then x is placed below y and there is a line joining x to y, else, no line joins x to y.
- A linear Hasse Diagram is a total order

- c is a minimal element if no $x \in A$ is strictly $\lesssim$-less than c, ie, $\forall x \in A\ (x \lesssim c \Rightarrow c = x)$ (Nothing is below c)
- c is a maximal element if no $x \in A$ is strictly $\lesssim$-bigger than c ie, $\forall x \in A\ (c \lesssim x \Rightarrow c = x)$ (Nothing is above c)
- c is the smallest element (or the minimum element) if all $x \in A$ are $\lesssim$-bigger than or equal to c ie, $\forall x \in A\ (c \lesssim x)$ (Everything is above c)
- c is the largest element (or the maximum element) if all $x \in A$ are $\lesssim$-less than or equal to c ie, $\forall x \in A\ (x \lesssim c)$ (Everything is below c)

Note: Smallest/Largest is a tighter definition than minimal/maximal ie,
if c is the smallest element, then c is a minimal element also.
If c is the largest element, then c is a maximal element also.

Proposition 7.4.4: Any smallest element is minimal.
Any largest element is maximal.

- Proposition 7.4.6: With respect to any partial order $\lesssim$ on a finite set $A \neq \emptyset$ one can find a minimal element
- Let A be a set and $\lesssim$ be a partial order on A. A linearization of $\lesssim$ is a total order $\lesssim^*$ on A such that
  $\forall x, y \in A\ (x \lesssim y \Rightarrow x \lesssim^* y)$ (go level by level in Hasse Diagram)
- Theorem 7.4.10: Every partial order $\lesssim$ has a linearization $\lesssim^*$
- A linearization of a partial order need not be unique. If there are several minimal elements (at any step in Kahn's algorithm), different choices give different linearizations.

In terms of graph theory, the topological sort of a directed acyclic graph need not be unique.

Some Extra Notes:

- The contrapositive of $\forall x (P(x) \to Q(x))$ is $\forall x (\sim Q(x) \to \sim P(x))$ and NOT, $\exists x (\sim Q(x) \to \sim P(x))$. i.e., the quantifier does not change.
- Properties of Real Numbers (Appendix A)

F4: Existence of Identity elements.
→ There exist 2 distinct real numbers, denoted by 0 and 1, such that for every real number 'a', $0+a = a+0 = a$, $1 \cdot a = a \cdot 1 = a$

F5: Existence of Additive Inverse
→ For every real number a, there is a real number, denoted by $-a$ and called the additive inverse of a s.t. $a+(-a) = (-a)+a = 0$

F6: Existence of Reciprocals.
→ For every real number $a \neq 0$ there exists a real number, denoted by $\frac{1}{a}$ and called the reciprocal of a, s.t. $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

T1: Cancellation Law for addition: $a+b = a+c \Rightarrow b = c$

~~T2~~ T3: $b-a = b+(-a)$

T4: $-(-a) = a$

T5: $a(b-c) = ab-ac$

T6: $0 \cdot a = a \cdot 0 = 0$

T7: Cancellation law for multiplication: $ab = ac$ and $a \neq 0 \Rightarrow b = c$

T9: $a \neq 0 \Rightarrow \frac{b}{a} = b \cdot a^{-1}$

T.10: $a \neq 0 \Rightarrow (a^{-1})^{-1} = a$

T11: Zero product property: If $ab = 0$ then $a = 0$ or $b = 0$

T12: Rule for multiplication with Negative Signs

$(-a)b = a(-b) = -(ab)$, $(-a)(-b) = ab$

and, $-\frac{a}{b} = \frac{-a}{b} = \frac{ab}{-b}$

T13: Equivalent Fractions Property

$\frac{a}{b} = \frac{ac}{bc}$ if $b \neq 0$ and $c \neq 0$

T14: Rule for addition of fractions: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, if $b \neq 0$ and $d \neq 0$

T15: Rule for multiplication of fractions: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ if $b \neq 0$ and $d \neq 0$

T16: Rule for division of fractions: $\frac{\left(\frac{a}{b}\right)}{\left(\frac{c}{d}\right)} = \frac{ad}{bc}$ if $b \neq 0$, $c \neq 0$ and $d \neq 0$

T17: Trichotomy Law: For arbitrary real numbers a and b, exactly one of the three relations $a < b$, $b < a$, or $a = b$ holds.

T18: Transitive Law: If $a < b$ and $b < c$ then $a < c$.

T19: If $a < b$ then $a + c < b + c$

T20: If $a < b$ and $c > 0$ then $ac < bc$

T21: If $a \neq 0$ then $a^2 > 0$

T22: $1 > 0$

T23: If $a < b$ and $c < 0$ then $ac > bc$

T24: If $a < b$ then $-a > -b$. In particular if $a < 0$ then $-a > 0$

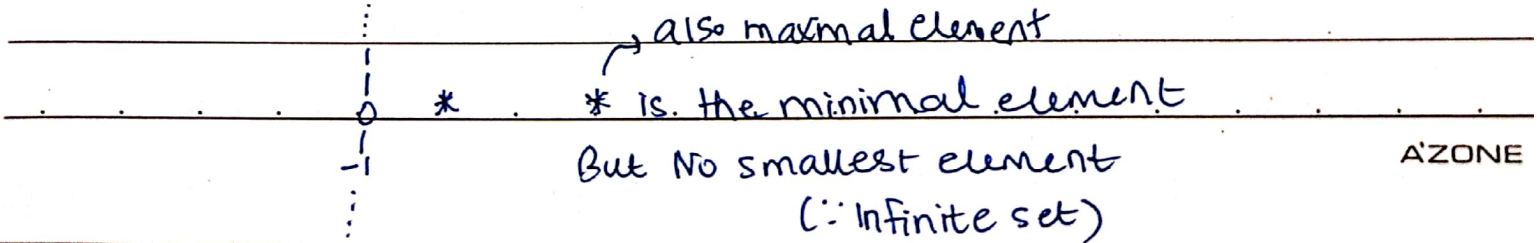
T25: If $ab > 0$ then both a and b are positive or both are negative.

T26: If $a < c$ and $b < d$ then $a + b < c + d$.

T27: If $0 < a < c$ and $0 < b < d$ then $0 < ab < cd$

Common Misconceptions Clarifications:

- A relation that is symmetric cannot be antisymmetric X
- A relation that is not symmetric must be antisymmetric X
- In a partially ordered set, any minimal element is smallest X
- In a partially ordered set, any smallest element is minimal ✓
- There can be 2 smallest elements in some partially ordered set X
- All finite non-empty partially ordered set has a smallest element X
- In a partially ordered set, if there is a smallest element, there must be exactly one minimal element ✓
- In a partially ordered set, if there is exactly one minimal element, then there is a smallest element X



eg. divisibility on $\mathbb{Z}^+$. 1 is smallest element

- An infinite set partial order relation can have a smallest element ✓
- If a partially ordered set does not have a smallest element, it must be an infinite set X

---

① Transitive closure: 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, $R^t \subseteq S$.

Similarly, we define reflexive closure and symmetric closure

② Theorem 8.3.4: The Partition Induced by an Equivalence Relation. If A is a set and R is an equivalence relation on A, then the distinct equivalence classes form a partition of A; ie, the union of the equivalence classes is all of A and the intersection of any 2 distinct classes is empty.

③ Theorem 8.4.1: Modular Equivalences

Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a-b)$ 2. $a \equiv b \pmod n$ 3. $a = b + kn$ for some $k \in \mathbb{Z}$
4. $a \bmod n = b \bmod n$ (ie, a and b have the same non-negative remainder when divided by n)

④ Given integers a and n with $n > 1$, the residue of a modulo n is $a \bmod n$, the non-negative remainder obtained when a is divided by n. The numbers $0, 1, 2 \ldots n-1$ are called a complete set of residues modulo n. To reduce a number modulo n means to set it equal to its residue modulo n.

(5) Theorem 8.4.3 Modular Arithmetic

Let a, b, c, d and n be integers ($n > 1$) and

$a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$

Then, 1. $(a+b) \equiv (c+d) \pmod{n}$

2. $(a-b) \equiv (c-d) \pmod{n}$

3. $ab \equiv cd \pmod{n}$

4. $a^m \equiv c^m \pmod{n}$ $\forall m \in \mathbb{Z}$

(6) An integer d is said to be a linear combination of integers a and b if, and only if, there exists s and $t \in \mathbb{Z}$ s.t. $as + bt = d$

(7) Integers a and b are relatively prime if, and only if, $\gcd(a,b) = 1$.

(8) Corollary 8.4.7 Existence of Inverses modulo n.

For all integers a and n if $\gcd(a,n) = 1$ then, there exists an integer s such that $as \equiv 1 \pmod{n}$. The integer s is called the inverse of a modulo n.

(9) Euclid's Lemma (Theorem 8.4.8.)

For all integers a, b, c if $\gcd(a,c) = 1$ and $a \mid bc$ then $a \mid b$.

(10) Theorem 8.4.10: Fermat Little Theorem

If p is any prime number and a is any integer such that $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

(11) Let A be a set that is partially ordered with respect to a relation $\preccurlyeq$. A subset B of A is called a chain, if and only if, the elements in each pair of elements in B is comparable. In other words, $a \preccurlyeq b$ or $b \preccurlyeq a$ $\forall a, b \in A$. The length of a chain is one less than the number of elements in the chain. Note that if B is a chain in A then, B is a totally ordered set w.r.t. the 'restriction' of $\preccurlyeq$ to B.

(12) Consider a partial order ($\preccurlyeq$) on a set A. Let $a, b \in A$. We say a, b are compatible if $\exists c \in A$ s.t. $a \preccurlyeq c$ and $b \preccurlyeq c$
Any 2 comparable elements are compatible (Proof: QS(a) Tut 5)

(13) Given partial order relations $\preccurlyeq$ and $\preccurlyeq'$ on a set A, $\preccurlyeq'$ is compatible with $\preccurlyeq$ if, and only if, $\forall a, b \in A$ if $a \preccurlyeq b$ then $a \preccurlyeq' b$
Note: The relation $\preccurlyeq'$ is a topological sorting for $\preccurlyeq$ if, and only if, $\preccurlyeq'$ is a total order that is compatible with $\preccurlyeq$

Some Results from Tutorial Qs / Impt Tut Qs.

Tut 1: 6(b): The bicenditional is transitive ie, $((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \rightarrow (p \leftrightarrow r)$
9: The product of any 2 odd integers is an odd integer

Tut 2: 'Nobody except John loves Mary' 2(d)
$Loves(John, Mary) \wedge \forall x ((x \neq John) \rightarrow \sim Loves(x, Mary))$

Tut 3: (7): $A \cap (B \setminus C) = (A \cap B) \setminus C$ $\forall$ sets A, B, C
(8): $(A \cup \bar{B}) \cap (\bar{A} \cup B) = (A \cap B) \cup (\bar{A} \cap \bar{B})$

Tut 4: Division Theorem / Quotient-Remainder Theorem.
- For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ such that, $n = dq + r$ and $0 \leq r < d$

(6) Fix $m, n \in \mathbb{Z}^+$. Let $\sim_m$ and $\sim_n$ denote respectively the congruence-mod-m and the congruence-mod-n relations on $\mathbb{Z}$. Then, $[x]_{\sim_m} \subseteq [y]_{\sim_n}$ for some $x, y \in \mathbb{Z}$ if and only if $n \mid m$

(7) Let $\mathcal{C}$ be a partition of a set A. Denote by $\sim$ the same-component relation w.r.t. $\mathcal{C}$ ie, $\forall x, y \in A$
$x \sim y \Leftrightarrow x$ is in the same component of $\mathcal{C}$ as y
$\Leftrightarrow x, y \in S$ for some $S \in \mathcal{C}$
- If $x \in S \in \mathcal{C}$ then $[x] = S$
- $A/\sim = \mathcal{C}$

Tut 5: (7) For a total order, all minimal elements are smallest

CS1231S Final Exam - cheat sheet (cont.)

- Everyone loves everyone except himself: $\forall x,y(x \neq y \leftrightarrow Loves(x,y))$
- Which of the following are true for all predicates $P(x), Q(x)$?

(a) $\forall x(P(x) \vee Q(x)) \Leftrightarrow \forall x P(x) \vee \forall x Q(x)$

(b) $\forall x (P(x) \wedge Q(x)) \Leftrightarrow \forall x P(x) \wedge \forall x Q(x)$

(c) $\exists x(P(x) \vee Q(x)) \Leftrightarrow \exists x P(x) \vee \exists x Q(x)$

(d) $\exists x(P(x) \wedge Q(x)) \Leftrightarrow \exists x P(x) \wedge \exists x Q(x)$

Midterm Exam Impt Qs:

1: To prove $\forall x \in D\ (P(x) \rightarrow Q(x))$, it suffices to prove

(a) $\exists x \in D\ (P(x) \wedge \sim Q(x)) \rightarrow \exists y \in D\ (P(y) \wedge \sim P(y))$

(b) $\forall x \in D\ (\sim Q(x) \rightarrow \sim P(x))$

(c) $\forall x \in D\ ((P(x) \wedge \sim Q(x)) \rightarrow (P(x) \wedge \sim P(x)))$

(d) $\exists x \in D\ (\sim Q(x) \rightarrow \sim P(x))$

Ans: (a, b, d)

2. Simplify: $(p \wedge q) \vee (q \wedge r) \vee (\sim p \wedge r)$

Note: Consensus Thm: $xy + x'z + yz = xy + x'z$

Ans: $(p \wedge q) \vee (q \wedge r) \vee (\sim p \wedge r)$

$\equiv (p \wedge q) \vee (q \wedge r) \vee (\sim p \wedge r) \vee$ false (Identity law)

$\equiv (p \wedge q) \vee (q \wedge r) \vee (\sim p \wedge r) \vee (p \wedge \sim p)$ (Negation law)

$\equiv (q \wedge p) \vee (q \wedge r) \vee (\sim p \wedge r) \vee (\sim p \wedge p)$ (Commutative law)

$\equiv (q \wedge (p \vee r)) \vee (\sim p \wedge (r \vee p))$ (distributive law)

$\equiv ((p \vee r) \wedge q) \vee ((p \vee r) \wedge \sim p)$ (Commutative law)

$\equiv (p \vee r) \wedge (q \vee \sim p)$ (distributive law)

Note: Define the graph of a function $f: A \rightarrow B$ to be $\{(x, f(x)) : x \in A\}$.

Then, a subset $S \subseteq A \times B$ is the graph of a function $A \rightarrow B$ if, and only if, $\forall x \in A\ \exists! y \in B\ (x,y) \in S$

: The following are equivalent: (1) R is symmetric ie, $\forall x,y \in A\ (xRy \rightarrow yRx)$

(2) $\forall x,y \in A\ (xRy \Leftrightarrow yRx)$

(3) $R = R^{-1}$

Topics Covered after Midterm.

Induction and Recursion.

- **Principle 8.1.1.** (Mathematical Induction)

Let $m \in \mathbb{Z}$. To prove that $\forall n \in \mathbb{Z}_{\geq m}$ $P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:

(base step) Show that $P(m)$ is true

(induction) show that $\forall k \in \mathbb{Z}_{\geq m}, (P(k) \Rightarrow P(k+1))$ is true.

↳ The assumption that $P(k)$ is true is called the induction hypothesis

↳ We call it 'induction on n' because n is the active variable in it.

- **Principle 8.2.1.** (Strong MI)

To prove that $\forall n \in \mathbb{Z}_{\geq m}$ $P(n)$ is true, where each $P(n)$ is a proposition, and $m \in \mathbb{Z}$, it suffices to choose some $l \in \mathbb{Z}_{\geq 0}$ and:

(base step) show that $P(m), P(m+1), \cdots P(m+l-1)$ are true;

(induction step) show that,

$$\forall k \in \mathbb{Z}_{\geq 0} \; (P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+l-1+k) \Rightarrow P(m+l+k)) \text{ is true.}$$

- **Theorem 8.2.10** (Well-Ordering Principle)

Every non-empty subset of $\mathbb{Z}_{\geq m}$ where $m \in \mathbb{Z}$ has a smallest element

- A sequence $a_0, a_1, a_2 \cdots$ is said to be recursively defined if the definition of a_n involves $a_0, a_1 \cdots, a_{n-1}$ for all but finitely many $n \in \mathbb{Z}_{\geq 0}$

- **Theorem 8.4.1.**

$\mathbb{Z}_{\geq 0}$ is the unique set with the following properties

(1) $0 \in \mathbb{Z}_{\geq 0}$ (base clause)

(2) If $x \in \mathbb{Z}_{\geq 0}$, then $x+1 \in \mathbb{Z}_{\geq 0}$ (recursion clause)

(3) Membership for $\mathbb{Z}_{\geq 0}$ can always be demonstrated by (finitely many) successive applications of the clauses above (minimality clause)

In general, a recursive definition of a set S consists of 3 types of clauses

(1) (base clause) founders are in S

(2) (Recursion clause) S is closed under the constructors, i.e. If f is a

constructor and $x \in S$, then $f(x) \in S$.

(3) Minimality clause

In other words, the members of S are precisely those objects that can be obtained from the founders by successively applying the constructors.

Structural Induction.

Let S be a recursively defined set. To prove that $\forall x \in S\ P(x)$ is true, where each $P(x)$ is a proposition, it suffices to:

(base step) show that $P(c)$ is true for every founder c

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

In other words, founders satisfy P and constructors preserve P.

Tutorial 6 Results

1. $\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \dots n^2 = \frac{n(n+1)(2n+1)}{6}$
2. If $x \in \mathbb{R}_{\geq -1}$, $1 + nx \leq (1+x)^n$ $\forall n \in \mathbb{Z}_{\geq 1}$
3. 3 divides $n^3 + 11n$ $\forall n \in \mathbb{Z}_{\geq 1}$
4. If a is an odd integer, 2^{n+2} divides $a^{2^n} - 1$
5. $\forall n \in \mathbb{Z}_{\geq 8}\ \exists x, y \in \mathbb{Z}_{\geq 0}\ (n = 3x + 5y)$
6. Every positive integer can be written as a sum of distinct non-negative powers of 2, ie,

$\forall n \in \mathbb{Z}_{\geq 1},\ \exists l \in \mathbb{Z}_{\geq 1},\ \exists i_1, i_2 \dots i_l \in \mathbb{Z}_{\geq 0}\ (i_1 < i_2 < \dots < i_l \wedge n = 2^{i_1} + 2^{i_2} + \dots 2^{i_l})$

Functions

- Let A, B be sets. A function or a map from A to B is an assignment to each element of A exactly one element of B. We write $f: A \to B$
  - ↳ If $x \in A$ and $f(x) = y$ for some $y \in B$, we write ~~$f \mapsto$~~ $f: x \mapsto y$
  - ↳ A: domain, B: codomain.
- A sequence $a_0, a_1, a_2, \ldots$ can be represented by the function a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $\forall n \in \mathbb{Z}_{\geq 0}\ a(n) = a_n$
  - ∴ any fn whose domain is $\mathbb{Z}_{\geq m}$ for some $m \in \mathbb{Z}$ represents a sequence.
- Note: In CS1231S, sequences are infinite & strings are finite.
- Let A be a set. A string or a word over A is an expression of the form $a_0 a_1 \ldots a_{\ell-1}$ where $\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_{\ell-1} \in A$. Here, ℓ is called the length of the string. Let A^* denote the set of all strings over A. The empty string, denoted ε, is the string of length 0.

- Def. 9.1.6 (Function Equality)
  Two functions $f: A \to B$ and $g: C \to D$ are equal if
  (1) $A = C$ and $B = D$ and, (2) $f(x) = g(x)$ for all $x \in A$

- Def 9.2.1 (Function Composition)
  Let $f: A \to B$ and $g: B \to C$. Then $g \circ f: A \to C$ s.t. $\forall x \in A\ (g \circ f)(x) = g(f(x))$
  - ↳ g composed with f / g circle f

  Note: for $g \circ f$ to be defined the codomain of f must be equal to the domain of g.

- Theorem 9.2.6 (Associativity of function composition)
  Let $f: A \to B$ and $g: B \to C$ and $h: C \to D$ then, $(h \circ g) \circ f = h \circ (g \circ f)$

- Let $f: A \to B$
  (1) If $X \subseteq A$, then $f(X) = \{f(x) : x \in X\}$ → Setwise image of X
  (2) If $Y \subseteq B$, then $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$ → Setwise pre-image of Y.

Caution: Let $f: A \to B$.

(1) If $X \subseteq A$ then $f(X)$ is a set. If $x \in A$, $f(x) \in B$.

(2) If $Y \subseteq B$ then $f^{-1}(Y)$ is a set. $f^{-1}(Y)$ exists even when the inverse function f^{-1} does not. If $y \in B$ and f^{-1} exists, then $f^{-1}(y) \in A$.

In general, we cannot make f^{-1} operate on elements instead of subsets.

- f is surjective/onto if $\forall y \in B \; \exists x \in A \; (y = f(x))$.
- f is injective/one-to-one if $\forall x_1, x_2 \in A \; (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$
- f is a bijection iff it is both an injection and surjection,
  $\forall y \in B \; \exists! x \in A \; (y = f(x))$

Note: To prove a function $f: A \to B$ is not surjective, prove that
$\exists y \in B \; \forall x \in A \; (y \neq f(x))$.

Similarly, to prove a function is not injective, $\exists x_1, x_2 \in A \; (f(x_1) = f(x_2) \wedge x_1 \neq x_2)$

- Let $f: A \to B$. Then $g: B \to A$ is an inverse of f if
  $\forall x \in A \; \forall y \in B \; (y = f(x) \iff x = g(y))$. $(g = f^{-1})$
- Proposition 9.3.17 (Uniqueness of Inverse)
  If g_1, g_2 are inverses of $f: A \to B$ then $g_1 = g_2$

- Theorem 9.3.19 : A function $f: A \to B$ is bijective if and only if it has an inverse

Tutorial 7 Results:

- The range or the image of $f: A \to B$ is defined as $\{f(x) : x \in A\}$
- for each $x \in \mathbb{Q}$, $\lfloor x \rfloor$: largest integer $n \leq x$
  $\lceil x \rceil$: smallest integer $n \geq x$
- (4) Let A be a set and $f: A \to A$. Suppose $g \circ f = g$ for all functions g with domain A. Then $f = id_A$
- (5) $f: B \to C$
  f is injective $\iff$ one can left-compose it with some fn to give an injection.

(6) f is surjective $\iff$ one can right-compose it with some fn to give a surjection.

5(a) f is injective $\Rightarrow$ g is injective $\Rightarrow$ g of injective

(b) $g \circ f$ injective $\rightarrow$ f injective

6. (a) f is surjective $\wedge$ h is surjective $\rightarrow$ $f \circ h$ is surjective

(b) $f \circ h$ is surjective $\rightarrow$ f is surjective.

8. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

In particular this shows that invertible functions are closed under composition ie, if f and g are invertible, so are $f \circ g$ and $g \circ f$.

9. $f: A \to B$. $X \subseteq A$, $Y \subseteq B$.

Then, $X \subseteq f^{-1}(f(X))$: always true. } Converse of both are not always true.

$f(f^{-1}(Y)) \subseteq Y$: always true. }

Cardinality.

- **Theorem 10.1.1** (Pigeonhole Principle – PHP)
Let A and B be finite sets. If there is an injection $f: A \to B$ then $|A| \leq |B|$

- **Theorem 10.1.2** (Dual Pigeonhole Principle)
Let A and B be finite sets. If there is a surjection, $f: A \to B$ then $|A| \geq |B|$

- **Theorem 10.1.3**
Let A and B be finite sets. Then there is a bijection $f: A \to B$ if and only if $|A| = |B|$.

- **Def 10.2.1.** (Cantor)
Set A is said to have the same cardinality as a set B if there is a bijection $A \to B$. In that case, we write $|A| = |B|$

- **Proposition 10.2.3** (Same cardinality is an Equivalence relation)
Let A, B, C be sets. then,

(1) $|A| = |A|$ (Reflexivity)

(2) $|A| = |B| \rightarrow |B| = |A|$ (Symmetry)

(3) $|A| = |B| \wedge |B| = |C| \rightarrow |A| = |C|$ (Transitivity)

- Def 10.3.1. (Cantor): A set is countable if it is finite or it has the same cardinality as $\mathbb{Z}_{\geq 0}$
- Note 10.3.4: An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2 \ldots \in B$ in which every element of B appears exactly once
- Lemma 10.3.5: An infinite set B is countable if and only if there is a sequence $c_0, c_1, c_2 \ldots$ in which every element of B appears.
- Proposition 10.3.6: Any subset A of a countable set B is countable
- Proposition 10.3.7: Every infinite set B has a countable infinite subset
- Proposition 10.4.1. Let A, B be countable infinite sets. Then $A \cup B$ is countable
- Theorem 10.4.2 (Cantor) $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is countable.
  In general, if A and B are countable sets, $A \times B$ is countable.
- Theorem 10.4.3 (Cantor)
  Let A be a countable infinite set, then $P(A)$ is not countable.

Examples of countable sets.

1. $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}$
2. $\mathbb{Q}$
3. Set of all strings over $\{s, u\}$
4. Set of all functions $f: A \rightarrow B$ where A and B are finite sets of integers.
5. Set of all computer programs.
6. Set of all strings over $\mathbb{Z}$
7. Set of all simple undirected graphs, whose vertex set is a finite subset of $\mathbb{Z}$.

Examples of uncountable sets.

1. $\mathbb{R}$, $\mathbb{C}$
2. Set of all sequences over $\{0, 1\}$
3. Set of all partitions of $\mathbb{Z}$
4. Set of all partial orders on $\mathbb{Z}$
5. Set of all functions $\mathbb{Z} \rightarrow \mathbb{Z}$

Tutorial & Results.

(1) Let $n \in \mathbb{Z}^+$. Let $[a], [b] \in \mathbb{Z}_n$. Then $|[a]| = |[b]|$

(2) If B is a countable infinite set and C is finite, $B \cup C$ is countable.

(4) A set B is infinite if and only if $\exists A \subsetneq B$ s.t. $|A| = |B|$

(5) Let S_i be a countable set for each $i \in \mathbb{Z}_{\geq 0}$. Then, $\bigcup_{i \in \mathbb{Z}_{\geq 0}} S_i$ is countable.

(7) For each $n \in \mathbb{Z}_{\geq 0}$, $F_n = \{X \in P(\mathbb{Z}_{\geq 0}) : |X| = n\}$. Let $F = \bigcup_{n \in \mathbb{Z}_{\geq 0}} F_n$

(a) F_n is countable for every $n \in \mathbb{Z}_{\geq 1}$.

(b) F is countable ie,

The set of all finite subsets of $\mathbb{Z}_{\geq 0}$ is countable.

(9) $A = \{x \in \mathbb{R} : 0 \leq x < 1\}$. A is uncountable.

Notation: $P_w(A) = \{S : S \subseteq A \text{ and } S \text{ is finite}\}$

↳ The set of all finite subsets of A.

If B is a countable set then $P_w(B)$ is countable → fact (I) Assignment 2

Counting.

- Sample space is the set of all possible outcomes of a random process. An event is a subset of a sample space.

- Theorem 9.1.1. (No. of elements in a list)
If m and n are integers ($m \leq n$) then there are $n - m + 1$ integers from m to n inclusive.

- Theorem 9.2.1 (Multiplication/Product Rule)
If an operation consists of k steps and the first step can be performed in n_1 ways, the second step in n_2 ways (regardless of the first step), ..., the entire operation can be performed in $n_1 \times n_2 \times \ldots \times n_k$ ways.

- Thm 5.2.4: $|P(A)| = 2^{|A|}$

- Thm 9.2.2 : No. of permutations of a set with n distinct elements (without repitions) is $n!$
- Thm 9.2.3 : $P(n,r) = \frac{n!}{(n-r)!} = n(n-1)(n-2)\cdots(n-r+1)$
- Thm 9.3.1: Suppose a finite set A equals the union of K distinct mutually disjoint subsets $A_1, A_2, \ldots A_K$ then
$|A| = |A_1| + |A_2| + \cdots |A_K|$ (Addition Rule)
- Thm 9.3.2 (Difference Rule)
If A is a finite set and $B \subseteq A$ then $|A \setminus B| = |A| - |B|$
ie, $P(\bar{A}) = 1 - P(A)$

- Thm 9.3.3 (Inclusion/Exclusion Rule)
$|A \cup B| = |A| + |B| - |A \cap B|$
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
In general,
1. Include the cardinalities of sets.
2. Exclude the cardinalities of pairwise intersections.
3. Include the cardinalities of triplewise intersections
⋮
Continue until the cardinality of the n-tuple wise intersection is included (if n is odd) or excluded (if n is even)
↳ Dirichlet box/drawer principle.
- PHP: A function from one finite set to a smaller finite set cannot be one-to-one. ie, there must be at least 2 elements in the domain that have the same image in the codomain.
- Generalised PHP
For any fn f from a finite set X with n elements to a finite set Y with m elements and for any positive integer $K < \frac{n}{m}$, there is some $y \in Y$ such that y is the image of at least K+1 distinct elements of X.
(given n pigeons and m pigeonholes, there is a pigeonhole with (at least) $\lceil \frac{n}{m} \rceil$ pigeons)

- Contrapositive form of PHP:
For any function $f: X \to Y$ where $|X|=n$, $|Y|=m$ and for any positive integer $k \leq \frac{n}{m}$ if for each $y \in Y$ $f^{-1}(\{y\})$ has at most k elements, then X has atmost km elements ie, $n \leq km$

- $\binom{n}{r} = \frac{n!}{(n-r)!\,r!} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdots r}$
↳ No. of subsets of a set with n elements that contain r elements ($r \leq n$)

- Thm 9.5.2 (Permutations with sets of indistinguishable objects)
Suppose a collection consists of n objects where,
r_1 objects of type 1 are indistinguishable from each other,
r_2 objects of type 2 " " "
⋮
r_k objects of type k " " "
then, number of permutations of n objects $= \frac{n!}{r_1!\, r_2! \cdots r_k!}$

- r-combinations with repitions allowed. ☆
→ Multiset: A multiset of size r chosen from a set X of n elements is an unordered selection of elements taken from X with repitition allowed.
∴ Thm 9.6.1: No. of multisets of size r that can be selected from a set n elements is $\binom{n+r-1}{r}$.

This equals the no. of ways r objects can be selected from n categories of objects with repititions allowed.

	Order matters.	Order does not matter.
Repitition allowed	n^k	$\binom{n+r-1}{r}$
Repitition not allowed	$P(n,k)$	$\binom{n}{r}$

Choosing k/r elements from n objects ↗

- Pascal's formula: $\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r}$
- Example 8: $\binom{n}{r} = \binom{n}{n-r}$
- Example 10: $k \cdot \binom{n}{k} = n\binom{n-1}{k-1}$
- Example 11: $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots \binom{n}{n} = 2^n$
- Thm 9.7.2 (Binomial Theorem)

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \cdots \binom{n}{n-1} ab^{n-1} + b^n$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

- Expected Value.

Suppose the possible outcomes of an expt are real numbers $a_1, a_2 \cdots a_n$ which occur with probabilities $p_1, p_2, \ldots, p_n$ respectively. The expected value of the expt is,

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + \cdots + a_n p_n$$

- Linearity of Expectation.

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 and Y (which may be dependent),

$$E[X+Y] = E[X] + E[Y]$$

More generally, for random variables $X_1, X_2, \ldots X_n$ and constants $c_1, c_2, \ldots, c_n$,

$$E\left[\sum_{i=1}^{n} c_i X_i\right] = \sum_{i=1}^{n} (c_i E[X_i])$$

- Conditional Probability: $P(A|B) = \frac{P(A \cap B)}{P(B)}$

- Total probability.
If $E_1, E_2 \dots E_K$ are mutually exclusive and exhaustive events and A is any event then,

$$P(A) = \sum_{i=1}^{K} P(E_i) \cdot P(A|E_i) = \sum_{i=1}^{K} P(A \cap E_i)$$

$$= P(E_1) \cdot P(A|E_1) + P(E_2) \cdot P(A|E_2) + \dots + P(E_K) \cdot P(A|E_K)$$

- Bayes' Theorem. (Probability of "causes")
Suppose $E_1, E_2, \dots, E_K$ are mutually disjoint exhaustive events and A is an event in the sample space then, for any $1 \le i \le K$,

$$P(E_i|A) = \frac{P(E_i) \cdot P(A|E_i)}{P(E_1) \cdot P(A|E_1) + P(E_2) \cdot P(A|E_2) + \dots + P(E_K) \cdot P(A|E_K)}$$

Note: False +ve : Result indicates +ve but person does not have disease
False -ve: Result indicates -ve but person has disease

- Independent Events.
2 events A and B are independent if and only if $P(A \cap B) = P(A) \cdot P(B)$
Note: $P(A|B) = P(A)$, $P(B|A) = P(B)$

- Pairwise Independent and Mutually Independent.
→ A, B, C are pairwise independent iff
$P(A \cap B) = P(A) \cdot P(B)$ and $P(B \cap C) = P(B) \cdot P(C)$ and $P(A \cap C) = P(A) \cdot P(C)$
→ A, B, C are mutually independent iff A, B, C are pairwise independent and, $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$.

In general,
events $A_1, A_2, \dots A_n$ 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.
In particular, $P(A_1 \cap A_2 \cap \dots \cap A_n) = P(A_1) \cdot P(A_2) \dots P(A_n)$

Tutorial 9 and 10 Results.

- **Circular permutations.** (without reflection)
  - ↳ Arranging n objects around a circle : $(n-1)!$
    (because of rotational symmetry ∵ when you put the first object, all positions are equivalent ∴ no choice for first obj)
  - ↳ How many permutations of n objects in a circle if both reflection and rotation are allowed? $\frac{(n-1)!}{2}$
    (eg. How many necklaces with n beads?)

- No. of injective functions from $A \to B$ where $|A|=a$, $|B|=b$, $a \leq b$
  $= P(b, a)$
- No. of surjective functions from $A \to B$ where $|A|=a$, $|B|=b$, $a \geq b$ is $S(a,b) = \sum_{i=1}^{b} (-1)^{b-i} \binom{b}{i} i^a$
- No. of reflexive relations on A (with $|A|=n$), $= 2^{n^2-n}$
- No. of symmetric relations on A ($|A|=n$) $= 2^{\frac{n^2-n}{2}} \cdot 2^n = 2^{\frac{n^2+n}{2}}$

Graphs and Trees.

- An undirected graph $G=(V, E)$ where
  - → $V = \{v_1, v_2, \ldots, v_K\}$: set of vertices (or nodes) in G
  - → $E = \{e_1, e_2, \ldots, e_K\}$: set of edges (undirected) in G.
  - → An undirected edge e connecting v_i and v_j is denoted by $e = \{v_i, v_j\}$
  - ↳ $V \neq \phi$
  - ↳ directed edge e connecting v_i to v_j is $e = (v_i, v_j)$

- **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.
  - ↳ Vertex colouring of a graph is an assignment of colours to vertices so that no 2 adjacent vertices have the same colour.

- **Simple Graph**: Undirected graph, does not have loops, parallel edges.
- **Complete graph**: K_n : Simple graph with n vertices and exactly 1 edge connecting each pair of distinct vertices.
  - ↳ K_n has $\binom{n}{2}$ edges.

- **Bipartite Graph** (Bigraph): simple graph whose vertices can be divided into 2 disjoint sets U and V such that every edge connects a vertex in U to one in V.
- **Complete Bipartite Graph** : $K_{m,n}$ has mn edges. — each of the m vertices is connected to n vertices.

- **Subgraph of a graph.**

A graph H is a subgraph of G iff 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.

- $deg(v)$ → No. of edges incident on v, with loops counted twice.
- $indegree(v)$ → No. of incoming edges on v ($deg^-(v)$)
- $outdegree(v)$ → No. of outgoing edges from v ($deg^+(v)$)

- **Thm 10.1.1.** (Euler's Handshake Theorem)
  Total degree of graph = 2 × (No. of edges in the graph)

- → ∴ Total degree of a graph is even ∴ Corollary 10.1.2
  → 'In any graph, there are an even number of vertices of odd degree' : Proposition 10.1.3

$$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = |E|$$ (Total indegree/outdegree of a directed graph need not be even)

- A walk from v to w is a finite alternating sequence of adjacent vertices and edges of G ie, $v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$ for $v_0 = v$, $v_n = w$ and $\forall i \in \{0, 1, 2 \cdots n\}$, v_{i-1} and v_i are the endpoints of edge e_i. The no. of edges, n, is the length of the walk.
- A 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 repeated edges.
- A path from v to w is a trail that does not contain a repeated vertex
- A closed walk is a walk that starts and ends at the same vertex.
- A circuit/cycle is a closed walk that does not contain a repeated edge.
- A simple circuit/cycle is a circuit that does not have any other repeated vertex except the first and the last.
- An undirected graph is cyclic if it contains a loop or a cycle; otherwise, it is acyclic.

- Two vertices v and w of a graph $G = (V, E)$ are connected iff there is a walk from v to w.
The graph G is connected iff $\forall v, w \in V$, $\exists$ walk from v to w

Lemma 10.2.1.
Let G be a graph
(a) If G is connected, any 2 distinct vertices of G can be joined by a path
(b) 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.
(c) If G is connected and G contains a circuit then an edge of the circuit can be removed without disconnecting G.

- A connected component of a graph is a connected subgraph of largest possible size.

A graph H is a connected component of 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.

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

An Eulerian graph is a graph that contains an Euler circuit

- Thm 10.2.2.

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

Contrapositive: If some vertex of a graph has odd degree (or deg = 0) then the graph does not have an Euler circuit.

- Thm 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.

- Thm 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.

- Euler Trail.

Let G be a graph, and let v and w be 2 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.

- Corollary 10.2.5.

Let G be a graph, and let v and w be 2 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

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

A Hamiltonian 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.

- Thm 10.3.2.

If a graph G has vertices $v_1, v_2 \cdots, v_m$ and A is the adjacency matrix of G, then for each positive integer n and for all integers $i, j = 1, 2, \cdots m$ the $(i,j)^{th}$ entry of A^n = the number of walks of length n from v_i to v_j.

Isomorphic Graphs.

Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be 2 graphs.

→ G is isomorphic to G', denoted $G \cong G'$ iff there exists bijections $g: V_G \to V_{G'}$ and $h: E_G \to E_{G'}$ 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 $\iff$ g(v) is an endpoint of h(e)

→ $G \cong G'$ iff $\exists$ permutation $\pi: V_G \to V_{G'}$ such that

$\{u, v\} \in E_G \iff \{\pi(u), \pi(v)\} \in E_{G'}$.

- Thm 10.4.1: Graph isomorphism is an equivalence relation on the set of all graphs.

- A planar graph is a graph that can be drawn on a plane (2D) without edges crossing.

- Kuratowski's Thm
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: $f = e - v + 2$ or in other words, ~~v + e = f~~ .
$$\boxed{v + f - e = 2}$$

- A graph is said to be circuit-free if and only if it has no circuits.
A graph is called a tree iff 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 deg = 1

- Let T be a tree. If T has only one or 2 vertices, then each is called a terminal vertex (or leaf). If T has ≥ 3 vertices, then a vertex of deg = 1 in T is called a terminal vertex (or leaf) and a vertex of deg > 1 in T is called an internal vertex.

- Thm 10.5.2. Any tree with n-vertices has n-1 edges.

- 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.

- **Thm 10.5.4.**

If G is a connected graph with n vertices and n-1 edges, then G is a tree

- 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 a unique path between it and the root
- The height of a rooted tree is the maximum level of any vertex of the tree
- The children of v are all those vertices that are adjacent to v and are one level farther from the root than v.
- If w is a child of v, then v is called the parent of w and 2 distinct vertices that are both children of the same parent are called siblings.
- Given 2 distinct vertices v and w, if v lies on the unique path b/w w and the root then v is an ancestor of w and w is a descendent of v.

- A binary tree is a rooted tree in which every parent has at most 2 children. Each child is designated either a left child or a right child (but not both), and every parent has at most 1 left child and one right child.

A full binary tree is a binary tree in which each parent has exactly 2 children.

- Thm 10.6.1. (Full BT theorem)

If T is a full binary tree with K internal vertices, then T has a total of 2K+1 vertices and has K+1 leaves (terminal vertices)

- Thm 10.6.2

For non-negative integers h, if T is a binary tree with ~~hight~~ height h and t terminal vertices (leaves) then, $t \leq 2^h$

Equivalently, $\log_2 t \leq h$

Tree Traversal

BFS. DFS

Pre-order	In order	Post-order
Print, Left, Right	Left, Print, Right	Left, Right, Print

- 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 2 spanning trees for a graph have the same number of edges.

- A minimum spanning tree (MST) ~~is a graph for which each edge~~ for a connected weighted graph is a spanning tree that has least possible total weight compared to all other spanning trees for the graph

Algorithms to find MST: (1) Kruskal's

(2) Prim's

- If G is a simple graph, the complement of G, denoted $\bar{G}$, contains all the vertices of G, and 2 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.

- A self-complementary graph is isomorphic with its complement
- A simple circuit (cycle) of length 3 is called a triangle.

Results from Tutorial 11.

(1) No. of self-complementary graphs with
(a) 4 vertices : 1 (b) 5 vertices : 2

(2) If G is a simple graph with n vertices where every vertex has degree at least $\lfloor \frac{n}{2} \rfloor$, G is connected.

(4) Every simple graph with ≥ 2 vertices has 2 vertices of same degree

(5) For any simple graph G with 6 vertices, G, or $\bar{G}$ contains a triangle.

(7) Pile of stones question ans: $\binom{n}{2}$

(8) No. of binary trees with in-order traversal: A, B, C, D is $5+2+2+5$

Results from Past Year Papers. (and Quizes)

20/21 Sem 1

(7) If $\bigcap_{i=1}^{n} R_i$ is reflexive, then each R_i is reflexive.
The same is not true for symmetry and transitivity.

(8) $(a,b)\ R\ (c,d) \Leftrightarrow ab \leq cd$
→ Reflexive, not symmetric, not antisymmetric, transitive.

(9) If x is a smallest element, then x is minimal.
If there is a ~~unique~~ smallest element, then there is a unique smallest element.

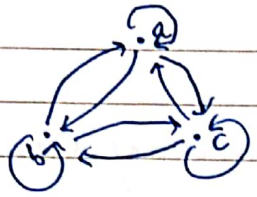
(13) The following are true for all predicates ~~on~~ P(x) on a non-empty set D,
(i) $\forall x \in D(P(x)) \rightarrow \exists x \in D(P(x))$
(ii) $(\exists x \in D(P(x)) \rightarrow \forall x \in D(P(x)))$ if $|D| = 1$
(iii) $(\forall x \in D(P(x)) \rightarrow \forall x \in E(P(x)))$ if $E \subseteq D$

(20) Out of 8 scrabble tiles 'I', 'C', 'A', 'N', 'D', 'O', 'I', 'T'
(i) how many ways can you select 4 tiles so that there are no duplicate letters : ${}^6C_2$ (the 2 I's are fixed)
(ii) No duplicate letters : ${}^7C_4$ (just remove 1 of the I's)
: ${}^8C_4 - {}^6C_2$ (if 2 I's are distinguishable)

(29(d) Assume no ll^el edges in a graph. (4)

(i) How many directed graphs on 3 vertices a, b, c are there: $2^9 = 512$

(ii) How many directed graphs on 3 vertices a, b, c with at least one loop are there: $2^9 - 2^6$ (All possible graphs − graphs with no loops)



(f) 21 students took an exam & their scores sum to 200. If the scores are non-negative integers, prove that there are 2 students with the same score. → PHP.

(21)(b) Suppose a self-complementary simple undirected graph G has n vertices, how many edges does G have? $\frac{\binom{n}{2}}{2}$

Note: $G \cup \bar{G} = K_n$

(i) There is no self-complementary graph with 4K+2 vertices.

→ because $\frac{(4k+2)(4k+1)}{2 \cdot 4}$ is not an integer. ↳ or even 4K+3

20/21 Sem 2.

(3) For a set A and function $f: A \to A$, define

$$C_f = \{ f^{-1}(\{y\}) : y \in A \text{ and } f(y) = y \}$$

Then the following are true for all sets A and all functions $f: A \to A$

(i) If $f \circ f = f$, then C_f is a partition of A.

(ii) If C_f is a partition of A, then $f \circ f = f$

Recall: to prove that C_0 is a partition of a set A, it suffices to

(0) Show that $\forall S \in C_0, S \neq \phi$

(1) $\forall S_1, S_2 \in C_0 \; (S_1 \neq S_2 \to S_1 \cap S_2 = \phi)$ (or) $S_1 \cap S_2 \neq \phi \to S_1 = S_2$

(2) $S_1 \cup S_2 \cup \ldots \cup S_K = A$ if there are K distinct components.

(4) For all functions $f: A \to B$ and all finite subsets $X \subseteq A$,
$|f(X)| \leq |X|$ (assuming $f(X)$ is finite)
→ However for $|f^{-1}(Y)|$ we cannot make any conclusion in general

(8) Define $f: P(\mathbb{Z}_{\geq 0}) \setminus \{\phi\} \to \mathbb{Z}_{\geq 0}$ by setting $f(S)$ to be the smallest element of S whenever $S \in P(\mathbb{Z}_{\geq 0}) \setminus \{\phi\}$. Then,
(i) f does not have an inverse.
(ii) $f^{-1}(\{n\})$ is uncountable for some $n \in \mathbb{Z}_{\geq 0}$

(13) Recall that $f = id_A \iff \forall g$ is a function, $g \circ f = g$. $g: A \to ?$
* Alternative definitions of id_A:
(i) $f = id_A \iff g \circ f = g$ is for all injective functions g with domain A.
(ii) $f = id_A \iff g \circ f = g$ for all surjective functions g with domain A
(iii) $f = id_A \iff g \circ f = g$ for all bijective functions g with domain A
(iv) $f = id_A \iff id_A \circ f = id_A$
(v) $f = id_A \iff g \circ f = g$ for some bijection g with domain A

(14)

Countable.	Uncountable.
→ Set of all strings over $\mathbb{Z}$	→ Set of all partitions of $\mathbb{Z}$
→ Set of all simple undirected graphs whose vertex is a finite subset of $\mathbb{Z}$	→ Set of all partial orders on $\mathbb{Z}$
	→ Set of all functions $\mathbb{Z} \to \mathbb{Z}$
	(v) Set of all functions $\mathbb{Z} \to \{0,1\}$

(19) Let A be a set. Let S be the set of all functions $\{0,1\} \to A$ ie,
$S = \{\alpha : \alpha : \{0,1\} \to A\}$
Then, $|S| = |A^2|$ acc. to Cantor's definition of same cardinality.

Then, (1) The set of all functions from $\{0,1\} \to \mathbb{Z}_{\geq 0}$ is countable.
(2) The set of all functions from any finite set (fixed) to any countable set (fixed) is countable
$\because |\mathbb{Z}_{\geq 0}| = |\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}| \times = |\mathbb{Z}_{\geq 0} \times \ldots \times \mathbb{Z}_{\geq 0}|$

2019/20 Sem 1.

(4) For all sets A, B, C: $A \times (B \cup C) = (A \times B) \cup (A \times C)$

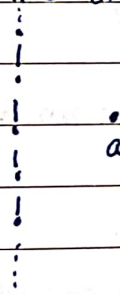
$A \times (B \cap C) = (A \times B) \cap (A \times C)$

(8) If $R^{\star}$ is reflexive then R^{-1} is reflexive
If R is symmetric then R^{-1} is symmetric
If R is transitive then R^{-1} is transitive
} Reversing the direction of arrows does not affect reflexivity, symmetry, transitivity.

(9) For all relations R and S on $\mathbb{Z}$, if $R \subseteq S$ and S is anti-symmetric, then R is antisymmetric. (ie, antisymmetry is inherited downwards)
→ This is not true for reflexivity, symmetry or transitivity

(10) The statement 'If whenever $x \in A$ is a minimal element, we have $x = a$ then a is the smallest element' depends on A and $\leq$.

eg.



Only 1 minimal element $\not\Rightarrow$ It is smallest.

(15) The maximum number of edges that a bipartite graph can have, if it has n vertices is, $\left\lfloor \frac{n^2-1}{4} \right\rfloor$

Note: How many ways can n people sit around a table : $(n-1)!$

How many necklaces can be made with n distinct beads : $\frac{(n-1)!}{2}$
(accounting for reflection symmetry also)

How many ways can $n-K$ people sit around a circular table with n chairs : ~~K~~ $\frac{(n-1)!}{K!}$

• Let R be a relation from $A \to B$ and S be a relation from $B \to C$ then $S \circ R = \{(x,z) \in A \times C : \exists y \in B ((x,y) \in R \wedge (y,z) \in S)\}$

Q. Given a fair coin what is the ~~probability~~ expected number of coin tosses to get 5 consecutive heads?

Ans: Solution 1: Let E be the expected no. of tosses. Then,

(1) If we get tail (with probability = $\frac{1}{2}$), expected value = E+1

(2) If we get HT (with probability = $\frac{1}{4}$), expected value = E+2

(3) If we get HHT (with probability = $\frac{1}{8}$), expected value = E+3

(4) If we get HHHT (with probability = $\frac{1}{16}$), expected value = E+4

(5) If we get HHHHT (with probability $\frac{1}{32}$), expected value = E+5

(6) If we get HHHHH (with p = $\frac{1}{32}$), expected value = 5

Observe that these are the only possible outcomes, (as soon as you get a tail, you reset the counter and start again)

$$\therefore E = \frac{1}{2}(E+1) + \frac{1}{4}(E+2) + \frac{1}{8}(E+3) + \frac{1}{16}(E+4) + \frac{1}{32}(E+5) + \frac{1}{32} \times 5$$

$$\therefore E = 62.$$

In general, expected number of tosses to get n consecutive heads, $2(2^n - 1)$

Even more generally, if the probability of an event (X) occuring is 'p' then the expected number of events to get 'n' consecutive event X's is given by, $\mu = \frac{p^{-n} - 1}{1-p}$

Soln 2: After getting (n-1) heads in a row,

Case 1: If you get a head, then $E_n = E_{n-1} + 1$

Case 2: If you get a tail, then, $E_n = (E_{n-1} + 1) + E_n$.

So, $E_n = \frac{1}{2}(E_{n-1} + 1) + \frac{1}{2}(E_{n-1} + 1 + E_n)$ and $E_0 = 0$

$E_1 = 2$

$$E_n = 2E_{n-1} + 2$$

Notes.

- A chordless cycle in a graph (also called a hole or an induced cycle) is a cycle such that no 2 vertices of the cycle are connected by an edge that does not itself belong to the cycle.

- Lemma: If G and H are isomorphic, then G and H have to satisfy the following: (1) G and H have same number of vertices
  (2) G and H have same number of edges.
  (3) G and H have the same degree sequence.
  (4) G and H have the same no. of connected components.
  (5) G and H have the same no. of chordless cycle of a fixed length.

We call any of the above properties of a graph invariant.

Caution: The above list of invariants is not complete ie, there exist non-isomorphic graphs which satisfy all the above conditions.

- Subdivision of a graph G (also known as expansion)
  ↳ The graph resulting from the subdivisions of edges in G.
  ↳ The subdivision of some edge e with endpoints $\{u, v\}$ yields a graph containing one new vertex w, and an edge set replacing e by 2 new edges $\{u, w\}$ and $\{w, v\}$

- Subdividing a graph preserves planarity.

- 2 graphs are said to be homeomorphic if both can be obtained from the same graph by subdivisions of edges ie, G and H are homeomorphic if there is a graph isomorphism from some subdivision of G to some subdivision of H.

- f is the inverse of g if, and only if, $f \circ g = g \circ f = id$

- A relation R is transitive $\iff R \circ R \subseteq R$

- If A is an infinite set and B is a finite set, then $A \setminus B$ is infinite

Results from Assignment 2.

2(b). Let $g : A \to B$ such that $|g(X)| \geq |X|$ for all finite subsets $X \subseteq A$.
Then g is injective.

(3) facts

(A) For all sets A and S, $S \subseteq A \Rightarrow S \setminus A = \phi$

(B) For all sets A, S and U, if $S \subseteq A \cup U$, then $S \setminus A \subseteq U \setminus A$

(C) $S = (S \cap A) \cup (S \setminus A)$

(D) $X \subseteq U$ and $Y \subseteq U$ then $X \cup Y \subseteq U$

(E) $X \subseteq A$ and $Y \subseteq U \setminus A \Rightarrow (X \cup Y) \setminus A = Y$

(F) $X_1, X_2 \subseteq A$ and $Y_1, Y_2 \subseteq U \setminus A$, if $X_1 \cup Y_1 = X_2 \cup Y_2$ then $X_1 = X_2$ and $Y_1 = Y_2$

(G) $U \setminus A \subseteq U$

(H) If P and Q are countable, then $P \times Q$ is countable.

(I) If B is countable then $P_\omega(B)$ is countable where
$P_\omega(B) = \{S : S \subseteq B \text{ and } S \text{ is finite}\}$ ie,
The set of all finite subsets of a countable set is countable.

- Cantor-Schröder-Bernstein Theorem.
$\exists$ inj. $f : A \to B \wedge \exists$ surj $g : A \to B \iff \exists$ bij. $h : A \to B$

- Let $A \subseteq X, B \subseteq Y$ $f : X \to Y$. If f is injective, $f^{-1}(f(A)) = A$

- Results from Quizes.
- $f : \mathbb{Z} \to \mathbb{N}$ $f(x) = |x|$ is surjective but not injective.
- $f : \mathbb{N} \to \mathbb{N}$ $f(x) = |x|$ is bijective
- $f : \mathbb{N} \to \mathbb{Z}$ $f(x) = |x|$ is injective but not surjective.
- $h \circ f$ is injective $\Rightarrow f$ is injective
$h \circ f$ is surjective $\Rightarrow h$ is surjective

- Which of the following are true for all sets A and B?
  - If $\exists$ bij $A \to B$ then $|A| = |B|$ True.
  - If $\exists$ (surj. $\wedge \sim$ inj.) $A \to B$ then $|A| \neq |B|$ False. eg. $f(2x) = x = f(2x+1)$ on $\mathbb{Z}_{\geq 0}$
  - If $\exists$ (inj. $\wedge \sim$ surj.) $A \to B$ then $|A| \neq |B|$ False. eg. $g(x) = x+1$ on $\mathbb{Z}_{\geq 0}$
  - If $\exists$ ($\sim$ inj. $\wedge \sim$ surj.) $A \to B$ then $|A| \neq |B|$ False. eg. $h: \{0,1\} \to \{0,1\}$ $h(0) = 0 = h(1)$.

- With respect to a fixed equivalence ~~class~~ relation on $\mathbb{Z}_{\geq 0}$, all equivalence classes are countable. (every subset of a countable set is countable) → True.
- With respect to a fixed equivalence ~~class~~ relation on $\mathbb{Z}_{\geq 0}$, all the equivalence classes have the same cardinality — FALSE

- $A = \{X \in \mathcal{P}(\mathbb{Z}) : 1,2,3 \in X\}$ is uncountable. (Define bij $\mathcal{P}(\mathbb{Z} \setminus \{1,2,3\}) \to A$)

- How many binary strings of length k have an even number of 0's?
  → 2^{k-1}. There are 2^k strings out of which half have an even number of 0's, and other half has odd number of 0's, by symmetry

- How many ways can you place 4 rooks on a 8x8 chessboard such that no 2 rooks attack each other?
  → 64 x 49 x 36 x 25 (After placing a rook, you eliminate a row & column)

- Let $n \in \mathbb{Z}^+$ and S be a subset of $\{1, 2, 3, \ldots 2n\}$. What is the minimum value of $|S|$ such that we can always find 2 elements in S where one divides the other?
  → n+1. Partition $\{1,2,\ldots,2n\}$ into $\{1,2,\ldots,n\}$ and $\{n+1, n+2, \ldots, 2n\}$.
  ↓ n elements. ↓ n elements

You can pick n elements from the second subset but as soon as you exceed n, you have to pick an element from the first subset (that is a factor)

∘ In a city with n towns ($n \geq 2$) there is a road b/w any 2 of these towns. On arrival, Aiken realizes that one of the rods is blocked. How many ways can Aiken visit every town exactly once?

Ans: Model the problem as following: arranging n names in a row in which 2 particular names cannot exist next to each other.

eg. a b cd would mean Aiken travelled from a → b → c → d

$n!$ → Total permutations (incl. broken road)

$2(n-1)!$ → Permutations in which 2 cities occur together (and they can be swapped b/w each other)

$\therefore n! - 2(n-1)!$

∘ Potts has 3 pairs of socks for each color of the rainbow (ie, 42 socks in total). Left socks cannot be differentiated from right socks. How many possible outcomes are possible where Potts finds a matching pair?

Ans: Total ways: Equivalent to choosing 5 socks from 7 colors with repitition

$\therefore \binom{11}{5} = 462$ (these are the possible outcomes but not all possible ways to achieve these outcomes.

Out of these ways, number of ways in which all socks are distinct: $\binom{7}{5} = 21$.

$\therefore$ finding matching pair = $462 - 21 = 441$

∘ What is the probability of Potts finding at least 1 matching pair if she draws 5 socks out of her drawer at random?

→ Total ways to draw 5 socks: ${}^{42}C_5$

(though many lead to same 'result')

7 colors, 6 socks for each ⇒ (No. of ways to choose 5 colors) × (No. of ways to choose a sock for a color)^5

$= {}^{7}C_5 \times (6)^5$

$= 163296.$

∘∘ Required probability $\dfrac{\binom{42}{5} - \binom{7}{5}6^5}{\binom{42}{5}}$

A'ZONE

Alternatively, first sock P(different) $= \frac{42}{42}$

Second sock $\therefore \frac{42}{42} \times \frac{36}{41}$

$\vdots$

P(5 dismismatching socks) $= 1 - \frac{42}{42} \times \frac{36}{41} \times \frac{30}{40} \times \frac{24}{39} \times \frac{18}{38}$

(after choosing a sock, you cannot choose any other socks of that colour

- Potts tosses a fair coin n times, where n is an odd integer greater than 1. What is the probability of Potts obtaining the same outcome every single toss (all heads or all tails)?

Ans: P(all head) $= \frac{1}{2^n}$, P(all tail) $= \frac{1}{2^n}$

$\therefore$ P(same outcome) $= \frac{1}{2^n} + \frac{1}{2^n} = \frac{1}{2^{n-1}}$

Alternatively, → first toss can be anything (no restrictions)

→ For all subsequent n-1 tosses, you must get exactly what you got in your first toss $\therefore \frac{1}{2^{n-1}}$

Note: FOR ODD 'n' >1

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \binom{n}{n-1} = 2^{n-1} = \binom{n}{1} + \binom{n}{3} + \cdots \binom{n}{n-2}$$

- Jack and Potts have 1 and 2 die resp. What is the probability of Jack rolling a higher number than the sum rolled by Potts?

Ans: Let Jack choose a number from 1 through 6.

Potts rolls die to give a sum < number chosen,

P(required) $= \frac{1}{6}\left(\underset{\text{Jack chooses 1}}{0} + \underset{\text{Jack chooses 2}}{0} + \frac{1}{36} + \frac{3}{36} + \frac{6}{36} + \frac{9}{36}\right) = \frac{5}{54}$

Tip: Problem Reduction. Try to model a problem in a way that you can solve it.
∴ Don't complicate it unnecessarily

- A, B independent and B, C independent $\Rightarrow P(A|B) = P(A)$, $P(A|C) = \frac{P(A \cap C)}{P(C|B)}$

$P(A|B \cap C) = P(A)$

We don't know if A and C are independent, or if A and $B \cap C$ are independent.

- A handy bijection from $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ (Tutorial 8, D4)

$$f(x,y) = \frac{(x+y)(x+y+1)}{2} + y$$

Assignment 2 Q3.

- Let U be a countable infinite set. If $A \subseteq U$, then

$\mathcal{P}(A) = \{S \subseteq U : S \subseteq A\} = \{S \subseteq U \mid S \setminus A \text{ is empty}\}$

$\mathcal{P}_U^*(A) = \{S \subseteq U : S \setminus A \text{ is finite}\}$

$\mathcal{P}_\omega(A) = \{S \subseteq U : S \subseteq A \text{ and } S \text{ is finite}\}$

→ $\mathcal{P}(A) \subseteq \mathcal{P}_U^*(A)$

→ If A is finite then, $\mathcal{P}_U^*(A)$ is countable

→ If A is infinite then $\mathcal{P}_U^*(A)$ is uncountable.

Prove that the set of all functions from $A \to B$, where A and B are finite sets, is countable.

→ Let us represent each function $f: A \to B$ by a 3-tuple (A, B, S) where S is the graph of f as defined in tutorial 5. Under this representation, every fn $f: A \to B$ is an element of $\mathcal{P}_\omega(\mathbb{Z}) \times \mathcal{P}_\omega(\mathbb{Z}) \times \mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$ where $\mathcal{P}_\omega(X)$ denotes the set of all finite subsets of X. So, $\mathcal{P}_\omega(\mathbb{Z}) \times \mathcal{P}_\omega(\mathbb{Z}) \times \mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$ is countable. ∴ The set of all functions from $A \to B$ is countable (∵ It is a subset of $\mathcal{P}_\omega(\mathbb{Z}) \times \mathcal{P}_\omega(\mathbb{Z}) \times \mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$

↓ It cannot include all elements of $\mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$

∵ It must satisfy 'well-defined fn')