1 Tables

Commutative	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r$	
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge \text{true} \equiv p$	$p \vee \text{false} \equiv p$
Negation	$p \vee \sim p \equiv \text{true}$	$p \wedge \sim p \equiv \text{false}$
Double Negative	$\sim (\sim p) \equiv p$	
Idempotent	$p \vee p \equiv p$	$p \wedge p \equiv p$
Universal bound	$p \vee \text{true} \equiv \text{true}$	$p \wedge \text{false} \equiv \text{false}$
de Morgan's	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Implication	$p \Rightarrow q \equiv \sim p \vee q$	
∼(Implication)	$\sim (p \Rightarrow q) \equiv p \wedge \sim q$	
Modus Ponens	$p \implies q, p$	q
Modus Tollens	$p \implies q, \sim q$	$\sim p$
Generalization	p	$p \vee q$
Specialization	$p \wedge q$	p
Conjunction	p, q	$p \wedge q$
Elimination	$p \vee q, \sim q$	p
Transitivity	$p \implies q, q \implies r$	$p \implies r$
Division into cases	$p \wedge q, p \implies r, q \implies r$	r
Contradiction	$\sim p \implies \text{false}$	p
Commutative	$A \cup B = B \cup A$	
Associative	$(A \cup B) \cup C = A \cup (B \cup C)$	
Distributive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity	$A \cup \emptyset = A$	$A \cap U = A$
Complement	$A \cup \bar{A} = U$	$A \cap \bar{A} = \emptyset$
Double Complement	$\bar{\bar{A}} = A$	
Idempotent	$A \cup A = A$	$A \cap A = A$
Universal Bound	$A \cup U = U$	$A \cap \emptyset = \emptyset$
De Morgan's	$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements of U and ∅	$\bar{U} = \emptyset$	$\bar{\emptyset} = U$
Set Difference	$A \setminus B = A \cap \bar{B}$	
F1 Commutative	$a + b = b + a$	$ab = ba$
F2 Associative	$(a + b) + c = a + (b + c)$	$(ab)c = a(bc)$
F3 Distributive	$a(b + c) = ab + ac$	$(b + c)a = ba + ca$
F4 Identity	$0 + a = a + 0 = a$	$1 \cdot a = a \cdot 1 = a$
F5 Additive inverses	$a + (-a) = (-a) + a = 0$	
F6 Reciprocals	$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$	$a \neq 0$
T1 Cancellation Add	$a + b = a + c$	$b = c$
T2 Possibility of Sub	There is one $x, a + x = b$	$x = b - a$
T3	$b - a = b + (-a)$	
T4	$-(-a) = a$	
T5	$a(b - c) = ab - ac$	
T6	$0 \cdot a = a \cdot 0 = 0$	
T7 Cancellation Mul	$ab = ac$	$b = c, a \neq 0$
T8 Possibility of Div	$a \neq 0, ax = b$	$x = \frac{b}{a}$
T9	$a \neq 0, \frac{b}{a} = b \cdot a^{-1}$	
T10	$a \neq 0, (a^{-1})^{-1} = a$	
T11 Zero Product	$ab = 0 \Rightarrow a = 0 \vee b = 0$	
T12 Mul with -ve	$(-a)b = a(-b) - -(ab)$	$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$
T13 Equiv Frac	$\frac{a}{b} = \frac{ac}{bc}$	$b \neq 0, c \neq 0$
T14 Add Frac	$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$	$b \neq 0, d \neq 0$
T15 Mul Frac	$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$	$b \neq 0, d \neq 0$
T16 Div Frac	$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ac}{bd}$	$b \neq 0, d \neq 0$

Ord1	$\forall a, b \in \mathbb{R}^+$	$a + b > 0, ab > 0$
Ord2	$\forall a, b \in \mathbb{R}_{\neq 0}$	a is positive or negative and not both
Ord3	0 is not positive	
$a < b$	means $b + (-a)$ is positive	
$a \leq b$	means $a < b$ or $a = b$	
$a < 0$	means a is negative	
T17 Trichotomy Law	$a < b \vee b > a \vee a = b$	
T18 Transitive Law	$a < b$ and $b < c$	$a < c$
T19	$a < b$	$a + c < b + c$
T20	$a < b$ and $c > 0$	$ac < bc$
T21	$a \neq 0$	$a^2 > 0$
T22	$1 > 0$	
T23	$a < b$ and $c < 0$	$ac > bc$
T24	$a < b$	$-a > -b$
T25	$ab > 0$	a and b are both positive or negative
T26	$a < c$ and $b < d$	$a + b < c + d$
T27	$0 < a < c$ and $< 0 < b < d$	$0 < ab < cd$

2 Math

Defn. Even and Odd Integers
n is even $\Leftrightarrow \exists$ an integer k s.t. $n = 2k$
n is odd $\Leftrightarrow \exists$ an integer k s.t. $n = 2k + 1$

Defn. Divisibility
n and d are integers and $d \neq 0$
$d|n \Leftrightarrow \exists k \in \mathbb{Z}$ s.t. $n = dk$

Theorem 4.2.1. Every Integer is a rational number

Theorem 4.2.2. The sum of any two rational numbers is rational

Theorem 4.3.1. For all $a, b \in \mathbb{Z}^+$, if $a|b$, then $a \leq b$

Theorem 4.3.2. Only divisors of 1 are 1 and -1

Theorem 4.3.3. $\forall a, b, c \in \mathbb{Z}$ if $a|b$, $b|c$, $a|c$

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.

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

Defn. Fraction in lowest term: fraction $\frac{a}{b}$ is lowest term if largest $\mathbb{Z}$ that divies both a and b is 1

Theorem 4.7.1. $\sqrt{2}$ is irrational

3 Logic of Combound Statements

Theorem 3.2.1. Negation of universal stmt $\sim (\forall x \in D, P(x)) \equiv \exists x \in D$ s.t. $\sim P(x)$

Theorem 3.2.1. Negation of existential stmt $\sim (\exists x \in D$ s.t. $P(x)) \equiv \forall x \in D, \sim P(x)$

Defn. Contrapositive of $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$

Defn. Converse of $p \Rightarrow q$ is $q \Rightarrow p$

Defn. Inverse of $p \Rightarrow q$ is $\sim p \Rightarrow \sim q$

Defn. Only if: p only if q means $\sim q \Rightarrow \sim p \equiv p \Rightarrow q$

Defn. Biconditional: $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

Defn. r is sufficient condition for s means if r then s, $r \Rightarrow s$

Defn. r is necessary condition for s means if $\sim r$ then $\sim s$, $s \Rightarrow r$

Defn. Proof by Contradiction
If you can show that the supposition that sttatement p is false leads to a contradiction, then you can conclude that p is true

4 Methods of Proof

Statement	Proof Approach
$\forall x \in D\ P(X)$	Direct: Pick arbitrary x, prove P is true for that x. Contradiction: Suppose not, i.e. $\exists x(\sim p)$... Hence supposition $\sim p$ is false (P3)
$\exists x \in D\ P(X)$	Direct: Find x where P is true. Contradiction: Suppose not, i.e. $\forall x(\sim p)$... Hence supposition $\sim p$ is false (P3)
$P \Rightarrow Q$	Direct: Assume P is true, prove Q Contradiction: Assume P is true and Q is false, then derive contradiction Contrapositive: Assume $\sim Q$, then prove $\sim P$
$P \Leftrightarrow Q$	Prove both $P \Rightarrow Q$ and $Q \Rightarrow P$
xRy. Prove R is equivalence	Prove Reflexive, Symmetric and Transitive

Defn. Proof by Contraposition
1. Statement to be proved $\forall x \in D\ (P(x) \Rightarrow Q(x))$
2. Contrapositive Form: $\forall x \in D\ (\sim Q(x) \Rightarrow \sim P(x))$
3. Prove by direct proof
3.1 Suppose x is an element of D s.t. $Q(X)$ is false
3.2 Show that P(x) is false.
4. Therefore, original statement is true

5 Set Theory

Defn. Set: Unordered collection of objects
Order and duplicates don't matter

Defn. Membership of Set $\in$: If S is set, $x \in S$ means x is an element of S

Defn. Cardinality of Set $|S|$: The number of elements in S

Common Sets:
$\mathbb{N}$ - Natural Numbers, $\{0, 1, 2\}$
$\mathbb{Z}$ - Integers
$\mathbb{Q}$ - Rational
$\mathbb{R}$ - Real
$\mathbb{C}$ - Complex
$\mathbb{Z}^{\pm}$ - Positive/Negative Integers

Defn. Subset $A \subseteq B \Leftrightarrow$ Every element of A is also an element of B
$A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$

Defn. Proper Subset $A \subsetneq B \Leftrightarrow (A \subseteq B \wedge A \neq B)$

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

Defn. Cartesian Product $A \times B = \{(a, b) : a \in A \wedge b \in B\}$

Defn. Set Equality $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$
$A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$

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

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

Defn. Difference: $B \setminus A = \{x \in U : x \in B \wedge x \notin A\}$

Defn. Disjoint: $A \cap B = \emptyset$

Theorem 4.4.1. Quotient-Remainder $n \in \mathbb{Z}, d \in \mathbb{Z}^+$
there exists unique integers q and r such that $n = dq + r$ and $0 \leq r < d$

Defn. Power Set: The set of all subsets of A, has 2^n elements.

Theorem 6.3.1. Suppose A is a finite set with n elements, then $P(A)$ has 2^n elements. $|P(A)| = 2^{|n|}$

Defn. Cartesian Product of $A_n = A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ...a_n) : a_1 \in A_1 \wedge a_2 \in A_2...$

Theorem 6.2.1. Subset Relations
1. Inclusion of Intersection: $A \cap B \subseteq A, A \cap B \subseteq B$
2. Inclusion in Union $A \subseteq A \cup B, B \subseteq A \cup B$
3. Transitive Property of Substs: $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

6 Relations

Defn. Relation from A to B is a subset of $A \times B$
Given an ordered pair$(x, y) \in A \times B$, x is related to y by R is written $xRy \Leftrightarrow (x, y) \in R$

Defn. Domain, Co-domain, Range
Let A and B be sets and R be a relation from A to B

1. Domain of R: is set $\{a \in A : aRb \text{ for some } b \in B\}$
2. Codomain of R: Set B
3. Range of R: is set $\{b \in B : aRb \text{ for some } a \in A\}$

Defn. Inverse Relation
Let R be a relation from A to B, $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$
$\forall x \in A, \forall y \in B((y, x) \in R^{-1} \Leftrightarrow (x, y) \in R)$

Defn. Relation on a Set A is a relation from A to A.

Defn. Composition of Relations
A, B and C be sets. $R \subseteq A \times B$ be a relation. $S \subset B \times C$ be relation. Composition of R with S, denoted $S \circ R$ is relation from A to C such that:
$\forall x \in A, \forall z \in C(xS \circ Rz \Leftrightarrow (\exists y \in B(xRy \wedge ySz)))$

Proposition. Composition is Associative A, B, C, D be sets. $R \subseteq A \times B$, $S \subseteq B \times C$, $T \subseteq C \times D$
$T \circ (S \circ R) = T \circ S \circ R$

Proposition. Inverse of Composition A, B, C be sets. $R \subseteq A \times B$, $S \subseteq B \times C$
$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Defn. Reflexivity, Symmetry, Transitivity

1. Reflexivity: $\forall x \in A(xRx)$
2. Symmetry: $\forall x, y \in A(xRy \Rightarrow yRx)$
3. Transitivity:$\forall x, y, z \in A(xRy \wedge yRz \Rightarrow xRz)$
   Refer to proof 6

Defn. Transitive Closure
Transitive closure of R is relation R^t on A that satiesfies

1. R^t is transitive
2. $R \subseteq R^t$
3. If S is any other transitive relation that contains R, then $R^t \subseteq S$

Defn. Partition
P is partition of set A if

1. P is a set of which all elements are non empty subsets of A, $\emptyset \neq S \subseteq A$ for all $S \in P$
2. Every element of A is in exactly on element of P,
   $\forall x \in A\ \exists S \in P(x \in S)$ and
   $\forall x \in A\ \exists S_1, S_2 \in P(x \in S_1 \wedge x \in S_2 \Rightarrow S_1 = S_2)$
   OR $\forall x \in A\ \exists! S \in P(x \in S)$
   Elements of a partition are called components

Defn. Relation Induced by a partition
Given partition P of A, the relation R induced by partition:
$\forall x, y \in A, xRy \Rightarrow \exists$ a component of S of P s.t. $x, y \in S$

Theorem 8.3.1 (Relation Induced by a Partition)**.** Let A be a set with a partition and let R be a relation induced by the partition. Then R is reflexive, symmetric and transitive

Defn (Equivalence Relation)**.** A be set and R be relation. R is equivalence relation iff R is reflexive, symmetric and transitive

Defn. Equivalence Class
Suppose A is set and $\sim$ is equivalence relation on A. For each $A \in A$, equivalence class of a, denoted $[a]$ and called class of a is set of all elements $x \in A$ s.t. $a \sim x$
$[a]_\sim = \{x \in A : a \sim x\}$

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 distinct equivalence classes of R form a partition of A; that is, the union of the equivalence classes is all of A, and the intersection of any 2 disctinct classes is empty.

Defn. 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 $k \in \mathbb{Z}$. In other words, $n|(a - b)$.
We write $a \equiv b (\text{mod } n)$

Defn. Set of equivalence classes
Let A be set and $\sim$ be an equivalence relation on A. Denote by $A/\sim$, the set of all equivalence classes with respect to $\sim$, i.e.
$A/\sim = \{[x]_\sim : x \in A\}$

Theorem Equivalence Classes. form a partition Let $\sim$ be an equiv. relation on A. Then $A/\sim$ is a partition of A.

Defn (Antisymmetry). R is antisymmetric iff $\forall x, y \in A(xRy \wedge yRx \Rightarrow x = y)$ *(DOES NOT IMPLY NOT SYMMETRIC)*

Defn (Partial Order Relation). R is Partial Order iff R is *reflexive*, *antisymmetric* and *transitive*.

Defn. Partially Ordered Set Set A is called poset with respect to partial order relation R on A, denoted by (A, R) (Proof 7)

Defn. $x \preccurlyeq y$ is used as a general partial order relation notation

Defn (Hasse Diagram). Let $\preccurlyeq$ be a partial order on set A. Hasse diagram satisfies the following condition for all distinct $x, y, m \in A$
If $x \preccurlyeq y$ and no $m \in A$ is s.t. $x \preccurlyeq m \preccurlyeq y$, then x is placed below y with a line joining them, else no line joins x and y.

Defn (Comparability). $a, b \in A$ are comparable iff $a \preccurlyeq b$ or $b \preccurlyeq a$. Otherwise, they are **noncomparable**

Defn (Maximal, Minimal, Largest Smallest). Set A be partially ordered w.r.t. a relation $\preccurlyeq$ and $c \in A$
1. c is maximal element of A iff $\forall x \in A$, either $x \preccurlyeq c$ or x and c are non-comparable. OR $\forall x in A(c \preccurlyeq x \Rightarrow c = x)$
2. c is minimal element of A iff $\forall x \in A$, either $c \preccurlyeq x$ or x and c are non-comparable. OR $\forall x in A(x \preccurlyeq c \Rightarrow c = x)$
3. c is largest element of A iff $\forall x \in A(x \preccurlyeq c)$
4. c is smallest element of A iff $\forall x \in A(c \preccurlyeq x)$

Proposition. A smallest element is minimal
Consider a partial order $\preccurlyeq$ on set A. Any smallest element is minimal.
1. Let c be smallest elemnt
2. Take any $x \in A$ s.t. $x \preccurlyeq c$
3. By smallestness, we know $c \preccurlyeq x$ too.
4. So $c = x$ by antisymmetry

Defn (Total Order Relations). All elements of the set are comparable
R is total order iff R is a partial order and $\forall x, y \in A(xRy \vee yRx)$

Defn (Linearization of a partial order). Let $\preccurlyeq$ be a partial order on set A. A linearization of $\preccurlyeq$ is a total order $\preccurlyeq *$ on A s.t. $\forall x, y \in A(x \preccurlyeq y \Rightarrow x \preccurlyeq * y)$

Defn (Kahn's Algorithm). Input: A finite set A and partial order $\preccurlyeq$ on A
1. Set $A_0 := A$ and $i := 0$
2. Repeat until $A_i = \emptyset$
   2.1. Find minimal element c_i of A_i wrt $\preccurlyeq$
   2.2. Set $A_{i+1} = A_i \setminus c_i$
   2.3. Set $i = i + 1$

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

Defn (Well ordered set). Let $\preccurlyeq$ be a total order on set A. A is well ordered iff every nonempty subset of A contains a smallest element. OR
$\forall S \in P(A), S \neq \emptyset \Rightarrow (\exists x \in S \forall y \in S(x \preccurlyeq y))$ E.g. $(\mathbb{N}, \leq)$ is well ordered but $(\mathbb{Z}, \leq)$ is not as there is no smallest integer (Theorem 4.6.1)

Functions

Defn (Function). A function f from set X to set Y, denoted $f : X \Rightarrow Y$ is a relation satisfying the following
(F1) $\forall x \in X, \exists y \in Y(x, y) \in f$
(F2) $\forall x \in X, \forall y_1, y_2 \in Y(((x, y_1) \in f \wedge (x, y_2) \in f) \Rightarrow y_1 = y_2)$
OR
Let f be a relation on sets X and Y, i.e. $f \subseteq X \times Y$. Then f is a function from X to Y denoted $f : X \Rightarrow Y$, iff $\forall x \in X \ \exists! y \in Y(x, y) \in f$

Defn (Argument, Image, Preimage, input, output). Let $f : X \Rightarrow Y$ be fn. We write $f(x) = y$ iff $(x, y) \in f$
f sends/maps x to y is also $x \overset{f}{\Rightarrow} y$ or $f : x \mapsto y$. x is **argument** of f.
$f(x)$ is read "f of x" or "the **output** of f for the **input** x", or "value of f at x or "image of x under f"
If $f(x) = y$, then x is a **preimage** of y

Defn (Setwise image and preimage)**.** Let $f : X \Rightarrow Y$ be a fn from set X to Y
- If $A \subseteq X$, then let $f(A) = \{f(x) : x \in A\}$
- If $B \subseteq Y$, then let $f^{-1}(B) = \{x \in X : f(x) \in B\}$

$f(A)$ is the **setwise image** of A and $f^{-1}(B)$ the **setwise preimage** of B under f. This is **NOT** the inverse function
If $f^{-1}(\alpha), \alpha$ is a set, f^{-1} is setwise preimage. else if x member of codomain, $f^{-1}(x)$ is inverse function. $f^{-1}(\alpha)$ need not be function. Use $f^{-1}(\{b\})$ for setwise preimage of single element in codomain

Defn (Domain, Co-Domain, Range)**.** Let $f : X \Rightarrow Y$ fn from set X to Y.
X is **domain** of f and Y the **co-domain** of f.
Range of f is the (setwise) image of X under f: $\{y \in Y : y = f(x)$ for some $x \in X\}$. Range $\subseteq$ Co-Domain

Defn (Sequence)**.** Sequence $a_0, a_1, a_2, ...$ can be represented by a function a whos domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geq 0}$
Any function whos domain is $\mathbb{Z}_{\geq m}$ for some $m \in Z$ represents a sequence
Fibonacci Sequence: $F(0) = 0, F(1) = 1, F(n+2) = F(n+1) + F(n)$

Defn (String)**.** Let A be a set. A **string** or a word over A is an expression in the form of $a_0a_1a_2...a_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, a_2, ..., a_{l-1} \in A$.
l is called length of string. Empty string ε is the string of length 0.
Let $A*$ denote the set of all strings over A

Defn (Equality of Sequences)**.** Given two sequences $a_0, a_1, a_2...$ and $b_0, b_1, b_2, ...$ defined by fn $a(n) = a_n$ and $b(n) = b_n$ for every $n \in \mathbb{Z}_{\geq 0}$, two sequences are equal if and only if $a(n) = b(n)$ for every $n \in \mathbb{Z}_{\geq 0}$

Defn (Equality of Strings)**.** Given two sequences $s1 = a_0a_1a_2...a_{l-1}$ and $s2 = b_0b_1b_2, ..., b_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$, we say that $s1 = s2$ if and only if $a_i = b_i$ for all $i \in 0, 1, 2, ..., l-1$

Theorem 7.1.1 Function Equality. Two functions $f : A \Rightarrow B$ and $g : C \Rightarrow D$ are equal if i.e. $f = g$, iff (i) $A = C$ and $B = D$ and (ii) $f(x) = g(x) \forall x \in A$

Defn (Injection)**.** One to one functions: $\forall x_1, x_2 \in X(f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$
or the contrapositive: $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

Defn (Surjection)**.** Onto function: $\forall y \in Y \exists x \in X(y = f(x))$
Every element in co-domain has a preimage. So range = co-domain. (Every element in Y has an x)

Defn (Bijection)**.** One to one correspondence: $\forall y \in Y\ \exists! x \in X(y = f(x))$

Defn (Inverse Functions)**.** Let $f : X \Rightarrow Y$. Then $g : Y \Rightarrow X$ is an **inverse** of f iff
$\forall x \in X, \forall y \in Y(y = f(x) \Leftrightarrow x = g(y))$ inverse of f is f^{-1}

Proposition (Uniqueness of Inverse)**.** If g_1 and g_2 are inverses of $f : X \Rightarrow Y$, then $g_1 = g_2$ (Proof S07L34)

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

Defn (Composition of Functions)**.** Let $f : X \Rightarrow Y$ and $g : Y \Rightarrow Z$ be fns
$g \circ f : X \Rightarrow Z$ is $(g \circ f)(x) = g(f(x)) \forall x \in X$

Theorem 7.3.1. Composition with an Identity Function
If $f : X \Rightarrow Y$ and id_x is identity fn on X and id_y is identity fn on Y, then
$f \circ id_x = f$ and $id_y \circ f = f$

Theorem 7.3.2. Composition of a Function with its inverse
If $f : X \Rightarrow Y$ is a bijection with inverse function $f^{-1} : Y \Rightarrow X$, then $f^{-1} \circ f = id_x$ and $f \circ f^{-1} = id_y$

Theorem Associativity of Function Composition. Let $f : A \Rightarrow B, g : B \Rightarrow C, h : C \Rightarrow D$. Then $(h \circ g) \circ f = h \circ (g \circ f)$

Defn (Noncommutativity of Function Composition)**.** $(g \circ f) \neq (f \circ g)$

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

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

Defn ($\mathbb{Z}/\sim_n$)**.** The quotient $\mathbb{Z}/\sim_n$ where $\sim_n$ is the congruence-mod-n relation on $\mathbb{Z}$, is denoted $\mathbb{Z}_n$
E.g. $\mathbb{Z}_3 = \{\{3k : k \in Z\}, \{3k+1 : k \in Z\}, \{3k+2 : k \in Z\}\}$

Defn (Addition and Multiplication on $\mathbb{Z}_n$)**.** Whenever $[x], [y] \in \mathbb{Z}_n$
$[x] + [y] = [x+y]$ and $[x] \cdot [y] = [x \cdot y]$

Function Proofs

Proof. Prove relation is function: T06Q1 $\forall x, y \in \mathbb{N}(xRy \iff x^2 = y^2)$

1. $\forall x \in \mathbb{N}, \exists y = x \in \mathbb{N}$ such that $(x, y) \in R$ (F1)
2. F2
   2.1. $\forall x \in \mathbb{N}$, let $y_1, y_2 \in \mathbb{N}$
   2.2. Suppose $(x, y_1) \in R \wedge (x, y_2) \in R$
   2.3. Then $y_1^2 = x^2$ and $y_2^2 = x^2$ (by defn of R)
   2.4. Then $y_1^2 = y_2^2$
   2.5. Hence $y_1 = y_2$ (as $y_1, y_2 \in \mathbb{N} > 0$)

Proof. Proof of Injection: T06Q2 $f(x) = x + 3$

1. Let $x_1, x_2 \in \mathbb{R}$ such that $f(x_1) = f(x_2)$
2. Then $x_1 + 3 = x_2 + 3$
3. Then $x_1 = x_2$, therefore f is injective

Proof. Proof of Surjection: T06Q2 $f(x) = x + 3$

1. Take any $y \in \mathbb{R}$
2. Let $x = y - 3$
3. Then $f(x) = f(y - 3) = (y - 3) + 3 = y$, Therefore, f is surjective

Proof. Proof of Bijection via Inverse T06Q5: $f(x) = 12x + 31$

1. $\forall x, y \in \mathbb{Q}, y = 12x + 31 \iff x = (y - 31)/12$
2. define $g : \mathbb{Q} \to \mathbb{Q}$ by setting, $\forall y \in \mathbb{Q}, g(y) = (y - 31)/12$
3. Then whenever $x, y \in \mathbb{Q}, y = f(x) \iff x = g(y)$
4. Thus g is the inverse of f, hence f is bijective (by Theorem 7.2.3)

Mathematical Induction

Defn (Sequence)**.** Ordered Set with members called **terms**. May have infinite terms. In the form: $a_m, a_{m+1}, a_{m+2}, ...$

Defn (Summation)**.** if m and n are integers and $m \leq n$, $\sum_{k=m}^{n} a_k$ is the sum of all terms $a_m, a_{m+1}, ..., a_n$
k is the **index** of summation, m is the **lower limit** and n the **upper limit**
$\sum_{k=m}^{m} a_k = a_m$ and $\sum_{k=m}^{n} a_k = (\sum_{k=m}^{n-1} a_k) + a_n$

Defn (Product)**.** if m and n are integers and $m \leq n$, $\prod_{k=m}^{n} a_k$ is the product of all terms $a_m, a_{m+1}, ..., a_n$
$\prod_{k=m}^{m} a_k = a_m$ and $\prod_{k=m}^{n} a_k = (\prod_{k=m}^{n-1} a_k) \cdot a_n$

Theorem 5.1.1. Properties of Summations and Products

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n}(a_k + b_k)$
2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n}(c \cdot b_k)$
3. $(\prod_{k=m}^{n} a_k) \cdot (\prod_{k=m}^{n} b_k) = \prod_{k=m}^{n}(a_k \cdot b_k)$

Defn. Arithmetic Sequence a_0, a_1, a_2 is arithmetic if there is a constant d s.t. $a_k = a_{k-1} + d$ for all integers $k \geq 1$
It follows that $a_n = a_0 + dn$ for all integers $n \geq 0$. d is the common difference. $\sum_{k=0}^{n-1} a_k = \frac{n}{2}(2a_0 + (n-1)d)$

Defn. Geometric Sequence a_0, a_1, a_2 is arithmetic if there is a constant r s.t. $a_k = ra_{k-1}$ for all integers $k \geq 1$
It follows that $a_n = a_0 r^n$ for all integers $n \geq 0$. r is the common ratio. $\sum_{k=0}^{n-1} a_k = a_0(\frac{1-r^n}{1-r})$

Defn. Principle of Mathematical Induction
To prove that "For all integers $n \geq a, P(n)$ is true"

- **Basis Step:** Show that $P(a)$ is true.
- **Inductive Step:** Show that for all integers $k \geq a, P(k) \implies p(k+1)$. To perform this, suppose that P(k) is true, where k is a particular but arbitrarily chosen integer $k \geq a$
- Therefore $P(n)$ is true for all $n \in \mathbb{Z}^+$

Theorem 5.2.2. Sum of first n integers: for all integers $n \geq 1, 1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$

Theorem 5.2.3. Sum of a geometric sequence: for any real number $r \neq 1$, and any integers $n \geq 0, \sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$

Proposition. 5.3.1 For all integers $n \geq 0, 2^{2n} - 1$ is divisible by 3

Defn (Strong induction (2PI))**.** If

- $P(a)$ holds
- For every $k \geq a$, $(P(a) \wedge P(a+1) \wedge ... \wedge P(k)) \Rightarrow P(k+1)$

Then $P(n)$ holds for all $n \geq a$

Defn (Strong Induction Variant (2PI))**.** If

- $P(a), P(a+1), ..., P(b)$ holds
- For every $k \geq a, P(k) \Rightarrow P(k+b-a+1)$

Then $P(n)$ holds for all $n \geq a$

Defn (Well-Ordering Principle)**.** Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element

Defn (Recurrance Relation)**.** for a sequence $a_0, a_1, a_2, ...$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, ..., a_{k-i}$, where i is an integer with $k - i \geq 0$
If i is a fixed integer, the **initial conditions** for such a recurrant relation specify the values of $a_0, a_1, a_2, ..., a_{i-1}$
If i depends on k, the initial conditions specify the values of $a_0, a_1, a_2, ..., a_m$, where m is an integer with $m \geq 0$
E.g. Fibonacci: $F_0 = 0; F_1 = 1; F_n = F_{n-1} + F_{n-2}$, for $n > 1$

Defn (Recusively Defined Sets)**.** Let S be a finite set with at least 1 element. A **string over** S is a finite sequence of elements from S. The elements of S are called **characters** of the string, and the length of a string is the number of characters it contains. The **null string over** S is defined to be the string with no characters (Length 0, ε).
E.g.

1. Base: () is in P
2. Recusion:
   (a) If E is in P, so is (E).
   (b) If E and F are in P, so is EF
3. Restriction: No configuration of parentheses are in P other than those derived from 1 and 2 above.

Defn (Recursive definition of a set S)**.**

- (base clause) - Specify that certain elements, called **founders** are in S: if c is a founder, then $c \in S$
- (recursion clause) - Specify certain functions, called **constructors** under which set S is closed: if f is a constructor and $x \in S$, then $f(x) \in S$
- (minimality clause) - Membership for S can always be demonstrated by (infinitely many) successive applications of the clauses above

Mathematical Induction Proofs

Proof. 1PI Example: Given any set $A, |P(A)| = 2^n$, where P(A) is power set of A and |A| = n.
1. For each $n \in \mathbb{N}$, let $P(n) \equiv (|P(A)| = 2^n$, where A is any n-element set
2. Basis Step: P(0) is true because $|P(\emptyset)| = |\{\emptyset\}| = 1 = 2^0$ as $P(\emptyset) = \{\emptyset\}$ and $|\emptyset| = 0$
3. Induction Step:
   3.1. Let $k \in \mathbb{N}$ such that P(k) is true, i.e. $|P(X)| = 2^k$, where X is any k-element set
   3.2. Let A be a $k+1$ element set.
   3.3. Since $k \geq 0$, there is at least one element in A. Pick $z \in A$.
   3.4. The subsets of A can be split to 2 groups: those that contain z and those that don't
   3.5. Subsets that don't contain z are the same as the subsets of $A \setminus \{z\}$, which has a cardinality of k, and hence $|P(A \setminus \{z\})| = 2^k$ (by induction hypothesis)
   3.6. Those subsets that contain z can be matched up one for one with those that do not contain z by unioninzing $\{z\}$ to the latter
   3.7. Hence there is equal no of subsets that contain z and subsets that don't
   3.8. Hence $|P(A)| = 2^k + 2^k = 2^{k+1}$
   3.9. Thus, P(k+1) is true
4. Therefore $\forall n \in \mathbb{N}, P(n)$ is true by MI

Proof. 2PI example: Any integer greater than 1 is divisible by a prime number
1. Let $P(n) \equiv (n$ is divisible by a prime), for $n > 1$
2. Basis Step: $P(2)$ is true since 2 is divisible by 2

3. Inductive step To show that for all integers $k \geq 2$, if $P(i)$ is true, for all integers i from 2 to k, then $P(k+1)$ is also true.
   3.1. Case 1 (k+1) is prime: in this case, K+1 is divisible by prime number, itself
   3.2. Case 2 (k+1) is not prime: In this case, $k+1 = ab$, a and b are integers with $1 < a < k+1$ and $1 < b < k+1$
      3.2.1. Thus, in particular, $2 \leq a \leq k$ and so by inductive hypothesis, a is divisble by prime number p
      3.2.2. In addition, because $k+1 = ab$, so $k+1$ is divisible by a
      3.2.3. By transitivity of divisibility, $k+1$ is divisible by prime p
4. Therefore any integer greater than 1 is divisible by prime

Proof. 2PI for Sums: Prove that for any positive int n, if $a_1, a_2, ..., a_n$ and $b_1, b_2, ..., b_n$ are $\mathbb{R}$, then $\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n}(a_i) + \sum_{i=1}^{n}(b_i)$

1. Let P(n) = $(\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n}(a_i) + \sum_{i=1}^{n}(b_i))$, for $n \geq 1$
2. Basis Step: P(1) is true since $\sum_{i=1}^{1}(a_i + b_i) = a_i + b_i = \sum_{i=i}^{1} a_i + \sum_{i=i}^{1} b_i$
3. Inductive Hypothesis: for some $k \geq 1$, $\sum_{i=1}^{k}(a_i + b_i) = \sum_{i=1}^{k}(a_i) + \sum_{i=1}^{k}(b_i)$
4. Inductive Step $= \sum_{i=1}^{k+1}(a_i + b_i) = \sum_{i=1}^{k}(a_i + b_i) + (a_{k+1} + b_{k+1})$ (By defn of $\sum$)
   $= \sum_{i=i}^{k} a_i + \sum_{i=i}^{k} b_i + (a_{k+1} + b_{k+1})$ (by inductive hypothesis)
   $= \sum_{i=i}^{k} a_i + a_{k+1} + \sum_{i=i}^{k} b_i + b_{k+1}$ (by assoc and commutative law of algebra)
   $= \sum_{i=i}^{k+1} a_i \sum_{i=i}^{k+1} b_i$ (By defn of $\sum$)
5. Therefore, P(k+1) is true, therefore P(n) is true for any positive integer n

Cardinality

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

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

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

Defn (Cardinality)**.** Cardinality of a finite set S, denoted $|S|$, is
(i) 0 if $S = \emptyset$, or
(ii) n if $f : S \Rightarrow Z_n$ is a bijection

Theorem Equality of Cardinality of Finite Sets. Let A and B be any finite sets.
$|A| = |B|$ iff there is a bijection $f : A \Rightarrow B$

Defn (Same Cardinality (Cantor))**.** Given any 2 sets A and B. A is said to have the same cardinality as B, $|A| = |B|$, iff there is a bijection $f : A \Rightarrow B$

Theorem 7.4.1 Properties of Cardinality. Cardinality is an equivalence relation

- **Reflexive**: $|A| = |A|$
- **Symmetric**: $|A| = |B| \Rightarrow |B| = |A|$
- **Transitive**: $(|A| = |B|) \land (|B| = |C|) \Rightarrow |A| = |C|$

Defn (Cardinal Numbers)**.** Define $\aleph_0 = |\mathbb{Z}^+|$

Defn (Coutably Infinite)**.** Set S is said to be countably infinite iff $|S| = \aleph_0$

Defn (Coutably Infinite)**.** Set S is said to be countable iff it is finite or countably infinite

Defn ($\mathbb{Z}$ is countable)**.** $f(n) = \begin{cases} n/2, & \text{if n is an even positive integer} \\ -(n-1)/2, & \text{if n is an odd positive integer} \end{cases}$

Defn ($\mathbb{Q}^+$ is countable)**.**

Defn ($\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable)**.**

Theorem [. Cartesian Product] If sets A and B are both countably infinite, then so is $A \times B$.

Corollary (General Cartesian Product)**.** Given $n \geq 2$ countably infinite sets $A_1, A_2, ..., A_n$, cartesian product $A_1 \times A_2 \times ... \times A_n$ is also countably infinite

Theorem [. Unions] Union of countably many countable sets is also countable.

Proposition (9.1)**.** Infinite set B is countable if and only if there is a sequence $b_0, b_1, ... \in B$ in which every element of B appears exactly once

Lemma (9.2)**.** Infinite set B is countable if and only if there is a sequence $b_0, b_1, ...$ in which every element of B appears

Theorem 7.4.2 (Cantor)**.** Set of real numbers between 0 and 1, $(0, 1) = \{x \in \mathbb{R} | 0 < x < 1\}$ is uncountable

Theorem 7.4.3. Any subset of any countable set is countable

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

Proposition (9.3)**.** Every infinite set has a countably infinite subset

Lemma (9.4 Union of countably infinite sets)**.** Let A and B be countably infinite sets. Then $A \cup B$ is countable

Counting and Probability

Defn (Sample Space)**.** is set of all possible outcomes of random process or experiment

Defn (Event)**.** is subset of sample space

Defn (Probability of Event E in Sample Space S)**.** $P(E) = \frac{|E|}{|S|}$, where |E| is number of outcomes in E and |S| is total number of outcomes

Theorem 9.1.1 (Number of Elements in a List)**.** If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

Theorem 9.2.1 (Multiplication/Product Rule)**.** If operation consists of k steps and 1st step performed in n_1 ways 2nd step in n_2 ways, k^{th} step can be done in n_k ways
Entire Operation in $n_1 \times n_2 \times ... \times n_k$ ways.
Should only be used for independent events

Theorem 9.2.2 (Permutations)**.** Number of permutations of a set with $n (n \geq 1)$ elements is $n!$ (Ordered selection)

Defn (R-Permutation)**.** of a set of n elements is an ordered selection of r elements taken from the set. Number of r-permutations of a set of n elements is $P(n, r)$

Theorem 9.2.3 (r-permutation from a set of n elements)**.** If n and r are integers and $1 \geq r \geq n$, then number of r-permutations fo a set n is given by $P(n, r) = n(n-1)(n-2)...(n-r+1) = \frac{n!}{(n-r)!}$

Theorem 9.3.1 (Addition/Sum Rule)**.** Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, ..., A_k$. Then $|A| = |A_1| + |A_2| + ... + |A_k|$

Theorem 9.3.2 (The Difference Rule)**.** if A is a finite set and $B \subseteq A$, then $|A \setminus B| = |A| - |B|$

Theorem [. Probability of complement of event] If S is a finite space and A is an event in S, then $P(\bar{A}) = 1 - P(A)$

Theorem 9.3.3 (Inclusion/Exclusion Rule for 2/3 sets)**.** If A, B and C are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$ and $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Theorem [. Pigeonhole Principle (PHP)] Function from one finite set to a smaller finite set cannot be one-to-one. There must at least be 2 other elements in the domain that have same image in codomain

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

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

Defn (R-combination)**.** Let n and r be non-negative intgers with $r \leq n$. An r-combination of a set of n elements is a subset of r of the n elements. (Unordered selection)
$\binom{n}{r}$, read "n choose r" denotes no of subsets of size r that can be chosen from a set of n elements.

Defn (Relationship between Permutation and Combination)**.** To get permutations of $\{0, 1, 2, 3\}$,

1. Write the 2-combinations of $\{0, 1, 2, 3\}$ –> $(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)$
2. Order the 2 combination to obtain 2 permutations: $(0, 1)$ and $(1, 0)$, etc

Therefore, $P(n, r) = \binom{n}{r} \cdot r! = \frac{n!}{(n-r)!}$

Theorem 9.5.1 (Formula for $\binom{n}{r}$)**.** $= \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}$

Theorem 9.5.2 (Permutations of sets of indistinguishable objects)**.** Suppose collection consists of n objects of which $n_1, n_2, ..., n_k$ are of types {1,2,...,k} and indistinguishable from each other
and suppose that $n_1 + n_2 + ... + n_k = n$.
Then number of distinguisiable permutations $= \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}...\binom{n-n_1-n_2-...-n_k-1}{n_k} = \frac{n!}{n_1!n_2!...n_k!}$

Defn (Example of 9.5.2)**.** Order letters in MISSISSIPPI, how many orders are there?
Subset of 4 positions for S = $\binom{11}{4}$, 4 positions for I = $\binom{7}{4}$, 2 positions for P = $\binom{3}{2}$, 1 positions for M = $\binom{1}{1}$, $\binom{11}{4}\binom{7}{4}\binom{3}{2}\binom{1}{1} = \frac{11!}{4!4!2!1!}$

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

Theorem 9.6.1 (Number of r-combinations with Repetition Allowed)**.** (multisets of size r) that can be selected from a set of n elements is $\binom{r+n-1}{r}$ = number of ways r objects can be selected from n categories of objects with repetitions allowed

Defn. Which formula to use?

	Order Matters	Order Does Not Matter
Repetition	n^k	$\binom{k+n-1}{k}$
No Repetition	$P(n,k)$	$\binom{n}{k}$

Theorem 9.7.1 (Pascals Formula)**.** Let n and r be positive integers, $r \leq n$. Then $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

Defn. Combinations
1. For $0 \leq k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$
2. For $0 \leq k \leq n$, $k\binom{n}{k} = n\binom{n-1}{k-1}$

Theorem 9.7.2. Binomial Theorem Given any real numbers a and b and any non-negative integer n,
$(a+b)^n = \sum\limits_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

Theorem [. Probability Axioms] P is a probability function from the set of all events in S.

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

Defn (Probability of General Union of 2 events)**.** If A and B are events in S, then $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Defn (Expected Value)**.** $= \sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + ... + a_n p_n$, where a is outcome and p is probability of outcome

Defn (Linearity of Expectation)**.** Expected Value of sum of random variables x and y $= E[X+Y] = E[X] + E[Y]$,

Defn (Conditional Probability)**.** of B given A, $P(B|A) = \frac{P(A \cap B)}{P(A)}$

Theorem 9.9.1 (Bayes' Theorem)**.** Sample space S is union of mutually disjoint events $B_1, B_2, ..., B_n$ and Suppose A is an event in S, and suppose $P(A) \neq 0$ and $P(B_i) \neq 0$.
$P(B_k|A) = \frac{P(A|B_k) \cdot P(B_k)}{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + ... + P(A|B_n) \cdot P(B_n)} = \frac{P(A|B_k) \cdot P(B_k)}{P(A)}$

Defn (Independent Event)**.** If A and B are events in S, then A and B are independent, if and only if $P(A \cap B) = P(A) \cdot P(B)$

Defn (Pairwise Independent and Mutually Independent)**.** A, B and C are events in S. A, B, C are pairwise independent iff they satisfy conditions 1-3. Mutually independent iff all 4 conditions satisfied

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. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

Graphs

Defn (Undirected Graph)**.** 2 finite sets: Nonempty set of vertices V, set of edges, where each edge is associated with 1 or 2 vertices.
Adjacent Vertice - 2 vertices connected by edge
Adjacent Edges - 2 edges incident on same endpoint

Defn (Directed Graph)**.** Same as undirected but has set of Directed Edges E, where each edge is an ordered pair of vertices

Defn (Simple Graph)**.** is undirected graph without any loops or parallel edges

Defn (Complete Graph)**.** on n vertices, $n > 0, K_n$ is simple graph with n vertices and exactly 1 edge connecting each pair of distinct vertices (All of the nodes are directly connected)

Defn (Bipartite Graph)**.** is simple graph whose vertices can be divided to 2 disjoint sets U and V such that every edge connects U to one in V

Defn (Complete Bipartite Graph)**.** is bipartite graph on 2 disjoint sets U and V such that every vertex in U connects to every in Vertex in V. If |U| = m, |V| = n, complete bipartite graph is $K_{m,n}$

Defn (Subgraph of a Graph)**.** H is subgraph of G iff every vertex in H is in G, every edge in H is in G, every edge in H has same endpoints as G

Defn (Degree of Vertex)**.** Degree of v, $deg(v)$ = number of edges incident on v, with loops counted twice.
Total degree of G, $deg(G)$ = sum of all degrees of all vertices in G

Theorem 10.1.1 (Handshake Theorem)**.** If G is any graph, $deg(G) = deg(v_1) + deg(v_2) + ... + deg(v_n) = 2 \times |E|$, where E is the set of edges in G.

Corollary. 10.1.2 Total Degree of a graph is even

Proposition. 10.1.3 There are even number of vertices of odd degree

Defn (Indegree, Outdegree)**.** G=(V,E) be directed graph and v a vertex of G.
Indegree of v, $deg^-(v)$ is number of directed edges that end at v.
Outdegree of v, $deg^+(v)$ is number of directed edges that originate from v.
$\sum_{v \in V} deg^-(v) = \sum_{v \in V}^+(v) = |E|$

Defn (Walks)**.** G be graph and v, w be vertices of G.
Walk from v to w is an finite alternating sequence of vertices and edges of G. Walk has the form $v_0 e_1 v_1 e_2 ... v_{n-1} e_n v_n$, where $v_0 = v, v_n = w$. Number of edges n is length of walk (repeat edge/vertex)
Trivial Walk from v to v - Single Vertex v
Trail from v to w - walk without repeated edge
Path from v to w - trail without repeated vertex and edges
Closed Walk - Walk that starts and ends at same vertex (Repeated Vertex)
Circuit - Closed Walk length at least 3 without repeated edge (Repeated Vertex)
Simple Circuit - No repeated vertex except first and last
Cyclic - Loops or cycle, otherwise **Acyclic**

Defn (Connecteddness)**.** Vertices are connected iff walk from v to w. G is connected iff $\forall$ vertices $v, w \in V, \exists$ a walk from v to w. (All vertices are connected)

Lemma. 10.2.1 Let G be a graph

1. If G is connected, any 2 distinct vertices are connected by path
2. If v and w are part of circuit in G, and one edge is removed, there exists trail from v to w in G
3. G is connected and G contains circuit, edge of circuit can be removed without disconnecting G

Defn (Connected Component)**.** (Subgraph of largest possible size) H is connected component iff

1. H is subgraph of G
2. H is connected
3. No connected subgraph of G has H as subgraph and contains vertices of edges not in H.

Defn (Euler Circuit)**.** Contains every vertex and traverses every edge exactly once (Can repeat vertices)

Defn (Euler Graph)**.** Contains Euler Circuit

Theorem 10.2.2. If graph has euler circuit, ever vertex of graph has positive even degree

Theorem 10.2.2. (Contrapositive) If vertex has odd degree, then graph does not have Euler circuit

Theorem 10.2.3. G is connected and degree of every vertex of G is even integer, then G has Euler circuit

Theorem 10.2.4. G has euler circuit iff G is connected and every vertex has even degree

Defn (Euler Trail)**.** passes through every vertex at least one and edge only once

Corollary. 10.2.5 Euler trail from v to w iff G is connected, v and w have odd degree and all other vertices have even degree

Defn (Hamiltonian Circuit)**.** Simple circuit that includes every vertex of G (Every vertex appears once

Defn (Hamilton Graph)**.** Contains Hamilton Circuit

Proposition. 10.2.6 If G has Hamiltonian Circuit, G has subgraph H with the following

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

Defn (Adjacency Matrix)**.** **A**$= (a_{ij})$ over the set of non-negative integers s.t. a_{ij} = number of arrows from v_i to v_j

Theorem 10.3.2 (Number of walks of length n)**.** A is adjacency matrix of G, the ij-th entry of A^n = number of walks of length n from v_i to v_j

Defn (Isomorphic Graph)**.** $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$
G is isomorphic to G', denoted $G \cong G'$, iff bijections $g : V_G \to V_{G'}$ and $h : E_G \to E_{G'}$, that preserve edge-edgepoint functions of G and G', in sense that $\forall v \in V_G, e \in E_G, v$ is an endpoint of $e \iff g(v)$ is and endpoint of $h(e)$

Theorem 10.4.1 (Graph Isomorphism is Equivalence Relation)**.** S be set of graphs and let $\cong$ be relation of graph isomorphism on S. $\cong$ is equivalence relation on S

Defn (Planar Graph)**.** is graph that can be drawn on 2D plane without edges crossing

Theorem Kuratowski's Theorem. Planar iff does not contain subgraph that is a subdivision of K_5 or complete bipartite $K_{3,3}$

Theorem Euler's Formula. For planar simple graph, let f be number of faces, $f = |E| - |V| + 2$

Trees

Defn (Tree)**. Tree** iff circuit free and connected
Trivial Tree iff Single Vertex
Forest iff circuit-free and not connected

Lemma. 10.5.1 Non trivial tree has at least one vertex of degree 1

Defn (Terminal Vertex and Internal Vertex)**.** Vertex of degree 1 in T is terminal vertex, vertex of degree greater than 1 is internal vertex

Theorem 10.5.2. Any tree with n vertices $(n > 0)$ has $n - 1$ edges

Defn. E.g. Find all non-isomorphic trees with 4 vertices 4 vertices means 3 edges = total degree of 6. So $deg(a) + deg(b) + deg(c) + deg(d) = 6$

Lemma. 10.5.3 G is connected graph, C is any circuit, one of the edges of C is removed from G, the graph remains connected

Theorem 10.5.4. G is a connected graph with n vertices and n-1 edges, G is a tree

Defn (Rooted Tree, Level, Height)**. Rooted tree** is a tree with 1 vertex distinguished from others called root
Level of a vertex is no of edges between it and root
Height of a rooted tree is max level of any vertex of the tree

Defn (Child, Parent, Sibling, Ancestor, Descendant)**. Children** of v are all vertices that are adjacent to v and 1 level farther away from the root than v
Parent if w is a child of v, then v is parent of w, and 2 vertices that are both children of same parent is **siblings**
Ancestor if v lies on unique path between w and root, v is ancestor of w, and w is **descendant** of v

Defn (Binary Tree, Full Binary Tree)**.** **Binary Tree** is rootred tree with every parent at most 2 children. Each child is either left child or right child.
Full Binary Tree is where every parent has exactly 2 children

Defn (Left Subtree)**.** Root is the left tree of v, vertices consist of left child o v and all its descendants, whose edges consist of all those edges of T that connect vertices of left subtree

Theorem 10.6.1 (Full Binary Tree Theorem)**.** If T is full binary tree with k internal vertices, then T has total of $2k+1$ vertices, and has $k+1$ terminal vertices (leaves

Theorem 10.6.2. non-negative integers h, if T is any binary tree with height h and terminal vertices (leaves), then $t \leq 2^h$, $\log_2 t \leq h$

Defn (Breadth-First Search)**.** Starts at root, visit adjacent vertices, and then next level

Defn. Depth-First Search
Pre-order Print root, traverse left, traverse right
In-order Traverse Left, Print Root, Traverse right
post-order Traverse Left, Traverse Right, Print Root

Defn (Spanning Tree)**.** Subgraph 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 same number of edges

Defn. Weighted Graph and Minimum Spanning Tree
Weighted Graph is a graph for which each edge has a positive real number weight. Total weight = sum of weights of all edges
Minimum Spanning Tree Least possible total weight compared to all other spanning trees for graph

Theorem Kruskal's Algorithm. , Input is a connected weighted graph with n vertices

1. Initialise T to have all vertices of G and no edges
2. Let E be set of Edges in G and m = 0
3. While $(m < n - 1)$
   (a) Find e in E of least weight
   (b) Delete e from E
   (c) If adding e to T does not create circuit, add e to T and set m = m + 1

Theorem Prim's Algorithm. Input is a connected weighted graph with n vertices

1. Pick vertex v of G and let T be graph with this vertex only
2. Let V be set of all vertices of G except v
3. For i = 1 to n - 1
   (a) Find edge e of G s.t. e connects T to one vertice in V, e has the least weight of all edges connecteing T to V. Let w be endpoint of e in V
   (b) Add e and w to T, delete w from V