CS1231S Discrete Structures

AY 24/25 Sem 1 — github/omgeta

Definitions

Special types of integers:

i. n is even $\leftrightarrow \exists k \in \mathbb{Z}\ (n = 2k)$
ii. n is odd $\leftrightarrow \exists k \in \mathbb{Z}\ (n = 2k + 1)$
iii. n is prime $\leftrightarrow (n > 1) \wedge \forall r, s \in \mathbb{Z}^+$ $(n = rs \rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$
iv. n is composite $\leftrightarrow \exists r, s \in \mathbb{Z}^+$ $(n = rs \wedge (1 < r < n) \wedge (1 < s < n))$

Floor and ceiling for $x \in \mathbb{R}$:

i. $\forall x \in \mathbb{R}, n \in \mathbb{Z}\ (\lfloor x \rfloor = n \leftrightarrow n \leq x < n + 1)$
ii. $\forall x \in \mathbb{R}, n \in \mathbb{Z}\ (\lceil x \rceil = n \leftrightarrow n - 1 < x \leq n)$

Divisibility:

i. $d|n \leftrightarrow \exists k \in \mathbb{Z}\ (n = dk)$

Congruence:

i. $a \equiv b \pmod{n} \leftrightarrow n \mid (a - b) \leftrightarrow a - b = nk$

Useful Results

Divisor results:

i. $\forall a, b \in \mathbb{Z}^+\ (a \mid b \rightarrow a \leq b)$ (Th. 4.4.1)
ii. Only divisors of 1 are 1 and -1 (Th. 4.4.2)
iii. $\forall a, b \in \mathbb{Z}\ (a \mid b \wedge b \mid c \rightarrow a \mid c)$ (Th. 4.4.3)
iv. $\forall n \in \mathbb{Z}^+$ (n is divisible by a prime) (Th. 4.4.4)

Real results:

i. $\forall x, y \in \mathbb{R}\ (|x + y| \leq |x| + |y|)$ (Triangle Inequality)
ii. $\forall x, m \in \mathbb{R}, \mathbb{Z}\ (\lfloor x + m \rfloor = \lfloor x \rfloor + m)$ (Th. 4.6.1)

Quotient-Remainder Theorem:

i. $\forall n \in \mathbb{Z}, d \in \mathbb{Z}^+, \exists q, r \in \mathbb{Z}\ (n = dq + r \wedge 0 \leq r < d)$
ii. n div $d = q \wedge n$ mod $d = r$

1. Logic

Statement forms are expressions made up of statement variables and logical operators.

Operators of a compound statement of p, q are given by:

i. $p \equiv q$ (equivalent)
ii. $\sim p$ (NOT)
iii. $p \wedge q$ (AND)
iv. $p \vee q$ (OR)
v. $p \oplus q$ (XOR)
vi. $p \rightarrow q$ (implies)
vii. $p \leftrightarrow q$ (iff)

where implication $p \rightarrow q$ can be re-expressed as:

i. if p then q
ii. p only if q
iii. p is sufficient for q
iv. q if p
v. q is necessary for r

Quantified statements are made up of predicates $P(x)$ over a domain D with logical operators and quantifiers in the form:

i. $\forall x \in D, P(x)$ (Universal statement)
ii. $\exists x \in D, P(x)$ (Existential statements)

Arguments

Arguments are a sequence of statements, beginning with premises and ending with a conclusion.

Valid arguments have the condition: if all premises are true, then the conclusion is true.

Sound arguments are valid and all premises are true.

Rules of Inference

i. $p \rightarrow q$
p
$\therefore q$ (Modus ponens)

ii. $p \rightarrow q$
$\sim q$
$\therefore \sim p$ (Modus tollens)

iii. p
$\therefore p \vee q$ (Generalization)

iv. $p \wedge q$
$\therefore p$ (Specialization)

v. p
q
$\therefore p \wedge q$ (Conjunction)

vi. $p \vee q$
$\sim p$
$\therefore q$ (Elimination)

vii. $p \rightarrow q$
$q \rightarrow r$
$\therefore p \rightarrow r$ (Transitivity)

viii. $p \vee q$
$p \rightarrow r$
$q \rightarrow r$
$\therefore r$ (Proof by division into cases)

ix. $\sim p \rightarrow \mathbf{f}$
$\therefore p$ (Contradiction)

x. $\forall x \in D, P(x)$
$\therefore P(c)$ if $c \in D$ (Universal instantiation)

xi. $P(c)$ for arbitary $c \in D$
$\therefore \forall x \in D, P(x)$ (Universal generalization)

xii. $\exists x \in D, P(x)$
$\therefore P(c)$ for some $c \in D$ (Existential instantiation)

xiii. $P(c)$ for some $c \in D$
$\therefore \exists x \in D, P(x)$ (Existential generalization)

2. Set Theory

Sets are unordered collections of objects with elements described as:

i. $\{a, b, \ldots\}$ (Set-Roster Notation)
ii. $\{x \in U : P(x)\}$ (Set-Builder Notation)
iii. $\{t(x) : x \in U\}$ (Replacement Notation)

Operators on sets A, B are given by:

i. $A \subseteq B \leftrightarrow x \in A \rightarrow x \in B$ (Subset)
ii. $A = B \leftrightarrow A \subseteq B \wedge B \subseteq A$ (Equality)
iii. $\overline{A} = \{x : x \notin A\}$ (Complement)
iv. $A \cap B = \{x : x \in A \wedge x \in B\}$ (Intersection)
v. $A \cup B = \{x : x \in A \vee x \in B\}$ (Union)
vi. $A \setminus B = \{x : x \in A \wedge x \notin B\}$ (Difference)
vii. $A \times B = \{(a, b) : a \in A \wedge b \in B\}$(Cartesian product)
viii. $\mathcal{P}(A) = \{X : X \subseteq A\}$ (Powerset)
ix. $|A|$ = number of elements in A (Cardinality)

Theorem 6.2.3.:

i. $A \cap B \subseteq A$ and $A \cap B \subseteq B$ (Inclusion of $\cap$)
ii. $A \subseteq A \cup B$ and $B \subseteq A \cup B$ (Inclusion in $\cup$)
iii. $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$ (Transitivity of subsets)

Partitions

Partitions of a set A are groupings of its elements into non-empty, mutually disjoint subsets such that every element of A is included in exactly one subset.

Properties of a partition $\{A_1, A_2, \ldots, A_n\}$ of set A, are:

i. $A_i \cap A_j = \phi$ for all $i \neq j$ (Mutually disjoint)
ii. $\bigcup_{i=1}^{n} A_i = A$ (Exhaustiveness)

3. Relations

Relation R from domain A to codomain B is given by:

i. $R = \{(a, b) \in A \times B : aRb \leftrightarrow P(a, b)\}$
ii. $R^{-1} = \{(b, a) \in B \times A : aRb\}$ (Inverse)

Possible properties of a relation R on A are:

i. $\forall a \in A\ (aRa)$ (Reflexive)
ii. $\forall a \in A\ (a \not R a)$ (Irreflexive)
iii. $\forall a, b \in A\ (aRb \rightarrow bRa)$ (Symmetric)
iv. $\forall a, b \in A\ (aRb \wedge bRa \rightarrow a = b)$ (Anti-symmetric)
v. $\forall a, b \in A\ (aRb \rightarrow b \not R a)$ (Asymmetric)
vi. $\forall a, b, c \in A\ (aRb \wedge bRc \rightarrow aRc)$ (Transitive)

Composition of relations $R \subseteq A \times B$, $S \subseteq B \times C$, $T \subseteq C \times D$ is given by:

i. $S \circ R = \{(a, c) \in A \times C : \exists b \in B\ (aRb \wedge bSc)\}$
ii. $T \circ (S \circ R) = (T \circ S) \circ R$ (Associative)
iii. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$ (Inverse)

Transitive closure R^t of relation R is the smallest transitive relation containing R such that:

i. R^t is transitive
ii. $R \subseteq R^t$
iii. S is any other transitive relation of $R \rightarrow R^t \subseteq S$

Equivalence Relation

Relation $\sim$ is an equivalence relation if and only if it is reflexive, symmetric and transitive.

Partitions induced by equivalence relation $\sim$ on A are defined by:

i. $[a]_\sim = \{x \in A : a \sim x\}$ (Equivalence class)
ii. $A/\!\sim\, = \{[x]_\sim : x \in A\}$ (Set of equivalence classes)

Useful Results:

i. $a \sim b \rightarrow [a]_\sim = [b]_\sim$ (Lem. 8.3.2)
ii. either $[a]_\sim = [b]_\sim$ or $[a]_\sim \cap [b]_\sim = \phi$ (Lem. 8.3.2)

Partial Order

Relation $\preccurlyeq$ is a partial order if and only if it is reflexive, anti-symmetric and transitive. Partially ordered set (poset) of A w.r.t. partial order $\preccurlyeq$ is denoted by $(A, \preccurlyeq)$.

Extremal elements $c \in A$ of a partial order $\preccurlyeq$ on A are given by:

i. c is maximal $\leftrightarrow \forall x \in A\ (c \preccurlyeq x \rightarrow c = x)$
ii. c is minimal $\leftrightarrow \forall x \in A\ (x \preccurlyeq c \rightarrow c = x)$
iii. c is the largest $\leftrightarrow \forall x \in A\ (x \preccurlyeq c)$
iv. c is the smallest $\leftrightarrow \forall x \in A\ (c \preccurlyeq x)$

Total Order

Total order $\preccurlyeq^*$ on A is a relation such that:

i. $\preccurlyeq^*$ is a partial order
ii. $\forall a, b \in A\ (a \preccurlyeq^* b \vee b \preccurlyeq^* a)$ (Totally comparable)

Totally ordered sets $(A, \preccurlyeq^*)$ are well-ordered if and only if every non-empty subset of A contains a smallest element:

$$\forall S \in \mathcal{P}(A), S \neq \phi \rightarrow (\exists x \forall y \in S\ (x \preccurlyeq^* y))$$

Linearizations

A linearization is a derivation of a total order $\preccurlyeq^*$ from a partial order $\preccurlyeq$ on A such that:

$$\forall a, b \in A\ (a \preccurlyeq b \rightarrow a \preccurlyeq^* b)$$

4. Functions

Function f from domain set X to codomain set Y, denoted $f : X \to Y$ is a relation satisfying:

i. $\forall x \in X\ \exists y \in Y\ ((x, y) \in f)$ (F1)
ii. $\forall x \in X\ \forall y_1, y_2 \in Y$
$(((x, y_1) \in f \land (x, y_2) \in f) \to y_1 = y_2)$ (F2)
iii. $\forall x \in X\ \exists! y \in Y\ ((x, y) \in f)$ (F3=F1+F2)

Setwise functions for $f : X \to Y$ on sets $A \subseteq X$, $B \subseteq Y$ are given by:

i. $f(A) = \{f(x) : x \in A\}$ (Setwise image)
ii. $f^{-1}(B) = \{x \in X : f(x) \in B\}$ (Setwise preimage)

Possible properties of a function $f : X \to Y$ are:

i. $\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \to x_1 = x_2)$ (Injective)
ii. $\forall y \in Y\ \exists x \in X\ (y = f(x))$ (Surjective)
iii. $\forall y \in Y\ \exists! x \in X\ (y = f(x))$ (Bijective)

Inverse function $f^{-1} : Y \to X$ is uniquely given by:

i. $\forall x \in X\ \forall y \in Y\ (y = f(x) \leftrightarrow x = f^{-1}(y))$
ii. f is bijective $\leftrightarrow$ f has an inverse (Th. 7.2.3)

Composition of functions $f : X \to Y$, $g : Y \to Z$, $h : Z \to W$ is given by:

i. $(g \circ f) : X \to Z = (g \circ f)(x) = g(f(x))$
ii. $(h \circ g) \circ f = h \circ (g \circ f)$ (Associative)
iii. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (Inverse)
iv. $f \circ id_X = f$ and $id_Y \circ f = f$ (Th. 7.3.1)
v. $g \circ f$ is injective $\leftrightarrow$ f, g are injective (Th. 7.3.3)
vi. $g \circ f$ is surjective $\leftrightarrow$ f, g are surjective (Th. 7.3.4)

Sequences

Sequence $a_0, a_1, \cdots$ can be represented by:

i. $a(n) = a_n, \forall n \in \mathbb{Z}_{\geq 0}$
ii. $a_0, a_1, \cdots = b_0, b_1, \cdots \leftrightarrow a(n) = b(n), \forall n \in \mathbb{Z}_{\geq 0}$

Strings

Strings over set A are given by:

i. $a_0 a_1 \cdots a_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$
ii. ε is the empty string
iii. $a_0 a_1 \cdots a_{l-1} = b_0 b_1 \cdots b_{l-1} \leftrightarrow a_i = b_i, \forall i \in [0, l-1]$

Well-Defined Functions

Function $f : X \to Y$ is well-defined if and only if $\forall x_1, x_2 \in X$:

i. $(x_1 = x_2 \to f(x_1) = f(x_2))$ (General)
ii. $(x_1 \sim x_2 \to f(x_1) = f(x_2))$ (w.r.t $\sim$)
iii. $([x_1] = [x_2] \to [f(x_1)] = [f(x_2)])$ (w.r.t $[x]$)

5. Cardinality

Cardinality of sets A, B is the same, $|A| = |B|$ if and only if there is a bijection $f : A \to B$

Countability of set A is given by:

i. $|A| = |\mathbb{Z}_n|$ for some $n \in \mathbb{Z}^+$ ((Countably) Finite)
ii. $|A| = |\mathbb{Z}^+| = \aleph_0$ (Countably Infinite)
iii. Otherwise (Uncountable)

Countabilility of set B via sequences is given by:

i. B is countable $\leftrightarrow b_0, b_1, \cdots \in B$ is a sequence in which every element of B appears (Lem. 9.2)

Useful Results:

i. Subset of countable set is countable (Th. 7.4.3)
ii. Sets with uncountable subsets are uncountable (Coro. 7.4.4)
iii. Every infinite set has a countably infinite subset (Prop. 9.3)
iv. $A_1, \cdots, A_n$ are countably infinite $\to A_1 \times \cdots \times A_n$ is countably infinite (Th. 9.2.5)
v. $A_1, A_2 \cdots$ are countable $\to \bigcup_{i=1}^{\infty} A_i$ is countable (Th. 9.2.5)
vi. B is countably infinite and C is finite $\to B \cup C$ is countable (Tut. 8Q2)
vii. $A_1, A_2, \cdots$ are finite $\to \Cup_{i=1}^{n} A_i$ is finite (Tut. 8Q3)
viii. $A_1, A_2, \cdots$ are countable $\to \Cup_{i=1}^{n} A_i$ is countable (Tut. 8Q4)
ix. B is infinite and C is finite $\to$ there is bijection $B \cup C \to B$ (Tut. 8Q6)
x. A is countably infinite $\to \mathcal{P}(A)$ is uncountable (Tut. 8Q7)

Pigeonhole Principle

For finite sets A, B:

i. $\exists$ injection $f : A \to B \to |A| \leq |B|$
ii. $\exists$ surjection $f : A \to B \to |A| \geq |B|$ (Dual)

Generalised PHP for a function $f : X \to Y$:

i. $k < \frac{|X|}{|Y|} \to \exists y \in Y \ (|f^{-1}(y)| \geq k+1)$
ii. $\forall y \in Y \ (|f^{-1}(y)| \leq k) \to |X| \leq k|Y|$ (Contrap.)

Cantor's Diagonalization

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

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots \\ x_2 &= 0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots \\ &\cdots \\ x_n &= 0.a_{n1}a_{n2}a_{n3}\cdots a_{nn}\cdots \\ &\cdots \end{aligned}$$

4. Construct $d = 0.d_1d_2d_3\cdots d_n\cdots$ s.t.

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

5. Note $\forall n \in \mathbb{Z}^+, d_n \neq a_{nn}$. Thus, $d \neq x_n, \forall n \in \mathbb{Z}^+$
6. This contradicts $d \in (0,1)$. $\therefore (0,1)$ is uncountable.

6. Counting

Counting Formula: $\binom{n}{r} = \dfrac{n!}{r!(n-r)!}, P(n,r) = \dfrac{n!}{(n-r)!}$

Binomial Theorem: $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$

Pascal's Formula: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

Inclusion/Exclusion Principle for finite sets A, B, C:

i. $|A \cup B| = |A| + |B| - |A \cap B|$
ii. $|A \cup B \cup C| = |A| + |B| + |C| + |A \cap B \cap C|$ $-|A \cap B| - |A \cap C| - |B \cap C|$

Number of ways to:

i. Permute n distinct $= n!$
ii. Permute n with n_1, n_2 identical $= \frac{n!}{n_1!n_2!}$
iii. Choose r of n distinct $= \binom{n}{r}$
iv. Choose r groups of n identical $= \binom{n+r-1}{n}$ $(x_1 + \cdots + x_r = n)$
v. Permute r of n distinct $= P(n,r)$
vi. Permute r of n distinct (repeat) $= n^r$

Useful results:

i. Choose 2 groups of r, m from n distinct $= \binom{n}{r}\binom{n-r}{m}$
ii. Choose k groups of r from n distinct $= \frac{\binom{n}{r}\binom{n-r}{r}\cdots\binom{r}{r}}{k!}$
iii. Permute n distinct with r together $= (n-r+1)!r!$
iv. Permute n, m distinct but separated $= m!\binom{m+1}{n}n!$
v. Permute n distinct in a circle $= (n-1)!$
vi. Permute n distinct with r together in a circle $= (n-r)!r!$
vii. Permute n, m distinct but separated in a circle $= m!\binom{m}{n}n!$
viii. Permute n distinct in a circle with 2 opposite $= (n-2)!$
ix. Permute n distinct in a circle with r identical $= \frac{(n-1)!}{r!}$

Probability

Probability of event E in sample space S, $P(E)$, is given by:

i. $P(E) = \frac{|E|}{|S|}$, where $0 \leq P(E) \leq 1$
ii. $P(\overline{E}) = 1 - P(E)$ (Complement)
iii. $A \cap B = \phi \to P(A \cup B) = P(A) + P(B)$ (Disjoint)
iv. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$ (Union)

Conditional probability of B given A, $P(B|A)$, is given by:

i. $P(B|A) = \dfrac{P(A \cap B)}{P(A)} = \dfrac{P(A|B)P(B)}{P(A)}$ (Th. 9.9.1)
ii. $P(A \cap B) = P(B|A) \cdot P(A)$ (Th. 9.9.2)
iii. $P(A) = \dfrac{P(A \cap B)}{P(B|A)}$ (Th. 9.9.3)

Baye's Theorem, for sample space S being a union of mutually disjoint $B_1, \cdots B_n$:

$$P(B_k|A) = \frac{P(A|B_k)P(B_k)}{P(A|B_1)P(B_1) + \cdots + P(A|B_n)P(B_n)}$$

Mutually exclusive events A, B have special results:

i. $P(A \cap B) = 0$ (Intersection)
ii. $P(A \cup B) = P(A) + P(B)$ (Union)

Independent events A, B have special results:

i. $P(A \cap B) = P(A) \cdot P(B)$ (Intersection)
ii. $P(A|B) = P(A)$ (Conditional)

Expected Value

Expected value of an experiment X, $E(X)$, with real numbers $a_1, \cdots, a_n$ at probabilities $p_1, \cdots, p_n$ is given by:

i. $E(X) = \displaystyle\sum_{k=1}^{n} a_k p_k = a_1p_1 + \cdots + a_np_n$
ii. $E(g(X)) = \displaystyle\sum_{k=1}^{n} g(a_k)p_k$
iii. $E(aX \pm b) = aE(X) \pm b$

Linearity of Expectation for (not necessarily independent) random experiments X, Y have their sum given by:

$$E(X+Y) = E(X) + E(Y)$$

7. Graphs

Undirected graph $G = (V, E)$ consists of edges $e = \{v, w\} \in E$ connecting adjacent vertices $v, w \in V$.
Adjacent edges are incident on the same endpoints.
Degree of vertex v, $\deg(v)$, is given by:

i. $\deg(v) =$ no. edges incident on v
ii. $\deg(G) = 2 \times |E|$ (Handshake Th.)
iii. $\deg(G)$ is even (Coro. 10.1.2)
iv. Any graph has even number of vertices of odd degree (Prop. 10.1.3)

Directed graph (digraph) $G = (V, E)$ consists of ordered edges $e = (v, w) \in E$ from $v \in V$ to $w \in V$.
Indegree and outdegree of vertex v, $\deg^-(v)$ and $\deg^+(v)$, is given by:

i. $\deg^-(v) =$ no. edges ending on v
ii. $\deg^+(v) =$ no. edges originating from v
iii. $\sum_{v \in V} \deg^-(v) + \sum_{v \in V} \deg^+(v) = |E|$

Graph $H = (V_H, E_H)$ is a subgraph of graph $G = (V, E)$ iff $V_H \subseteq V$ and $E_H \subseteq E$.

Trails, Paths and Circuits

Walk is a finite alternating sequence of adjacent vertices and edges in the form $v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$ with length being the number of edges n.
Trivial walk consists of the single vertex.
Closed walk is a walk starting and ending at the same vertex.

Trail is a walk with no repeated edge.
Path is a trail with no repeated vertex.

Circuit/cycle is a closed walk of length at least 3 with no repeated edge (i.e. a trail).
Simple circuit/cycle is a cycle with no repeated vertex except the first and last (i.e. a partial path).

Adjacency matrix of graph G with $|V| = n$ is the $n \times n$ matrix $A = (a_{ij})$ such that $a_{ij} =$ edges connecting v_i to v_j:

i. $(A^n)_{ij} =$ number of walks of length n from v_i to v_j

Connectedness

Vertices are connected iff there is a walk between them.
Graphs are connected iff there is a walk between every two vertices.
Lemma 10.2.1 for connected graph G:

i. There is a path between any two distinct vertices
ii. If G contains a cycle with vertices v, w and one edge is removed from the cycle, then there still exists a trail from v to w
iii. If G contains a cycle, then an edge can be removed from the cycle without disconnecting G

Graph H is a connected component of G iff H is a connected subgraph of G, and no other connected subgraph of G has H as a subgraph.

Euler and Hamilton

Euler trail is a trail passing every vertex atleast once, and every edge exactly once:

i. $\exists$ Euler trail from v to $w \leftrightarrow G$ is connected, v and w have odd degree and all other vertices have even degree (Coro. 10.2.5)

Euler circuit is an Euler trail which is also a circuit, enstarting and ending at the same vertex:

i. G has Euler circuit $\rightarrow$ every vertex has positive even degree (Th. 10.2.2)
ii. Some vertex has odd degree $\rightarrow G$ nas no Euler circuit (Contra. Th. 10.2.2)
iii. G is connected and every vertex has positive even degree $\leftrightarrow G$ has Euler circuit (Th. 10.2.4)

Hamiltonian circuit is a simple circuit passing every vertex exactly once.
Proposition 10.2.6 for Hamiltonian graph G, there is a subgraph H:

i. H contains every vertex in G
ii. H is connected
iii. H has same number of vertices as edges
iv. Every vertex of H has degree 2

Special Graphs

Simple graph is an undirected graph with no loops or parallel edges (at most one edge between distinct vertices). It has max $\binom{n}{2}$ edges.

Complete graph of $n > 0$ vertices, K_n is a simple graph with exactly one edge between all distinct vertices. It has exactly $\binom{n}{2}$ edges.

Bipartite graph (bigraph) is a simple graph divisible into two disjoint sets U, V such that every edge connects a vertex in U to a vertex in V. It has max mn edges.

Complete bipartite graph of $|U| = m, |V| = n$, $K_{m,n}$, is a bipartite graph with exactly one edge between each vertex in U to each vertex in V. It has exactly mn edges.

Eulerian graph is a graph that contains an Euler circuit.

Hamiltonian graph is a graph that contains a Hamiltonian circuit.

Planar Graph is a graph that can be drawn without edges crossing:

i. A finite graph is planar $\leftrightarrow$ it does not contain a subgraph that is a subdivision of K_5 or $K_{3,3}$
ii. faces $= |E| - |V| + 2$ (Euler's Formula)

Weighted Graph is a graph where each edge has a positive real weight, $w(e)$, and total weight of the graph, $w(G)$.

Isomorphisms

Graphs $G = (V, E)$ and $G' = (V', E')$ are isomorphic iff there are bijections which preserve the edge-endpoint functions:

$$g : V -> V', \quad h : E -> E'$$
$$v \text{ is an endpoint of } e \leftrightarrow g(v) \text{is an endpoint of } h(e)$$

Simple graphs $G = (V, E)$ and $G' = (V', E')$ are isomorphic iff there is a permutation:

$$\pi : V \rightarrow V' \ \{v, w\}E \leftrightarrow \{\pi(v), \pi(w)\} \in E'$$

Theorem 10.4.1: Isomorphism relation is an equivalence relation on the set of all graphs.

8. Trees

Trees are simple graphs which are acylic and connected.
Terminal vertices/ leafs are vertices with degree 1.
Internal vertices are vertices with degree more than 1.

Properties of Trees:

i. Non-trivial trees has at least one vertex of degree 1 (Lem. 10.5.1)
ii. Any tree with $n > 0$ vertices has $n - 1$ edges (Th. 10.5.2)
iii. If G is any connected graph, removing an edge of a circuit C keeps G connected (Lem. 10.5.3)
iv. If G is a connected graph with n vertices and $n - 1$ edges, then G is a tree (Th. 10.5.4)

Forests are simple graphs which are acyclic and not connected.

Special Trees

Rooted tree is a tree with a designated root vertex:

i. Level of a vertex is the number of edges to the root
ii. Height of a rooted tree is the maximum level of any vertex
iii. A vertex's children are adjacent vertices one level deeper, with the vertex is their parent
iv. A vertex is an ancestor if it lies on the path between the descendant vertex and the root

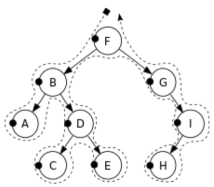
Binary tree is a rooted tree where each parent has maximum two children:

i. Left/Right subtree is the binary tree whose root is the left/right child
ii. Height h with t leaves $\to t \leq 2^h \leftrightarrow \log_2 t \leq h$ (Th. 10.6.2)

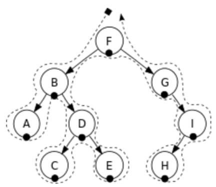
Full binary tree is a binary tree where each parent has exactly two children:

i. k internal vertices $\to 2k + 1$ vertices and $k + 1$ leaves (Th. 10.6.1)

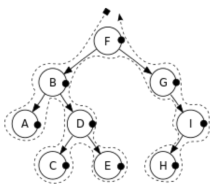
DFS Traversal



Pre-order:
F, B, A, D, C, E, G, I, H



In-order:
A, B, C, D, E, F, G, H, I



Post-order:
A, C, E, D, B, H, I, G, F

Pre-order (print root first):

i. Print root
ii. Traverse left subtree recursively
iii. Traverse right subtree recursively

In-order:

i. Traverse left subtree recursively
ii. Print root
iii. Traverse right subtree recursively

Post-order (print root last):

i. Traverse left subtree recursively
ii. Traverse right subtree recursively
iii. Print root

Spanning Trees

Spanning tree of a graph G is a subgraph tree containing every vertex of G.

Proposition 10.7.1:

i. Every connected graph has a spanning tree
ii. Any two spanning trees for a graph have the same number of edges

Minimum spanning tree of a weighted graph G is the spanning tree with the least possible total weight compared to other spanning trees of G.

Kruskal's Algorithm

Greedily add all lightest edges to the tree that do not form a cycle, until $n - 1$ edges are added.

1. Input: Connected weighted graph $G = (V, E)$ with n vertices
2. $T = (V, E')$, where $E' = \phi$
3. While $|E'| < n - 1$:
   3.1. Pop edge $e \in E$ of least weight
   3.2. Add e to E' if it does not produce a circuit
4. Output: Minimum spanning tree T

Prim's Algorithm

Beginning from a single vertex, find the adjacent edge with the least weight incident on a vertex not in the tree, and add it to the tree, until $n - 1$ edges are added.

1. Input: Connected weighted graph $G = (V, E)$ with n vertices
2. Choose v in V
3. Initialise $T = (V', E')$, where $V = \{v\}, E' = \phi$
4. For $i = 1, n - 1$:
   4.1. Find $e \in E$ adjacent to a vertex in V and a vertex in V' with the least weight
   4.2. Pop edge $w \in V$ incident to e
   4.3. Add e to E' and w to V'
5. Output: Minimum spanning tree T

Catalan Numbers

Catalan number term C_n given by:

$$C_n = \frac{(2n)!}{(n+1)!n!}$$

provides the solution for:

i. Number of full binary trees with $n + 1$ leaves or n internal vertices
ii. Number of non-isomorphic ordered trees/ binary search trees with n vertices

Methods of Proof

Direct Proof

1. Suppose $P(x)$
   1.1. ...
   1.2. $Q(x)$
2. $\therefore P(x) \rightarrow Q(x)$

Proof by Exhaustion

1. Since $x \in A_1 \cup \ldots \cup A_n$
2. Case 1: $x \in A_1$
   2.1. ...
   2.2. $S(x)$
3. ...
4. Case n: $x \in A_n$
   4.1. ...
   4.2. $S(x)$
5. $\therefore S(x)$ for all cases

Proof by Construction

1. Let $x = x_0$
   1.1. $S(x_0)$
2. $\therefore \exists x(S(x))$

Or

1. Suppose $P(x)$
   1.1. ...
   1.2. Find valid conditions for x
2. $\therefore \exists x(S(x))$

Disproof by Counterexample

1. Let $x = x_0$
   1.1. $\sim S(x_0)$
2. $\therefore \sim(\forall x(S(x)))$

Proof by Contradiction

1. Suppose not, i.e. $\sim S(x)$
   1.1. ...
   1.2. This contradicts ...
2. Hence, the supposition is false.
3. $\therefore S(x)$

Proof by Contraposition

1. Suppose $\sim Q(x)$
   1.1. ...
   1.2. $\sim P(x)$
2. Hence, $\sim Q(x) \rightarrow \sim P(x)$.
3. $\therefore P(x) \rightarrow Q(x)$

Proof by 1MI/ Weak Induction

1. Let $P(n) \equiv \cdots, \forall n \in A_{\geq a}$
2. Basis step:
   Show $P(a)$ is true.
3. Inductive hypothesis:
   Assume $P(k)$ is true for some $k \geq a$
4. Inductive step:
   Show $P(k+1)$ is true
5. $\therefore P(n)$ is true for all $n \in A_{\geq a}$

Proof by 2MI/ Strong Induction

1. Let $P(n) \equiv \cdots, \forall n \in A_{\geq a}$
2. Basis step:
   Show $P(a)$ is true.
3. Inductive hypothesis:
   Assume $P(i)$ is true for some $a \leq i \leq k$
4. Inductive step:
   Show $P(k+1)$ is true
5. $\therefore P(n)$ is true for all $n \in A_{\geq a}$

Or

1. Let $P(n) \equiv \cdots, \forall n \in A_{\geq a}$
2. Basis step:
   Show $P(a) \wedge \cdots \wedge P(b)$ are true.
3. Inductive hypothesis:
   Assume $P(k)$ is true for some $k \geq a$
4. Inductive step:
   Show $P(k+b-a+1)$ is true
5. $\therefore P(n)$ is true for all $n \in A_{\geq a}$

Structural Induction

1. Let $P(n) \equiv \cdots, \forall n \in H$
2. Basis step:
   Show $P(a)$ is true for all founders a.
3. Inductive hypothesis:
   Assume $P(x)$ is true for some $x \in H$
4. Inductive step:
   Show $P(f(x))$ is true for all constructors f
5. $\therefore P(n)$ is true for all $n \in H$

Boolean Algebra Laws

Identity	$p \wedge \mathbf{t} = p$	$p \vee \mathbf{f} = p$
Universal bound	$p \wedge \mathbf{f} = \mathbf{f}$	$p \vee \mathbf{t} = \mathbf{t}$
Idempotent	$p \wedge p = p$	$p \vee p = p$
Negation	$p \wedge {\sim}p = \mathbf{f}$	$p \vee {\sim}p = \mathbf{t}$
Double Negation	${\sim}({\sim}p) = p$	
Commutative	$p \wedge q = q \wedge p$	$p \vee q = q \vee p$
Associative	$(p \wedge q) \wedge r = p \wedge (q \wedge r)$	$(p \vee q) \vee r = p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$
Absorption	$p \wedge (p \vee q) = p$	$p \vee (p \wedge q) = p$
De Morgan's	${\sim}(p \wedge q) = {\sim}p \vee {\sim}q$	${\sim}(p \vee q) = {\sim}p \wedge {\sim}q$
Implication	$p \to q \equiv {\sim}p \vee q$	
Contrapositive	$p \to q \equiv {\sim}q \to {\sim}p$	
Converse	$converse(p \to q) \equiv q \to p$	
Inverse	$inverse(p \to q) \equiv {\sim}p \to {\sim}q$	

Set Algebra Laws

Identity	$A \cap U = A$	$A \cup \phi = A$
Universal bound	$A \cap \phi = \phi$	$A \cup U = U$
Idempotent	$A \cap A = A$	$A \cup A = A$
Complement	$A \cap \overline{A} = \phi$	$A \cup \overline{A} = U$
Double Negation	$\overline{\overline{A}} = A$	
Commutative	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Associative	$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$
Distributive	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Absorption	$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$
De Morgan's	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	$\overline{A \cup B} = \overline{A} \cap \overline{B}$
Set Difference	$A \setminus B = A \cap \overline{B}$	

Appendix A

Field Axioms:

F1. $a + b = b + a$ and $ab = ba$

F2. $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$

F3. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

F4. $0 + a = a + 0 = a$ and $1 \cdot a = a \cdot 1 = a$

F5. $a + (-a) = (-a) + a = 0$

F6. $a \cdot (\frac{1}{a}) = (\frac{1}{a}) \cdot a = 1$ $(a \neq 0)$

Order Axioms:

O1. $a + b > 0$ and $ab > 0$ $(a > 0 \wedge b > 0)$

O2. a is positive $\oplus$ $-a$ is positive $(a >\neq 0)$

O3. 0 is not positive

Algebra Laws:

T1. $b = c$ $(a + b = a + c)$

T2. $\exists x(a + x = b)$

T3. $b - a = b + (-a)$

T4. $-(-a) = a$

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

T6. $0 \cdot a = a \cdot 0 = 0$

T7. $b = c$ $(ab = ac \wedge a \neq 0)$

T8. $\exists x(ax = b)$ $(a \neq 0)$

T9. $b/a = b \cdot a^{-1}$ $(a \neq 0)$

T10. $(a^{-1})^{-1} = a$ $(a \neq 0)$

T11. $a = 0 \vee b = 0$ $(ab = 0)$

T12. $(-a)b = a(-b) = -ab$, $(-a)(-b) = ab$ and $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$

T13. $\frac{a}{b} = \frac{ac}{bc}$ $(b \neq 0 \wedge c \neq 0)$

T14. $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ $(b \neq 0 \wedge d \neq 0)$

T15. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ $(b \neq 0 \wedge d \neq 0)$

T16. $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$ $(b \neq 0 \wedge c \neq 0 \wedge d \neq 0)$

T17. $a < b \oplus b < a \oplus a = b$

T18. $a < c$ $(a < b \wedge b < c)$

T19. $a + c < b + c$ $(a < b)$

T20. $ac < bc$ $(a < b \wedge c > 0)$

T21. $a^2 > 0$ $(a \neq 0)$

T22. $1 > 0$

T23. $ac > bc$ $(a < b \wedge c < 0)$

T24. $-a > -b$ $(a < b)$

T25. a and b are both positive or both negative $(ab > 0)$

T26. $a + b < c + d$ $(a < c \wedge b < d)$

T27. $0 < ab < cd$ $(0 < a < c \wedge 0 < b < d)$