CS1231 Cheat Sheet

Appendix A (Epp)

T1 $(a+b=a+c) \to (b=c)$

T2 $\forall a, b \in \mathbb{Z}, \exists! x \ni a+x=b, x=a-b$

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

T4 $-(-a)=a$

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

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

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

T8 $\forall a, b \in \mathbb{Z} \wedge a \neq 0, \exists! x \ni ax=b, x=\frac{b}{a}$

T9 If $a \neq 0$, $\frac{b}{a} = b \cdot a^{-1}$

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

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

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

T13 $\frac{a}{b} = \frac{ac}{bc}$ if $b \neq 0 \wedge c \neq 0$

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

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

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

T17 For all real numbers a and b, exactly one of the following is true: $a<b$, $b<a$ or $a=b$

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

T19 $(a<b) \to (a+c<b+c)$

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

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

T22 $1 > 0$

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

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

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

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

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

Ord1 $\forall a, b \in \mathbb{R}, (a>0) \wedge (b>0) \to (a+b>0) \wedge (ab>0)$

Ord2 For every real number $a \neq 0$, a is positive or $-a$ is positive but not both.

Ord3 The number 0 is not positive.

Logic

Theorems from Epp

Thm 3.2.1 $\sim(\forall x, Q(x)) \equiv \exists x, \sim Q(x)$
Thm 3.2.2 $\sim(\exists x, Q(x)) \equiv \forall x, \sim Q(x)$

Logical Equivalences (Thm 2.1.1)

Commutative	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Identity	$p \wedge true \equiv p$	$p \vee false \equiv p$
Negation	$p \wedge \sim p \equiv false$	$p \vee \sim p \equiv true$
Double Negative	$\sim(\sim p) \equiv p$	
Idempotent	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal Bound	$p \wedge false \equiv false$	$p \vee true \equiv true$
De Morgan's	$\sim(p \vee q) \equiv \sim p \wedge \sim q$	$\sim(p \wedge q) \equiv \sim p \vee \sim q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Implication	$p \to q$	$\sim p \vee q$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Rules of Inference

1. **(Universal) Modus Ponens**
   $p \to q$
   p
   $\therefore q$
2. **(Universal) Modus Tollens**
   $p \to q$
   $\sim q$
   $\therefore \sim p$
3. **Generalization**
   p
   $\therefore p \vee q$
4. **Specialization**
   $p \wedge q$
   $\therefore p$
5. **Conjunction**
   p
   q
   $\therefore p \wedge q$
6. **Elimination**
   $p \vee q$
   $\sim p$
   $\therefore q$
7. **(Universal) Transitivity**
   $p \to q$
   $q \to r$
   $\therefore p \to r$
8. **Division into cases**
   $p \vee q$
   $p \to r$
   $q \to r$
   $\therefore r$
9. **Contradiction rule**
   $\sim p \to false$
   $\therefore p$
10. **Universal Instantiation**
    $\forall x, P(x) \to Q(x)$
    $P(a) \to Q(a)$ for a particular a
11. **Existential Instantiation**
    $\exists x, P(x)$
    $P(a)$
12. **Existential Generalization**
    $P(a)$
    $\exists x, P(x)$

Number Theory

Definitions

Divisibility $d \mid n \leftrightarrow \exists k \in \mathbb{Z} \ni n = dk$

Even d is even iff $\exists k \in \mathbb{Z} \ni d = 2k$

Odd d is odd iff $\exists k \in \mathbb{Z} \ni d = 2k+1$

Rational n is rational iff $\exists a, b \in \mathbb{Z}, b \neq 0, n = \frac{a}{b}$

Prime n is prime iff
$\forall r, s \in \mathbb{Z}^+, n = rs \to (r=1 \wedge s=n) \vee (r=n \wedge s=1)$

Composite n is composite iff $\exists r, s \in \mathbb{Z} \ni n = rs, 1<r<n \wedge 1<s<n$

Lower Bound An integer b is said to be a lower bound for an integer set X if b is less than or equal to every element in the set.

GCD Let $d = gcd(a, b)$. (i) $d \mid a \wedge d \mid b$. (ii) $\forall c \in \mathbb{Z}, c \mid a \wedge c \mid b \to c \leq d$.

Coprime Integers a and b are coprime iff $gcd(a, b) = 1$.

LCM Let $m = lcm(a, b)$. (i) $a \mid m \wedge b \mid m$.
(ii) $\forall c \in \mathbb{Z}^+, a \mid c \wedge b \mid c \to m \leq c$.

Congruence $m \equiv n \pmod{d} \leftrightarrow d \mid (m-n)$.

Theorems from Epp

Thm 4.1.1 The sum of any two even integers is even.

Thm 4.2.1 Every integer is rational.

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

Thm 4.3.1 $\forall a, b \in \mathbb{Z}^+, a \mid b \to a \leq b$

Thm 4.3.2 $d \mid 1 \to d = 1 \vee d = -1$

Thm 4.3.3 $\forall a, b, c \in \mathbb{Z}, a \mid b \wedge b \mid c \to a \mid c$

Thm 4.3.4 Any integer greater than 1 is divisible by a prime.

Thm 4.3.5 Every positive integer greater than 1 can be uniquely factorized into a product of prime numbers.

Thm 4.4.1 $\forall a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z} \ni a = bq + r, 0 \leq r < b$

Thm 4.4.2 Any consecutive integers have opposite parity.

Thm 4.4.3 The square of any odd integer has the form $8m+1$ for some integer m.

Thm 4.4.6 For all real numbers x and y, $|x+y| \leq |x| + |y|$.

Thm 4.5.1 For all real numbers x and integers m, $\lfloor x+m \rfloor = \lfloor x \rfloor + m$.

Thm 4.5.2 For any integer n, $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$ if n is even and $\frac{n-1}{2}$ if n is odd.

Thm 4.5.3 If n is any integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d\lfloor n/d \rfloor$, then $n = dq + r$ and $0 \leq r < d$.

Thm 4.6.1 There is no greatest integer.

Thm 4.6.2 There is no integer that is both even and odd.

Thm 4.6.3 The sum of any rational number and any irrational number is irrational.

Prop 4.6.4 m^2 is even $\to m$ is even.

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

Prop 4.7.2 $1 + 3\sqrt{2}$ is irrational.

Prop 4.7.3 For any prime p, $\forall a \in \mathbb{Z}, p \mid a \to p \nmid (a+1)$.

Thm 4.7.4 The set of primes is infinite.

Thm 8.4.1 For all integers a, b and n, and $n > 1$, the following are the same:

1. $n \mid (a - b)$
2. $a \equiv b \pmod n$
3. $a = b + kn$ for some integer k
4. a and b have the same non-negative remainder when divided by n
5. $a \mod n = b \mod n$

Thm 8.4.3 Suppose $a \equiv c \pmod n$ and $b \equiv d \pmod n$.

1. $(a+b) \equiv (c+d) \pmod n$
2. $(a-b) \equiv (c-d) \pmod n$
3. $ab \equiv cd \pmod n$
4. $a^m \equiv c^m \pmod n, \forall m \in \mathbb{Z}^+$

Corollary 8.4.4 $ab \equiv [(a \mod n)(b \mod n)] \pmod n$

Thm 8.4.8 For all integers a, b and c, if $gcd(a,c) = 1$ and $a \mid bc$, then $a \mid b$.

Thm 8.4.9 For all integers $a, b, c, n, n > 1$ and a and n are coprime, $ab \equiv ac \pmod n \to b \equiv c \pmod n$.

Thm 8.4.10 Fermat's Little Theorem For any prime p and integer a, $a^p \equiv a \pmod p$. OR for any prime p and any integer a, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$.

Theorems from Lecture Notes

Thm 4.1.1 $\forall a, b, c \in \mathbb{Z}, a \mid b \wedge a \mid c \to \forall x, y \in \mathbb{Z}, a \mid (bx + cy)$

Prop 4.2.2 For any primes p and q, $p \mid q \to p = q$

Thm 4.2.3 If p is a prime and $x_1, x_2, \cdots x_n$ are any integers such that $p \mid x_1 x_2 \cdots x_n$, then $p \mid x_i$ for some x_i $(1 \le i \le n)$.

Thm 4.3.2 Well Ordering Principle and Well Ordering Principle 2

Prop 4.3.3 If a set S of integers has a least element, then the least element is unique.

Prop 4.3.4 If a set S of integers has a greatest element, then the greatest element is unique.

Prop 4.5.2 For any integers a, b, not both zero, their gcd exists and is unique.

Thm 4.5.3 Let a, b be integers not both zero, and let $d = gcd(a,b)$. Then there exists integers x, y such that $ax + by = d$. These are not unique, and the other solutions are $x + kb/d$ and $y - ka/d$ where k is any integer.

Prop 4.5.5 For any integers a, b, not both zero, if c is a common divisor, then $c \mid gcd(a,b)$.

Thm 4.7.3 For any integer a, its multiplicative inverse module n (where $n > 1$) exists iff a and n are coprime.

Sequences

Definitions

Second-order Linear Homogeneous Recurrence Relation with Constant Coefficients $a_k = Aa_{k-1} + Ba_{k-2}$

Theorems from Epp

Thm 5.1.1 For any sequences a_k and b_k, and for integers $n \ge m$,

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

Thm 5.8.3 If a sequence has the form $a_k = Aa_{k-1} + Ba_{k-2}$ and the characteristic equation $t^2 - At - B = 0$ has two distinct roots r and s, then $a_n = Cr^n + Ds^n$ where C and D are constants that can be determined using the initial conditions.

Thm 5.8.5 If the characteristic equation has only one root r, then $a_n = Cr^n + Dnr^n$ where C and D are constants determined using the initial conditions.

Sets

Definitions

Subset $S \subseteq T \leftrightarrow \forall x \in S, x \in T$

Empty Set $\forall Y \in \mathcal{U}, Y \notin \varnothing$

Set Equality Two sets are equal iff they have the same elements.

Power Set Given any set S, if $T = \mathcal{P}(S)$, then $T = \{X \mid X \subseteq S\}$. If $|S| = n, |T| = 2^n$.

Union It is written as $T = \bigcup S$ if given S, T is such that $T = \{y \in \mathcal{U} \mid y \in X \text{for some} X \in S\}$.

Intersection It is written as $T = \bigcap S$ if given S, T is such that $T = \{y \in \mathcal{U} \mid \forall X((X \in S) \to (y \in X))$.

Disjoint S and T are disjoint iff $S \cap T = \varnothing$.

Mutually Disjoint Let V be a set of sets. $\forall X, Y \in V(X \neq Y \to X \cap Y = \varnothing)$.

Partition Let S be a set and V be a set of non-empty subset of S. V is said to be a parition of S iff

1. The sets in V are mutually disjoint.
2. The union of the sets in V equals S.

Non-Symmetric Difference $S - T = \{y \in \mathcal{U} \mid y \in S \wedge y \notin T\}$.

Symmetric Difference $S \ominus T = \{y \in \mathcal{U} \mid y \in S \oplus y \in T\}$

Set Complement $A^C = \mathcal{U} - A$.

Theorems from Epp

Thm 6.2.1

For all sets A and B

1. $A \cap B \subseteq A$ and $A \cap B \subseteq B$
2. $A \subseteq A \cup B$ and $B \subseteq A \cup B$
3. $A \subseteq B \wedge B \subseteq C \to A \subseteq C$

Thm 6.2.2

This is the same as Theorem 2.1.1. Treat $false$ as $\varnothing$ and $true$ as U. The following additional rules apply.

1. **Complements of U and $\varnothing$:** $U^c = \varnothing$ and $\varnothing^c = U$
2. **Set difference law** $A - B = A \cap B^c$

Thm 6.2.3 If $A \subseteq B$, $A \cap B = A$ and $A \cup B = B$.

Thm 6.2.4 For all sets S, $\varnothing \subseteq S$.

Corollary 6.2.5 The empty set is unique.

Prop 6.2.6 If $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \varnothing$.

Thm 6.3.1 If a set has n elements, its powerset has 2^n elements.

Theorem from Notes

Prop 6.2.3 $\forall X \forall Y (X \subseteq Y \wedge Y \subseteq X \leftrightarrow X = Y)$.

Prop 6.3.2

1. $\bigcup \varnothing = \bigcup_{A \in \varnothing} A = \varnothing$
2. $\bigcup \{A\} = A$
3. $A \cup \varnothing = A$
4. $A \cup B = B \cup A$
5. $A \cup (B \cup C) = (A \cup B) \cup C$
6. $A \cup A = A$
7. $A \subseteq B \leftrightarrow A \cup B = B$

Prop 6.3.4

1. $A \cap \varnothing = \varnothing$
2. $A \cap B = B \cap A$
3. $A \cap (B \cap C) = (A \cap B) \cap C$
4. $A \subseteq B \leftrightarrow A \cap B = A$
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Relations

Definitions

Ordered Pair $(x, y) = (a, b)$ iff $x = a \wedge y = b$.

Ordered n-tuple Generalization of the ordered pair to n elements.

Cartesian Product The set $S \times T$ is such that $\forall X, Y((X, Y) \in S \times T \leftrightarrow (X \in S) \wedge (Y \in T))$.

Generalized Cartesian Product Cartesian products generalized to n products.

Binary Relation A binary relation from S to T, is a subset of the cartesian product $S \times T$.

Domain $\mathcal{D}om(\mathcal{R}) = \{s \in S \mid \exists t \in T(s\,\mathcal{R}\,t)\}$.

Image $\mathcal{I}m(\mathcal{R}) = \{t \in T \mid \exists s \in S(s\,\mathcal{R}\,t)\}$.

Co-domain $co\mathcal{D}om(\mathcal{R}) = T$.

N-ary Relation It is the subset of the cartesian product $\prod_{i=1}^{n} S_i$.

Composition $\forall x \in S, \forall z \in U(x\,\mathcal{R}' \circ \mathcal{R}\,z \leftrightarrow (\exists y \in T \ni x\mathcal{R}y \wedge y\mathcal{R}z))$

Reflexive $\forall x \in A(x\,\mathcal{R}\,x)$

Symmetric $\forall x, y \in A(x\,\mathcal{R}\,y \rightarrow y\,\mathcal{R}\,x)$

Transitive $\forall x, y, z \in A(x\,\mathcal{R}\,y \wedge y\,\mathcal{R}\,z \rightarrow x\,\mathcal{R}\,z)$

Equivalence Relation $\mathcal{R}$ is said to be an equivalence relation iff it is reflexive, symmetric and transitive.

Equivalence Class $[x] = \{y \in A \mid x\,\mathcal{R}\,y\}$

Transitive Closure The transitive closure of $\mathcal{R}$, denoted $\mathcal{R}^t$ is a relation that satisfies the following properties:

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

Anti-Symmetric $\forall x, y \in A((x\,\mathcal{R}\,y \wedge y\,\mathcal{R}\,x) \rightarrow x = y)$.

Partial Order $\mathcal{R}$ is a partial order if it is reflexive, anti-symmetric and transitive.

Comparable Let $\preceq$ be a partial order relation on A. Elements a, b of A are comparable iff $a \preceq b \vee b \preceq a$.

Total Order $\forall a, b \in A, (a \preceq b \vee b \preceq a)$

Maximal x is the maximal element if $\forall y \in A, x \preceq y \rightarrow x = y$.

Maximum $\top$ is the maximum element if $\forall x \in A, x \preceq \top$.

Minimal x is the minimal element if $\forall y \in A, y \preceq x \rightarrow x = y$.

Minimum $\perp$ is the minimum element if $\forall x \in A, \perp \preceq x$.

Well-Ordered Let $\preceq$ be a total order on A. A is well-ordered if $\forall S \in \mathcal{P}(A)(S \neq \varnothing \rightarrow (\exists x \in S, \forall y \in S(x \preceq y))$

Theorems from Notes

Prop 8.2.5 $\mathcal{I}m(\mathcal{R}) \subseteq co\mathcal{D}om(\mathcal{R})$

Prop 8.2.9 Composition is associative.

Prop 8.2.10 $(\mathcal{R}' \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{R}'^{-1}$

Thm 8.3.1 Given a partition $S_1, S_2, \cdots$ of A, there exists an equivalence relation $\mathcal{R}$ on A whose whose equivalence classes make up precisely that partition.

Lemma 8.3.2 Let $\mathcal{R}$ be an equivalence relation on A and a, b be elements of A. $a\,\mathcal{R}\,b \rightarrow [a] = [b]$.

Lemma 8.3.3 Let $\mathcal{R}$ be an equivalence relation on A and a, b be elements of A. Then either $[a] \cap [b] = \varnothing$ or $[a] = [b]$.

Thm 8.3.4 Let $\mathcal{R}$ be an equivalence relation on A. Then the set of distinct equivalence classes form a parition of A.

Prop 8.5.2 Let $\mathcal{R}$ be a relation on A. $\mathcal{R}^t = \bigcup_{i=1}^{\infty} R^i$

Functions

Definitions

Function Let f be a relation such that $f \subseteq S \times T$. Then f is a function from S to T, denoted $f : S \rightarrow T$ iff $\forall x \in S, \exists! y \in T(x\,f\,y)$.

Pre-Image Let $x \in S, y \in T$ such that $f(x) = y$. Then, x is the pre-image of y. Pre-image need not be unique.

Inverse Image The inverse image of y is the set of all its pre-images. The inverse image of a subset of the range is the set that contains all the pre-images of all elements in the subset.

Restriction Let $U \subseteq S$ where S is the domain. The restriction of f to U is the set $\{(x, y) \in U \times T \mid f(x) = y\}$.

Injective $\forall y \in T, \forall x_1, x_2 \in S((f(x_1) = y \wedge f(x_2) = y) \rightarrow x_1 = x_2)$.

Surjective $\forall y \in T, \exists x \in S(f(x) = y)$.

Bijective A function f is bijective if it is injective and surjective.

Identity Function $\forall x \in A, \mathcal{I}_A(x) = x$.

Theorems from Epp

Thm 7.1.1 If $F : X \rightarrow Y$ and $G : X \rightarrow Y$ are functions, then $F = G$ iff $F(x) = G(x)$ for all $x \in X$.

Thm 7.2.1 Logarithm laws

Thm 7.2.2 Suppose F is one-to-one and onto. Then $F^{-1}(y) = x \leftrightarrow y = F(x)$.

Thm 7.2.3 If F is one-to-one and onto, then so is F^{-1}.

Thm 7.3.1 Composing any function with the identity function makes no difference to the function.

Thm 7.3.2 Composing a bijective function with its inverse results in the identity function.

Thm 7.3.3 The composition of two one-to-one function is another one-to-one function.

Thm 7.3.4 The composition of two onto functions is another onto function.

Theorems from Notes

Prop 7.2.4 f is bijective $\leftrightarrow$ f^{-1} is a function.

Prop 7.3.1 If $f : S \rightarrow T$ and $g : T \rightarrow U$, then $gcircf$ is another function from S to U.

Prop 7.3.3 Let $f : A \rightarrow A$ be an injective function on A. Then $f^{-1} \circ f = \mathcal{I}_A$.

Graphs

Definitions

Simple Graph is an undirected graph with no loops or parallel edges.

Complete Graph with n vertices, denoted by K_n, is a simple graph with exactly one edge connecting each pair of distinct vertices.

Complete Bipartite Graph on (m, n) vertices, where $m, n > 0$, denoted $K_{m,n}$, is a simple graph with distinct vertices $v_1, v_2, ..., v_m$, and $w_1, w_2, ..., w_n$ that satisfies the following properties:
For all $i, k = 1, 2, ..., m$ and for all $j, l = 1, 2, ..., n$,

1. There is an edge from each vertex v_i to each vertex w_j.
2. There is no edge from any vertex v_i to any other vertex v_k.
3. There is no edge from any vertex w_j to any other vertex w_l.

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

A graph H is a **Connected Component** of a graph G if, and only if,

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

An **Euler circuit** for G is a circuit that contains every vertex and every edge of G. That is, an Euler circuit for G is a sequence of adjacent vertices and edges in G that has at least one edge, starts and ends at the same vertex, uses every vertex of G at least once, and uses every edge of G exactly once. An Eulerian graph is a graph that contains an Euler circuit.

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.

That is, a **Hamiltonian Circuit** for G is a sequence of adjacent vertices and distinct edges in which every vertex of G appears exactly once, except for the first and the last, which are the same.

	Repeated Edge?	Repeated Vertex?	Starts and Ends at Same Point?	Must Contain at Least One Edge?
Walk	allowed	allowed	allowed	no
Trail	no	allowed	allowed	no
Path	no	no	no	no
Closed walk	allowed	allowed	yes	no
Circuit	no	allowed	yes	yes
Simple circuit	no	first and last only	yes	yes

Theorems from Epp

Thm 10.1.1: Handshake If G is any graph, then the sum of the degrees of all the vertices of G equals twice the number of edges of G.

Corollary 10.1.2 The total degree of a graph is even.

Prop 10.1.3 In any graph, there are an even number of vertices with an odd degree.

Lemma 10.2.1 Let G be a graph.

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

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, 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.

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

Prop 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 10.3.1 Matrix representation of a graph with more than one connected components.

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

Thm 10.4.1 Let S be a set of graphs and let R be the relation of graph isomorphism on S. Then R is an equivalence relation on S.

Euler's Formula $f = e - v + 2$.

Lemma 10.5.1 Any non-trivial tree has at least one vertex of degree 1.

From tutorial 11, q4 Every non-trivial tree has at least two vertices of degree 1.

Thm 10.5.2 Any tree with n vertices (n > 0) has n – 1 edges.

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.

Thm 10.6.1 If T is a full binary tree with k internal vertices, then T has a total of 2k + 1 vertices and has k + 1 terminal vertices (leaves).

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

Prop 10.7.1 Every connected graph has a spanning tree. Any two spanning trees for a graph have the same number of edges.

Probability

Theorems from Epp

Thm 9.1.1 If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

Thm 9.2.1 Multiplication Rule If an operation consists of k steps and the first step can be performed in n_1 ways, the second step can be performed in n_2 ways (regardless of how the first step was performed), $\cdots$, the k-th step can be performed in n_k ways (regardless of how the preceding steps were performed), Then the entire operation can be performed in $n_1 \times n_2 \times n_3 \times \cdots \times n_k$ ways.

Thm 9.2.2 The number of permutations of a set with n $(n \geq 1)$ elements is $n!$.

Thm 9.2.3 If n and r are integers and $1 \leq r \leq n$, then the number of r-permutations of a set of n elements is given by the formula $P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$ or, equivalently, $P(n,r) = \frac{n!}{(n-r)!}$

Thm 9.3.1 Addition Rule Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \cdots, A_k$. Then $N(A) = N(A_1) + N(A_2) + \dots + N(A_k)$.

Thm 9.3.2 Difference Rule If A is a finite set and B is a subset of A, then $N(A - B) = N(A) - N(B)$.

Thm 9.3.3 If A, B, and C are any finite sets, then $N(A \cup B) = N(A) + N(B) - N(A \cap B)$ and $N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$

Thm 9.4.1 Pigeonhole Principle A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain.

Thm 9.4.2 Let X and Y be finite sets with the same number of elements and suppose f is a function from X to Y. Then f is one-to-one if, and only if, f is onto.

Generalized Pigeonhole Principle If n pigeons fly into m pigeonholes and, for some positive integer k, $k < n/m$, then at least one pigeonhole contains $k+1$ or more pigeons. **Contrapositive** If there are m pigeonholes and at most n pigeons in each pigeonhole, then there are at most mn pigeons in total.

Thm 9.5.1 $\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}$

Thm 9.5.2 Suppose a collection consists of n objects of which n_1 are of type 1 and are indistinguishable from each other, n_2 are of type 2 and are indistinguishable from each other, $\cdots$, n_k are of type k and are indistinguishable from each other, and suppose that $n_1 + n_2 + \cdots + n_k = n$. Then the number of distinguishable permutations of the n objects is $\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2\cdots n_{k-1}}{n_k}$ or $\frac{n!}{n_1!n_2!\cdots n_k!}$

Thm 9.6.1 The number of r-combination with repetition allowed (multisets of size r) that can be selected from a set of n elements is $\binom{r+n-1}{r}$

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

Theorem from Notes

Thm 9.7.1 $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$

Thm 9.7.2 Binomial $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

Thm 9.9.1 Bayes

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

MCQ Hacks

RAY Conjecture The number of onto functions from a set with m elements to a set with n elements, where $m \geq n$, is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$$

Vasavadaddy's Hypothesis In a set with n elements,

1. The number of possible relations is
$$2^{n \times n}$$
2. The number of reflexive relations is
$$2^{n^2 - n}$$
3. The number of symmetric relations is
$$2^{(n^2+n)/2}$$
4. The number of reflexive and symmetric relations is
$$2^{(n^2-n)/2}$$
5. The number of anti-symmetric relations is
$$2^n 3^{(n^2-n)/2}$$
6. The number of asymmetric relations is
$$3^{(n^2-n)/2}$$

Graph Isomorphism (Thm 10.4.2)

Invariants for Isomorphic graphs

1. n vertices

2. m edges
3. has a vertex of degree k
4. has m vertices of degree k
5. has a circuit of length k
6. has a simple circuit of length k
7. has m simple circuits of length k
8. is connected
9. has an Euler circuit
10. has a Hamiltonian circuit

Edges in a Complete Graph

$$\frac{n(n-1)}{2}$$

Created by **Mohideen Imran Khan**

Template from http://wch.github.io/latexsheet/