# CIS 160 Final Cheat Sheet

## Contents

# 1 Logic

A *proposition* is a statement that is either true or false.

*Negation*, denoted as $\neg p$, is the proposition that is true when $p$ is false and vice-versa.

*Conjunction*, $p \wedge q$, is the proposition that is true when both $p$ and $q$ are true.

*Disjunction*, $p \vee q$, is the proposition that is true when at least one of $p$ or $q$ is true.

*Exclusive or*, $p \oplus q$, is the proposition that is true when exactly one of $p$ and $q$ is true, false otherwise.

*Implication*, $p \implies q$, is the proposition that is false when $p$ is true and $q$ is false and true otherwise. The implication $q \implies p$ is called the *converse* of the implication $p \implies q$. The implication $\neg p \implies \neg q$ is called the *inverse* of $p \implies q$. The implication $\neg q \implies \neg p$ is the *contrapositive* of $p \implies q$.

*Biconditional*, $p \iff q$, is the proposition that is true if $p$ and $q$ have the same truth values and is false otherwise.

$p$ is a *sufficient* condition for $q$ means $p \implies q$. $p$ is a *necessary* condition for $q$ means that $\neg p \implies \neg q$, or equivalently $q \implies p$.

# 2 Number Theory

## 2.1 Definitions:

An integer $n$ is *even* iff $n = 2k$ for some integer $k$. An integer is *odd* iff $n = 2k + 1$ for some integer $k$.

An integer $n$ is *prime* iff $n > 1$ and for all positive integers $r$ and $s$, if $n = r$, then $r = 1$ or $s = 1$. Otherwise, $n$ is *composite*.

An integer $n$ being divisible by an integer $k$ is denoted by $k|n$. By the *prime factorization theorem*, every positive integer can be uniquely represented as a product of primes.

## 2.2 Proofs:

**From L1T:**

If the sum of two integers is even, then so is their difference.

**From L1T:**

For all integers $n$, if $n$ is odd then $n^2 + n + 1$ is odd.

**From L1T:**

Let $x$ be an integer. If $x > 1$, then $x^3 + 1$ is composite.

**From L1H:**

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

**From L2T:**

For all real numbers $x$ and all integers $m$

$$\lfloor x + m \rfloor = \lfloor x \rfloor + m$$

**From L2T:**

If $x$ and $y$ are integers where $x + y$ is even, then $x$ and $y$ are both odd or both even.

**From L2T:**

If $3n + 2$ is odd then $n$ is odd.

**From L2T:**

For all real numbers $a$ and $b$, if the product $ab$ is an irrational number, then either $a$, $b$, or both $a$ and $b$ must be irrational.

**From L3T:**

The product of two odd numbers is an odd number.

**From L3T:**

For all positive integers $n$, $n$ is even iff $7n$ + 4 is even.

**From L3T:**

There are infinitely many prime numbers.

**From L3H:**

$$\binom{n}{r} = \binom{n}{n-r}$$

**Pascal's Formula:**

If $n$ and $k$ are positive integers such that $n \geq k$ then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

**From L3H:**

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

**From L3H:**

$$\sum_{k=0}^{r} \binom{n}{k} \binom{m}{r-k} = \binom{n+m}{r}$$

**From L4T:**

The sum of the first $n$ positive odd numbers is $n^2$.

**From L4T:**

For all integers $n \geq 0$, if $r \neq 1$,

$$\sum_{i=0}^{n} ar^i = \frac{a(r^{n+1} - 1)}{r - 1}$$

**From L4T:**

For all non-negative integers $n$

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

**From L4T:**

For all $n \in \mathbb{N}$, $n > 1 \implies n! < n^n$

**From L4T:**

For all $n \geq 1$, $n$ lines separate the plane into

$$\frac{n^2 + n + 2}{2}$$

regions assuming that no two lines are parallel and no three pass through a common point.

**Binomial Theorem:**

For any real numbers $a$ and $b$ and non-negative integer $n$

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

**From L4H:**

For any positive integer $n$

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

**From L4H:**

Given a sequence of $n$ integers, there exists a subsequence of consecutive integers whose sum is a multiple of $n$.

**From L5T:**

If $n$ is an integer greater than 1 then either $n$ is prime or it can be written as a product of primes.

**From L5H:**

Every sequence of $n^2+1$ distinct real numbers $x_1, x_2, x_3, ..., x_{n^2+1}$ contains a subsequence of length $n+1$ that is either strictly increasing or strictly decreasing.

**From HW2T:**

For any positive integer $w$ and non-negative, real number $r$, if $r$ is irrational then $r^{\frac{1}{w}}$ is irrational.

**From HW3H:**

For every integer $m \geq 2$, if there is no prime number $p$ such that $p \leq \sqrt{m}$ and $p|m$, then $m$ must be a prime.

**From HW4T:**

For all $n \in \mathbb{Z}^+$

$$\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$$

**From HW4T:**

For all $n \in \mathbb{Z}^+$

$$\sum_{i=1}^{n} i(i+1)(i+2) = \frac{n(n+1)(n+2)(n+3)}{4}$$

**From HW5H:**

For all $n \in \mathbb{Z}+$

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} < 2\sqrt{n}$$

**From R3:**

For any $m \leq n$

$$\sum_{k=0}^{m} \binom{n}{k}\binom{n-k}{m-k} = 2^m \binom{n}{m}$$

# 3 Combinatorics

## 3.1 Definitions:

By the *Multiplication Rule*, if a procedure can be broken down into $k$ steps and steps 1, 2, 3, ... can be performed $n_1, n_2, n_3, ...$ ways respectively, then the entire procedure can be performed $n_1 \cdot n_2 \cdot n_3 \cdot ...$ ways. Note the Multiplication Rule can only be applied if the number of ways to perform a step remain constant regardless of the action taken in prior steps.

A *permutation* of a set of distinct objects is an ordering of the objects in a row. A set with $n$ elements can be permuted $n!$ ways.

$r$-permutations of a set of $n$ elements are the permutations of $r$ elements of the total $n$ elements. Denoted by $P(n, r)$.

Let $n$ and $r$ be non-negative integers. An $r$-combination of a set of $n$ elements means an unordered selection of $r$ of the $n$ elements of $S$. This is denoted by $\binom{n}{r}$ or $n$ choose $r$.

*Stars and Bars* is a counting method to construct $r$-combinations with repetition allowed. The $n$ total items in the set are imagined in the context of a multiset with two object types: $n-1$ bars (used as dividers) and $r$ stars (placed between the bars). The number of permutations of that multiset returns the number of $r$-combinations of the $n$ elements with repetition allowed.

## 3.2 Proofs:

**From L2H:**

For the number of $r$-permutations of a set of $n$ elements:

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

**From L2H:**

For the number of $r$ combinations of a set of $n$ elements:

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

**From L3H:**

Using the Stars and Bars method, the number of $r$-combinations of a set of $n$ elements with repetition allowed is given by

$$\text{Number of combinations } = \frac{n+r-1}{(n-1)!r!}$$

# 4 Sets

## 4.1 Definitions:

A *set* is an *unordered* collection of distinct objects. The objects of a set are referred to as its *elements* or *members*.

Two sets are *equal* iff they have the same elements.

The *cardinality* of $S$, denoted by $|S|$, is the number of distinct elements in $S$.

A set $A$ is said to be a *subset* of $B$ iff every element of $A$ is also an element of $B$, denoted by $A \subseteq B$. If $A \subseteq B$ and $A \neq B$, then we say $A$ is a *proper subset* of $B$, denoted by $A \subset B$.

A *power set* of set $S$, denoted by $\mathcal{P}(S)$, is a set of all possible subsets of $S$.

Common sets include

$$\mathbb{N} = \{0, 1, 2, 3, ...\}$$

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$$

$$\mathbb{Q} = \{p/q | p \in \mathbb{Z} \text{ and } p \in \mathbb{Z}, \text{ and } q \neq 0\}$$

$\mathbb{R}$ is the set of real numbers.

Sets can be described using *set builder notation* by defining it within curly braces and using the $|$ as 'such that': $\{x | x$ is a positive integer less than 100$\}$.

Let $A$ and $B$ be sets. The *union* of the sets $A$ and $B$, denoted by $A \cup B$, is the set that contains those elements that are either in $A$, $B$, or both.

The *intersection* of sets $A$ and $B$, denoted by $A \cap B$, is the set that contains those elements that are in both $A$ and $B$.

Two sets are called *disjoint* if their intersection is an empty set.

A collection of nonempty sets $A_1, A_2, A_3, ..., A_n$ is a *partition* of set $A$ iff

1. $A = \bigcup_{i=1}^{n} A_i$
2. Sets $A_1, A_2, A_3, ..., A_n$ are mutually (pairwise) disjoint.

The *difference* of sets $A$ and $B$, denoted by $A \setminus B$ is the set containing those elements that are in $A$ but NOT in $B$.

The *complement* of a set $A$ is the set of elements not in $A$, denoted by $\overline{A}$.

The *cartesian product* of $A$ and $B$, denoted by $A \times B$, is the set of all ordered pairs formed by taking an element from $A$ together with an element from $B$ in all possible ways.

Let $A, B, C$ be sets. Then, by *DeMorgan's Laws*,

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

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

By the *Principle of Inclusion-Exclusion* (PIE), if $A$, $B$, and $C$ are any finite sets

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Note this can be applied to any number of finite sets, where the cardinalities of the sets are addded, pairwise intersections subtracted, triowise intersections added, and so on. If $A$, $B$, and $C$ are mutually disjoint, then

$$A \cup B = |A| + |B|$$

$$A \cup B \cup C = |A| + |B| + |C|$$

This is called the *addition rule* or the *sum rule*.

A *multiset* is a set with some number of elements $n$ of which some are identical to one other.

## 4.2 Proofs:

**From L2T:**

Let $A$ and $B$ be sets. Then, $A = B$ iff $A \subseteq B$ and $B \subseteq A$. **From L3H:**

For a multiset $S$ with $n$ objects and $k$ object types:

$$\text{Number of Permutations} = \frac{n!}{n_1!n_2!n_3!...n_k!}$$

**From L4T:**

For set $A$ with $n$ elements, for all positive integers $n$

$$|\mathcal{P}(A)| = 2^n$$

**From HW2H:**

For any sets $S, T, R$

$$S \setminus (T \setminus R) \neq (S \setminus T) \setminus R$$

$$S \setminus (T \setminus R) \subseteq (S \setminus T) \cup R$$

**From HW3H:**

For any sets $A$ and $Z$

$$\mathcal{P}(A \cap Z) = \mathcal{P}(A) \cap \mathcal{P}(Z)$$

**From R2:**

For any sets $A, B, C$

$$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$$

# 5 Proof Techniques

## 5.1 Induction

*Induction* is a proof technique that asserts that, for a proven *base case*, *induction hypothesis*, and *induction step*, a proposition is sufficiently proven over the range of values between the base case and the induction step. The base case proves the proposition for the lower or upper bound on the range of the value being inducted upon, the induction hypothesis is the formal statement assuming the theorem works for some arbitrary value within the range of induction, and the induction step is the proof that, given the induction hypothesis, the statement holds for the proposition with the inducted value incremented/decremented.

### 5.1.1 Strong Induction

For any property $P$, if $P(0)$ and $\forall n \in \mathbb{N}$, $P(0) \wedge P(1) \wedge P(2) \wedge ... \wedge P(k) \implies P(k+1)$, then $\forall n \in \mathbb{N}, P(n)$. Essentially, strong induction functions identically to standard induction, but the induction hypothesis assumes the theorem applies for all values between the base case and the value immediately before the induction step, as opposed to only assuming the theorem applies for the value immediately before the induction step. Note that any induction proof can be completed as a standard induction or strong induction proof (proven in $L5T$), but sometimes one is easier.

## 5.2 Combinatorial Proofs

To prove an equivalence identity, we can pose a counting question that is counted in two different ways. If one question can be counted to be equal to the Left Hand Side and counted an alternative way to be equal to the Right Hand Size, then the equivalence is proven.

## 5.3 Pigeonhole Principle

If $k+1$ or more objects are distributed among $k$ bins, then there must be at least one bin that has two or more objects. In general, if $n$ objects are placed into $k$ boxes, then there is at least one box containing at least $\lceil \frac{n}{k} \rceil$ objects.

## 5.4 The Probabilistic Method

For some event $A$ or random variable $X$, it is shown that $\Pr[A] > 0$ or $\mathbf{E}[X] = x$ then it is proven respectively that there exists an outcome in the sample space in event $A$ or there is an event in the sample space where $X \geq x$. In general, defining a random process in some mathematical context and deriving probabilities of events can be a useful tool for proving the existence of an arrangement or distribution where a defined event happens.

# 6 Graphs

## 6.1 Definitions:

A *graph* consists of two sets, a non-empty set, $V$, of vertices or nodes, and a possibly empty set, $E$, of 2-element subsets of $V$. Such a graph is denoted by $G = (V, E)$.

Each element of $E$ is called an *edge*. We say that an edge $u, v \in E$ *connects* vertices $u$ and $v$.

Two nodes $u$ and $v$ are *adjacent* if $u, v \in E$. Nodes adjacent to a vertex $u$ are called *neighbors* of $u$.

The number of neighbors of a vertex $v$ is called the *degree* of $v$ and is denoted by $deg(v)$.

The value of $\delta(G) = \min_{v \in V} deg(v)$ is the *minimum degree* of $G$, the value $\Delta(G) = \max_{v \in V} deg(v)$ is the *maximum degree* of $G$.

An edge that connects a node to itself is called a *loop* and multiple edge between the same pair of nodes are called *parallel edges*.

Graphs without loops and parallel edges are called *simple* graphs, otherwise they are called *multigraph*.

The *girth* of a graph $G$, $g(G)$, is the length of the smallest cycle in $G$.

## 6.2 Proofs:

**Handshaking Lemma:**

$$\sum_{v \in V} deg(c) = 2|E|$$

**From L6T:**

In any graph, there are en even number of vertices of odd degree.

**From L6T:**

Every graph with $n$ vertices and $m$ edges has at least $n - m$ connected components.

**From L6T:**

Every connected graph with $n$ vertices has $\geq n - 1$ edges

**From L15T:**

For every $g, k > 0$, there exists a graph $G$ with $\chi(G) \geq k$ and $g(G) \geq g$.

**From HW7H:**

For a connected graph with $n \geq 1$ vertices and $m \geq 1$ edges, $n \leq n^2 - 2m$

**From HW8H:**

For a connected graph with $n \geq 3$ vertices, there exists exactly 1 cycle in the graph iff there are $n$ edges.

**From HW11H:**

For a connected graph $G$ without triangles with minimum degree $\delta(G) = d \geq 0$, $G$ has at least $2d$ vertices.

## 6.3 Trees

### 6.3.1 Definitions:

A $graph$ with no cycles is $acyclic$.

A $tree$ is a connected acyclic graph.

A vertex of degree greater than 1 in a tree is called an $internal\ vertex$, otherwise it is called a $leaf$.

A $forest$ is an acyclic graph.

A $spanning\ subgraph$ of a graph $G$ is a subgraph with vertex set $V(G)$.

A $spanning\ tree$ is a spanning subgraph that is a tree.

A $rooted\ tree$ is a tree in which one vertex is distinguised from the others and is called the $root$.

The $level$ of a vertex, say $u$, is the number of edges along the unique path between $u$ and the root.

The $height$ of a rooted tree is the maximum level of any vertex in the tree.

A $binary\ tree$ is a rooted tree in which every internal vertex has at most two children. Each child in the binary tree is designated either a left child or a right child (but not both).

A $full\ binary\ tree$ is a binary tree in which each internal vertex has exactly 2 children.

A $three\text{-}tree$ is a tree such that all vertices have degree either 1 or 3.

### 6.3.2 Proofs:

**From L7T**

Every tree with $\geq 2$ vertices has $\geq 2$ leaves and deleting a leaf from an $n$-vertex tree produces a tree with $n - 1$ vertices.

**From L7T:** The following are equivalent

1. $G$ is a tree.
2. $G$ is connected and has exactly $n - 1$ edges.
3. $G$ is minimally connected, i.e., $G$ is connected but $G - \{e\}$ is disconnected for every edge $e \in G$.
4. $G$ contains no cycle but $G + \{x, y\}$ does, for any two non-adjacent vertices $x, y \in G$.
5. Any two vertices of $G$ are linked by a unique path in $G$.

**From L9T:**

Every connected graph $G$ contains a spanning tree

**From L9T:**

If $k$ is a positive integer and $T$ is a full binary tree with $k$ internal vertices then $T$ has a total of $2k + 1$ vertices and has $k + 1$ leaves.

**From L9T:**

Any binary tree of height at most $h$ has at most $2^h$ leaves.

**From HW8H:**

Any tree $T$ with $n > 1$ vertices has $2 + \sum_{\substack{v_i \in V \\ \deg(v_i) \geq 3}} (deg(v_i) - 2)$ leaves.

**From HW9H:**

Any three-tree $T$ with $l$ leaves has $l - 2$ vertices of degree 3.

**From R7:**

Any tree $T$ with maximum degree $\Delta$ has $\geq \Delta$ leaves.

**From R7:**

All maximal paths in a tree must start and end with leaves.

**From R9:**

For a connected graph $G$ and an arbitrary partition of $G$'s vertex set $V$ into nonempty sets $S$ and $V \setminus S$, if there exists only one edge $e$ between the vertices in $S$ and the vertices in $V \setminus S$, then $e$ must be in every spanning tree of $G$.

## 6.4 Graph Coloring

### 6.4.1 Definitions:

A graph is $k\text{-}colorable$ if each vertex can be colored using one of the $k$ colors so that adjacent vertices are colored using different colors.

The $chromatic\ number$ of a graph $G$, $\chi(G)$, is the smallest value of $k$ for which $G$ is $k$-colorable.

A $bipartite\ graph$ is a graph that is 2-colorable.

### 6.4.2 Proofs:

**From L11T:**

A graph with a maximum degree at most $k$ is $(k+1)$-colorable. **From L15T:**

For any $k \geq 1$, there exist triangle-free graphs with chromatic number greater than $k$.

**From R11:**

A graph is bipartite iff it has no odd length cycles.

## 6.5 Eulerian, Hamiltonian, and Tournament Graphs

### 6.5.1 Definitions:

An $Eulerian\ circuit$ is a closed walk in which each edge appears exactly once. A connected graph is $Eulerian$ if it contains an Eulerian circuit.

A $Hamiltonian\ cycle$ in a graph $G$ is a cycle in which each vertex of $G$ appears exactly once. A graph is $Hamiltonian$ if it contains a Hamiltonian cycle.

A $tournament\ graph$ is a directed graph with exactly one directed edge between any pair of vertices.

A tournament $G = (V, E)$ is called $k$-dominated if for every set of $k$ vertices $v_1, v_2, v_3, ..., v_k$ there exists another vertex $u \in V$ such that $(u, u_i) \in E$, for $i = 1, 2, ..., k$.

### 6.5.2 Proofs:

**From L10T:**

If $\delta(G) \geq 2$ then $G$ contains a cycle.

**From L10T:**

A connected graph $G$ is Eulerian iff every vertex in $G$ has even degree.

**From L10T:**

Let $G$ be a graph with $n \geq 3$ vertices. If every vertex in $G$ has degree $\geq \frac{n}{2}$ then $G$ is Hamiltonian. Note the converse is NOT necessarily true.

**From L14T:**

Every tournament graph has at least one Hamiltonian path.

**From L14T:**

There is a $n$-vertex tournament with at least $\frac{n!}{2^{n-1}}$ distinct Hamiltonian paths.

**From L15T:**

For any positive integer $k$, if $n$ is large enough then there is a $k$-dominated tournament on $n$ vertices.

**From HW10H:**

For any Eulerian graph, an edge can be removed and the graph will remain connected.

**From R10:**

For any graph $G$ with an Eulerian Circuit, its edges can be partitioned into a set of edge-disjoint cycles (cycles that do not share any edges).

## 6.6 Matchings:

### 6.6.1 Definitions:

A $matching$ in a graph is a set of edges with no shared end-points. The vertices incident on the edges of a matching $M$ are called $M - saturated$, the others are called $M - unsaturated.$

A $perfect\ matching$ in a graph is a matching that saturates every vertex in the graph.

A $maximal\ matching$ in a graph is a matching that is not contained in a larger matching. A $maximum\ matching$ is a matching of maximum size among all matchings in the graph.

Given a matching $M$, an $M - alternating\ path$ is a path that alternates between edges in $M$ and edges not in $M$.

An $M$-alternating path whose endpoints are $M$-unsaturated is called an $M - augmenting$ path.

For Graphs $G$ and $H$, the $symmetric\ difference\ G \oplus H$ is a subgraph of $G \cup H$ whose edges are the edges of $G \cup H$ that appear in either $G$ or $H$, but not both.

An $independent\ set$ of a graph is a set of pair-wise non-adjacent vertices.

$Hall's\ condition$ is the necessary and sufficient condition for Hall's Theorem.

### 6.6.2 Proofs:

**From L11T:**

A matching $M$ in $G$ is maxmimum iff $G$ contains no $M - augmenting$ path.

**Hall's Theorem:**

Let $G = (X, Y, E)$ be a bipartite graph. For any set $S$ of vertices, let $N_G(S)$ be the set of vertices adjacent to vertices in $S$. $G$ contains a matching that saturates very vertex in $X$ iff

$$|N_G(S)| \geq |S|, \forall S \subseteq X$$

**From HW14T:**

If all vertices in a bipartite graph $G = (X, Y, E)$ have the same degree $m > 0$, then the partitions $X$ and $Y$ of the vertex sets are of the same magnitude. That is, $|X| = |Y|$.

**From HW14H:**

A bipartite graph $G = (X, Y, E)$ has a perfect matching iff for all subsets $A \subseteq (X \cup Y)$, the inequality $|A| \leq |N(A)|$ holds.

**From R12:**

Any $k$-regular bipartite graph has a perfect matching.

## 6.7 Ramsey Numbers

### 6.7.1 Definitions:

An $independent\ set\ S$ in $G$ is a subset of vertices such that no two vertices in $S$ share an edge. The $independence\ number$ of a graph $G$, denoted by $\alpha(G)$ is the size of the largest independent set in $G$.

For any graph $G = (V, E)$, a set of vertices $D \subseteq V$ is called a $dominating\ set$ if every vertex in $V \setminus D$ is adjacent to a vertex in $D$.

A $clique$ in a graph $G$ is a set of vertices such that any pair of vertices share an edge.

The $Ramsey\ number\ R(k, l)$ is the smallest number $n$ such that any graph with $n$ vertices has a clique or size $k$ or an independent set of size $l$. Another way to formulate this is: in any two-coloring on edges of the complete graph on $n$ vertices, there is a monochromatic clique of size $k$ or a monochromatic clique of size $l$.

Diagonal Ramsey Number asks for the value of $R(k, k)$ for any integer $k$.

### 6.7.2 Proofs:

**From L14H:**

Let $n$ be the number of vertices in $G$ and $m$ be the number of edges, and let $d = \frac{2m}{n} \geq 1$ be the average degree. Then

$$\alpha(G) \geq \frac{2}{2d}$$

**From L14H:**

Any connected graph $G = (V, E)$ with $n \geq 2$ vertices and minimum degree $\sigma(G) = \sigma$ contains a dominating set of size at most

$$\frac{n(1 + ln(1 + \sigma))}{1 + \sigma}$$

**From L15T:**

IF $\binom{n}{k} 2^{1-\binom{k}{2}} < 1$, then $R(k, k) > n$. In particular $R(k, k) > \lfloor 2^{\frac{k}{2}} \rfloor$, for $k \geq 3$.

**From HW15T:**

Where $I(G)$ is the size of the maximum independent set in $G$ and $Q(G)$ is the size of the maximum clique $G$,

$$I(G) = Q(\overline{G})$$

$$\chi(G) \geq Q(G)$$

# 7 Probability

## 7.1 Definitions:

The *sample space*, denoted by $\Omega$, of a random process or experiment is the set of all possible outcomes.

The *probability space* is a sample space together with a *probability distribution* in which a probability is assigned to each outcome $\omega \in \Omega$.

An *event* is any subset of the sample space.

## 7.2 Fundamental Equations:

**Basic Equations** For any events $A$ and $B$ such that $A, B \subseteq \Omega$

$$\Pr[A] = \sum_{\omega \in A} \Pr[\omega]$$

$$\Pr[B] = 1 - \Pr[\overline{B}]$$

$$\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]}$$

$$\Pr[A \cap B] = \Pr[A|B] \Pr[B]$$

**Inclusion-Exclusion Formula for Probabilities**

For two events $A$ and $B$ we have

$$\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$$

For any number of events, the formula applies just as PIE about sets where the probabilities of each individidual event are added, the pairwise intersections subtracted, triowise probabilities added, and so on.

**Union Bound** For the union of any number of events

$$\Pr[\bigcup_{i=1}^{n} A_i \leq \sum_{i=1}^{n} \Pr[A_i]]$$

## 7.3 Markov's and Chebyshev's

Markov's Inequality:

$$\Pr[X > a] \leq \frac{\mathbf{E}[X]}{a}$$

Chebyshev's Inequality:

$$\Pr[|X - \mathbf{E}[X]| > a] = \frac{\mathbf{V}[X]}{a^2}$$

## 7.4 Independence

Two events $A$ and $B$ are *independent* if and only if:

$$\Pr[A \cap B] = \Pr[A] \times \Pr[B]$$

$$\Pr[A|B] = \Pr[A]$$

$$\Pr[B|A] = \Pr[B]$$

Note: Independence does NOT imply Disjointness

Two random variables $X$ and $Y$ are independent if and only if:

$$\Pr[X = x \cap Y = y] = \Pr[X = x] \times \Pr[Y = y]$$

for *all* values of $x$ and $y$

## 7.5 Random Variables

A *random variable* $X$ on a sample space $\Omega$ is a real-valued function that assigns to each sample point $\omega \in \Omega$ a real number $X(\omega)$. For a discrete random variable $X$ and a real value $a$, the event $X = a$ is the set of outcomes in $\Omega$ for which the random variable assumes the value $a$.

### 7.5.1 Geometric Random Variable

**Conditions:** The following must be met for a random variable to have a negative binomial distribution:

1. Experiment consists of a sequence of independent trials
2. Each trial has two outcomes
3. The probability of success, $p$, is constant
4. Trials are performed until a total of $r$ successes have been observed, where $r \in \mathbb{Z}^+$

**pmf:** For a random variable $X$ where $p$ represents the probability of success

$$\Pr[X = x] = (1 - p)^{x-1} p$$

**Mean and Variance:** If $X$ has a geometric distribution

$$\mathbf{E}[X] = \frac{1}{p}$$

$$\mathbf{V}[X] = \frac{1 - p}{p^2}$$

**Memoryless Property:** The geometric distribution is the only discrete distribution with the memoryless property, defined by

$$\Pr[X \geq x + s | X \geq x] = \Pr[X \geq s]$$

### 7.5.2 Binomial Random Variable

**Conditions:** The following must be met for a random variable to have a binomial distribution

1. $n$ trials with $n$ fixed in advance
2. Each trial has two outcomes
3. Probability of success, $p$, is constant
4. Trials are independent

**pmf:** where $x$ represents number of successes ($0 \leq x \leq n$), $n$ represents number of trials, and $p$ represents probability of success

$$\Pr[X = x] = \binom{n}{x} p^x (1-p)^{n-x}$$

**Mean and Variance:** If $X$ has a binomial distribution with parameters $n$ and $p$ then

$$\mathbf{E}[X] = np$$

$$\mathbf{V}[X] = np(1-p)$$

### 7.5.3 Expectation

The $expectation$ of a random variable is the weighted average of the possible values of $X$.
$\mathbf{E}[X] = \sum_i i \Pr[X = i]$

By Linearity of Expectation,
$\mathbf{E}[\sum_{i=1}^{n} X_i] = \sum_{i=1}^{n} \mathbf{E}[X_i]$

If $X$ and $Y$ are independent real-valued random variables then.
$\mathbf{E}[X \cdot Y] = \mathbf{E}[X] \cdot \mathbf{E}[Y]$

For any random variable $Y$ that only takes on non-negative integer values, $\mathbf{E}[Y] = \sum_{i=0}^{\infty} \Pr[Y > i]$

The following is the definition of conditional expectation:

$$\mathbf{E}[Y|Z = z] = \sum_y y \Pr[Y = y|Z = z]$$

As proven in lecture for random variables $X$ and $Y$,

$$\mathbf{E}[X] = \sum_y \Pr[Y = y]\mathbf{E}[X|Y = y]$$

### 7.5.4 Variance

$variance$ is the measure of how much a random variable deviates from its mean. The $standard\ deviation$ is a measure of the same thing but provides a tighter magnitude.

By definition,
$\mathbf{V}[X] = \mathbf{E}[X^2] - \mathbf{E}[X]^2$

By definition,
$\sigma[X] = \sqrt{\mathbf{V}[X]}$

If $X$ and $Y$ are independent real-valued random variables then,

$\mathbf{V}[X+Y] = \mathbf{V}[X] + \mathbf{V}[Y]$

Let $Y$ be a random variable such that $Y = \sum_{i=1}^{n} Y_i$, where each $Y_i$ is a random variable. If $\mathbf{E}[Y_i Y_j] = \mathbf{E}[Y_i]\mathbf{E}[Y_j]$ for every pair $i, j$ such that $1 \leq i \leq j \leq n$, then

$$\mathbf{V}[Y] = \sum_{i=1}^{n} \mathbf{V}[Y_i]$$

# 8 Relations

## 8.1 Definitions:

A $binary\ relation$ is a set of ordered pairs.
For sets $A$ and $B$, a relation $from\ A\ to\ B$ is a subset of the cartesian product $A \times B$. When $A = B$, we say that relation $R$ is $on$ set $A$.
For a relation $R$ on set $A$, we say that a relation is $reflexive$ if for all $x \in A, (x, x) \in R$.
If $(1, 2) \in R$, we say that 1 is related to 2 by relation $R$, denoted by $1R2$. A relation is $irreflexive$ if for all $x \in A, (x, x) \notin R$.
A relation is $symmetric$ if for all $x, y \in A, (x, y) \in R \implies (y, x) \in R$.
A relation is $antisymmetric$ if for all $x, y \in A$, $xRy$ and $yRx \implies x = y$.
A relation is $transitive$ if for all $x, y, z \in A$, $xRy$ and $yRz \implies xRz$.

## 8.2 Proofs:

**From L12T:**
There are $2^{n^2}$ relations on a set $A$ of $n$ elements.
**From L12H:**
There are $2^{n(n-1)}$ reflexive relations on a set $A$ of $n$ elements.

## 8.3 Equivalence Relations

### 8.3.1 Definitions:

A relation $R$ on a set $A$ is an $equivalence\ relation$ iff it is reflexive, symmetric, and transitive.
If $m$ is a positive integer then integers $x$ and $y$ are $congruent\ modulo$ $m$, written as $x \cong y$ (mod $m$), if $m|(x-y)$.
Let $R$ be an equivalence relation on a set $A$ and let $a \in A$. The $equivalence\ class$ of $a$, denoted by $[a]_R$, is the set of all elements of $A$ related (by $R$) to $a$.
If $b \in [a]_R$, then $b$ is called the $representative$ of the equivalence class $[a]_R$.
A $directed\ graph$, or $digraphG = (V, E)$ consists of a set $V$ of vertices and a subset $E \subseteq V \times V$ of edges or arcs. An edge of the from $(u, u)$ is represented as an arc from $u$ to itself. Note that a binary relation $R$ on a set $A$ can be represented as a directed graph in which the vertices represent the elements of $A$ ad for every ordered pair $(a, b) \in R$, there is an edge from vertex $a$ to vertex $b$.
Note that all operations that can be performed on sets can be equivalently performed on relations, where the elements of relation $R$ are its ordered pairs.
Let $R$ be a relation from $A$ to $B$. Then the $inverse$ of $R$, written $R^{-1}$, is the relation from $B$ to $A$ defined by

$$R^{-1} = \{(b, a)|(a, b) \in R\}$$

Let $R$ be a relation from $A$ to $B$ and $S$ be a relation from $B$ to $C$. The $composition\ of\ S\ with\ R$ is the relation from $A$ to $C$:

$$S \circ R = \{(x,z) | \text{ there exists a } y \in B \text{ such that } xRy \text{ and } ySz\}$$

Let $R$ be a relation on set $A$. The powers $R^n$, $n = 1, 2, 3, ...$ are defined recursively by

$$R^{n+1} = R^n \circ R$$

### 8.3.2 Proofs:

**From L12H:**
Let $m$ be a positive integer. The $congruent\ modulo\ m$ relation

$$R = \{(a,b) : a \cong b \text{ (mod } m)\}$$

is an equivalence relation on the set of integers.
**From L12H:**
Let $R$ be an equivalence relation on a set $A$. Then the following statements for elements $a, b \in A$ are equivalent:

1. $b \in [a]$
2. $[a] = [b]$
3. $[a] \cap [b] \neq \emptyset$

**From L12H:**
Let $R$ be an equivalence relation on a set $A$. Then the set $\{[a]_R | a \in A\}$ is a partition of the set $A$. Each element of the set is called an $equivalence\ class$ of $R$. Conversely, given a partition $\{A_i\}$ of the set $A$, there is an equivalence relation $R$ that has sets $A_i$ as its equivalence classes.
**From L14T:**
A relation $R$ on a set $A$ is symmetric iff $R = R^{-1}$
**From L14T:**
Let $R$ be a relation on set $A$. Then $R$ is transitive iff $R^n \subseteq R$, for all $n \geq 1$.
**From HW14H:**
If sets $R$ and $S$ are equivalence relation on set $A$, the union of sets $R$ and $S$ are NOT necessarily an equivalence relation. The intersection of sets $R$ and $S$ is ALWAYS an equivalence relation.
**From HW14H:**
An antisymmetric equivalence relation $R$ on set $A$ has $|R| = |A|$

## 8.4 Functions

### 8.4.1 Definitions:

Let $A$ and $B$ be sets. A $function$ from $A$ to $B$ is a relation, $f$, from $A$ to $B$ such that for all $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in f$.
If $(a, b) \in f$, we write $b = f(a)$.
A function from $A$ to $B$ is also called a $mapping$ from $A$ to $B$ and we write it as $f : A \to B$.
The set $A$ is called the $domain$ of $f$ and the set $B$ the $codomain$.
if $a \in A$ then the element $b = f(a)$ is called the $image$ of $a$ under $f$.
The $range$ of $f$, denoted by Ran($f$), is the set

$$Ran(f) = \{b \in B | \exists a \in A \text{ such that } b = f(a)\}$$

Two functions are $equal$ if they have the same domain, have the same codomain, and map each element of the domain to the same element of the codomain.
Let $f : A \to B$ be a function. $f$ is said to be $one - to - one$ or $injective$, iff for every $x, y \in A$ such that $x \neq y, f(x) \neq f(y)$.
$f$ is called $onto$ or $surjective$, iff for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$.
$f$ is a $one-to-one\ correspondence$ or $bijection$, if it is both one=to-one and onto.
Let $f$ be a one-to-one correspondence from the set $A$ to the set $B$. The $inverse$ function of $f$ is the function that maps an element $b \in B$ to the unique element $a \in A$ such that $f(a) = b$. The inverse function of $f$ is denoted by $f^{-1}$. Hence $f^{-1}(b) = a$ when $f(a) = b$. Note that if $f$ is not bijective then its inverse does not exist.
Let $f : A \to B$ and $g : B \to C$ be functions. The $composition$ of the function $g$ with $f$ is the function $g \circ f : A \to C$, defined by

$$(g \circ f)(x) = g(f(x)), \forall x \in A$$

### 8.4.2 Proofs:

**From L14H:**
Let $A$ to $B$ be finite sets of size $a$ and $b$, respecitvely. There are $b^a$ number of ways to create a function from $A \to B$.
**From L14H:**
Let $f$ and $g$ be the functions. $(f \circ g)(x) = (g \circ f)(x)$ is not always true.
**From L14H:**
Let $f : A \to B$ and $g : B \to C$ be two functions. Then

1. if $f$ and $g$ are surjective then so is $g \circ f$.
2. if $f$ and $g$ are injective then so is $g \circ f$.
3. if $f$ and $g$ are bijective then so is $g \circ f$.