Discrete Mathematics – Comprehensive Study Guide

I. Propositional Logic and Proof Techniques

Definitions & Operators

Concept	**Definition/Formula/Truth Condition**
Proposition	A declarative statement that is either true or false, but not both.
Propositional Formula	A proposition containing propositional variables and operators.
Equivalent Propositions	$p \equiv q$ iff they have the same truth tables.
Negation ($\neg p$)	True when p is false, false when p is true.
Conjunction ($p \wedge q$)	True iff both p and q are true.
Disjunction ($p \vee q$)	True if at least one of p or q is true.
Exclusive-OR ($p \oplus q$)	True whenever exactly one of p or q is true.
Implication ($p \Rightarrow q$)	False only when p true and q false; otherwise true.
Biconditional ($p \Leftrightarrow q$)	True when p and q have same truth value.
Converse (of $p \Rightarrow q$)	$q \Rightarrow p$.
Contrapositive (of $p \Rightarrow q$)	$\neg q \Rightarrow \neg p$ (Equivalent to $p \Rightarrow q$).
Inverse (of $p \Rightarrow q$)	$\neg p \Rightarrow \neg q$ (Equivalent to the converse).
Disjunctive Normal Form (DNF)	Disjunction ($\vee$) of AND-terms.
Conjunctive Normal Form (CNF)	Conjunction ($\wedge$) of OR-terms.

Rules of the Algebra of Propositional Logic

Rule Category	**Rule/Equivalence**
Commutativity	$p \wedge q \equiv q \wedge p$; $p \vee q \equiv q \vee p$
Associativity	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$; $p \vee (q \vee r) \equiv (p \vee q) \vee r$
Identity	$p \wedge T \equiv p$; $p \vee F \equiv p$
Idempotence	$p \wedge p \equiv p$; $p \vee p \equiv p$
Domination	$p \wedge F \equiv F$; $p \vee T \equiv T$
Complement/Negation	$p \wedge \neg p \equiv F$; $p \vee \neg p \equiv T$; $\neg\neg p \equiv p$
Distributivity	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$; $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
De Morgan's Laws	$\neg(p \wedge q) \equiv \neg p \vee \neg q$; $\neg(p \vee q) \equiv \neg p \wedge \neg q$
Non-Basic Operator	$p \Rightarrow q \equiv \neg p \vee q$

Induction

Technique	**Template/Conditions**
Proof by Induction	1. **Base Case:** Prove $P(n_0)$ true. 2. **Induction Hypothesis:** Assume $P(n)$ true for $n \geq n_0$. 3. **Induction Step:** Prove $P(n+1)$ using hypothesis.
Proof by Strong Induction	1. **Base Case:** Prove $P(n_0)$ true. 2. **Induction Hypothesis:** Assume $P(k)$ true for every $k \in \{n_0+1, \ldots, n\}$. 3. **Induction Step:** Prove $P(n+1)$ using hypothesis.
Arithmetic Formula	$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ (Claim 5.1, $n \geq 1$)
Geometric Progression	$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$ (Claim 5.2, $r \neq 1, n \geq 1$)
Bernoulli's Inequality	$(1+x)^n \geq 1 + nx$ (Claim 5.4, $x > -1, n \geq 1$)
Euclid's Lemma	If p prime divides ab, then p divides a or p divides b.
Fundamental Theorem of Arithmetic	Every $n > 1$ has unique prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ (up to reordering).

II. Set Theory, Relations, and Functions

Set Definitions and Properties

Concept	**Definition/Formula/Property**
Equality of Sets ($S = T$)	$S = T$ iff $S \subseteq T$ and $T \subseteq S$.
Power Set (pow(A))	Set of all subsets of A; $B \in \text{pow}(A) \iff B \subseteq A$.
Cardinality of Power Set	If $\|A\| = n$, then $\|\text{pow}(A)\| = 2^n$.
Set Operations	Union: $A \cup B := \{x : x \in A \vee x \in B\}$ Intersection: $A \cap B := \{x : x \in A \wedge x \in B\}$ Difference: $A - B := \{x : x \in A \wedge x \notin B\}$ Complement: $\bar{A} := \{x : x \in U \wedge x \notin A\}$ Cartesian Product: $A \times B := \{(a,b) : a \in A \wedge b \in B\}$
Disjoint Sets	A and B disjoint if $A \cap B = \phi$.
Set Identities	$A \cup \phi = A$; $A \cap \phi = \phi$; $A \cup \bar{A} = U$; $A \cap \bar{A} = \phi$; $\overline{\bar{A}} = A$; $A \times \phi = \phi \times A = \phi$.
De Morgan's Laws (Sets)	$\overline{A \cup B} = \bar{A} \cap \bar{B}$; $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

Relations and Partitions

Concept	**Definition/Property**
Binary Relation (R)	Subset of $A \times B$ (or $A \times A$).
Reflexive Relation	For every $a \in A$, $(a, a) \in R$.
Symmetric Relation	For every $(a, b) \in R$, $(b, a) \in R$.
Transitive Relation	If $(a, b), (b, c) \in R$, then $(a, c) \in R$.
Equivalence Relation	Reflexive, symmetric, and transitive.
Equivalence Class ($[x]_R$)	$[x]_R := \{a \in A : (a, x) \in R\}$.
Set of Equivalence Classes (A/R)	$A/R := \{[x]_R : x \in A\}$.
Properties of Equivalence Classes	1. For every $x \in A$, $x \in [x]_R$. 2. $(x, y) \in R$ iff $[x]_R = [y]_R$. 3. $(x, y) \notin R$ iff $[x]_R \cap [y]_R = \phi$.
Partition of A	Collection P of non-empty subsets of A such that: a) $\forall X \in P, X \neq \phi$ b) $\forall X, Y \in P$, either $X = Y$ or $X \cap Y = \phi$ c) $\forall a \in A$, $\exists X \in P$ such that $a \in X$.

Functions

Concept	**Definition/Property**
Function ($F : X \to Y$)	Subset $F \subseteq X \times Y$ such that $\forall x \in X$, $\exists! y \in Y$ with $(x, y) \in F$.
Injective (One-to-One)	If $f(x_1) = f(x_2)$ then $x_1 = x_2$.
Surjective (Onto)	$\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$ (i.e., Range$(F) = Y$).
Bijective	Both injective and surjective.
Composition ($G \circ F$)	$(G \circ F)(x) := G(F(x))$, provided Range$(F) \subseteq$ Domain(G).
Composition Properties	If F, G injective $\Rightarrow G \circ F$ injective. If F, G surjective $\Rightarrow G \circ F$ surjective. If F, G bijective $\Rightarrow G \circ F$ bijective.

III. Cardinality and Countability

Concept	**Definition/Formula/Result**
Countably Infinite Set	Set X for which $\exists$ bijection $F : \mathbb{N} \to X$.
Countable Set	Finite or countably infinite.
Uncountable Set	Not countable.
Characteristic Function (χ_S)	For $S \subseteq A$, $\chi_S(a_i) = 1$ if $a_i \in S$, else 0.
Pigeonhole Principle (V1)	If $\|X\| > \|Y\|$, any $F : X \to Y$ is not injective.
Cardinality of Set Operations	$\|X \cup Y\| \leq \|X\| + \|Y\|$; $\|X \cap Y\| \leq \min\{\|X\|, \|Y\|\}$; $\|X \times Y\| = \|X\| \cdot \|Y\|$.
Key Uncountability Results	pow$(\mathbb{N})$, $[0, 1]$, $\mathbb{R}$, $\mathbb{C}$ are uncountable.

IV. Combinatorics (Counting Rules)

Rule/Claim	Formula/Description
Bijective Rule	If $F : X \to Y$ bijection, then $\lvert X\rvert = \lvert Y\rvert$.
Product Rule	$\lvert A_1 \times \cdots \times A_n\rvert = \lvert A_1\rvert \cdot \lvert A_2\rvert \cdots \lvert A_n\rvert$.
Generalized Product Rule	For k entries with n_i options each: total $= n_1 n_2 \cdots n_k$.
Sum Rule	For disjoint $A_1, \dots, A_n$: $\lvert\bigcup_{i=1}^n A_i\rvert = \sum_{i=1}^n \lvert A_i\rvert$.
Division Rule	If $F : A \to B$ is k-to-1, then $\lvert A\rvert = k \cdot \lvert B\rvert$.
Subset Rule (Binomial Coeff.)	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$.
Multinomial Coefficient	$\binom{n}{k_1, k_2, \dots, k_m} = \frac{n!}{k_1! k_2! \cdots k_m!}$.
Binomial Theorem	$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i$.
Inclusion-Exclusion (2 Sets)	$\lvert A \cup B\rvert = \lvert A\rvert + \lvert B\rvert - \lvert A \cap B\rvert$.
Pascal's Identity	$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
Counting Subsets Identity	$\sum_{i=0}^n \binom{n}{i} = 2^n$.
n-bit 0,1 sequences	2^n.
Number of functions ($\lvert A\rvert = n$, $\lvert B\rvert = m$)	m^n.
Number of injective functions ($n \le m$)	$m \cdot (m-1) \cdots (m-n+1)$.
Number of permutations (n elements)	$n!$.
Arrangements in a round table (n distinct)	$(n-1)!$.
Identical balls in distinct bins (n balls, m bins)	$\binom{n+m-1}{m-1}$.

V. Basic Graph Theory

Definitions

Concept	Definition/Type
Undirected Graph ($G = (V, E)$)	Pair of sets V (vertices) and E (edges).
Simple Graph	No loops, no multiple edges.
Degree of a Vertex ($\deg(v)$)	Number of edges incident to v (loop counts twice).
Bipartite Graph	$V = V_1 \cup V_2$, $V_1 \cap V_2 = \phi$, edges only between V_1 and V_2.
Complete Graph (K_n)	All $\binom{n}{2}$ edges present.
Tree	Connected acyclic undirected graph.
Acyclic Graph (Forest)	Contains no cycles.
Matching (M)	$M \subseteq E$, no loops, no two edges share an endpoint.
Perfect Matching	Matching saturating all vertices.
Complete Matching (bipartite)	Matching of size $\lvert V_1\rvert$ ($\lvert V_1\rvert \le \lvert V_2\rvert$).
Isomorphic Graphs	$\exists$ bijection $\pi : V_1 \to V_2$ preserving adjacency.
Directed Graph	Edges have direction $\langle u, v\rangle$.
In-degree/Out-degree	in-deg(v): edges where v is head; out-deg(v): edges where v is tail.

Key Theorems and Lemmas

Result	**Statement**
Handshaking Lemma	$\sum_{v \in V} \deg(v) = 2\|E\|$.
Odd Degree Vertices	An undirected graph has an even number of odd-degree vertices.
Tree Edge Count	Tree with n vertices has $n - 1$ edges.
Sum of Degrees (Directed)	$\sum_v \text{in-deg}(v) = \sum_v \text{out-deg}(v) = \|E\|$.
Hall's Marriage Theorem	Bipartite $G = (V_1 \cup V_2, E)$, $\|V_1\| \leq \|V_2\|$, has complete matching iff $\forall A \subseteq V_1$, $\|N(A)\| \geq \|A\|$.
Perfect Matchings in K_{2n}	Number $= \frac{(2n)!}{2^n \cdot n!}$.

Analogy for Understanding Induction

The Principle of Mathematical Induction can be visualized like **setting up dominoes**:

- **Base Case:** You must push the first domino (Prove $P(n_0)$ is true).
- **Induction Hypothesis/Step:** You assume that if any one domino falls ($P(n)$ is true), it will knock down the next one ($P(n+1)$ is true).

If you satisfy the base case and ensure the transfer property (the inductive step) holds, you guarantee that *all* dominoes (all propositions $P(n)$ for $n \geq n_0$) will eventually fall.