Discrete Mathematics – Comprehensive Study Guide

I. Propositional Logic and Proof Techniques

Definitions & Operators

Concept	Definition / 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 identical truth tables.
Negation $\neg p$	True when p is false.
Conjunction $p \land q$	True iff both p and q are true.
Disjunction $p \lor q$	True iff at least one of p, q is true.
Exclusive-OR $p \oplus q$	True iff exactly one of p, q is true.
Implication $p \Rightarrow q$	False only when p is true and q is false.
Biconditional $p \Leftrightarrow q$	True when p and q have the same truth value.
Converse	$q \Rightarrow p$.
Contrapositive	$\neg q \Rightarrow \neg p$ (equivalent to $p \Rightarrow q$).
Inverse	$\neg p \Rightarrow \neg q$.
DNF	A disjunction of conjunctions.
CNF	A conjunction of disjunctions.

Rules of Propositional Logic

$$
\begin{aligned}
\text{Commutativity: } & p \wedge q \equiv q \wedge p, \quad p \vee q \equiv q \vee p \\
\text{Associativity: } & p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r \\
\text{Identity: } & p \wedge T \equiv p, \quad p \vee F \equiv p \\
\text{Idempotence: } & p \wedge p \equiv p, \quad p \vee p \equiv p \\
\text{Domination: } & p \wedge F \equiv F, \quad p \vee T \equiv T \\
\text{Complement: } & p \wedge \neg p \equiv F, \quad p \vee \neg p \equiv T, \quad \neg(\neg p) \equiv p \\
\text{Distributivity: } & p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \\
\text{De Morgan: } & \neg(p \wedge q) \equiv \neg p \vee \neg q, \quad \neg(p \vee q) \equiv \neg p \wedge \neg q \\
\text{Implication: } & p \Rightarrow q \equiv \neg p \vee q
\end{aligned}
$$

Induction Techniques

Mathematical Induction:

1. Base Case: prove $P(n_0)$
2. Induction Hypothesis: assume $P(n)$
3. Induction Step: prove $P(n+1)$

Strong Induction:

1. Base Case: prove $P(n_0)$
2. Hypothesis: $P(k)$ true for all $k \in [n_0, n]$
3. Step: prove $P(n+1)$

Key Results

$$
\begin{gathered}
\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \\
\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}, \quad r \neq 1 \\
(1+x)^n \geq 1 + nx, \quad x > -1
\end{gathered}
$$

Euclid's Lemma: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Fundamental Theorem of Arithmetic: Unique prime factorization for every $n > 1$.

II. Set Theory, Relations, and Functions

Sets

$$
\begin{aligned}
S = T \iff& S \subseteq T \text{ and } T \subseteq S \\
\text{Power set:} \quad \mathrm{pow}(A) =& \{B : B \subseteq A\} \\
|\mathrm{pow}(A)| =& 2^{|A|} \\
A \cup B =& \{x : x \in A \vee x \in B\} \\
A \cap B =& \{x : x \in A \wedge x \in B\} \\
A - B =& \{x : x \in A \wedge x \notin B\}
\end{aligned}
$$

De Morgan (Sets):

$$(A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c.$$

Relations and Partitions

Relation: $R \subseteq A \times A$.

- Reflexive: $(a, a) \in R$.
- Symmetric: $(a, b) \in R \Rightarrow (b, a) \in R$.
- Transitive: $(a, b), (b, c) \in R \Rightarrow (a, c) \in R$.
- Equivalence relation: reflexive, symmetric, transitive.

$$[x]_R = \{a \in A : (a, x) \in R\}.$$

Partition: nonempty subsets that are pairwise disjoint and whose union is A.

Functions

A function $F : X \to Y$ satisfies uniqueness of outputs.

- Injective: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
- Surjective: range $= Y$.
- Bijective: injective and surjective.

Composition: $(G \circ F)(x) = G(F(x))$.

III. Cardinality and Countability

- Countably infinite: bijection $\mathbb{N} \to X$.
- Uncountable: no such bijection.
- Characteristic function: $\chi_S(a) = 1$ if $a \in S$, else 0.

Pigeonhole Principle: If $|X| > |Y|$, no injective $X \to Y$ exists.

IV. Combinatorics (Counting Rules)

Rules

Bijection Rule: If $F : X \to Y$ bijective, $|X| = |Y|$.

Product Rule:

$$|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n|.$$

Generalized Product Rule: If n_i choices at step i, total $= \prod n_i$.

Sum Rule:

$$\left| \bigcup A_i \right| = \sum |A_i| \quad \text{(disjoint)}.$$

Division Rule: If a k-to-1 map $A \to B$ exists, $|B| = \frac{|A|}{k}$.

Subset Rule:

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

Multinomial:

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1! k_2! \cdots k_m!}.$$

Binomial Theorem:

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

Inclusion-Exclusion (2 sets):

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

Pascal Identity:

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

Counting Identities:

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n, \qquad \text{number of } n\text{-bit strings} = 2^n.$$

Functions:

$$\text{Total } A \to B = |B|^{|A|}, \qquad \text{Injective } A \to B = P(|B|, |A|) = |B|(|B|-1) \cdots$$

Permutations: $n!$.

Circular arrangements: $(n-1)!$.

Stars and Bars:

$$\binom{n+m-1}{m-1}.$$

V. Basic Graph Theory

Definitions

- Graph: $G = (V, E)$.
- Simple graph: no loops, no multiedges.
- Degree: number of incident edges; loop counts twice.
- Bipartite: $V = V_1 \cup V_2$, edges between parts.
- Complete graph: K_n.
- Tree: connected, acyclic.
- Forest: acyclic.
- Matching: no two edges share endpoints.
- Perfect Matching: all vertices covered.
- Isomorphism: bijection preserving adjacency.
- Directed graph: edges $\langle u, v \rangle$.

Theorems

Handshaking Lemma:

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

Odd Degree Lemma: Number of odd-degree vertices is even.
Tree Edge Count: $|E| = |V| - 1$.
Directed sum of degrees:

$$\sum \text{in-deg}(v) = \sum \text{out-deg}(v) = |E|.$$

Hall's Theorem: A bipartite graph has a perfect matching iff every subset $S \subseteq V_1$ satisfies $|N(S)| \geq |S|$.
Perfect Matchings in K_{2n}:

$$\frac{(2n)!}{2^n n!}.$$

Analogy: Induction

Mathematical induction is like dominoes:

- Base case: the first domino falls.
- Induction step: each domino knocks over the next.

Thus all dominos fall $\Rightarrow$ all $P(n)$ are true for $n \geq n_0$.