Cheat Sheet

Propositional Logic

Logical Equivalences	
Equivalence	***Name***
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity Laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination Laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws
$\neg(\neg p) \equiv p$	Double Negation Law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$	De Morgan's Laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption Laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation Laws

Logical Equivalences Involving Conditional Statements
$p \to q \equiv \neg p \lor q$
$p \to q \equiv \neg q \to \neg p$
$p \lor q \equiv \neg p \to q$
$p \land q \equiv \neg(p \to \neg q)$
$\neg(p \to q) \equiv p \land \neg q$
$(p \to q) \land (p \to r) \equiv p \to (q \land r)$
$(p \to r) \land (q \to r) \equiv (p \lor q) \to r$
$(p \to q) \lor (p \to r) \equiv p \to (q \lor r)$
$(p \to r) \lor (q \to r) \equiv (p \land q) \to r$

Logical Equivalences Involving Biconditional Statements
$p \leftrightarrow q \equiv (p \to q) \land (q \to p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Definitions for Exclusive Or (XOR)
$p \oplus q \equiv \neg(p \leftrightarrow q)$
$p \oplus q \equiv (p \land \neg q) \lor (\neg p \land q)$
$p \oplus q \equiv (p \lor q) \land (\neg p \lor \neg q)$

Definitions:

- A **tautology** is a proposition which is always true
- A **contradiction** is a proposition which is always false
- A **contingency** is a proposition which is neither a tautology nor a contradiction
- A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that make it true
- $q \to p$ is the **converse** of $p \to q$
- $\neg p \to \neg q$ is the **inverse** of $p \to q$
- $\neg q \to \neg p$ is the **contrapositive** of $p \to q$
- A **Disjunctive Normal Form (DNF)** is a disjunction of conjunctions where every variable or its negation is represented once in each conjunction
- A **Conjunctive Normal Form (CNF)** is a conjunction of disjunctions where every variable or its negation is represented once in each disjunction

Predicate Logic

De Morgan's Laws for Quantifiers			
Negation	***Equivalent Statement***	***When is Negation True ?***	***When False ?***
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is true for every x.	$P(x)$ is false.

Quantifications of Two Variables.		
Statement	***When True ?***	***When False ?***
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

Proofs

Rules of Inference		
Rule of Inference	***Tautology***	***Name***
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

In the following, unless stated oterhwise, we are going to assume that p is the premise and q is the conclusion.
Definitions:

- An **argument** in propositional logic is a sequence of propositions.
  - All but the final proposition are called **premises**.
  - The last statement is the **conclusion**.
  - The argument is **valid** if the premises imply the conclusion.
- **Indirect Proof:**
  - Proof by **Contraposition**: assume that $\neg q$ is True; then use definitions, axiom and theorems together with rules of inference till the statement $\neg p$ results.
  - Proof by **Contradiction**: assume that p and $\neg q$ are true; then perform a direct proof to produce a contradiction
- **Proof by Cases:**
  - To prove a conditional statement of the form: $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$
  - Use $[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$
  - Each of the implication $p_i \rightarrow q$ is a **case**.
- **Counterexamples:** to show that $\forall x P(x)$ is False, we need to find one counterexample, i.e. an x for which $P(x)$ is False
- **Proofs of equivalence:** To prove a theorem that is a biconditional statement, i.e. a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.
- **Existence Proofs:** The theorem is in the form of a statement $\exists x P(x)$
  - Constructive: find an element a for which $P(a)$ is True
  - Nonconstructive: show that assuming $\neg \exists x P(x)$ leads to a contradiction (proof by contradiction)
- **Uniqueness Proofs:** Some theorems assert the existence of a unique element with a particular property. Uniqueness Proof has two parts:
  - **Existence**: we show that an element x with the desired property exists
  - **Uniqueness**: we show that if x and y both have the desired property, then $x = y$.

Rules of inference for Quantified Statements	
Rule of inference	***Name***
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization
$\forall x(P(x) \rightarrow Q(x))$ $P(c)$, where c is a particular element in the domain $\therefore \exists x Q(x)$	Universal modus ponens
$\forall x(P(x) \rightarrow Q(x))$ $\neg Q(c)$, where c is a particular element in the domain $\therefore \neg P(c)$	Universal modus tollens

Sets, Functions, Relations

Sets of Numbers:

- Set of **natural numbers** (non negative integers): $N = \{0, 1, 2, 3, ...\}$
- Set of **integers**: $Z = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
- Set of **positive integers**: $Z^+ = \{1, 2, 3, ...\}$
- Set of all **real numbers**: R
- Set of all **positive real numbers**: R^+
- Set of **rational numbers**: $Q = \{p/q \mid p \in Z,\ q \in Z,\ q \neq 0\}$

Sets:

- The **empty set** $\emptyset$ is the set with no elements.
- The **universal set** U is the set containing everything currently under consideration.
- The set A is a **subset** of B, and B is a superset of A, if and only if every element of A is also an element of B. We write $A \subseteq B$
- The set of all subsets of a set A, denoted as $\mathcal{P}(A)$, is called the **power set** of A.
- The **Cartesian Product** of two sets A and B, denoted by $A \times B$, is the set of ordered pairs (a, b) where $a \in A$ and $b \in B$: $A \times B = \{(a, b) | a \in A \wedge b \in B\}$
- Let S be a finite set with n elements. $|S| = n$ is the **cardinality** of S.
- Let A and B be sets. The **union** of the sets A and B, denoted by $A \cup B$, is the set: $\{x | x \in A \vee x \in B\}$
- Let A and B be sets. The **intersection** of the sets A and B, denoted by $A \cap B$, is the set: $\{x | x \in A \wedge x \in B\}$
- **Inclusion-Exclusion**: $|A \cup B| = |A| + |B| - |A \cap B|$
- The **difference** of sets A and B, denoted by $A - B$, is the set containing the elements of A that are not in B: $A - B = \{x | x \in A \wedge x \notin B\}$
- The **complement** of the A with respect to the universe U, denoted by $\overline{A}$ is the set: $\overline{A} = U - A$
- A **partition** of a set S is a collection of disjoint nonempty subsets of S that have S as their union.

Set Identities (U is the universal set)	
Identity	***Name***
$A \cap U = A$ $A \cup \emptyset = A$	Identity Laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination Laws
$A \cup A = A$ $A \cap A = A$	Idempotent Laws
$\overline{(\overline{A})} = A$	Complementation Law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative Laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's Laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption Laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement Laws

Functions:

- Let A and B be nonempty sets. A **function** f from A to B is an assignment of exactly one element of B to each element of A. We write $f : A \to B$.
  - A is the **domain** of f
  - B is the **codomain** of f
  - if $f(a) = b$, we design b as the **image** of a and a as the **preimage** of b
- **Injection**: A function f is said to be **one-to-one**, or **injective**, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.
- **Surjection:** A function f from A to B is called **onto** or **surjective**, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$.

- **Bijection:** A function f from A to B is a **one-to-one correspondence**, or a **bijection**, if it is both one-to-one and onto (surjective and injective).
- Let f be a *bijection* from A to B. Then the **inverse** of f, denoted as f^{-1}, is the function from B to A defined as: $f^{-1}(y) = x$ iff $f(x) = y$
- Let $f : B \to C$ and $g : A \to B$. The **composition** of f with g, denoted $f \circ g$ is the function from A to C defined as: $f \circ g(x) = f(g(x))$

Relations:

- A **binary relation** R from a set A to a set B is a subset $R \subseteq A \times B$.
- A **binary relation** R on a set A **itself** is a subset $R \subseteq A \times A$.
- A relation R on a set A itself is:
  - **Reflexive** iff $(a, a) \in R$ for every element $a \in A$.
  - **Symmetric** iff $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.
  - **Antisymmetric** iff $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ for all $a, b \in A$.
  - **Transitive** iff $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ for all $a, b, c \in A$.
- The **composite** of R and S is the relation consisting of ordered pairs (a, c), where $a \in A$, $c \in C$, and for which there exists an element $b \in B$, such that $(a, b) \in R$ and $(b, c) \in S$. We denote the composite of R and S by $S \circ R$.
- A relation on a set A is called an **equivalence relation** if it is reflexive, symmetric, and transitive.
- Two elements a, and b that are related by an equivalence relation are called **equivalent**.
- Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the **equivalence class** of a. It is denoted by $[a]_R$.
- **Theorem:** Let R be an equivalence relation on a set S. Then the set of equivalence classes of R form a partition of S.
- A relation R on a set S is called a **partial ordering**, or partial order, if it is reflexive, antisymmetric, and transitive.
- A set together with a partial ordering R is called a **partially ordered set**, or **poset**, and is denoted by (S, R).
- The elements a and b of a poset $(S, \preccurlyeq)$ are **comparable** if $a \preccurlyeq b$ or $b \preccurlyeq a$.
- If $(S, \preccurlyeq)$ is a poset and every two elements of S are comparable, S is called a totally ordered set, and $\preccurlyeq$ is called a **total order**.
- $(S, \preccurlyeq)$ is a **well-ordered** set if it is a poset such that $\preccurlyeq$ is a total ordering and every nonempty subset of S has a least element.
- Let $(S, \preccurlyeq)$ be a partially ordered set:
  - An **upper bound** u of a subset A of S, is an element of S such that $a \preccurlyeq u$ for all $a \in A$.
  - A **lower bound** u of a subset A of S, is an element of S such that $u \preccurlyeq a$ for all $a \in A$.
  - A **least upper bound** u of a subset A of S, is an upper bound of A that is less than every other upper
  - A **greatest lower bound** u of a subset A of S, is a lower bound of A that is greater than every other lower bound of A.
- A **lattice** is a partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound.

- Given two posets $(A_1, \preccurlyeq_1)$ and $(A_2, \preccurlyeq_2)$, the **lexicographic ordering** on $A_1 \times A_2$ is defined by specifying that (a_1, a_2) is less than (b_1, b_2), that is, $(a_1, a_2) \prec (b_1, b_2)$, either if $a_1 \prec_1 b_1$ or (if $a_1 = b_1$ and $a_2 \prec_2 b_2$).

Sequences:

- A **sequence** is a function from a subset of the integers to a set S.
- An **arithmetic progression** is defined by the function $f(n) = a + nd$
- An **geometric progression** is defined by the function $f(n) = ar^n$
- A **recurrence relation** for the sequence $\{a_n\}$ is an equation that expresses an in terms of a finite number k of the preceding terms of the sequence, i.e., $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$. The **initial conditions** for a sequence specify the terms $a_0, a_1, \ldots, a_k$
- A **string** is a finite sequence of characters from a finite set A (an alphabet).
- The **Fibonacci sequence** $f_0, f_1, f_2, \ldots$ is defined as:
  - Initial Conditions: $f_0 = 0, f_1 = 1$
  - Recurrence Relation: $f_n = f_{n-1} + f_{n-2}$

Some Useful Summation Formulae.

Sum	*Closed Form*
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1}-a}{r-1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x\rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x\rvert < 1$	$\frac{1}{(1-x)^2}$

Countability:

- The **cardinality** of a set A is **equal** to the **cardinality** of a set B, denoted by $|A| = |B|$ iff there is a **bijection** from A to B.
- If there is an **injection** from A to B, the **cardinality** of A is less than or the same as the cardinality of B and we write $|A| \leq |B|$.
- If there is an **surjection** from A to B, the **cardinality** of B is less than or the same as the cardinality of A and we write $|B| \leq |A|$.
- A set that is either finite or has the same cardinality as the set of positive integers Z^+ is called **countable**. A set that is not countable is **uncountable**.
- **Theorem:** An infinite set S is countable iff it is possible to list the elements of the set in a sequence indexed by the positive integers.
- **Properties of countable sets:**

- A subset of a countable set is countable
- The cartesian product of finitely many countable sets is countable
- The union of finitely many countable sets is countable
- The set of all strings associated to a finite alphabet is countable
- If there is an injective function from A to B and B is countable: then A is countable
- If there is a surjective function from A to B and A is countable: then B is countable

- **Cantor's Diagonal Argument for** $[0, 1]$:

  1. We assume that we can list the real numbers in $[0, 1]$ in a sequence indexed by the positive integers $\{a_n\}$
  2. We associate each element of $\{a_n\}$ to the decimal representation of each real numbers in $[0, 1]$
  3. We show that we can build a real number in $[0, 1]$ that is not in $\{a_n\}$
  4. By contradiction, our initial assumption is False

- **Theorems related to uncountable sets:**

  - If A is uncountable and $A \subseteq B$, then B is uncountable
  - The set of real numbers R is uncountable.

Algorithms

Searching:

Linear Search ($a_1, a_2, \cdots a_n$**: list,** x**)**

```
i = 1
location = 0
while x ≠ a_i and i ≤ n do
  i ← i + 1
end while
if i ≤ n then
  location = i
end if
return location
```

Binary Search($a_1, a_2, \cdots a_n$**: ordered list,** x**)**

```
lower_bound = 1
upper_bound = n
while lower_bound < upper_bound do
  middle = ⌊(lower_bound + upper_bound)/2⌋
  if x > a_middle then
    lower_bound = middle + 1
  else
    upper_bound = middle
  end if
end while
if x = a_lower_bound then
  location = lower_bound
else
  location = 0
end if
return location
```

Sorting:

Bubble Sort($a_1, a_2, \cdots a_n$**: list)**

```
for i = 1 to n − 1 do
  for j = 1 to n − i do
    if a_j > a_{j+1} then
      swap a_j and a_{j+1}
    end if
  end for
end for
```

Selection Sort($a_1, a_2, \cdots a_n$**: list)**

```
for i = 1 to n − 1 do
  min ← i + 1
  for j = i + 1 to n do
    if a_min > a_j then
      min ← j
    end if
  end for
  if a_i > a_min then
    swap a_i and a_min
  end if
end for
```

Insertion Sort($a_1, a_2, \cdots a_n$**: list)**

```
for j = 2 to n do
  i ← 1
  while a_j > a_i do
    i ← i + 1
  end while
  m ← a_j
  for k = 0 to j − i − 1 do
    a_{j−k} ← a_{j−k−1}
  end for
  a_i ← m
end for
```

Greedy Algorithms:

- **Optimization problems** minimize or maximize some parameter over all possible inputs.
- A **greedy algorithm**, which makes the optimal or "best" choice at each step.
- **Cashier's Algorithm:**
  - **Task:** Given a set of coin values find for an amount of any n cents the least total number of coins that adds up to n.
  - **Greedy Approach:** At each step choose the coin with the largest possible value that does not exceed the amount left.
  - **Theorem:** Cashier's Algorithm for U.S. coins (1, 5, 10, 25) leads to an optimal solution.

Matching:

- Given a finite set A, a **matching** of A is a set of (unordered) pairs of distinct elements of A where any element occurs in at most one pair (such pairs are called independent).
- A **maximum matching** is a matching that contains the largest possible number of independent pairs.
- A **preference list** L_x defines for every element $x \in A$ the order in which the element prefers to be paired with another element. x prefers y over z if y precedes z on L_x.
- A matching is **unstable** if there are two pairs (x, y), (v, w) in the matching such that x prefers v to y and v prefers x to w.
- A **stable matching** is a matching that is not unstable.
- **The marriage problem:** Find a **maximum stable matching** for $A_1 \cup A_2 = A$ with A_1 and A_2 being two disjoint subsets such that $|A_1| = |A_2|$, and pairs can only consist of one element of A_1 and A_2 each.

Gale-Shapley Algorithm

$M = \emptyset$
while $|M| < |A_1|$ **do**
  Select an unpaired $x \in A_1$
  Let x propose to the first element $y \in A_2$ on L_x
  if y is unpaired **then**
    add the pair (x, y) to M
  else
    Let $x' \in A_1$ be the element that y is paired to, (i.e., $(x', y) \in M$)
    if x' precedes x on L_y **then**
      remove y from L_x
    else
      Replace $(x', y) \in M$ by (x, y) and remove y from $L_{x'}$
    end if
  end if
end while
return M

Complexity

A few log formulas. If the base of the log is not specified, you can assume it is 2:

- $\log(a \cdot b) = \log(a) + \log(b)$
- $\log(a^n) = n \log(a)$
- $a^{\log_a(n)} = n$
- $\log_a(n) = \frac{\log_b(n)}{\log_b(a)}$

Big-O Notation:

- Let f and g be functions from the set of integers (or real numbers) to the set of real numbers. We say that $f(x)$ is $O(g(x))$, if there are constants C and k, with C positive, such that: $\forall x > k, |f(x)| \leq C|g(x)|$
- n^c is $O(n^d)$, but n^d is not $O(n^c)$ for $d > c > 1$
- $(\log_b(n))^c$ is $O(n^d)$, but n^d is not $O((\log_b(n))^c)$ for $b > 1, c, d > 0$
- n^d is $O(b^n)$, but b^n is not $O(n^d)$ for $d > 0, b > 1$
- b^n is $O(c^n)$, but c^n is not $O(b^n)$ for $c > b > 1$
- c^n is $O(n!)$, but $n!$ is not $O(c^n)$ for $c > 1$
- **Theorem:** Suppose that $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$. Then $(f_1 + f_2)(x)$ is $O(g(x))$, where $g(x) = \max(|g_1(x)|, |g_2(x)|)$.
- **Theorem:** Suppose that $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$. Then $(f_1 \cdot f_2)(x)$ is $O(g_1(x) \cdot g_2(x))$.
- **Theorem:** Suppose that $f(x)$ is $O(g(x))$ and $g(x)$ is $O(h(x))$. Then $f(x)$ is $O(h(x))$.
- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \cdots a_n$ are real number with $a_n \neq 0$, then: $f(x)$ is $O(x^n)$

Big-Omega Notation:

- Let f and g be functions from the set of integers (or real numbers) to the set of real numbers. We say that $f(x)$ is $\Omega(g(x))$, if there are constants C and k, with C positive, such that: $\forall x > k, |f(x)| \geq C|g(x)|$
- $f(x)$ is $\Omega(g(x))$ if and only if $g(x)$ is $O(f(x))$

Big-Theta Notation:

- Let f and g be functions from the set of integers (or real numbers) to the set of real numbers. We say that $f(x)$ is $\Theta(g(x))$, if $f(x)$ is $O(g(x))$ and $f(x)$ is $\Omega(g(x))$
- $f(x)$ is $\Theta(g(x))$ if and only if there exist positive constants C_1, C_2 and k such that: $\forall x > k, C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|$
- When $f(x)$ is $\Theta(g(x))$, then also $g(x)$ is $\Theta(f(x))$

Little-o Notation:

- $f(x)$ is $o(g(x))$, if $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0$
- if $f(x)$ is $o(g(x))$, then $f(x)$ is $O(g(x))$

Worst-case Time Complexity:

- The **worst-case time complexity** of an algorithm provides an upper bound on the number of operations an algorithm uses to solve a problem with input of a particular size. In the following, n is the size of the array/list
  - Linear Search: $\Theta(n)$
  - Binary Search: $\Theta(\log_2(n))$
  - Bubble Sort: $\Theta(n^2)$
  - Insertion Sort: $\Theta(n^2)$
  - Selection Sort: $\Theta(n^2)$

Induction and Recursion

Mathematical induction:

- To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:
  1. **Basis Step:** Show that $P(1)$ is true.
  2. **Inductive Step:** Show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

Strong induction:

- To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:
  1. **Basis Step:** Show that $P(1)$ is true.
  2. **Inductive Step:** Show that $[P(1) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers k.

Recursively Defined Functions:

- A recursive or inductive definition of a function f with the set of nonnegative integers as its domain consists of two steps:
  1. **Basis Step:** Specify the value of f at 0.
  2. **Recursive Step:** Give a rule for finding its value at an integer from its values at smaller integers.

Recursively Defined Sets and Structures:

- Recursive definitions of sets have two parts:
  1. **Basis Step:** Specify an initial collection of elements.
  2. **Recursive Step:** Give the rules for forming new elements in the set from those already known to be in the set.

Structural Induction:

- To prove a property of the elements of a recursively defined set, we use structural induction.
  1. **Basis Step:** Show that the result holds for all elements specified in the basis step of the recursive definition to be in the set.
  2. **Recursive Step:** Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

Recursive Algorithms:

- An algorithm is called recursive if it solves a problem by reducing it to an instance of the same problem with smaller input.
- For the algorithm to terminate, the instance of the problem must eventually be reduced to some initial case for which the solution is known.

recursive_factorial(n: integer)

```
if n = 0 then
   return 1
else
   return n*recursive_factorial(n-1)
end if
```

recursive_multiplication(n: integer, x : real number)

```
if n = 0 then
   return 0
else
   return x + recursive_multiplication(n-1, x)
end if
```

Divide and Conquer:

- Strategy for solving a problem of size n:

1. **Divide:**
   - if $n > 1$: divide the problem of size n into 2 (almost) equally sized subproblems
   - else: solve the problem of size 1 directly
2. **Conquer:** Solve the sub-problems in the same way (recursively).
3. **Merge:** Merge the sub-solutions into an overall solution.

binary_search(x, l, r: integers)

```
if l > r then
  return -1
else
  m = ⌊(l + r)/2⌋
  if x < a_m then
    binary_search(x, l, m − 1)
  else if x > a_m then
    binary_search(x, m + 1, r)
  else
    return m
  end if
end if
```

mergesort($L = a_1, a_2, \cdots a_n$: integers/reals list)

```
if n > 1 then
  m = ⌊n/2⌋
  L_1 = a_1, a_2, ··· a_m
  L_2 = a_{m+1}, a_{m+2}, ··· a_n
  L = merge(mergesort(L_1), mergesort(L_2))
end if
```

MergeSort has worst case and best case complexity $O(n \log_2(n))$

Number Theory

Base b expansion of n:

Notation: for a positive integer n and an integer greater or equal than 2 b,

Write $(a_k a_{k-1} \dots a_1 a_0)_b$

When $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$

Constructing a base b expansion

- Find k by computing successive powers of b until you find the smallest k such that $b^k \leq n < b^{k+1}$
- For each value of i from 0 to k
  - Set a_{k-i} to be the largest number between 0 and b - 1 for which $a_{k-i} b_{k-i} \leq n$.
  - Update remaining value: $n = n - a_{k-i} b_{k-i}$

Division

- If a and b are integers with $a \neq 0$, then a divides b if there exists an integer c such that $b = ac$
- The notation $a|b$ denotes that a divides b.
- The notation $a \nmid b$ denotes that a does not divide b.
- **Theorem:** If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$. $q = a$ **div** d is called the **quotient** and $r = a$ **mod** d is called the **remainder**.

base_b_expansion(n, b: positive integers with $b > 1$)

```
q = n
k = 0
while q ≠ 0 do
  a_k = q mod b
  q = q div b
  k = k + 1
end while
return a_k, a_{k-1}, ..., a_1, a_0
```

Counting

The Product Rule:

The number of sequences $(s_1, s_2, \ldots, s_n)$ such that there are a_i choices for s_i after having chosen $s_1, s_2, \ldots, s_{i-1}$ for each $i = 1, 2, \ldots n$ is exactly $a_1 \cdot a_2 \cdot \cdots \cdot a_n$.

The Sum Rule:

If $S_1, S_2, \ldots, S_n$ are finite disjoint sets, then $|\bigcup_{i=1}^{n} S_i| = |S_1| + |S_2| + \cdots + |S_n|$

Combinations ans Permutations With and Without Repetition.			
Type	***Repetition Allowed ?***	***Ordered ?***	***Formula***
r-permutation	No	Yes	$P(n,r) = \frac{n!}{(n-r)!}$
r-combinations	No	No	$C(n,r) = \frac{n!}{r!(n-r)!}$
r-permutation	Yes	Yes	n^r
r-combinations	Yes	No	$C(n+r-1,r) = \frac{(n+r-1)!}{r!(n-1)!}$

Permutations with Indistinguishable Objects:

The number of different permutations of n objects, where there are n_1 indistinguishable objects of type 1, n_2 indistinguishable objects of type 2, ..., and n_k indistinguishable objects of type k, such that $n_1 + n_2 + \cdots + n_k = n$ is: $\frac{n!}{n_1!n_2!\cdots n_k!} = C(n, n_1) \cdot C(n - n_1, n_2) \cdots C(n - n_1 - \cdots - n_{k-1}, n_k)$

The Pigeonhole Principle:

If k is a positive integer and $k + 1$ objects are placed into k boxes, then at least one box contains two or more objects.

The Generalized Pigeonhole Principle:

If N objects are placed into k boxes, then at least one box contains at least $\lceil N/k \rceil$ objects.

Binomial Theorem:

Let x and y be variables, and n a nonnegative integer. Then: $(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$

Pascal's Identity:

If n and k are integers with $n \leq k \leq 0$, then: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Linear Homogeneous Recurrence Relations:

- A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form: $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$, where $c_k \neq 0$

Characteristic Equation:

- The characteristic equation of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ is: $r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$

Solving Linear Homogeneous Recurrence Relations of Degree 2:

- Let c_1 and c_2 be real numbers. Suppose that the characteristic equation $r^2 - c_1 r - c_2 = 0$ has two **distinct** roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n = 0,1,2, \ldots$, where α_1 and α_2 are constants.
- Let c_1 and c_2 be real numbers with $c_2 \neq 0$. Suppose that the characteristic equation $r^2 - c_1 r - c_2 = 0$ has **only one** root r_0. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, if and only if $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$ for $n = 0,1,2, \ldots$, where α_1 and α_2 are constants.

Solving Linear Homogeneous Recurrence Relations of Degree k:

- Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that the characteristic equation $r^k - c_1 r^{k-1} - \cdots - c_k = 0$ has t **distinct** roots $r_1, r_2, \ldots, r_t$ with multiplicities $m_1, m_2, \ldots, m_t$, respectively so that $m_i \geq 1$ for $i = 0,1,2, \ldots, t$ and $m_1 + m_2 + \cdots + m_t = k$. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$, if and only if

$$\begin{aligned} a_n = {} & (\alpha_{1,0} + \alpha_{1,1} n + \alpha_{1,2} n^2 + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n \\ & + (\alpha_{2,0} + \alpha_{2,1} n + \alpha_{2,2} n^2 + \cdots + \alpha_{2,m_2-1} n^{m_2-1}) r_2^n \\ & \cdots \\ & + (\alpha_{t,0} + \alpha_{t,1} n + \alpha_{t,2} n^2 + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n \end{aligned}$$

  for $n = 0,1,2, \ldots$, where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_i - 1$.

Generating Functions:

- The generating function for the infinite sequence $a_0, a_1, \ldots, a_k, \ldots$ is the infinite series

$$G(x) = a_0 + a_1 x + \cdots + a_k x^k + \cdots = \sum_{k=0}^{\infty} a_k x^k$$

- Let $\mathcal{A}$ be a class of objects to be enumerated (counted). We call $A(x)$ the generating function of this class: $A(x) = \sum_{k=0}^{\infty} a_k x^k$, where a_k is the number of objects in $\mathcal{A}$ that have size k.
- Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$, then

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

$$f(x) \cdot g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k$$

Extended Binomial Coefficient:

- Let u be a real number and k a nonnegative integer. Then the extended binomial coefficient $\binom{u}{k}$ is defined as

$$\binom{u}{k} = \begin{cases} \frac{u(u-1)\cdots(u-k+1)}{k!} & \text{if k>0} \\ 1 & \text{if k=0} \end{cases}$$

Extended Binomial Theorem:

Let x be real number with $|x| < 1$ and let u be a real number. Then: $(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k$

The principle of Inclusion-Exclusion:

Let $A_1, A_2, \ldots, A_n$ be finite sets. Then:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < k \le n}^{n} |A_i \cap A_k| + \sum_{1 \le i < k < j \le n}^{n} |A_i \cap A_k \cap A_j| - \cdots + (-1)^{n+1} \left| \bigcap_{i=1}^{n} A_i \right|$$

Derangements:

A **derangement** is a permutation of objects that leaves no object in the original position.

The number of derangements of a set with n elements is

$$D_n = n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right]$$

Useful Generating Functions.

$G(x) = (1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$	$G(x) = (1+ax)^n = \sum_{k=0}^{n} \binom{n}{k} a^k x^k$
$G(x) = (1+x^r)^n = \sum_{k=0}^{n} \binom{n}{k} x^{rk}$	$G(x) = \frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k$
$G(x) = \frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$	$G(x) = \frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k$
$G(x) = \frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk}$	$G(x) = \frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1) x^k$
$G(x) = \frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k$	$G(x) = \frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} (-1)^k x^k$
$G(x) = \frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} a^k x^k$	$G(x) = e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$
$G(x) = \ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k$	

Probabilities

Definition (Laplace):

If S is a finite sample space of equally likely outcomes, and E is an event, that is, a subset of S, then the probability of E is: $p(E) = \frac{|E|}{|S|}$

Probability of Complements of Events:

Let E be an event in sample space S. The probability of the event $\overline{E} = S - E$, the complementary event of E, is given by: $p(\overline{E}) = 1 - p(E)$

Probability of Unions of Events:

Let E_1 and E_2 be events in the sample space S. Then: $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$

Probability Distribution:

Let S be a sample space of an experiment with a finite or countable number of outcomes. We assign a probability $p(s)$ to each outcome $s \in S$, so that

1. $0 \leq p(s) \leq 1$ for each $s \in S$
2. $\sum_{s \in S} p(s) = 1$

The function p from the set of all outcomes of the sample space S is called a **probability distribution**.

Uniform Distribution:

Suppose that S is a set with n elements. The **uniform distribution** assigns the probability $\frac{1}{n}$ to each element of S.

Probability of an Event:

The probability of the event E is the sum of the probabilities of the outcomes in E: $p(E) = \sum_{s \in E} p(s)$

Combination of disjoint events:

If $E_1, E_2, ...$ is a sequence of **pairwise disjoint** events in a sample space S, then: $p\left(\bigcup_i E_i\right) = \sum_i p(E_i)$

Conditional Probability:

Let E and F be events with $p(F) > 0$. The **conditional probability** of E given F, denoted by $p(E|F)$, is defined as: $p(E|F) = \frac{p(E \cap F)}{p(F)}$

Independence:

- The events E and F are **independent** if and only if $p(E \cap F) = p(E)p(F)$
- If E and F are **independent**, then $p(E|F) = p(E)$

Pairwise and Mutual Independence:

- The events $E_1, E_2, ... E_n$ are **pairwise independent** if and only if $p(E_i \cap E_j) = p(E_i)p(E_j)$ for all pairs i and j with $i \leq j \leq n$
- These events are **mutually independent** if $p(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_m}) = p(E_{i_1}) \cdot p(E_{i_2}) \cdots p(E_{i_m})$ whenever $i_j, j = 1, 2, \ldots, m$ are integers with $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ and $m \geq 2$.
- Mutual independence implies pairwise independence

Bernoulli Trials:

- Given an experiment that can have only **two** possible outcomes.

Each performance of the experiment is called a **Bernoulli trial**.

One outcome is called a **success** and the other a **failure**.

If p is the probability of success and q the probability of failure, then $p + q = 1$.

- The probability of exactly k successes in n independent Bernoulli trials, with probability of success p and probability of failure $q = 1 - p$ is: $C(n, k) \cdot p^k \cdot q^{n-k}$.

Binomial Distribution:

- We denote by $b(k : n, p)$ the probability of k successes in n independent Bernoulli trials with p the probability of success. Viewed as a function of k, $b(k : n, p)$ is the **Binomial Distribution**: $b(k : n, p) = C(n, k) \cdot p^k \cdot q^{n-k}$

Bayes' Theorem:

- Suppose that E and F are events from a sample space S such that $P(E) \neq 0$ and $P(F) \neq 0$. Then:

$$p(F|E) = \frac{p(E|F)p(F)}{p(E)} = \frac{p(E|F)p(F)}{p(E|F)p(F) + p(E|\overline{F})p(\overline{F})}$$

Generalized Bayes' Theorem:

- Suppose that E is an event from a sample space S and that $F_1, F_2, \ldots, F_n$ are mutually exclusive events such that $\bigcup_{i=1}^{n} F_i = S$. Assume that $P(E) \neq 0$ and $P(F_i) \neq 0$ for $i = 1, \cdots, n$. Then:

$$p(F_j|E) = \frac{p(E|F_j)p(F_j)}{p(E)} = \frac{p(E|F_j)p(F_j)}{\sum_{i=1}^{n} p(E|F_i)p(F_i)}$$

Random Variable:

- A random variable X is a function $X : S \to R$ from the sample space S of an experiment to the set of real numbers R.
- The **distribution** of a random variable X on a sample space S is the set of pairs $(r, p(X = r))$ for all $r \in X(s)$ where $p(X = r)$ is the probability that X takes the value r: $p(X = r) = \sum_{s \in S | X(s) = r} p(s)$

Probability Mass Function:

If the range of the function X is countable, then $p(X = r)$ can be interpreted as a function $p : X(S) \to R$. This function is called **probability mass function** and it is a probability distribution over the sample space $X(S)$.

Expected Value:

- The **expected value** of the random variable X on the sample space S is equal to:

$$E(X) = \sum_{s \in S} p(s)X(s)$$

- Let X denote the number of successes, when n mutually independent **Bernoulli trials** are performed, where p is the probability of each trial. Then the **expected value** of X is np.
- If $X_i, i = 1, \ldots, n$ with n a positive integer, are random variables on S, and if a and b are real numbers, then:
  1. $E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$
  2. $E(aX + b) = aE(X) + b$
- Law of the Unconscious Statistician: $E(g(X)) = \sum_{x \in X(S)} g(x)p(X = x)$

Variance:

– Let X be a random variable on the sample space S. The **variance** of X, denoted by $V(X)$ is:

$$V(X) = \sum_{s \in S} (X(s) - E(X))^2 \cdot p(s)$$

– The **standard deviation** of X, denoted by $\sigma(X)$ is defined as $\sqrt{V(X)}$.
– If X is a random variable on a sample space S, then $V(X) = E(X^2) - E(X)^2$:
– If X is a random variable on a sample space S, and $E(X) = \mu$, then $V(X) = E\left((X - \mu)^2\right)$

Independent Random Variables:

– The random variables X and Y on a sample space S are independent if

$$p(X_1 = r_1 \wedge Y = r_2) = p(x = r_1) \cdot p(Y = r_2)$$

– If X and Y are independent random variables on sample space S, then:
  1. $E(X \cdot Y) = E(X) \cdot E(Y)$
  2. $V(X + Y) = V(X) + V(Y)$
– If $X_1, X_2, \ldots, X_n$ are pairwise independent random variables on S, then
  1. $V(X_1 + X_2 + \cdots + X_n) = V(X_1) + V(X_2) + \cdots + V(X_n)$

Chebyshev's Inequality:

– Let X be a random variable on a sample space S with probability function p. If r is a positive real number, then :

$$p(|X(s) - E(X)| \geq r) \leq V(X)/r^2$$