CS40 Notes: Foundations of Computer Science

Alex Mei

Winter, 2020

1 Proofs and Logic

1.1 Propositional Logic

Truth Value: the value true or false
Proposition: statements that declares a fact that is either true or false
Atomic Proposition: a single proposition which cannot be broken down into simpler statements
Compound Proposition: a proposition formed by atomic propositions and logical operators

Logical Connectives

Negation: a unary operator ($\neg$) that negates the truth value
Conjunction: a binary operator ($\wedge$) that evaluates to true only when both propositions are true
Disjunction: a binary operator ($\vee$) that evaluates to true only when at least one propositions is true (also known as an **inclusive or**).
Exclusive Or: a binary operator ($\oplus$) that evaluates to true only when one proposition is true and not the other
Implication: a binary operator ($\rightarrow$) for propositions p and q such that p implies q (also known as a **conditional statement**) *Note: implication doesn't imply causation*

Ways of Stating Implications ($p \rightarrow q$):

if p, then q	p implies q
if p, q	p only if q
p is sufficient for q	a sufficient condition for q is p
q if p	q whenever p
q when p	q is necessary for p
a necessary condition for p is q	q follows them p
q unless $\neg$ p	

Biconditional: a binary operator ($\leftrightarrow$) for propositions p and q such that p if and only if q

Ways of Stating Biconditionals ($p \leftrightarrow q$):

p is necessary and sufficient for q
if p, then q, and conversely
p if and only if (iff) q

Truth Table: a table that displays all possible truth values for a proposition

$\neg$ P	P	Q	P $\wedge$ Q	P $\vee$ Q	P $\oplus$ Q	P $\rightarrow$ Q	P $\leftrightarrow$ Q
F	T	T	T	T	F	T	T
F	T	F	F	T	T	F	F
T	F	T	F	T	T	T	F
T	F	F	F	F	F	T	T

Converse: If p $\rightarrow$ q, then the converse statement is q $\rightarrow$ p
Contrapositive: If p $\rightarrow$ q, then the contrapositive statement is $\neg$ q $\rightarrow$ $\neg$ p
Inverse: If p $\rightarrow$ q, then the inverse statement is $\neg$ p $\rightarrow$ $\neg$ q

P	Q	P $\rightarrow$ Q	$\neg$ Q $\rightarrow$ $\neg$ P	Q $\rightarrow$ P	$\neg$ P $\rightarrow$ $\neg$ Q
T	T	T	T	T	T
T	F	F	F	T	T
F	T	T	T	F	F
F	F	T	T	T	T

Logical Equivalence: compound propositions with the same truth values are equivalent ($\equiv$)

$$Thus,\ P \rightarrow\ Q \equiv \neg\, Q \rightarrow \neg\, P.\ Also,\ Q \rightarrow\ P \equiv \neg\, P \rightarrow \neg\, Q.$$

1.2 Propositional Equivalences

Contingency: a compound proposition that is neither a tautology or a contradiction
Tautology: a compound proposition that is always true regardless of the truth values of the propositional variables (tautologies are logical equivalences)
Contradiction: a compound proposition that is always false regardless of the truth values of the propositional variables; such proposition is said to be **unsatisfiable**
Satisfiable Proposition: if any values of the proposition variables makes a compound proposition true then it satisfiable (the particular assignment of variables is said to be a **solution**)
Consistent: a set of propositions satisfied by same truth values for their atomic propositions
Logic Gate: a circuit which receives a set of input signals and outputs a true or false; there exists an inverter (negation) denoted by a triangle and a circle, an 'and' gate denoted by a bullet, and an 'or' gate denoted by half a cylinder

Bitstrings: strings of bits which operations are performed upon; (i.e., the negation of 0110 is 1001)
Fundamental Conjunctions: a conjunction of all the atomic propositions and their negation
Disjunctive Normal Form: a disjunction of the fundamental conjunctions

Logical Equivalence Laws:

Identity Laws:

$$P \wedge T \equiv P$$

$$P \vee F \equiv P$$

Domination Laws:

$$P \vee T \equiv T$$

$$P \wedge F \equiv F$$

Idempotent Laws:

$$P \vee P \equiv P$$

$$P \wedge P \equiv P$$

Commutative Laws:

$$P \vee Q \equiv Q \vee P$$

$$P \wedge Q \equiv Q \wedge P$$

Associative Laws:

$$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$$

Distributive Laws:

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

De Morgan's Laws:

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$$

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$$

Absorption Laws:

$$P \vee (P \wedge Q) \equiv P$$

$$P \wedge (P \vee Q) \equiv P$$

Negation Laws:

$$P \vee \neg P \equiv T$$

$$P \wedge \neg P \equiv F$$

Double Negation Law:

$$\neg(\neg P) \equiv P$$

1.3 Predicate Logic (Calculus)

Predicate: a property of the subject; also known as an **open sentence**
Propositional Function: a function with regards to a variable; when that variable is assigned a value, the function becomes a proposition with a truth value
Quantification: expresses to what extent a predicate is true
Domain: also known as the **domain of discourse** or **universal discourse**, range of values for a variable which makes a proposition true
Universal Quantification: P(x) is true for all values of x in the domain; evaluates to true when P(x) is true for every x in the domain; false when there exists at least 1 counter example
Universal Quantifier: $\forall$
Existential Quantification: There exists an element x in the domain such that P(x) is true
Existential Quantifier: $\exists$
Uniqueness Quantifier: There exists one unique element x in the domain such that P(x) is true; denoted by $\exists!$
Nested Quantifiers: quantifiers inside the scope of other quantifiers
Bounded Variables: A variable is bound if a quantifier is used on it
Free Variables: A variable is free if it isn't bound by a quantifier or set equal to a particular value
Scope: The part of a logical expression a quantifier is applied; a variable is free if it isn't in the scope of any quantifiers
Contingent: A statement is contingent if it must evaluate to true or false but depends on a variable.
Logical Equivalence of Predicates and Quantifiers: Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value regardless of which predicates are substituted into these statements and which domain of discourse is used for these variables.
DeMorgan's Laws of Quantifiers:

$$\neg\exists x P(x) \equiv \forall x \neg P(x)$$

$$\neg\forall x P(x) \equiv \exists x \neg P(x)$$

1.4 Rules of Inference

Argument: a series of propositions that result in a conclusion
Valid: the conclusion logically follows from the truths of the premises
True Conclusion: also known as a **sound argument**, a conclusion formed by a valid argument given that the premises are true
Clause: a disjunction of variables (and their negations)
Modus Ponens:

$$(P \land (P \to Q)) \to Q$$

Modus Tollens:

$$(\neg Q \land (P \to Q)) \to \neg P$$

Hypothetical Syllogism:

$$((P \to Q) \land (Q \to R)) \to (P \to R)$$

Disjunctive Syllogism:

$$((P \lor Q) \land \neg P) \to Q$$

Addition:

$$P \to (P \lor Q)$$

Simplification:

$$(P \land Q) \to P$$

Conjunction:

$$((P) \land (Q)) \to (P \land Q)$$

Resolution:

$$((P \lor Q) \land (\neg P \lor R)) \to (Q \lor R)$$

Universal Modus Ponens: $\forall$x (P(x) $\to$ Q(x)), P(a) where a is a particular element in the domain; $\therefore$ Q(a)
Universal Modus Tollens: $\forall$x (P(x) $\to$ Q(x)), $\neg$ Q(a) where a is a particular element in the domain; $\therefore$ $\neg$ P(a)

Fallacies

Fallacies: common forms of incorrect reasoning that lead to invalid arguments
Affirming the Conclusion: (Q $\land$ (P $\to$ Q)) $\to$ P
Denying the Hypothesis: ($\neg$ P $\land$ (P $\to$ Q)) $\to$ $\neg$ Q
Begging the Question: a statement is proved by using itself (or a statement equivalent to it), also known as **circular reasoning**

1.5 Proofs

Informal Proofs: a proof that combines the rules of inference in a single step, skips steps, assumes axioms, or not explicitly state the rules of inference
Theorem: statement (that is important) that can be shown to be true; less important statements that can be shown to be true is known as a **fact**
Corollary: a theorem that can be established from a theorem that has been proved
Lemma: a less important theorem (used as intermediary steps in a proof)
Conjecture: a statement that is proposed to be a true statement on the basis of partial evidence; when proved, it becomes a theorem
Proof: a valid argument that establishes the truth of a theorem
Axiom: also known as a **postulate**, a statement assumed to be true that do not require definition
Even Integer: an integer n is even when there exists an integer k such that $n = 2k$
Odd Integer: an integer n is odd when there exists an integer k such that $n = 2k + 1$
Rational Real Number: there exists integers p and q such that $q \neq 0$ and $r = p/q$ where r is real
Parity: two integers have the same parity when they are both even or odd; they have opposite parity when one is even and the other is odd
Indirect Proof: proofs that do not start with the premises and end with the conclusion **Counterexample:** a single x for which P(x) is false to show that $\forall x\ P(x)$ is false

1.6 Proof Methods

Direct Proof: a proof of the conditional $P \rightarrow Q$ (for all x in the domain) where the first step is the assumption that P is true; subsequent steps come from the rules of inference, with the final conclusion showing that Q must also be true (shows that the combination P = T and Q = F never occurs)
Proof by Contraposition: since an implication and its contrapositive are logically equivalent, a proof to show that the contrapositive must be true shows that the implication must also be true; the proof by contraposition of $P \rightarrow Q$ starts with the premise $\neg Q$, and using the rules of inference, shows that $\neg P$ must follow
Vacuous Proof: a proof to show that P is false, since if P is false, $P \rightarrow Q$ must be true
Trivial Proof: a proof to show that Q is true, since if Q is true, $P \rightarrow Q$ must be true
Proof by Contradiction: a proof to show that $\neg P \rightarrow (R \wedge \neg R)$ because then, P must evaluate to true; for proofs by contradiction involving conditional statements, assume the P and $\neg Q$ are true; then, if $\neg Q$ results in $\neg P$ is true by rules of inference, there is a contradiction since $P \wedge \neg P$ cannot be both true
Proofs of Equivalence: A theorem in the form $P \leftrightarrow Q$ can be proved by showing that both $P \rightarrow Q$ and $Q \rightarrow P$ are true since $(P \leftrightarrow Q) \leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$; this can also be used to show equivalent statements since if $P \equiv Q$, $P \leftrightarrow Q$

Proof by Cases: a proposition P can be split into cases such that $(P_1 \vee P_2 \vee ... \ P_N) \rightarrow Q$ since it has a logical equivalence of $((P_1 \rightarrow Q \wedge (P_2 \rightarrow Q) \wedge ... \ (P_N \rightarrow Q))$ and each case of the proposition can be proved individually
Exhaustive Proofs: proving every possibility is true
Without Loss of Generality: completing a different case using the exact same argument
Existence Proof: a proof such that there $\exists x \ P(x)$
Constructive Existence Proof: a proof where an element a, called a **witness**, is found such that P(a) is true
Nonconstructive Existence Proof: a proof to prove the existence in a manner other than finding a witness
Uniqueness Proof: a proof showing both the existence of an element x with the desired property, and that when $y \neq x$, y does not have the desired property (or x and y are equivalent)
Fermat's Last Theorem: $x^n + y^n + z^n$ has no integer solutions x, y, z with $xyz \neq 0$ whenever n is an integer with $n > 2$

Order of Precedence:

$\forall, \exists, \exists!$
$\neg$
$\wedge$
$\vee$
$\rightarrow$
$\leftrightarrow$

2 Set Theory

2.1 Sets

Set: an unordered collection of unique objects called **elements** or **members** denoted by { ... }
Member Notation: a member a in set S is denoted by $a \in S$
Roster Method: describing a set S by listing all the elements denoted by S = {...}
Set Builder Method: describing a set by listing all the properties it must satisfy denoted by S = { generic element | conditions need to be satisfied }
Closed Interval: [a, b] denotes $\{ x \mid a \leq x \leq b \}$
Open Interval: (a, b) denotes $\{ x \mid a < x < b \}$
Equal Sets: two sets A and B are equal if and only if $\forall x \ (x \in A \leftrightarrow x \in B)$; if $A \subseteq B$ and $B \subseteq A$, then A = B
Empty Sets: also known as a **null set**, an empty set has no elements denoted by $\emptyset$

Singleton Set: an element with a single set
Universal Set: denoted by the letter U, this set contains all the elements under consideration represented by a rectangle in a Venn Diagram
Cardinality: if there are exactly n distinct elements of set S, then the cardinality of the **finite** set S is n, denoted by $| S | = n$
Power Set: given the set S, the power set of S denoted by $\mathcal{P}(S)$ is the set of all the subsets of S
Ordered n-Tuple: an ordered collection (a_1, a_2, ..., a_n) where a_1 is the first element, a_2 is the second element, ..., and a_n is the nth element
Equal Ordered Tuples: two ordered tuples are equal if $a_i = b_i$ for elements $i = 1$ to $i = n$
Cartesian Product: the cartesian product of sets A and B is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$: $A \times B = \{(a, b) \mid a \in A \land b \in b\}$
Set Notation and Quantifiers: $\forall x\ S(P(x))$ denotes P(x) for all elements x in the set S
Truth Set: the truth set of a predicate P(x) for a domain D is the set of elements in D such that P(x) is true: $\{x \in D \mid P(x)\}$

Common Infinite Sets

N: Natural Numbers: {0, 1, 2, 3, ...}
Z: Integers: {..., -2, -1, 0, 1, 2, ...}
Z^+: Positive Integers: {1, 2, 3, ...}
Q: Rational Numbers: $\{a / b \mid a, b \in Z, b \neq 0\}$
Q^+: Positive Rational Numbers: $\{a / b \mid a, b \in Z, a \geq 0, b > 0\}$
R: Real Numbers

2.2 Subsets

Subset: The set A is a subset of B, denoted by $A \subseteq B$, if and only if every element in A is in B
Proper Subset: The set A is a proper subset of B, denoted by $A \subset B$, if $A \subseteq B$ and there exists an element in B that isn't in A: $\forall x\ (x \in A \rightarrow x \in B) \land \exists x\ (x \in B \rightarrow x \notin A)$
Subset Quantification: $A \subseteq B \leftrightarrow \forall x\ (x \in A \rightarrow x \in B)$
Note: to show that $A \nsubseteq B$, find a single element $x \in A$ such that $x \notin A$
Subset Theorem: Given a nonempty set S, the set S is guaranteed to contain at least 2 subsets, $\emptyset \subseteq S$ and $S \subseteq S$

2.3 Set Operations

Union: The union of two sets A and B, denoted by A ∪ B is the set that contains the elements in A, B, or both.

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Generalized Union: The union of a collections of sets is the set that contains all elements that are in at least one set of the collection.

$$A_1 \cup A_2 \cup ...A_n = \bigcup_{i=1}^{n} A_i$$

Intersection: The intersection of two sets A and B, denoted by A ∩ B is the set that contains the elements in both A and B.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Generalized Intersection: The intersection of a collections of sets is the set that contains all elements that are in every set of the collection.

$$A_1 \cap A_2 \cap ...A_n = \bigcap_{i=1}^{n} A_i$$

Disjoint: Two sets A and B are considered disjoint if their intersection is the empty set.

$$A \cap B = \emptyset$$

Inclusion Exclusion Principle (for two sets): The cardinality of the union of sets A and B is the sum of the cardinalities of sets A and B minus the cardinality of the intersection of sets A and B.

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

Difference: The difference of sets A and B, denoted by A - B or A \B, is the set containing elements in A and not B, also known as the complement of B with respect to A.

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Complement: The complement of the set A, denoted by $\overline{A}$ or $A^{\complement}$, is the complement of A with respect to U (the universal set.)

$$\overline{A} = \{x \in U \mid x \notin A\}$$

Membership Table: a truth table for sets where all combinations of each element is listed (1 denoting the element is in the set and 0 denoting they aren't)

Set Identities

Identity Laws:

$$A \cap U = A$$

$$A \cup \emptyset = A$$

Domination Laws:

$$A \cup U = U$$

$$A \cap \emptyset = \emptyset$$

Idempotent Laws:

$$A \cup A = A$$

$$A \cap A = A$$

Complementation Law:

$$\overline{(\overline{A})} = A$$

Commutative Laws:

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

Associative Laws:

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

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

Distributive Laws:

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

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

De Morgan's Laws:

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

De Morgan's Laws, Generalized:

$$\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$$

$$\overline{\bigcap_{i=1}^{n} A_i} = \bigcup_{i=1}^{n} \overline{A_i}$$

Absorption Laws:

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

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

Complement Laws:

$$A \cup \overline{A} = U$$

$$A \cap \overline{A} = \emptyset$$

2.4 Functions

Function: A function, also known as a **mapping** or **transformation**, f from set A to set B is an assignment of one unique element of B to each element of A, denoted by f : A $\rightarrow$ B (f maps A to B) where f(a) = b and a $\in$ A and b $\in$ B.
Domain: A is the domain of f : A $\rightarrow$ B.
Codomain: B is the codomain of f : A $\rightarrow$ B.
Image: If f(a) = b, then b is the image of a.
Preimage: If f(a) = b, then a is the preimage of b.
Range: Also known as the **image**, the range is the set of all images of the elements of A.
Equal Functions: Two functions are equal when they have the same domain, codomain, and map each element of their common domain to the same element in their common codomain.
Real-Valued Function: A function with the set of all real numbers (**R**) as its codomain.
Integer-Valued Function: A function with the set of all integers (**Z**) as its codomain.
Sum of Functions: The sum of functions f_1 and f_2 from A to **R** can be expressed as:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

Product of Functions: The product of functions f_1 and f_2 from A to **R** can be expressed as:

$$(f_1 f_2)(x) = f_1(x) f_2(x)$$

One-to-One Function: A function is said to be one-to-one, or an **injunction**, if and only if f(a) = f(b) implies that a = b for all a and b in the domain of f.

$$\forall a \forall b (a \neq b \rightarrow f(a) \neq f(b))$$

Note: to prove an injective function, show if f(x) = f(y) for any x, y $\in$ A with x $\neq$ y, then x = y.
Note: to prove a non-injective function, find particular elements x, y $\in$ A with x $\neq$ y and f(x) = f(y).

Increasing Function: A function f whose domain and codomain are subset of the set of all real numbers is said to be increasing if f(x) $\leq$ f(y) whenever x $<$ y and x and y are in the domain of f.

$$\forall x \forall y (x < y \rightarrow f(x) \leq f(y))$$

Decreasing Function: A function f whose domain and codomain are subset of the set of all real numbers is said to be decreasing if f(x) $\geq$ f(y) whenever x $<$ y and x and y are in the domain of f.

$$\forall x \forall y (x < y \rightarrow f(x) \geq f(y))$$

Strictly: A function is strictly increasing or decreasing if the if a strict inequality is used instead ($>$ or $<$).

Onto Function: A function is called onto, or a **surjection**, if and only if for every element b $\in$ B there is an element a $\in$ A with f(a) = b.

$$\forall b \exists a (f(a) = b)$$

Note: to prove a surjective function, consider any element $y \in B$ and find an element $x \in A$ where $f(x) = y$.

Note: to prove a non-surjective function, find an element $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

One-to-One Correspondence: A function f is a one-to-one correspondence, or a **bijection**, if it is both an injection and a surjection.

Identity Function: A function f : A $\rightarrow$ A is an identity function when f(x) = x for all x $\in$ A.

$$\forall x \in A (f(x) = x)$$

Inverse Function: The inverse function of a function f that is a one-to-one correspondence from set A to set B is the function that assigns an element b $\in$ B and a unique element a $\in$ A such that f(a) = b, denoted by f^{-1}.

Invertible: A function is invertible if the inverse of a function is defined.

Not Invertible: A function is not invertible if it is not a one-to-one correspondence, because the inverse of such function doesn't exist.

Composition: The compositions of functions f : B $\rightarrow$ C and g : A $\rightarrow$ B, denoted by (f $\circ$ g)(a) is defined to be f(g(a)).

Graph: The graph of a function f : A $\rightarrow$ B is the set of ordered pairs: {(a, b) | a $\in$ A and f(a) = b}.

Floor: The floor function assigns the real number x the largest integer less than or equal to x, denoted by $\lfloor x \rfloor$.

Ceiling: The floor function assigns the real number x the smallest integer greater than or equal to x, denoted by $\lceil x \rceil$.

Partial Function: A partial fraction f : A $\rightarrow$ B is an assignment of each element a in a subset of A, called the **domain of definition**, to a unique element b $\in$ B. For elements in A and not the domain of definition of f, f is undefined. When the domain of definition equals A, f is a total function.

Floor and Ceiling Properties

- $\lfloor x \rfloor$ = n iff n $\leq$ x < n + 1
- $\lceil x \rceil$ = n iff n - 1 < x $\leq$ n
- $\lfloor x \rfloor$ = n iff x - 1 < n $\leq$ x
- $\lceil x \rceil$ = n iff x $\leq$ n < x + 1
- x - 1 < $\lfloor x \rfloor$ $\leq$ x $\leq$ $\lceil x \rceil$ < x + 1
- $\lfloor -x \rfloor$ = -$\lceil x \rceil$
- $\lceil -x \rceil$ = -$\lfloor x \rfloor$
- $\lfloor x + n \rfloor$ = $\lfloor x \rfloor$ + n
- $\lceil x + n \rceil$ = $\lceil x \rceil$ + n

2.5 Sequences

Sequence: A function from a subset of the set of integers to the set S where a_n denotes the nth term in the sequence and $\{a_n\}$ denotes the sequence.
Geometric Progression: A sequence with an initial term a and a common ratio r between each term in the sequence: a, ar, ar^2, ..., ar^n, ...
Arithmetic Progression: A sequence with an initial term a and a common difference d between each term in the sequence: a, a + d, a + 2d, ..., a + nd, ...
Recurrance Relation: A recurrance relation for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms in the sequence for term n $\geq$ n_0 where n_0 is a nonnegative integer.
Solution of a Recurrance Relation: A sequence is called a solution of a recurrance relation if its terms satisfy the recurrance relation.
Initial Condition: The terms that precede the first term where the recurrance relation takes effect.
Fibonacci Sequence: A sequence defined by the initial conditions $f_0 = 0$ and $f_1 = 1$, and the recurrance relation $f_n = f_{n-1} + f_{n-2}$.
Closed Formula: An explicit formula for the terms of the sequence.

2.6 Summations

Summation Notation: The sum of the terms a_m, a_{m+1}, ..., a_n can be expressed as:

$$\sum_{j=m}^{n} a_j = \sum_{m \leq j \leq n} a_j$$

where j is the **index of summation**, m is the **lower limit**, and n is the **upper limit**.

Geometic Series: A sum of the terms of a geometric progression. When a and r are real numbers such that $r \neq 0$, the sum can be expressed as:

$$\sum_{j=0}^{n} ar^j = \begin{cases} \dfrac{ar^{n+1} - a}{r - 1} & r \neq 0 \\ (n+1)a & r = 1 \end{cases}$$

Common Summation Formulas

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

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

$$\sum_{k=0}^{\infty} x^k, \mid x \mid < 1 = \frac{1}{1-x}$$

$$\sum_{k=1}^{\infty} kx^{k-1}, \mid x \mid < 1 = \frac{1}{(1-x)^2}$$

2.7 Cardinality of Sets

Equal Cardinality: Sets A and B have the same cardinality if and only if there exists a one-to-one correspondence from A to B.

$$\mid A \mid = \mid B \mid$$

One-to-One Cardinality: If there is a one-to-one function from A to B, the cardinality of A is less than or equal to the cardinality of B.

$$\mid A \mid \leq \mid B \mid$$

Countable: A countable set is a set that is either finite or has the same cardinality as the set of positive integers and is denoted by $\aleph_0$.

Note: a countable union of countable sets is countable
Note: a countably infinite union with countably infinite sets is countably infinite
Uncountable: An uncountable infinite set has greater cardinality as the set of positive integers.
Countability Theorem: If A and B are countable sets, A ∪ B is also countable.
Schroder-Bernstein Theorem: If there are one-to-one functions f : A → B and g : B → A, then there is a one-to-one correspondence between A and B.

$$((|\ A\ |\leq|\ B\ |) \wedge (|\ B\ |\leq|\ A\ |)) \leftrightarrow (|\ A\ |=|\ B\ |)$$

Computable: A function is computable if a computer program can find values of this function. Otherwise, it is **uncomputable**.
Cardinality of Power Sets: The cardinality of the power set of a countably infinite set is the same as the cardinality of the real numbers

3 Number Theory

3.1 Division

Divisible: If a and b are integers where a ≠ 0, then a divides b if there is an integer c such that b = ac (e.g., $\frac{b}{a}$). Also, a divides b means a is a **factor** of b, and b is a **multiple** of a, denoted by a | b.

$$\exists c(b = ac)$$

Divisibility Theorems:

- If a | b and a | c, then a | (b + c)
- If a | b, then a | bc for all integers c
- If a | b and b | c, then a | c
- **Corollary:** If a, b, and c are integers where a ≠ 0 such that a | b and a | c, then a | (mb + nc) whenever m and n are integers

Division Algorithm: Let a and d be integers where d is positive. Then, there are unique integers q and r with 0 ≤ r < d, such that a = dq + r. Also, d is called the **divisor**, a the **dividend**, q the **quotient**, and r the **remainder**.
Div Function: q = a **div** d = $\lfloor a/d \rfloor$
Mod Function: r = a **mod** d = $a - d\lfloor a/d \rfloor$

3.2 Modular Arithmetic

Congruence: If a, b, and m are integers where m is positive, then a is congruent to b modulo m if m divides a - b, denoted by a $\equiv$ b (**mod** m), which is a **congruence** and m is its **modulus**.
Congruence Theorems:

- Let a, b, and m be integers where m is positive. Then a $\equiv$ b (**mod** m) if and only if a **mod** m = b **mod** m.
- Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that a = b + km.
- Let m be a positive integer. If a $\equiv$ b (**mod** m) and c $\equiv$ d (**mod** m), then a + c $\equiv$ b + d (**mod** m) and ac = bd (**mod** m).
- **Corollary:** Let a, b, and m be integers where m is positive. Then, (a + b) **mod** m = ((a **mod** m) + (b **mod** m) **mod** m) and ab **mod** m = ((a **mod** m)(b **mod** m)) **mod** m.

Congruence Class: The set of all integers congruent to an integer a modulo m is the congruence class of a **mod** m.
Z_m: The set of nonnegative integers less than m
Addition Modulo: a $+_m$ b = (a + b) **mod** m
Multiplication Modulo: a $*_m$ b = (a * b) **mod** m
Arithmetic Modulo Properties:

- **Closure:** If a and b belong to Z_m, then a $+_m$ b and a $*_m$ b belong to Z_m
- **Associativity:** If a, b, and c belong to Z_m, then the addition and multiplication modulo is associative.
- **Commutativity:** If a and b belong to Z_m, then the addition and multiplication modulo is associative.
- **Distributivity:** If a and b belong to Z_m, then the addition and multiplication modulo is associative.
- **Identity:** The elements 0 and 1 are the identity elements for addition and multiplication modulo respectively.
- **Additive Inverses:** If a $\neq$ 0 belongs to Z_m, then m - a is an additive inverse of a **mod** m and 0 is its own additive inverse.

Modular Exponent Algorithm: To solve a modular exponent in the form b^n mod m, the following algorithm is used:
a_i = ith digit of the binary representation of n
x = 1
power = b mod m
for i in range[0, k]:
    if a_i = 1, then x = (x * power) mod m
    power = (power * power) mod m
return x

3.3 Integer Representations

Base Expansion Theorem: Let b be an integer greater than 1. Then, if n is a positive integer, it can be expressed uniquely in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b^1 + a_0 b^0$$

Binary: base 2 expansion
Octal: base 8 expansion
Hexadecimal: base 16 expansion (denoted by 0-9, A-F)
Base Conversion: The algorithm for converting from decimal to a different base is as follows.

$$n = bq_0 + a_0$$

$$q_0 = bq_1 + a_1$$

... and continues until q = 0.
Binary, Octal, Hex Conversions: Group digits into blocks (from the right) and convert using a table.

3.4 Prime Numbers:

Prime: An integer p greater than 1 is called prime if the only positive factors of p are 1 and p.
Prime Theorem: There are infinitely many primes.
Prime Number Theorem: The ratio of the number of primes not exceeding x, and x / ln(x) approaches 1 as x grows without bound.
Composite: An positive integer that is greater than 1 and is not prime is called composite.
Fundamental Theorem of Arithemtic: Every integer can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Composite Divisor Theorem: If n is a composite integer, then n has a prime divisor less than or equal to the square root of n.
Trivial Division Algorithm: To show an a number is prime, divide by all prime numbers smaller or equal to that number.
Greatest Common Divisor: Let a and b be non-zero integers. The largest integer d such that d | a and d | b is called the greatest common divisor of a and b, denoted gcd(a, b).

$$gcd(a,b) = p_1^{min(a_1,b_1)} * p_2^{min(a_2,b_2)} * ... * p_n^{min(a_n,b_n)}$$

where a_i and b_i is the exponent of the prime number (p_i) in the prime factorization of a and b
Relatively Prime: Two integers a and b are relatively prime if gcd(a, b) = 1.
Pairwise Relatively Prime: The integers a_1, a_2, ..., a_n are pairwise relatively prime if gcd(a_i, a_j) = 1 whenever $1 \leq i < j \leq n$.
Least Common Multiple: The least common multiple of positive integers a and b is the smallest positive integer divisible by both a and b, denoted by lcm(a, b).

$$lcm(a,b) = p_1^{max(a_1,b_1)} * p_2^{max(a_2,b_2)} * ... * p_n^{max(a_n,b_n)}$$

where a_i and b_i is the exponent of the prime number (p_i) in the prime factorization of a and b
GCD, LCM Theorem: For positive integers a and b, ab = gcd(a, b) * lcm(a, b).
GCD Lemmas:

- Let a = bq + r where a, b, q, and r are integers. Then, gcd(a, b) = gcd(b , r).
- If a, b, and c are positive integers such that gcd(a, b) = 1 and a | bc, then a | c.
- If p is a prime and p | a_1 * a_2 * ... * a_n where each a_i is an integer, then p | a_i for some i.

Euclidean Algorithm: To find the gcd(a, b) where a and b are positive integers,
x = a
y = b
while(y $\neq$ 0):
    r = x mod y
    x = y
    y = r
return x
Bezout's Theorem: If a and b are positive integers, then there exists integers s and t such that gcd(a, b) = sa + tb.
Bezout's Identity: gcd(a, b) = sa + tb
Bezout's Coefficients: s and t of Bezout's identity

Extended Euclidean Algorithm: Substitute intermediary quotients back into the equation to determine Bezout's coefficients.
GCD Congruence Theorem: Let a, b, c, and m be integers where m is positive. If ac $\equiv$ bc (mod m) and gcd(c, m) = 1, then a $\equiv$ b (mod m).

3.5 Congruences

Linear Congruence: A congruence in the form ax $\equiv$ b (mod m), where m, a, and b are integers with m being positive, and x being a variable.
Inverse: The inverse of a mod m, denoted by $\overline{a}$ has the property $\overline{a}$ a = 1 (mod m).
Inverse Theorem: If a and m are relatively prime integers and m > 1, then an inverse of a mod m exists where the inverse is unique modulo m.
Chinese Remainder Theorem: Let m_1, m_2, ..., m_n be pairwise relatively prime positive integers > 1 and a_1, a_2, ..., a_n be integers. Then the system...
x $\equiv$ a_1 (mod m_1),
x $\equiv$ a_2 (mod m_2),
...
x $\equiv$ a_n (mod m_n)
has a unique solution modulo m = m_1 * m_2 * ... * m_n such that 0 $\leq$ x < m and x $\equiv$ a_1 * s_1 * M_1 + a_2 * s_2 * M_2 + ... + a_n * s_n * M_n where s_i is the Bezout Coefficient and M_i is m / m_i.
Back Substitution: Starting from the smallest mod m, substitute the congruence into the next smallest mod m until the entire system is substituted; then, find the inverse and solve for x.
Fermat's Little Theorem: If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1(\mod p)$$

$$\forall a(a^p \equiv a(\mod p))$$

Pseudoprimes: A psuedoprime to the base b is a composite integer n that satisfies the congruence,

$$b^{n-1} \equiv 1(\mod n)$$

Pseudo Random: a systematic method of generating random numbers
Linear Congruential Method: Given a modulus m, increment c, multiplier a, and seed x_0, the ith random number is equal to...

$$x_i = (ax_{i-1} + c) \mod m$$

Parity Check Bits: An extra bit appended to the end of a bit string equal to the sum of the digits of the bits mod 2, which allows to ensure that an odd number of errors did not occur.
Single Error: error in a single digit

Transposition Error: swapped placement of two digits
ISBN Check Digit: A digit at the end of an ISBN to satisfy the equation,

$$\sum_{i=1}^{10} d_i * i$$

Note: If C = 10, since a digit cannot be two digits, then C = X.
Totient Function: Denoted, $\Phi(n)$, the function returns the number of integers relatively prime to n.
Euler's Theorem: If gcd(a, n) = 1, then $a^{\Phi(n)} \equiv 1 \pmod{n}$.

4 Induction

Mathematical Induction: To prove that P(n) is true for all positive integers n, where P(n) is a proposition function, prove two steps:

- Base Step: Verify P(1) is true
- Inductive Step: Show that P(k) implies P(k + 1) for all positive integers k

$$(P(1) \land \forall k(P(k) \to P(k+1))) \to \forall n P(n)$$

Inductive Hypothesis: Assumption that P(k) is true
Harmonic Series: Sum of 1 + 1/2 + 1/3 + ... + 1/n + ...
Strong Induction: To prove that P(n) is true for all positive integers n, where P(n) is a proposition function, prove two steps:

- Base Step: Verify P(1) is true
- Inductive Step: Assume that P(j) is true for all j $\leq$ k and show that P(k+1) is true

$$(P(1) \land ((P(1) \land P(2) \land ...P(k)) \to P(k+1))) \to \forall n P(n)$$

Well-Ordering Property: Every nonempty subset of nonnegative integers has a smallest element

5 Recursion

Recursively Defined Functions: A function defined by a base case and a recursive step:

- Base Step: The initial values in which the function
- Recursive Step: Rules of finding new values that are true based off known values

Fibonacci Sequence: $f_0 = 0; f_1 = 1; f_n = f_{n-1} + f_{n-2}$ for n > 1 with the difference between two terms approaching **the golden ratio**, $\Phi = \frac{1+\sqrt{(5)}}{2}$.
Well-Defined: Every valued can be determined unambiguously
Lame's Theorem: Let a and b be positive integers where a $\geq$ b. Then, the number of divisions used by the Euclidean algorithm to find gcd(a, b) is less than or equal to 5x the digits in b (base-10).
Exclusion Rule: An (assumed) rule which states that elements not in the definition of a recursively defined set is not in the set
Well-Formed Formulae: Recursion can define a set based on truth values, logical connectives, arithmetic operators, etc
Exponentation Symbol: $\uparrow$
Rooted Trees: A set of vertices containing a distringuished vertex call the **root** and edges connecting those vertices defined by recursive rules
Extended Binary Trees: recursively defined as...
Basis Step: Empty Set is an extended Binary Tree
Recursive Step: If T_1 and T_2 are nonempty disjoint extended binary trees, there is an extended binary tree consisting of T_1, the root, and T_2.
Full Binary Trees: (when each parent has either no children or two children) recursively defined as...
Basis Step: The root is a full binary tree
Recursive Step: If T_1 and T_2 are nonempty disjoint full binary trees, there is an full binary tree consisting of T_1, the root, and T_2.
Height of a Full Binary Tree: h(t) is the height of a full binary tree, recursively defined as...
Basis Step: The height of a full binary tree consisting only of the root h(r) = 0.
Recursive Step: If T_1 and T_2 are nonempty disjoint full binary trees, then the full binary tree T has height h(T) = max(h(T_1), h(T_2)).
Nodes of a Full Binary Tree: n(t) is the number of nodes of a full binary tree...

$$n(T) \leq 2^{h(T)+1} - 1$$

Structural Induction:

- Base Step: Show the result holds for all elements defined in the basis step of the recursive definition
- Inductive 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 the new elements

Recursive Algorithm: An algorithm which solves a problem by reducing its input to an instance of the same problem the smaller input

Iterative Solution: Applying the recursive definition to the base cases to get to larger inputs
Merge Sort Lemma: Two sorted lists with m and n elements can be merged into a sorted list using no more than m + n - 1 comparisons.
Merge Sort Theorem: The number of comparisons total for merge sort with an n element list is O(n * log(n))

6 Algorithms

6.1 Algorithms

Algorithm: Finite sequence of instructions to solve an algorithm
Optimization Problem: maximize or minimize the value of some parameter
Greedy Algorithm: make the best choice at each step
Algorithmic Paradigm: general approach to construct algorithms for solving problems
Brute Force Algorithm: solve the problem using the statement of the problem and definitions of terms
Tractable: problem solvable by using an algorithm with worst case polynomial-complexity (belong to the class P)
Unsolvable: a problem which cannot be solved using an algorithm

6.2 The Growth of Functions

Big-O Notation: Let f and g be functions from Z to Z or R to R. f(x) is O(g(x)) if there are constants C and k such that

$$| f(x) | \leq C | g(x) |$$

whenever x > k, where C and k are called the **witnesses**. Two functions with the same Big-O have the same order.
Big O Theorems:

- The big-O of a nth-degree polynomial is O(x^n).
- The big-O of the sum of two functions f(x) and g(x) is O(max(f(x), g(x))).
- The big-O of the product of two functions f(x) and g(x) is O(f(x))*O(g(x)).
- log(n!) is O(n * log(n))

Master Theorem: For a function $f(n) = a * f(n/b) + c * n^d$ whenever $n = b^k$ where $k \in Z^+$, $a \geq 1$, $b \in Z > 1$ and $c, d \in R$ with c being positive and d being nonnegative,

$$O(f(n)) = \begin{cases} O(n^d) & a < b^d \\ O(n^d * log(n)) & a = b^d \\ O(n^{log_b(a)}) & a > b^d \end{cases}$$

7 Counting

7.1 Counting Methods:

Counting Principle: Suppose an experiment's outcome has k independent components. Then, the total number of outcomes is the product of the outcomes of each component, denoted by n_i.

$$\prod_{i=1}^{k} n_i$$

$$\mid A_1 \times A_2 \times ... \times A_n \mid = \mid A_1 \mid * \mid A_2 \mid * ... * \mid A_m \mid$$

Addition Principle: Suppose a collection of outcomes is partitioned into k subcollections. Then, the total number of outcomes is the sum of the outcomes of each subcollection, denoted by n_i.

$$\sum_{i=1}^{k} n_i$$

Permutation Principle: Given n distinguishable objects, there are n! ways to arrange them.

$$0! = 1; (n > 0) : n! = \prod_{i=1}^{n} i$$

R-Permutation: Given n distinguishable objects, the number of ways to arrange r objects is

$$\prod_{i=n-r+1}^{n} i = \frac{n!}{(n-r)!}$$

Distinguishable Principle: In a collection of n total outcomes, each outcome is part of a family of k distinguishable outcomes. The total number of distinguishable outcomes is equal to:

$$\frac{n}{k}$$

Choose Notation:

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

Choosing Principle: The number of ways to choose k objects out of n objects where order doesn't matter is:

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

Note: When the order does matter, it is considered a permutation.

Permutation Notation:

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

Word Counting Principle: Given n letters, k of which are distinct, such that the first letter repeated r_i times up to the kth letter repeated r_k times, the total number of words that can be creased from the n letters is:

$$\binom{n}{r_1, r_2, ..., r_k} = \frac{n!}{(r_1)!(r_2)!...(r_k)!} = \binom{n}{r_1}\binom{n-r_1}{r_2}...\binom{n-r_1-r_2-...r_{k-1}}{r_k}$$

Non-Negative Integer Solutions: The number of ways to divide n indistinguishable objects into k bins (where bins may have 0 objects) is:

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

Positive Integer Solutions: The number of ways to divide n indistinguishable objects into k bins where each bin must have at least i objects is:

$$\binom{(n-i*k)+(k-1)}{k-1}$$

Partition: Let S be a non-empty set. A partition π of S is a family $\pi = \{A_i\}_{i=1}^{n}$ of non-empty subsets of S satisfying the condition that every element in S belongs to exactly 1 A_i.

$$\bigcup_{i=1}^{n} A_i = S$$

$$A_i \neq A_j; i \neq j$$

7.2 Pigeonhole Principle

Pigeonhole Principle: If k is a positive integer and k + 1 or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

Generalized Pigeonhole Principle: If N objects are placed into k boxes, then there is at least one

box containing at least $\lceil N/k \rceil$ objects.

Sequence Theorem: Every sequence of $n^2 + 1$ distinct real numbers contains a subsequence of length n + 1 that is either strictly increasing or decreasing.

7.3 Binomial Coefficients

Binomial Expansion: Given the polynomial $(x+y)^n$, the binomial expansion of the polynomial is:

$$\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Note: when x and y both equal 1, then:

$$\sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$$

Note: when x = 1 and y = -1, then:

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

Note: when x = 1 and y = 2, then:

$$\sum_{k=0}^{n} \binom{n}{k} 1^k (2)^{n-k} = \sum_{k=0}^{n} \binom{n}{k} = (1+2)^n = 3^n$$

Pascal's Identity: For positive integers n and k with $n \geq k$,

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

Pascal's Triangle: A triangle of binomial coefficients with rows starting at n = 0 and diagonals from the top right starting at k = 0.

Vandermonde's Identity: For nonnegative integers m, n, and r with $r \leq n$ and $r \leq m$,

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

Note: when m = n = r, then:

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

Hockey Stick Theorem: For nonnegative integers with r $\leq$ n,

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$$

8 Relations

8.1 Properties of Relations

Binary Relation: Let A and B be sets. A binary relation from A to B is a subset A x B. When an element (a, b) $\in$ R where a $\in$ A and b $\in$ B, a is said to be related to b by relation R.
Inverse Relation: For sets A and B, the inverse of relation R = $\{$(a, b)| a $\in$ A $\wedge$ b $\in$ B$\}$, is R^{-1} = $\{$(b, a)| a $\in$ A $\wedge$ b $\in$ B$\}$.
Functions as Relations: A function f assigns exactly one element of B to each element of A. The graph of f is the set of ordered pairs (a, b) such that b = f(a).
Relation on a Set: A relation on a set A is a relation from A to A.
Reflexive: A relation R on set A is called reflexive if (a, a) $\in$ R for every element a $\in$ A.

$$\forall a((a, a) \in R)$$

Symmetric: A relation R on a set A is called symmetric if (b, a) $\in$ R whenever (a, b) $\in$ R for all a, b $\in$ A.

$$\forall a \forall b((a, b) \in R \rightarrow (b, a) \in R)$$

Antisymmetric: A relation R on set A is called antisymmetric if for all a, b $\in$ A, if (a, b) $\in$ R and (b, a) $\in$ R, then a = b.

$$\forall a \forall b(((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b))$$

Transitive: A relation R on set A is called transitive if whenever (a, b) $\in$ R and (b, c) $\in$ R implies (a, c) $\in$ R for all a, b, c $\in$ A.

$$\forall a \forall b \forall c(((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R)$$

Composite Relation: Let R be a relation from set A to set B and S be a relation from set B to set C. Then, the composite relation of R and S is a relation consisting of ordered pairs (a, c) where a $\in$ A and c $\in$ C, where there exists an element b $\in$ B such that (a, b) $\in$ R and (b, c) $\in$ S, denoted by S $\circ$ R.
Powers of Relations: Let R be a relation of set A. The powers R^n for $n \in Z^+$ are defined recursively by $R^1 = R; R^{n+1} = R^n \circ R$.
Transitive Theorem: A relation R on set A is transitive if and only if $R^n \subseteq R$ for $n \in Z^+$.

8.2 Equivalence Relations

Equivalence Relation: A relation on a set A is called an equivalence relation if it is reflexive, symmetric, and transitive.

Equivalent Elements: Two elements a and b that are related by a equivalence relation are called equivalent, denoted a $\sim$ b.