

CPT107 Revision

「 Number Systems 」

Brief Description

Natural Numbers

These are the numbers that we use to count things. They are also known as the counting numbers and are denoted by the symbol \mathbb{N} . The natural numbers are 1, 2, 3, 4, 5, 6, etc.

Integers

These are the numbers that include the natural numbers, their negatives, and zero. They are denoted by the symbol \mathbb{Z} . The integers are ..., -3, -2, -1, 0, 1, 2, 3, ...

Rational Numbers

These are numbers that can be expressed as the ratio of two integers. They are denoted by the symbol \mathbb{Q} . Examples of rational numbers include $1/2$, $3/4$, $5/6$, etc.

Real Numbers

These are numbers that can be represented on a number line. They include all of the rational numbers as well as some numbers that cannot be expressed as the ratio of two integers (such as the square root of 2 or π). They are denoted by the symbol \mathbb{R} .

Prime Numbers

These are numbers that are divisible only by 1 and themselves. The first few prime numbers are 2, 3, 5, 7, 11, etc.

Even Numbers

These are numbers that are divisible by 2. Examples of even numbers include 2, 4, 6, 8, 10, etc.

Odd Numbers

These are numbers that are not divisible by 2. Examples of odd numbers include 1, 3, 5, 7, 9, etc.

Closure Table

Here is a table that lists the various sets of numbers and whether they are closed under various operations:

Set of Numbers	Addition	Subtraction	Multiplication	Division
Natural numbers	Yes	Yes	Yes	No
Integers	Yes	Yes	Yes	No
Rational numbers	Yes	Yes	Yes	Yes
Real numbers	Yes	Yes	Yes	Yes
Prime numbers	No	No	No	No
Even numbers	Yes	Yes	Yes	No
Odd numbers	No	No	Yes	No

「 Proof Techniques 」

Proof by Contradiction

Definition

If $(\neg p \rightarrow \text{false})$ is true, then p is true.

Steps

Assume $\neg p$ and find contradiction.

Proof by Induction

Definition

Let $P(n)$ be a predicate. If $P(0) \wedge (\forall n \in \mathbb{N}, P(n) \rightarrow P(n+1))$ is true, then $\forall n \in \mathbb{N}, P(n)$ is true.

Steps

Base case: When $n = 0$, ...

Induction step: Let $k \in \mathbb{N}$ be given and suppose ... is true for $n = k$.

...

Thus, ... holds for $n = k + 1$, and the proof of the induction step is complete.

Conclusion: By the principle of induction, ... is true for all $n \in \mathbb{N}$.

「 Set Theory 」

Notation

- Set-Roster Notation eg. $\{0, 2, 4, 6, \dots\}$
- Set-Builder Notation eg. $\{x \mid P(x)\}$

Equality

Order and repetition do not matter

Subset

If every element in A is also in B, then $A \subseteq B$.

Operations

- **Union:** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- **Intersection:** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- **Relative complement:** $A - B = \{x \mid x \in A \text{ and } x \notin B\}$
- **Complement:** $\sim A = \{x \mid x \notin A\} = U - A$ (U is the universal set)
- **Symmetric difference:** $A \Delta B = \{x \mid (x \in A \text{ and } x \notin B) \text{ or } (x \notin A \text{ and } x \in B)\}$
- **Power set:** $\text{Pow}(A) = \{C \mid C \subseteq A\}$
- **Cartesian product:** $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$

Algebra

Associative Laws

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

Commutative Laws

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

Identity Laws

- $A \cup \emptyset = A$
- $A \cap U = A$

Distributive Laws

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

Complement Laws

- $A \cup \sim A = U$
- $A \cap \sim A = \emptyset$
- $\sim(\sim A) = A$
- $\sim \emptyset = U$
- $\sim U = \emptyset$

De Morgan's Laws

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

Cardinality

Definition

The cardinality of a finite set S is the number of elements in S , and is denoted by $|S|$.

Computation

- Union of two sets: $|A \cup B| = |A| + |B| - |A \cap B|$
- Union of three sets: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
- Power set of a set: $|\text{Pow}(A)| = |A| * |A + 1| / 2 + 1$
- Cartesian product: $|A \times B| = |A| * |B|$

Bit String

Definition

A sequence of bits (binary digits), which can be either 0 or 1.

Characteristic Vectors

A characteristic vector is a way of representing a subset of a larger set using bit string. The length of the characteristic vector is equal to the number of elements in the larger set, and each element is represented by a single bit. If the bit corresponding to an element is 1, it means that the element is in the subset; if the bit is 0, it means that the element is not in the subset.

For example, Let $S = \{1, 2, 3, 4, 5\}$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- The characteristic vector of A is (1, 0, 1, 0, 1).
- The characteristic vector of B is (0, 0, 1, 1, 0).
- The characteristic vector of $A \cap B$ is (0, 0, 1, 0, 0).
- The characteristic vector of $A \cup B$ is (1, 0, 1, 1, 1).

「 Relations 」

Definition

Binary Relation

A binary relation R from a set A to a set B is a subset of $A \times B$, denoted as $R \subseteq A \times B$.

Unary Relation

Unary relations are just subsets of a set.

Notation

Symbols

$(a, b) \in R$ can be denoted as aRb , which is a predicate that a is R -related to b .

Directed Graphs (digraph)

- Let A and B be two finite sets and R a binary relation between these two sets (i.e., $R \subseteq A \times B$).
- We represent the elements of these two sets as vertices of a graph.
- For each $(a, b) \in R$, we draw an arrow linking the related elements.
- This is called the directed graph (or digraph) of R .

Matrices

- Another way of representing a binary relation between finite sets uses an array.
- Let $A = \{a_1, \dots, a_n\}$, $B = \{b_1, \dots, b_m\}$ and $R \subseteq A \times B$. We represent R by an array M of n rows and m columns.
- Such an array is called a n by m matrix.
- The entry in row i and column j of this matrix is given by $M(i, j)$ where

$$M(i, j) = \begin{cases} T & \text{if } (a_i, b_j) \in R \\ F & \text{if } (a_i, b_j) \notin R \end{cases} \quad (1)$$

Properties

Reflexive

- $\forall x \in A, xRx$
- To check for reflexivity, you can verify that every element in the set appears on the left-hand side of the relation at least once and is related to itself.

Symmetric

- $\forall x, y \in A, xRy \rightarrow yRx$
- To check for symmetry, you can verify that for every pair of elements A and B that are related, if (A, B) is in the relation, then (B, A) is also in the relation.

Antisymmetric

- $\forall x, y \in A, (xRy \wedge yRx) \rightarrow x = y$
- To check for antisymmetry, you can verify that for every pair of elements A and B that are related, if (A, B) and (B, A) are both in the relation, then A and B can't be different elements.

Transitive

- $\forall x, y, z \in A, (xRy \wedge yRz) \rightarrow xRz$
- To check for transitivity, you can verify that for every triple of elements A , B , and C , if (A, B) and (B, C) are both in the relation, then (A, C) is also in the relation.
- To compute the **transitive closure**:

1. Start with the original relation as the transitive closure.
2. Repeat the following step until the transitive closure does not change:
 - For each pair (x,y) in the transitive closure, if there exists a z such that (x,z) and (z,y) are also in the transitive closure, add (x,y) to the transitive closure.

Special Relations

Equivalence Relation

- It is reflexive, symmetric and transitive.
- **Equivalence class**
 - A set of elements that are equivalent to each other under a given equivalence relation.
 - $E_x = \{ y \in S \mid yRx \}$

Partial Order

- It is reflexive, antisymmetric and transitive.
- A set S with a partial ordering R is called a **partially ordered set**, or **poset**, denoted by (S,R)
 - x is a **predecessor** of y iff $x \neq y \wedge xRy$
 - If x is a predecessor of y and there is no $z \notin \{x,y\}$ for which xRz and zRy , we call x an **immediate predecessor** of y .
 - **Hasse diagram** is a digraph where:
 - Vertices of the digraph are the elements of the partial order.
 - The edges of the digraph are given by the "immediate predecessor" relation.

Total Order

- It is comparable partial order.
- **Comparable** means $\forall x,y \in S, xRy \vee yRx$

Operations

- Given a relation $R \subseteq A \times B$, we define the **inverse relation** $R^{-1} \subseteq B \times A$ by

$$R^{-1} = \{(b,a) \mid (a,b) \in R\}.$$
- Let $R \subseteq A \times B$ and $S \subseteq B \times C$. The **composition** of R and S , denoted by $S \circ R$, is the binary relation between A and C given by

$$S \circ R = \{(a,c) \mid (\exists b \in B)(aRb \wedge bSc)\}.$$

「 Functions 」

Definition

$F: A \rightarrow B$ is a relation that:

1. $\forall a \in A, \exists b \in B, (a, b) \in F$
2. if $(a, b) \in F \wedge (a, c) \in F$, then $b = c$

Concepts

Suppose $f : A \rightarrow B$.

- A is called the **domain** of f .
- B is called the **codomain** of f .
- The **image** or **range** of f is the set of all output values that the function can produce.

Properties

Injective (one-to-one)

- A function $f: X \rightarrow Y$ is injective if for all x_1, x_2 in X , $f(x_1) = f(x_2)$ implies $x_1 = x_2$.
- This means that the function maps different elements of the domain to different elements of the codomain.

Surjective (onto)

- A function $f: X \rightarrow Y$ is surjective if for all y in Y , there exists an x in X such that $f(x) = y$.
- This means that the function maps every element of the codomain to some element in the domain.

Bijjective

- A function $f: X \rightarrow Y$ is bijective if it is both injective and surjective.
- This means that the function is a one-to-one correspondence between the elements of the domain and the codomain.

Invertible

- A function $f: X \rightarrow Y$ is invertible if there exists a function $g: Y \rightarrow X$ such that for all x in X , $g(f(x)) = x$ and for all y in Y , $f(g(y)) = y$.
- In other words, the function has an inverse function that "undoes" the original function.
- **Theorem:** a function f is invertible iff it is a bijection.
- How to find the inverse for $f(x)$:
 1. Let $y = f(x)$
 2. Solve for " x " in terms of " y "
 3. Replace " x " with " $f^{-1}(y)$ "
 4. Replace every " y " with " x "

Composition of Functions

Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$

Then $(g \circ f)(x) = g(f(x))$.

Pigeonhole Principle

If there are more elements in the domain than in the range, then there must be at least one element in the domain that is related to more than one element in the range. Thus, the function is not one-to-one.

「 Propositional Logic and FOL 」

Notations

Symbol	Name	Description
\neg	Negation	Negates the truth value of a proposition. For example, if p is a proposition that is true, then $\neg p$ is a proposition that is false.
\wedge	Conjunction	A conjunction is a compound proposition that is true only if both of its conjuncts (the propositions it connects) are true. For example, if p and q are propositions, then the conjunction " $p \wedge q$ " is true if both p and q are true.
\vee	Disjunction	A disjunction is a compound proposition that is true if at least one of its disjuncts (the propositions it connects) is true. For example, if p and q are propositions, then the disjunction " $p \vee q$ " is true if either p or q (or both) are true.
\rightarrow	Implication	An implication is a compound proposition that is true only if the antecedent (the proposition that comes before the " \rightarrow ") is false or the consequent (the proposition that comes after the " \rightarrow ") is true. For example, if p and q are propositions, then the conditional " $p \rightarrow q$ " is true if either p is false or q is true (or both).
\equiv	Biimplication	A biimplication is a compound proposition that is true only if both of its sides (the propositions on either side of the " \equiv ") are either both true or both false. For example, if p and q are propositions, then the biimplication " $p \equiv q$ " is true if both p and q are true, or if both p and q are false.
\top	True	A symbol that represents a proposition that is always true, which is a tautology .
\perp	False	A symbol that represents a proposition that is always false, which is a contradiction .
\forall	Universal quantifier	A quantifier that is used to indicate that a proposition holds for all values of a variable. For example, if x is a variable and p(x) is a proposition that depends on x, then the universal quantification " $\forall x, p(x)$ " is a proposition that is true if p(x) is true for all values of x.
\exists	Existential quantifier	A quantifier that is used to indicate that a proposition holds for at least one value of a variable. For example, if x is a variable and p(x) is a proposition that depends on x, then the existential quantification " $\exists x, p(x)$ " is a proposition that is true if p(x) is true for at least one value of x.
\models	Semantic consequence	A relationship between two statements or propositions, where one statement (the conclusion) logically follows from the other statement (the premise). For example, if the premise is "All dogs are mammals" and the conclusion is "Fido is a mammal", then the conclusion "Fido is a mammal" is a semantic consequence of the premise "All dogs are mammals". This can be symbolized as "All dogs are mammals \models Fido is a mammal".

Laws for Equivalences

Associative Laws

- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- $(p \vee q) \vee r \equiv p \vee (q \vee r)$

Commutative Laws

- $p \wedge q \equiv q \wedge p$
- $p \vee q \equiv q \vee p$

Identity Laws

- $p \wedge \top \equiv p$
- $p \vee \perp \equiv p$

Distributive Laws

- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Complement Laws

- $p \wedge \neg p \equiv \perp$
- $p \vee \neg p \equiv \top$
- $\neg \neg p \equiv p$
- $\neg \top \equiv \perp$
- $\neg \perp \equiv \top$

De Morgan's Laws

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Predicate Logic

First-order predicate logic is a formal system for representing and reasoning about the relationships between objects and predicates. It is a type of first-order logic, which means that it allows the use of quantifiers to range over variables that represent objects.

Syntax

The syntax of first-order predicate logic consists of a set of logical symbols and a set of well-formed formulas (wffs). The logical symbols include:

- Predicate symbols: These represent properties or relations that hold between objects. For example, "x is taller than y" could be represented by the predicate symbol $T(x, y)$.
- Function symbols: These represent functions or operations that take one or more arguments and return a value. For example, "the mother of x" could be represented by the function symbol $M(x)$.
- Individual constants: These represent specific objects. For example, a could represent the object "Alice".
- Individual variables: These represent objects that can be replaced with any individual constant. For example, x could represent any object.

- Logical connectives: These include symbols such as "and" (\wedge), "or" (\vee), "not" (\neg), "implies" (\rightarrow), and "if and only if" (\Leftrightarrow).
- Quantifiers: These include the symbols "for all" (\forall) and "there exists" (\exists).

Semantics

The semantics of first-order predicate logic specify the meaning of the logical symbols and how to determine the truth or falsity of a formula. The truth or falsity of a formula is determined by its truth value, which can be either true or false.

The truth value of a formula is determined by the truth values of its **atomic formulas**, which are formulas that cannot be broken down into smaller formulas. Atomic formulas are either true or false based on their interpretation in a given domain. For example, the atomic formula $T(a, b)$ is true if "a is taller than b" is true in the given domain, and false otherwise.

Evaluation

The process of determining the truth value of a formula is called evaluation. In first-order predicate logic, the rules for evaluating formulas are based on the truth table method, which specifies the truth value of a formula based on the truth values of its subformulas.

「Combinatorics」

Notations

Sums

- A sum is a mathematical operation that adds together a set of numbers.
- In combinatorics, we often use the summation symbol (\sum) to represent a sum.
- The summation symbol is usually followed by an index variable (i, j, k, etc.), which represents the values that are being added together.
- For example, the sum $\sum_{i=1}^n i$ represents the sum of the numbers from 1 to n.

Products

- A product is a mathematical operation that multiplies a set of numbers.
- In combinatorics, we often use the product symbol (\prod) to represent a product.
- The product symbol is usually followed by an index variable (i, j, k, etc.), which represents the values that are being multiplied together.
- For example, the product $\prod_{i=1}^n i$ represents the product of the numbers from 1 to n.

Factorials

- A factorial is a mathematical operation that multiplies a number by all of the numbers below it.
- For example, the factorial of 5 (written as $5!$) is equal to $5 * 4 * 3 * 2 * 1$, which is equal to 120.
- The factorial symbol (!) is usually placed after a number to indicate that it should be multiplied by all of the numbers below it.
- The base case for factorials is $0! = 1$. This is because anything multiplied by 1 is equal to itself, so $0! = 1 * 0 = 1$.

Basic Counting Rules

Product Rule

- If there are m ways to perform one task and n ways to perform a second task, then there are $m \times n$ ways to perform both tasks.
- This principle is used when two events are independent, meaning that the outcome of one event does not affect the outcome of the other event.
- For example, if there are 2 ways to choose a shirt (red or blue) and 3 ways to choose a pair of pants (jeans, slacks, or shorts), then there are $2 * 3 = 6$ ways to choose a complete outfit.
- Explanation with set theory: $|A \times B| = |A| * |B|$

Sum Rule

- If there are m ways to perform one task and n ways to perform a second task, then there are $m + n$ ways to perform either task.
- This principle is used when two events are mutually exclusive, meaning that the outcome of one event precludes the possibility of the other event occurring.
- For example, Friday night you can see one of five movies, go to one of two concerts, or stay home. There are $5 + 2 + 1 = 8$ choices for spending Friday night.
- Explanation with set theory: $|A \cup B| = |A| + |B|$ when $A \cap B = \emptyset$

Subtraction Rule

- If there are m ways to perform a task and n of those ways are not allowed, then there are $m - n$ ways to perform the task.
- This principle is used when there are restrictions on the ways in which a task can be performed.

Division Rule

- If a task can be performed in m ways and each of those ways can be divided into n sub-tasks, then there are $\frac{m}{n}$ ways to perform each sub-task.
- This principle is used when a task can be divided into smaller sub-tasks that can be performed independently.
- For example, Bob counts the number of people in the room by counting the number of ears (assume every person has two ears). To get the number of people, he needs to divide the number of ears by 2.

About Formulas

In the following formulas:

- n is the number of elements of the set
- r is the number of elements we choose
- $0 \leq r \leq n$

Permutations

Permutations are **arrangements** of objects in which the order matters.

Permutation with Repetitions

- This refers to permutations in which an object can be used more than once.
- $P(n, r) = n^r$
- For example, the number of 5-digit positive integers without digits 6, 7, 8, and 9 in their decimal representation is $6^5 - 6^4 = 6480$.

Permutation without Repetition

- This refers to permutations in which each object can only be used once.
 - $P(n, r) = \frac{n!}{(n-r)!}$
 - For example, let $A = \{a, b, c, d\}$. All 2-arrangements without repetitions of the elements of set A are the following: $ab, ac, ad, ba, bc, bd, ca, cb, cd, da, db, dc$.
- The total number of such arrangements is $\frac{4!}{(4-2)!} = 12$.

Permutation of Identical Objects

- This refers to permutations in which some of the objects are identical.
- The number of permutations of n objects with n_1 identical objects of type 1, n_2 identical objects of type 2, ..., and n_k identical objects of type k is $\frac{n!}{n_1!n_2!\dots n_k!}$
- For example, the number of seven-letter words that can be formed using the letters of the word "BENZENE" is $\frac{7!}{3!2!} = 420$.

Combinations

Combinations are **selections** of objects in which the order does not matter.

Combinations with Repetitions

- This refers to combinations in which an object can be used more than once.
- $C(n + r - 1, r) = \binom{n+r-1}{r} = \frac{(n+r-1)!}{r!(n-1)!}$

Combinations without Repetition

- This refers to combinations in which each object can only be used once.
- The number of r-combinations of a set of size n is called **binomial coefficient**, denoted $C(n, r)$, pronounced "n choose r", and given by $C(n, r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$.
- For example, the number of binary strings of 17 zeros and 8 ones in which no two ones are adjacent is $\binom{18}{8} = 43758$.

「 Probability 」

Experiments

- **Deterministic**: allow perfect prediction.
- **Non-deterministic**: no perfect prediction.
 - **Random**: exhibit statistical regularity in the long-run.
 - **Haphazard**: unpredictable outcomes, no regularity.

Sample Space and Events

Sample Space

Sample space, denoted Ω , is the set of all possible outcomes of an experiment.

Event

Event is a subset of the sample space.

Special Events

- **Null event**, denoted \emptyset , never occurs.
- **Entire event**, denoted Ω , always occurs.

Compound Event

Compound event is the combination of two or more simple events.

- **Simple event** consists of exactly one outcome.

Operations on Events

Complement (not)

- $P(A') = 1 - P(A)$

Union (or)

- $P(A \cup B) = P(A) + P(B)$ if A and B are mutually exclusive events.
 - **Mutually exclusive events** are events that have no outcome in common.
- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$ if A and B are inclusive events.
 - **Inclusive events** are events that have one or more outcomes in common.

Intersection (and)

- $P(A \cap B) = P(A) * P(B)$ if A and B are independent events.
 - Events are **independent events** if the occurrence of one event does not affect the probability of the other (sample space is not changed). Otherwise, they are **dependent events**.

Definition

Probability is a measure of the likelihood of an event occurring, and it is usually expressed as a decimal or fraction between 0 and 1. The probability of an event occurring is denoted by the symbol P, and it is calculated using the following formula:

$$P(\text{event}) = \frac{\text{number of outcomes in the event}}{\text{total number of outcomes}} \quad (2)$$

Conditional Probability

If the probability of "X" is conditional (affected by) "Y" (what happens before it) then the probability of "X" given "Y" is

$$P(X|Y) = \frac{P(X \cap Y)}{P(Y)} \quad (3)$$

Random Variable

A random variable (r.v.) is a set of possible values from a random experiment.

For example, when tossing a coin, we could get Heads or Tails. Let's give them the values Heads=0 and Tails=1 and we have a Random Variable $X = \{0, 1\}$.

Expected Value

Definition

The expected value of a discrete random variable is equal to the mean of the random variable.

$$E(X) = \sum_{x \in \Omega} f(x)P(x) \quad (4)$$

- $f(x)$ is the value of the random variable at a particular point x in the sample space Ω .
- $P(x)$ is the probability of the random variable taking on the value x .

For example, consider a random variable X that represents the outcome of a dice roll. The sample space for this variable is $\Omega = \{1, 2, 3, 4, 5, 6\}$, and the probability of each outcome is $P(x) = \frac{1}{6}$ for all $x \in \Omega$. If we want to calculate the expected value of X , we can use the formula above:

$$E(X) = \sum_{x \in \Omega} f(x)P(x) = \sum_{x \in \Omega} x \cdot \frac{1}{6} = \frac{1}{6}(1 + 2 + 3 + 4 + 5 + 6) = \frac{21}{6} = 3.5 \quad (5)$$

Linearity of Expectation

Consider two random variables X and Y , with expected values $E(X)$ and $E(Y)$, respectively. If we want to calculate the expected value of a new random variable $Z = aX + bY$, where a and b are constants, we can use the linearity of expectation to simplify the calculation:

$$E(aX + bY) = aE(X) + bE(Y) \quad (6)$$