Discrete Math

Kim JaeHwan

Chapter 10 & 11. Number Theory and Cryptography

10.1. Divisibility and Modular Arithmetic

$a|b$ is read as a divides b.

proerties of Divisibility:

- If $a|b$ and $b|c$, then $a|c$.
- If $a|b$ and $a|c$, then $a|(b+c)$ and $a|(b-c)$.
- IF $a|b$, then $a|bc$ for any integer c.

Division algorithm. $a = dq + r$, d is divisor, q is quotient, r is remainder, a is called dividend. Then, $q = a \text{div} d$ and $r = a \mod d$.
Congruence Relation
$(\mod m)$ vs $\mod m$

10.2. Integer Representations

representations of integer (n-ary, base b) base conversion binary addition and binary multipulication

---

10.3. Primes and Greatest Common Divisors

prime, fundamental thm of Arithmetic GCD, finding GCD, euclidean algorithm, LCM, GCD as linear combination, dividing congruence by an integer

---

10.4. Solving Congruence

linear congruence, inverse of a modulo m, finding inverse to solve congruence,

---

11.1. Applications of Congruence

Hashing functions, pseudorandom number, check digits

11.2. Cryptography

Caesar Cipher, shift Cipher cryptanalysis of shift cipher, affine cipher, block cipher,

Chapter 12 & 13. Graph Theory

12.1. Graphs and Graph Models

Graph definition, remarks, some terminology, Directed graph, graph Model: computer networks, others, social netowrks, web graphs, software design.

12.2. Graph Terminology and Special Types of Graphs

Basic terminology : neighbors, neighborhood, degree, thm1: handshaking thm thm2: degree sum thm thm3: in digraph, indeg = outdeg special type of simple graph : complete, cycles, wheel, n-cubes, bipartite graph,

13.1. Representing Graphs and Graph Isomorphism

Adjacency List, Adjacency Matrix, Incidence Matrix, isomorphism of graph, algorithm

13.2. Connectivity

path, degrees of seperation, erdos number, bacon numbers, connectedness in undirected graph, connected components, connectedness in directed graph, counting paths between vertices

13.3. Euler and Hamilton Paths

Euler path and circuits, necessary condition, algorithm, application, hamilton path and circuits, sufficient conditions for hamilton circuit

Chapter 14. Induction and Recursion

14.1. Mathematical Induction

Principle, important point, validity of induction, how work, mistaken proof by induction, Guideline for induction proof,

14.2. Strong Induction

strong induction, compare with Mathematical induction, which will be used, fundamental thm of Arithmetic

14.3. Recursive Definitions and Structural Induction

recursively defined, fibonacci, recursively defined set and structure, string, Well-formed formula in propositional logic, rooted tree, full binary tree, indution and recursively defined set, structure

14.4. Recursive Algorithms

recursive algorithm, proving, recursion and iteration, merge sort

.

Chapter 15. Counting

15.1. The Basics of Counting

We have to count the number of cases to solve a counting problem. For example, uppercase letter 6 digit password which must contain at least one digit, then how many possible passwords are there? The answer is $36^6 - 26^6$. To solve this problem, we can use three basic principles: the product rule, the sum rule, and the subtraction rule. Note that each cases are independent to use these.

15.2. The Pigeonhole Principle

Theorem 1. ***The pigeonhole principle:*** *If k is a possible integer and $k+1$ objects are placed into k boxes, then at least one box contains two or more objects.*

Proof. By contradiction. Suppose none of the k boxes has more than one object, then the total number of objects is at most k. This is contradiction. □

Corollary 2. *A function f from a set with $k+1$ elements to a set with k elements is not one-to-one by the pigeonhole principle.*

Theorem 3. ***Generalized pigeonhole principle:*** *If N objects are placed into k boxes, then there is at least one box containing least $\lceil N/k \rceil$ objects.*

Proof. Same as the pigeonhole principle. □

Note a lots of examples.

15.3. Permutations and Combinations

Definition 4. ***Permutations:*** *A permutation of a set of distinct objects is an ordered arrangement of these objects, An ordered arrangement of r elements of a set is called an r-permutation. The number of r-permutations of a set with n elements is denoted by $P(n, r)$.*

Definition 5. ***Combinations:*** *An r-combination of elements of a set is an unordered selection of r elements from the set. An r-combination is simply a subset of the set with r elements. Notation is $C(n, r)$ or $\binom{n}{r}$*

Some easy theorem and corollary.

1. $P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$
2. If n and r are integers with $1 \le r \le n$, then $P(n, r) = \frac{n!}{(n-r)!}$
3. $C(n, r) = \frac{n!}{r!(n-r)!}$
4. $C(n, r) = C(n, n-r)$, when $0 \le r \le n$

15.4. Binomial Coefficients

Binomial expression is $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$. This is called binomail theorem. There is useful corollary.

Corollary 6.

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \textit{with } n \ge 0$$

Theorem 7. ***Pascal's Identity:*** *If n and k are integers with $n \ge k \ge 0$, then $binomn + 1k = \binom{n}{k-1} + \binom{n}{k}$*

Proof. Proof by combinatorial. □

Pascal's triangle is skipped in this paper.

15.5 Generalized Permutations and Combinations

Easy to understand, already known. Just look lecture notes.

Chapter 16. Probability

16.1. Introduction to Discrete Probability

Key terms:

- **Experiment:** A procedure that yields one of a given set of possible outcomes.
- **Sample space:** The set of all possible outcomes of an experiment.

- **Event:** A subset of the sample space.

Definition 8. ***Probability (by Pierre-Simon Laplace):*** *If S is a finite sample space for an experiment and E is an event, then the probability of E is $P(E) = \frac{|E|}{|S|}$. ($0 \leq P(E) \leq 1$)*

- Complement of E: $P(\bar{E}) = 1 - P(E)$
- Union of E_1 and E_2: $P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$

16.2. Probability Theory

- Assigning Probability: It assumes that all outcomes are equally likely.
- Conditional Probability

$$P(E|F) = \frac{P(E \cap F)}{P(F)}$$

- Independence
The events E and F are independent if and only if $P(E \cap F) = P(E)P(F)$
Pairwise independence and Mutual independence
- Bernoulli Trials and the Binomail Distribution
Suppose an experiment can have only two possible outcomes, each performance of the experiment is called a Bernoulli trial.
- Random Variables
A random variable is a function from the sample space of an experiment to the set of real numbers. **A random variable is a function. It is not a variable, and it is not random!**

16.3. Bayes' Theorem

Theorem 9. *Suppose that E and F are events from a sample space S such that $P(E) \neq 0$ and $P(F) \neq 0$. Then:*

$$P(E|F) = \frac{P(E|F)P(F)}{P(E|F)P(F) + P(E|\bar{F})P(\bar{F})}$$

Proof.

$$P(F|E) = \frac{P(E \cap F)}{P(E)} = \frac{P(E \cap F)}{P(E \cap F) + P(E \cap \bar{F})}$$
$$= \frac{P(E|F)P(F)}{P(E|F)P(F) + P(E|\bar{F})P(\bar{F})}$$

□

Theorem 10. ***Generalized Bayes' Theorem:*** *Suppose that E is an event from a sample space S and that $F_1, F_2, \cdots F_n$ are mutually exclusive events, and assume that $P(E) \neq 0$ for $i = 1, 2, \cdots, n$. Then:*

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

Interpreting Bayes' Theorem:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

- The event of out interest A
- The event as an observation B
- Prior probability $P(A)$, based only on our prior knowledge about A with no observation.
- Likelihood $P(B|A)$, the probability of observing B when A happens
- Posterior probability $P(A|B)$, the probability of A if we observed B.

Note lecture note if you need "A little taste of machine learning" part.

16.4. Expected Value and Variance

Definition 11. ***Expected Value:*** *The expected value of a random variable $X(s)$ of the random variable $X(s)$ on the sample sace S is equal to*

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

Q. What is the expected value of n mutually independent Bernoulli trials with probability p of success? (np)

- $E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$
- $E(aX + b) = aE(X) + b$
- $E(XY) = E(X)E(Y)$ if X and Y are independent.

Note lecture note if you need "Average-case computational complexity" and "Varaince" parts.

Chapter 17. Relations

17.1. Definition and Properties

Binary relation.

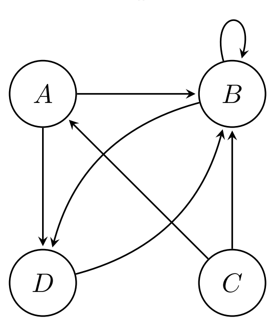
1. **Reflexive:** $\forall x[x \in A \to (x,x) \in R]$
2. **Symmetric:** $\forall x \forall y[(x,y) \in R \to (y,x) \in R]$
3. **Antisymmetric:** $\forall x \forall y[(x,y) \in R \land (y,x) \in R \to x = y]$
4. **Transitive:** $\forall x \forall y \forall z[(x,y) \in R \land (y,z) \in R \to (x,z) \in R]$

Combining relations: $R_1 \cup R_2, R_1 \cap R_2, R_1 - R_2$.
The composition of relations: $R_1 \circ R_2$.
Powers of a relation: $R^1 = R, R^{n+1} = R^n \circ R$.

Theorem 12. *Relation R is transitive if and only if $R^n \subseteq R$ for all $n \geq 1$.*

17.2. Representing Relations

1. **Ordered pairs:** $R = \{(a,b),(b,c),(c,a)\}$
2. **Matrix:** R is relation from A to B, and A has m elements, B has n elements.
   $R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ ex. $m = 3, n = 3$.
   (a) Reflexivity: All diagonal elements are 1.
   (b) Symmetry: $m_{ij} = 1 \Leftrightarrow m_{ji} = 1$.
   (c) Antisymm: $m_{ij} = 0 \lor m_{ji} = 0$ when $i \neq j$.
3. **Directed Graph:** Note an example.



$$R = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

   (a) Reflexivity: All nodes have a self-loop.
   (b) Symmetry: If there is an edge from A to B, there is an edge from B to A.
   (c) Antisymm: If there is an edge from A to B, there is no edge from B to A.
   (d) Transitivity: (x, y) and (y, z) $\to$ (x, z).

17.3. Closures

Let R is a relation on a set A. Then, R may or may not have the some properties like reflexivity, symmetry, antisymmetry, and transitivity. Then, S is called the **closure** of R if R with respect to P, if there is a relation S with property P containing R such that S is a subset of every relation with property P containing R. In other words, S is the smallest relation with property P containing R.

1. **Reflexive Closure:**
   $R \cup \Delta, \Delta = \{(a,a) | a \in A\}$
2. **Symmetric Closure:**
   $R \cup R^{-1}, R^{-1} = \{(b,a) | (a,b) \in R\}$
3. **Transitive Closure:**
   * **Connectivity relation:** R^* consist of the pairs (a,b) such that there is a path of length at least one from a to b. Then, $R^* = \cup_{i=1}^{\infty} R^i$

Here are something.
path: if $(a,x_1) \in R, (x_1,x_2) \in R, \cdots, (x_{n-1},b) \in R$, then $(a,b) \in R^n$, The length of path is n.

Theorem 13. *There is a path of length $n > 0$ from a to b if and only if $(a,b) \in R^n$.*

Then, how to show R^* is transitive closure of R?
1. Show R^* is transitive.
2. $R^* \subseteq S$ whenever S is a transitive relation containing R.
//TODO !!!!!!!!!!!!

17.4. Equivalence Relations

Definition 14. *A relation on a set A is called equivalence relation if it is reflexive, symmetric, and transitive.*
*Two elements a and b that are related by an equivalence relation are called **equivalent**, denoted by $a \sim b$.*

Example 15. *Let m be an integer with $m > 1$. Show that the relation $R = (a,b) | a \equiv b \mod m$ is an equivalence relation on the set of integers. Show that the relation R has reflexive, symmetric, and transitive properties.*

Definition 16. ***Equivalence class:*** *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, denoted by $[a]_R$.*
$[a]_R = \{s | (a, s) \in R\}$.
If $b \in [a]_R$, then b is called a representative of this equivalence class.

Theorem 17. *Let R be an equivalence relation on a set A. Then these statements for element a and b of A are equivalent.*

1. aRb
2. $[a] = [b]$
3. $[a] \cap [b] \neq \phi$

Definition 18. ***Partition:*** *A partition of a set A is a set of nonempty subsets of A such that every element of A is in exactly one of these subsets. $A_i \neq \phi$, $A_i \cap A_j = \phi$ for $i \neq j$, and $\cup_{i=1}^{\infty} A_i = A$.*

The equivalcne classes form a partition of the set A because they split A into disjoint subsets.

Theorem 19. *Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S. Conversely, ggiven a partition $\{A_i | i \in I\}$ of the set S, there is an equivalence relation R that has the sets $A_i, i \in I$, as its equivalence classes.*

Proof. Note lecture note. □