Discrete Mathematics for Computer Science

Lecture 22: Review Part 1

Dr. Ming Tang

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)
Email: tangm3@sustech.edu.cn

Topics of This Course

- Logic and Mathematical Proofs
  - Sets and Functions
    - Relations
      - Graphs I
        - Graphs II
          - Trees
    - Complexity of Algorithms
      - Number Theory
        - Cryptography
        - Groups, Rings, and Fields*
          - Finite Fields*
        - Mathematical Induction and Recursion
          - Counting
            - Discrete Probability*

Lecture Schedule

1. Logic and Mathematical Proofs
2. Sets and Functions
3. Complexity of Algorithms
4. Number Theory and Cryptography
5. Mathematical Induction
6. Recursion
7. Counting
8. Relations
9. Graph
10. Trees

Propositional Logic

Proposition: a declarative sentence that is either true or false (not both).

- Conventional letters used for propositional variables are p, q, r, s, ...
- **Truth value** of a proposition: true, denoted by T; false, denoted by F.

Compound propositions are build using logical connectives:

- Negation $\neg$
- Conjunction $\wedge$
- Disjunction $\vee$
- Exclusive or $\oplus$
- Implication $\rightarrow$
- Biconditional $\leftrightarrow$

Tautology and Logical Equivalences

- Tautology: A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it.
  - E.g., $p \lor \neg p$
- Contradiction: A compound proposition that is always false.

The compound propositions p and q are called logically equivalent, denoted by $p \equiv q$, if $p \leftrightarrow q$ is a tautology.

- E.g., $\neg(p \lor q)$ and $\neg p \land \neg q$

That is, two compound propositions are equivalent if they always have the same truth value.

Determine logically equivalent propositions using:

- Truth table
- Logical Equivalences

Important 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

Important Logical Equivalences

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

$$p \rightarrow q \equiv \neg p \vee q$$

Useful Law

Predicate Logic and Quantified Statements

Predicate Logic: make statements with variables: $P(x)$.

Propositional function $P(x) \overset{\text{specify } x}{\Longrightarrow}$ Proposition

Quantified Statements: Universal quantifier $\forall x P(x)$; Existential quantifier $\exists x P(x)$

Statement	When true?	When false?
$\forall$x P(x)	P(x) true for all x	There is an x where P(x) is false.
$\exists$x P(x)	There is some x for which P(x) is true.	P(x) is false for all x.

Propositional function $P(x) \overset{\text{for all/some } x \text{ in domain}}{\Longrightarrow}$ Proposition

Negation and Nest Quantifier

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 false.	$P(x)$ is true for every x.

Statement	***When True?***	***When False?***
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ 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.

Southern University of Science and Technology

Validity of Argument Form:

The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q \text{ is a tautology.}$$

Note: According to the definition of $p \rightarrow q$, we do not worry about the case where $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ is false.

Rules of Inference for Propositional Logic

Rule of Inference	*Tautology*	*Name*
p $p \rightarrow q$ $\therefore q$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism

Rules of Inference for Propositional Logic

$\begin{array}{rl} & p \\ \hline \therefore & p \vee q \end{array}$	$p \rightarrow (p \vee q)$	Addition
$\begin{array}{rl} & p \wedge q \\ \hline \therefore & p \end{array}$	$(p \wedge q) \rightarrow p$	Simplification
$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\begin{array}{rl} & p \vee q \\ & \neg p \vee r \\ \hline \therefore & q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

SUSTech Southern University of Science and Technology

Rules of Inference for Propositional Logic

Rule of Inference	*Name*
$\dfrac{\forall x P(x)}{\therefore\ P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x P(x)}$	Universal generalization
$\dfrac{\exists x P(x)}{\therefore\ P(c) \text{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x P(x)}$	Existential generalization

SUSTech Southern University of Science and Technology

Methods of Proving Theorems

A proof is a valid argument that establishes the truth of a mathematical statement.

- **Direct proof**

  $p \rightarrow q$ is proved by showing that if p is true then q follows
- **Proof by contrapositive**

  show the contrapositive $\neg q \rightarrow \neg p$
- **Proof by contradiction**

  show that $(p \wedge \neg q)$ contradicts the assumptions
- **Proof by cases**

  give proofs for all possible cases
- **Proof of equivalence**

  $p \leftrightarrow q$ is replaced with $(p \rightarrow q) \wedge (q \leftarrow p)$

Proof Exercise 1

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.)

Since $\sqrt{2} = a/b$, it follows that $2b^2 = a^2$. By the definition of an even integer, it follows that a^2 is even, so a is even (see Exercise 16).

Since a is even, $a = 2k$ for some integer k. Thus, $b^2 = 2k^2$. This implies that b^2 is even, so b is even.

As a result, a and b have a common factor 2, which contradicts our assumption.

Proof Exercise 2

Prove that there are infinitely many prime numbers.

Proof: Suppose that there are only a finite number of primes. Then, there exists a prime number p that is the largest of all the prime numbers. Also, we can list the prime numbers in ascending order: $2, 3, 5, 7, 11, ..., p$

Let $n = (2 \times 3 \times 5 \times \cdots \times p) + 1$. Then, $n > 1$, and n cannot be divided by any prime number in the list above. This means that n is also a prime.

Clearly, n is larger than all the primes in the list above. This is contrary to the assumption that all primes are in the list.

Proof Exercise 3

Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ with $x^y = \sqrt{2}^{\sqrt{2}}$ rational.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We have $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ is rational.

Note that although we do not know which case works, we know that one of the two cases has the desired property.

Lecture Schedule

1 Logic and Mathematical Proofs
2 Sets and Functions
3 Complexity of Algorithms
4 Number Theory and Cryptography
5 Mathematical Induction
6 Recursion
7 Counting
8 Relations
9 Graph
10 Trees

Sets

A set is an unordered collection of objects.

- listing (enumerating) the elements
- if enumeration is hard, use ellipses (...)
- definition by property, using the set builder

$$\{x \mid x \text{ has property } P \text{ or property } P(x))\}$$

Proof of Subset:

- Showing $A \subseteq B$: if x belongs to A, then x also belongs to B.
- Showing $A \nsubseteq B$: find a single $x \in A$ such that $x \notin B$.

Prove $A = B$?

Cardinality, Power Set, Tuples, and Cartesian Product

Cardinality: If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a finite set and n is the cardinality of S, denoted by $|S|$.

Power Set: Given a set S, the power set of S is the set of all subsets of the set S, denoted by $\mathcal{P}(S)$.

Tuples: The ordered n-tuple $(a_1, a_2, ..., a_n)$ is the ordered collection that has a_1 as its first element and a_2 as its second element and so on.

Cartesian Product: Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$:

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Set Operations

Union: Let A and B be sets. The union of the sets A and B, denoted by $A \cup B$, is the set $\{x \mid x \in A \vee x \in B\}$.

Intersection: The intersection of the sets A and B, denoted by $A \cap B$, is the set $\{x \mid x \in A \wedge x \in B\}$.

Complement: If A is a set, then the complement of the set A (with respect to U), denoted by $\bar{A}$ is the set $U - A$, $\bar{A} = \{x \in U \mid x \notin A\}$

Difference: Let A and B be sets. The difference of A and B, denoted by $A - B$, is the set containing the elements of A that are not in B. $A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \bar{B}$.

Principle of inclusion–exclusion: $|A \cup B| = |A| + |B| - |A \cap B|$

Set Identities

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

Set Identities

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

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

A	B	$\overline{A}$	$\overline{B}$	$\overline{A \cap B}$	$\overline{A} \cup \overline{B}$
1	1	0	0	0	0
1	0	0	1	1	1
0	1	1	0	1	1
0	0	1	1	1	1

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

- $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:
    - Suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, $\neg((x \in A) \wedge (x \in B))$ is true.
    - By applying De Morgan's law, $\neg(x \in A) \vee \neg(x \in B))$. Thus, $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, $x \in \bar{A}$ or $x \in \bar{B}$.
    - By the definition of union, we see that $x \in \bar{A} \cup \bar{B}$.Thus, $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.
- $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: using membership tables.
Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$
Proof 3: Using set builder and logical equivalences

$$\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement} \\
&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol} \\
&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection} \\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences} \\
&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol} \\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} && \text{by definition of complement} \\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} && \text{by definition of union} \\
&= \overline{A} \cup \overline{B} && \text{by meaning of set builder notation}
\end{aligned}$$

Function

Let A and B be two sets. A function from A to B, denoted by $f : A \to B$, is an assignment of exactly one element of B to each element of A.

- **One-to-one (injective) function**:
  - A function f is called one-to-one or injective if and only if $f(x) = f(y)$ implies $x = y$ for all x, y in the domain of f.
- **Onto (surjective) function**:
  - A function f is called onto or surjective if and only if for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$.
- **One-to-one (bijective) correspondence**
  - One-to-one and onto

Proof for One-to-One and Onto

Suppose that $f : A \to B$.

To show that f is *injective*	Show that if $f(x) = f(y)$ for all $x, y \in A$, then $x = y$
To show that f is not *injective*	Find specific elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is *surjective*	Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$
To show that f is not *surjective*	Find a specific element $y \in B$ such that $f(x) \neq y$ for all $x \in A$

Inverse Function and Composition of Functions

Inverse function: Let f be a one-to-one correspondence (bijection) from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.

Let f be a function from B to C and let g be a function from A to B. The composition of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(x) = f(g(x))$.

The floor function assigns a real number x the largest integer that is $\leq x$, denoted by $\lfloor x \rfloor$. E.g., $\lfloor 3.5 \rfloor = 3$.

The ceiling function assigns a real number x the smallest integer that is $\geq x$, denoted by $\lceil x \rceil$. E.g., $\lceil 3.5 \rceil = 4$.

Sequences

A sequence is a function from a subset of the set of integers (typically the set $\{0, 1, 2, \dots\}$ or $\{1, 2, 3, \dots\}$) to a set S.

We use the notation a_n to denote the image of the integer n. $\{a_n\}$ represents the ordered list $\{a_1, a_2, a_3, \dots\}$

Recursively Defined Sequences: provide

- One or more initial terms
- A rule for determining subsequent terms from those that precede them.

Cardinality of Sets

A set that is either finite or has the same cardinality as the set of positive integers $\mathbf{Z}^+$ is called countable.

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, denoted by $|A| \leq |B|$.

Theorem: If there is a one-to-one correspondence between elements in A and B, then the sets A and B have the same cardinality.

Theorem: If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Lecture Schedule

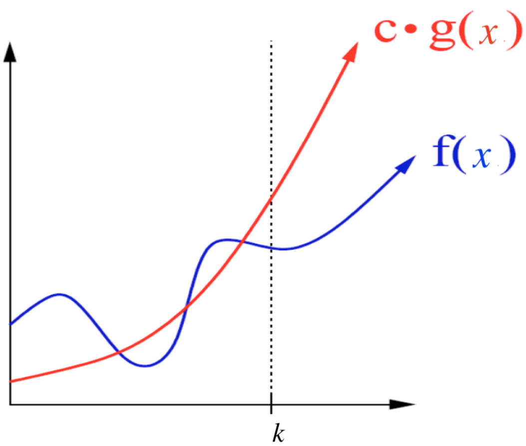
1 Logic and Mathematical Proofs
2 Sets and Functions
3 Complexity of Algorithms
4 Number Theory and Cryptography
5 Mathematical Induction
6 Recursion
7 Counting
8 Relations
9 Graph
10 Trees

Big-O Notation

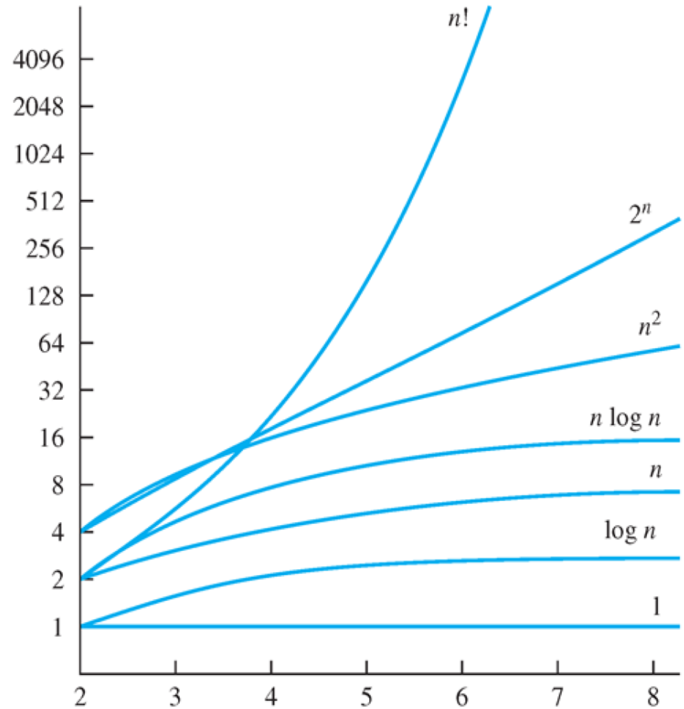
Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers.We say that $f(x)$ is $O(g(x))$ if there are constants C and k such that

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

whenever $x > k$. [This is read as "$f(x)$ is big-oh of $g(x)$."]



Big-O Estimates for Some Functions



Big-Omega Notation

Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers.We say that $f(x)$ is $\Omega(g(x))$ if there are positive constants C and k such that

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

whenever $x > k$. [This is read as "$f(x)$ is big-Omega of $g(x)$."]

Let f and g be functions from the set of integers or the set of 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 $\Omega(g(x))$.

When $f(x)$ is $\Theta(g(x))$, we say that $f(x)$ is big-Theta of $g(x)$, that $f(x)$ is of order $g(x)$, and that $f(x)$ and $g(x)$ are of the same order.

Lecture Schedule

Division

Divisibility: We say that a divides b if there is an integer c such that $b = ac$, or equivalently b/a is an integer.

- If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb + nc)$ whenever m and n are integers.

Congruence Relation: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$, denoted by $a \equiv b \pmod{m}$.

The integers a and b are congruent modulo m if and only if there is an integer k such that

$$a = b + km$$

.

Congruence: Properties

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

Corollary: Let m be a positive integer and let a and b be integers. Then,

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Primes

A integer p that is greater than 1 is called a prime if the only positive factors of p are 1 and p.

- If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Let a and b be integers, not both 0. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, denoted by $\gcd(a,b)$. Let $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$. Then,

$$\gcd(a,b) = p^{\min(a_1,b_1)} p^{\min(a_2,b_2)} \ldots p^{\min(a_n,b_n)}$$

The least common multiple of a and b is the smallest positive integer that is divisible by both a and b, denoted by $\operatorname{lcm}(a,b)$.Let $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$. Then,

$$\operatorname{lcm}(a,b) = p^{\max(a_1,b_1)} p^{\max(a_2,b_2)} \ldots p^{\max(a_n,b_n)}.$$

Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations can be time consuming since we need to find all factors of the two integers.

For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

GCD as Linear Combinations

Bezout'S Theorem: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

This equation is called Bezout's identity.

We can use extended Euclidean algorithm to find Bezout's identity.

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Lemma: If p is prime and $p|a_1a_2...a_n$, then $p|a_i$ for some i.

Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

Solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

$$x \equiv \bar{a}b \pmod{m}.$$

Modular Inverse

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

When does inverse exist?

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m. That is,

- there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and
- every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.

If we obtain an arbitrary inverse of a modulo m, how to obtain the inverse that is less than m?

Modular Inverse

How to find inverses?

Using extended Euclidean algorithm:

Example: Find an inverse of 101 modulo 4620. That is, find $\bar{a}$ such that $\bar{a} \cdot 101 \equiv 1 \pmod{4620}$.

With extended Euclidean algorithm, we obtain $\gcd(a, b) = sa + tb$, i.e., $1 = -35 \cdot 4620 + 1601 \cdot 101$. It tells us that -35 and 1601 are Bezout coefficients of 4620 and 101. We have

$$1 \bmod 4620 = 1601 \cdot 101 \bmod 4620.$$

Thus, 1601 is an inverse of 101 modulo 4620.

The Chinese Remainder Theorem

Theorem (The Chinese Remainder Theorem): Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots,$ a_n arbitrary integers. Then, the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$.
(That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

The Chinese Remainder Theorem: Example

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

1 Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2 Compute y_k, i.e., the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1 \pmod 3$ $y_1 = 2$
   - $21 \equiv 1 \pmod 5$ $y_2 = 1$
   - $15 \equiv 1 \pmod 7$ $y_3 = 1$
3 Compute a solution $x = a_1 M_1 y_1 + \ldots + a_n M_n y_n$:
   $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$
4 The solutions are all integers x that satisfy $x \equiv 23 \pmod{105}$.

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

Example:

(1) $x \equiv 1 \pmod 5$
(2) $x \equiv 2 \pmod 6$
(3) $x \equiv 3 \pmod 7$

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2 \pmod 6$, which means that $t \equiv 5 \pmod 6$. Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3 \pmod 7$, which implies that $u \equiv 6 \pmod 7$. Thus, $u = 7v + 6$, where v is an integer.

Thus, we must have $x = 210v + 206$. Translating this back into a congruence,

$$x \equiv 206 \pmod{210}.$$

Fermat's Little Theorem

FERMAT'S LITTLE THEOREM If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer a we have

$$a^{p} \equiv a \pmod{p}.$$

RAS Cryptosystem

Pick two large primes p and q. Let $n = pq$. **Encryption key** (n, e) and **decryption key** (n, d) are selected such that

(1) $\gcd(e, (p-1)(q-1)) = 1$

(2) $ed \equiv 1 \pmod{(p-1)(q-1)}$

RSA encryption: $C = M^e \bmod n$;
RSA decryption: $M = C^d \bmod n$.

Lecture Schedule

The Principle of Mathematical Induction

Well-Ordering Property: Every nonempty set of nonnegative integers has a least element.

Principle. (Weak Principle of Mathematical Induction)

(a) Basic Step: the statement $P(b)$ is true

(b) Inductive Step: the statement $P(n-1) \rightarrow P(n)$ is true for all $n > b$

Thus, $P(n)$ is true for all integers $n \geq b$.

Principle (Strong Principle of Mathematical Induction):

(a) Basic Step: the statement $P(b)$ is true

(b) Inductive Step: for all $n > b$, the statement

$$P(b) \land P(b+1) \land \ldots \land P(n-1) \rightarrow P(n) \text{ is true.}$$

Then, $P(n)$ is true for all integers $n \geq b$.

Lecture Schedule

Recurrence

To specify a function on the basis of a recurrence:

- Basis step (initial condition): Specify the value of the function at zero.
- Recursive step: Give a rule for finding its value at an integer from its values at smaller integers.

Find a closed-form solution? "Top-down" and "bottom-up"

$$
\begin{aligned}
T(n) &= rT(n-1)+a \\
&= r(rT(n-2)+a)+a \\
&= r^2T(n-2)+ra+a \\
&= r^2(rT(n-3)+a)+ra+a \\
&= r^3T(n-3)+r^2a+ra+a \\
&= r^3(rT(n-4)+a)+r^2a+ra+a \\
&= r^4T(n-4)+r^3a+r^2a+ra+a.
\end{aligned}
$$

Recurrence

To specify a function on the basis of a recurrence:

- Basis step (initial condition): Specify the value of the function at zero.
- Recursive step: Give a rule for finding its value at an integer from its values at smaller integers.

Find a closed-form solution? "Top-down" and "bottom-up"

$$\begin{aligned}
&T(0) = b \\
&T(1) = rT(0) + a = rb + a \\
&T(2) = rT(1) + a = r(rb + a) + a = r^2 b + ra + a \\
&T(3) = rT(2) + a = r^3 b + r^2 a + ra + a
\end{aligned}$$

Mathematical induction.

Lecture Schedule

1 Logic
2 Mathematical Proofs
3 Sets and Functions
4 Complexity of Algorithms
5 Number Theory
6 Cryptography
7 Mathematical Induction
8 Recursion
9 Counting
10 Relations
11 Graph
12 Trees

Counting

Product Rule: If a count of elements can be broken down into a sequence of dependent counts where the first count yields n_1 elements, the second n_2 elements, and k-th count n_k elements, then the total number of elements is

$$n = n_1 \times n_2 \times \ldots \times n_k$$

Sum Rule:

- A task can be done either in one of n_1 ways or in one of n_2 ways
- None of the set of n_1 ways is the same as any of the set of n_2 ways

The Subtraction Rule:

- A task can be done in either n_1 ways or n_2 ways
- **Principle of inclusion–exclusion**:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Pigeonhole Principle

Assume that there are a set of objects and a set of bins to store them.

The 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.

If N objects are placed into k bins, then there is at least one bin containing at least $\lceil N/k \rceil$ objects.

Permutations and Combinations

Theorem: If n is a positive integer and r is an integer with $1 \leq r \leq n$, then there are

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

r-permutations of a set with n distinct elements.

Theorem: For integers n and r with $0 \leq r \leq n$, the number of r-element subsets of an n-element set is

$$\binom{n}{r} = C(n, r) = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}$$

Combinatorial Proof

Theorem: Let n and r be nonnegative integers with $r \leq n$. Then $C(n, r) = C(n, n-r)$.

Definition: A combinatorial proof of an identity is

- a proof that uses counting arguments to prove that both sides of the identity count the same objects but in different ways
- or a proof that is based on showing that there is a bijection between the sets of objects counted by the two sides of the identity.

These two types of proofs are called double counting proofs and bijective proofs, respectively.

The Binomial Theorem

Let x and y be variables, and let n be a nonnegative integer:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

Corollary: Let n be a nonnegative integer,

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

Theorem: Let n and k be positive integers with $n \geq k$. Then,

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

Labelling and Trinomial Coefficients

If we have k_1 labels of one kind (e.g., red), k_2 labels of a second kind (e.g., blue), and $k_3 = n - k_1 - k_2$ labels of a third kind (e.g., green).

How many different ways to label n distinct objects?

$$\begin{aligned}\binom{n}{k_1}\binom{n-k_1}{k_2} &= \frac{n!}{k_1!(n-k_1)!}\frac{(n-k_1)!}{(k_2)!(n-k_1-k_2)!} \\ &= \frac{n!}{k_1!k_2!(n-k_1-k_2)!} = \frac{n!}{k_1!k_2!k_3!}\end{aligned}$$

This is called a trinomial coefficient and denote it as

$$\binom{n}{k_1 \quad k_2 \quad k_3} = \frac{n!}{k_1!k_2!k_3!},$$

where $k1 + k2 + k3 = n$.

Solving Linear Homogeneous Recurrence Relations

Definition: A linear homogeneous relation of degree k with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

By induction, such a recurrence relation is uniquely determined by this recurrence relation and k initial conditions $a_0, a_1, \ldots, a_{k-1}$.

Solving Linear Homogeneous Recurrence Relations

The characteristic equation (CE) is:

$$r^k - \sum_{i=1}^{k} c_i r^{k-i} = 0.$$

Theorem: Suppose that there are t roots $r_1, \ldots, r_t$ with multiplicities $m_1, \ldots, m_t$. Then,

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

- Solving the roots with CE
- Solving the α_i for all i using initial conditions

Linear Nonhomogeneous Recurrence Relations

Definition: A linear nonhomogeneous relation with constant coefficients may contain some terms $F(n)$ that depend only on n

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} + F(n).$$

The recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$ is called the associated homogeneous recurrence relation.

Theorem: If $\{a_n^{(p)}\}$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} + F(n),$$

Then all its solutions are of the form

$$a_n = a_n^{(p)} + a_n^{(h)},$$

where $\{a_n^{(h)}\}$ is any solution to the associated homogeneous recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$.

Linear Nonhomogeneous Recurrence Relations

Suppose that $\{a_n\}$ satisfies the linear nonhomogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and

$$F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n,$$

where $b_0, b_1, \ldots, b_t$ and s are real numbers. When s is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form

$$(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

When s is a root of this characteristic equation and its multiplicity is m, there is a particular solution of the form

$$n^m (p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

Linear Nonhomogeneous Recurrence Relations

Find all solutions of the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2} + 7^n$.

Solution:

- $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$
- Let $a_n^{(p)} = C \cdot 7^n$:

$$C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n.$$

  Thus, $C = 49/20$, and $a_n^{(p)} = (49/20)7^n$.

- Solve α_i in $a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + (49/20)7^n$ using initial conditions.

Generalized Permutations and Combinations

- Permutations with repetition

  Repetition: Distinct objects; each can be selected multiple times

  Theorem: The number of r-permutations of a set of n objects with repetition allowed is n^r.

- Permutations with indistinguishable objects

  Indistinguishable objects: E.g., "SUCCESS"

  Theorem: 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, is

$$C(n, n_1)(n - n_1, n_2) \cdots C(n - n_1 - \cdots n_{k-1}, n_k) = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

- Combinations with repetition

Combinations with Repetition

Example: How many ways are there to select five bills from a cash box containing \$1 bills, \$2 bills, \$5 bills, \$10 bills, \$20 bills, \$50 bills, and \$100 bills?

Theorem: There are $C(n+r-1, r) = C(n+r-1, n-1)$ r-combinations from a set with n elements when repetition of elements is allowed.