Discrete Mathematics and Its Applications

Lecture 8: Summarization

MING GAO

DaSE@ECNU
(for course related communications)
mgao@sei.ecnu.edu.cn

Jan. 10, 2019

Outline

1. Introduction
2. The Foundations: Logic and Proofs
3. Basic Structures
4. Counting
5. Advanced Counting
6. Discrete Probability
7. Relations
8. Graphs

The goals of this course

There are three goals:

- To learn how to make mathematical arguments.
- To learn various fundamental mathematical concepts that are very useful in computer science.
- To learn how to model a real problem in mathematical manner.

Proposition

Definition

A *proposition* is a **statement** which is either **true** or **false**.

Proposition

Definition

A *proposition* is a **statement** which is either **true** or **false**.

Connectives

- **Negation (not)**: $\neg$ (unary connective)
- **Conjunction (and)**: $\wedge$ (binary connective)
- **Disjunction (or)**: $\vee$ (binary connective)
- **Exclusive or**: $\oplus$ (binary connective)
- **Implication (if $\cdots$, then)**: $\rightarrow$ (binary connective)
- **Biconditional (if and only if)**: $\leftrightarrow$ (binary connective)

Based on the atomic propositions and connectives, we can obtain compound propositions.

Logical equivalences I

Definition

Compound propositions that have the same truth values in all possible cases are called **logically equivalent**.

equivalence	name
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$	Commutative laws
$(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$	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
$\neg(\neg p) \equiv p$	Double negation law

Logical equivalences II

equivalence	name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \wedge p \equiv p$ $p \vee p \equiv p$	Idempotent laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \wedge \neg p \equiv F$ $p \vee \neg p \equiv T$	Negation laws

Logical equivalences II

equivalence	name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \wedge p \equiv p$ $p \vee p \equiv p$	Idempotent laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \wedge \neg p \equiv F$ $p \vee \neg p \equiv T$	Negation laws

Question: How to show that two propositions are logical equivalences?

Logical equivalences II

equivalence	name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \wedge p \equiv p$ $p \vee p \equiv p$	Idempotent laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \wedge \neg p \equiv F$ $p \vee \neg p \equiv T$	Negation laws

Question: How to show that two propositions are logical equivalences?

Solution: Truth table or logical operations.

Predicates and quantifiers

Definition

In general, a statement involving n variables $x_1, x_2, \cdots, x_n$ can be denoted by $P(x_1, x_2, \cdots, x_n)$, where P is also called an n-place predicate or a n-ary predicate, and $x_1, x_2, \cdots, x_n$ is a n-tuple.

Predicates and quantifiers

Definition

In general, a statement involving n variables $x_1, x_2, \cdots, x_n$ can be denoted by $P(x_1, x_2, \cdots, x_n)$, where P is also called an n-place predicate or a n-ary predicate, and $x_1, x_2, \cdots, x_n$ is a n-tuple.

Quantification

Quantification expresses the extent to which a predicate is true over a range of elements. In general, all values of a variable is called the *domain of discourse* (or *universe of discourse*), just referred to as *domain*.

Statement	When True?	When False?
$\forall x P(x)$	$P(x)$ is true for every x	$\exists x$ for which $P(x)$ is false
$\exists x P(x)$	$\exists x$ for which $P(x)$ is true	$P(x)$ is false for every x

Argument and valid argument

Definition

An *argument* in propositional logic is a sequence of propositions. All but the final proposition in the argument are called *premises* or *hypotheses* and the final proposition is called the *conclusion*.

Argument and valid argument

Definition

An *argument* in propositional logic is a sequence of propositions. All but the final proposition in the argument are called *premises* or *hypotheses* and the final proposition is called the *conclusion*.

- We say that the statement is *valid* if when all hypotheses are true, the conclusion must be true as well.

Argument and valid argument

Definition

An *argument* in propositional logic is a sequence of propositions. All but the final proposition in the argument are called *premises* or *hypotheses* and the final proposition is called the *conclusion*.

- We say that the statement is *valid* if when all hypotheses are true, the conclusion must be true as well.
- More precisely, to show that conclusion q logically follows from hypotheses $p_1, p_2, \cdots, p_n$, we need to show that

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \rightarrow q$$

  is always true, i.e., is a tautology.
  That is

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q.$$

Inference rules

Modus ponens

$$\begin{array}{l} \quad p \\ \quad p \to q \\ \hline \therefore q \end{array}$$

$(p \wedge (p \to q)) \to q$

Modus tollens

$$\begin{array}{l} \quad \neg q \\ \quad p \to q \\ \hline \therefore \neg p \end{array}$$

$(\neg q \wedge (p \to q)) \to \neg p$

Hypothetical syllogism

$$\begin{array}{l} \quad p \to q \\ \quad q \to r \\ \hline \therefore p \to r \end{array}$$

$((p \to q) \wedge (q \to r)) \to (p \to r)$

Disjunction syllogism

$$\begin{array}{l} \quad p \vee q \\ \quad \neg p \\ \hline \therefore q \end{array}$$

$(p \vee q) \wedge \neg p \to q$

Inference rules Cont'd

Addition

$$\frac{p}{\therefore p \vee q}$$

$p \rightarrow p \vee q$

Simplification

$$\frac{p \wedge q}{\therefore p}$$

$p \wedge q \rightarrow p$

Conjunction

$$\frac{\begin{matrix} p \\ q \end{matrix}}{\therefore p \wedge q}$$

$p \wedge q \rightarrow p \wedge q$

Resolution

$$\frac{\begin{matrix} p \vee q \\ \neg p \vee r \end{matrix}}{\therefore q \vee r}$$

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

Inference rules for quantified statements

Universal instantiation

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal generalization

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Existential instantiation

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element}}$$

Existential generalization

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(c)}$$

Inference rules for quantified statements

Universal instantiation

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal generalization

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Existential instantiation

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element}}$$

Existential generalization

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(c)}$$

Question

How to show that an argument is valid?

Inference rules for quantified statements

Universal instantiation

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal generalization

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Existential instantiation

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element}}$$

Existential generalization

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(c)}$$

Question

How to show that an argument is valid?

- Logical inference;
- Truth table;
- Logical operations.

Proofs

Using inference rules, we can prove facts in propositional logic. However, in many cases, we want to prove wider range of mathematical facts. Inference rules play crucial parts in providing high-level structures for our proofs.

Proofs

Using inference rules, we can prove facts in propositional logic. However, in many cases, we want to prove wider range of mathematical facts.

Inference rules play crucial parts in providing high-level structures for our proofs.

In this lecture, we will focus on two general proof techniques that originate from five simple inference rules.

- Direct proofs
- Proofs by contraposition
- Proofs by contradiction
- Proofs by cases
- Mathematical induction

Set

Definition

Set A is a collection of objects (or elements).

- Bag of words model: documents, reviews, tweets, news, etc;
- Transactions: shopping list, app downloading, etc;
- Neighbors of a vertex in a graph;

Set

Definition

Set A is a collection of objects (or elements).

- Bag of words model: documents, reviews, tweets, news, etc;
- Transactions: shopping list, app downloading, etc;
- Neighbors of a vertex in a graph;

Operators

Let A and B be two sets, and U be the universal set

- Union: $A \cup B = \{x : x \in A \vee x \in B\}$;
- Intersection: $A \cap B = \{x : x \in A \wedge x \in B\}$;
- Difference: $A - B = \{x : x \in A \wedge x \notin B\}$ (or $A \setminus B$);
- Complement: $\overline{A} = U - A = \{x \in U : x \notin A\}$;
- Cartesian product: $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.

Function

Definition

Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to *each element* of A.

If f is a function from A to B, we say that A is the *domain* of f and B is the *codomain* of f. If $f(a) = b$, we say that b is the *image* of a and a is a *preimage* of b.

Function

Definition

Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to *each element* of A.
If f is a function from A to B, we say that A is the *domain* of f and B is the *codomain* of f. If $f(a) = b$, we say that b is the *image* of a and a is a *preimage* of b.

Operations

Let f_1 and f_2 be functions from A to R.

- Add: $(f_1 + f_2)(x) = f_1(x) + f_2(x)$;
- Product: $(f_1 f_2)(x) = f_1(x) f_2(x)$;
- Projection: $f(S) = \{t | \forall s \in S \subset A, t = f(s)\}$;
- Composition: $(f \circ g)(a) = f(g(a))$;
- Inverse: $f^{-1}(b) = a$ when $f(a) = b$.

Types of functions

A function f from A to B

- **One-to-one (injunction)**: iff $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.
- **Onto (surjection)**: iff $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.
- **One-to-one correspondence (bijective)**: iff it is both one-to-one and onto.

Types of functions

A function f from A to B

- **One-to-one (injunction)**: iff $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.
- **Onto (surjection)**: iff $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.
- **One-to-one correspondence (bijective)**: iff it is both one-to-one and onto.

Monotonicity

A function f whose domain and codomain are subsets of the set of real numbers is called increasing if $f(x) \leq f(y)$, and strictly increasing if $f(x) < f(y)$, whenever $x < y$ and x and y are in the domain of f. Similarly, we can define decreasing and strictly decreasing function.

Some important functions

- Floor function: it assigns to a real number x the largest integer that is less than or equal to x, denoted by $\lfloor x \rfloor$;
- Ceiling function: it assigns to a real number x the smallest integer that is greater than or equal to x, denoted by $\lceil x \rceil$;
- Indicator function: it is a function on set S related to the set $A \subset S$, denoted as

$$I_A : X \to \{0, 1\},$$

  For $x \in S$, it's value is defined as

$$I_A(x) := \begin{cases} 1, & \text{if } x \in A; \\ 0, & \text{else.} \end{cases}$$

- Sigmoid functions: it has a characteristic "S"-shaped curve or sigmoid curve, such as $S(x) = \frac{1}{1+e^{-x}}$, etc.

Cardinality

Definition

Sets A and B have the same cardinality if and only if there is a one-to-one correspondence from A to B. When A and B have the same cardinality, we write $|A| = |B|$.

- Countable sets: either finite or has the same cardinality as Z^+, such as $\{1, 2, 3\}$, N, Z, Q, etc;
- Uncountable sets: $[0, 1], R$, etc;
- If A and B are countable sets, then $A \cup B$ is also countable.

Matrix

Definition

An $m \times n$ matrix $A = (a_{ij})$ $(1 \leq i \leq m, 1 \leq j \leq n)$ is a rectangular array of mn scalars in m rows and n columns, such as

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

The i-th row of A is the $1 \times n$ matrix $[a_{i1}, a_{i2}, \cdots, a_{in}]$. The $j-$th column of A is the $m \times 1$ matrix $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \cdots \\ a_{mj} \end{pmatrix}$.

Operations of matrix

Operations

- Addition: Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $m \times n$ matrices, $A + B = (a_{ij} + b_{ij})$
  - $A + cB = (a_{ij} + cb_{ij})$, where $c \in R$
  - $A + B = B + A$
  - $A + (B + C) = (A + B) + C$
- Manipulation: If A is an $n \times m$ matrix and B is an $m \times p$ matrix, then $AB = (\sum_{k=1}^{m} a_{ik} b_{kj})$
  - Not commutative: $AB \neq BA$
  - Distributive over matrix addition: $(A + B)C = AC + BC$
  - Scalar multiplication is compatible with matrix multiplication: $\lambda AB = (\lambda A)B = A(\lambda B)$
  - $(AB)^T = B^T A^T$
  - Power: $A^0 = I_n, A^k = \underbrace{AA \cdots A}_{k \text{ times}}$

Zero-one matrices

Operations

A matrix all of whose entries are either 0 or 1 is called a zero-one matrix.

- $\wedge$: $A \wedge B = [a_{ij} \wedge b_{ij}]$;
- $\vee$: $A \vee B = [a_{ij} \vee b_{ij}]$;
- $\bigodot$: $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

$$A \bigodot B = \begin{pmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Counting principle I

Product rule

Suppose that a procedure consists of a sequence of two tasks. If there are n_1 ways to do the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Counting principle I

Product rule

Suppose that a procedure consists of a sequence of two tasks. If there are n_1 ways to do the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Extended version: A procedure is followed by tasks $T_1, T_2, \cdots, T_m$ in sequence. If each task T_i can be done in n_i ways independently, then there are $n_1 \cdot n_2 \cdot \cdots \cdot n_m$ ways to carry out the procedure.

Counting principle I

Product rule

Suppose that a procedure consists of a sequence of two tasks. If there are n_1 ways to do the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Extended version: A procedure is followed by tasks $T_1, T_2, \cdots, T_m$ in sequence. If each task T_i can be done in n_i ways independently, then there are $n_1 \cdot n_2 \cdot \cdots \cdot n_m$ ways to carry out the procedure.

Sum rule

If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Counting principle I

Product rule

Suppose that a procedure consists of a sequence of two tasks. If there are n_1 ways to do the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Extended version: A procedure is followed by tasks $T_1, T_2, \cdots, T_m$ in sequence. If each task T_i can be done in n_i ways independently, then there are $n_1 \cdot n_2 \cdot \cdots \cdot n_m$ ways to carry out the procedure.

Sum rule

If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Extended version: A procedure can be done by m ways, each way W_i has n_i possibilities (not intersect), then there are $n_1 + n_2 + \cdots + n_m$ ways to carry out the procedure.

Counting principle II

Subtraction rule

There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.

Counting principle II

Subtraction rule

There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.

Subtraction rule

If a task can be done in either n_1 ways or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways. The rule is also called the principle of **inclusion-exclusion**, i.e.,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Permutations and combinations

Permutations

An ordered arrangement of m elements of a set is called an m-permutation. # m-permutations of a set with n distinct elements is

$$P(n,m) = n(n-1)(n-2)\cdot\dots\cdot(n-m+1) = \frac{n!}{(n-m)!}.$$

Permutations and combinations

Permutations

An ordered arrangement of m elements of a set is called an m-permutation. $\#$ m-permutations of a set with n distinct elements is

$$P(n,m) = n(n-1)(n-2)\cdot\cdots\cdot(n-m+1) = \frac{n!}{(n-m)!}.$$

Combinations

An m-combination of elements of a set is an unordered selection of m elements from the set. $\#$ m-combinations of a set with n elements equals

$$C(n,m) = \frac{n!}{m!(n-m)!},$$

where $C(n,m)$ is also denoted as $\binom{n}{m}$.

Applications

Counting functions

- How many functions are there from set A with m elements to set B with n elements?
- How many one-to-one functions are there from a set with m elements to one with n elements?
- How many onto functions are there from a set with six elements to a set with three elements?

Applications

Counting functions

- How many functions are there from set A with m elements to set B with n elements?
- How many one-to-one functions are there from a set with m elements to one with n elements?
- How many onto functions are there from a set with six elements to a set with three elements?

Derangement

A derangement is a permutation of objects that leaves no object in its original position. # derangements of a set with n elements is

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

$$D_n = (n-1)(D_{n-2} + D_{n-1}), \text{ with } D_1 = 0, D_2 = 1.$$

Distributing objects into boxes and the pigeonhole principle

- Distinguishable objects and distinguishable boxes
- Indistinguishable objects and distinguishable boxes
- Distinguishable objects and indistinguishable boxes
- Indistinguishable objects and indistinguishable boxes

Distributing objects into boxes and the pigeonhole principle

- Distinguishable objects and distinguishable boxes
- Indistinguishable objects and distinguishable boxes
- Distinguishable objects and indistinguishable boxes
- Indistinguishable objects and indistinguishable boxes

The pigeonhole principle

If we put $n+1$ objects into n boxes, at least one box gets more than one objects (also called Dirichlet drawer principle).

Distributing objects into boxes and the pigeonhole principle

- Distinguishable objects and distinguishable boxes
- Indistinguishable objects and distinguishable boxes
- Distinguishable objects and indistinguishable boxes
- Indistinguishable objects and indistinguishable boxes

The pigeonhole principle

If we put $n+1$ objects into n boxes, at least one box gets more than one objects (also called Dirichlet drawer principle).

The generalized pigeonhole principle

Theorem: If N objects are placed into k boxes, then there is at least one box containing at least $\lceil \frac{N}{k} \rceil$ objects.

The binomial coefficient

Theorem

If you expand $(x+y)^n$, the coefficient of the term $x^k y^{n-k}$ is $\binom{n}{k}$. That is,

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

$$\binom{n}{n} x^n + \binom{n}{n-1} x^{n-1} y^1 + \binom{n}{n-2} x^{n-2} y^2 + \cdots + \binom{n}{1} x y^{n-1} + \binom{n}{0} y^n.$$

The binomial coefficient

Theorem

If you expand $(x+y)^n$, the coefficient of the term $x^k y^{n-k}$ is $\binom{n}{k}$. That is,

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

$$\binom{n}{n} x^n + \binom{n}{n-1} x^{n-1} y^1 + \binom{n}{n-2} x^{n-2} y^2 + \cdots + \binom{n}{1} x y^{n-1} + \binom{n}{0} y^n.$$

Equations

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

The binomial coefficient

Theorem

If you expand $(x+y)^n$, the coefficient of the term $x^k y^{n-k}$ is $\binom{n}{k}$. That is,

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

$$\binom{n}{n} x^n + \binom{n}{n-1} x^{n-1} y^1 + \binom{n}{n-2} x^{n-2} y^2 + \cdots + \binom{n}{1} x y^{n-1} + \binom{n}{0} y^n.$$

Equations

- $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots = 0$;
- $\sum_{k=0}^{n} \binom{n}{k} 2^k = 3^n$;
- $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$;
- $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \binom{n}{k}$;
- $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$;
- $\binom{n+1}{r+1} = \sum_{k=r}^{n} \binom{k}{r}$;

Recurrence relations

Instead of defining the value of each number in the sequence explicitly, we do so by using the values of other numbers in the sequence, the relation is called a **recurrence relation**.

- Fibonacci sequence $F_n = F_{n-1} + F_{n-2}$ with $n \geq 2$;
  - $F_0 + F_1 + \cdots + F_n = F_{n+2} - 1$;
  - $F_n^2 + F_{n-1}^2 = F_{2n-1}$;
- The Tower of Hanoi

Recurrence relations

Instead of defining the value of each number in the sequence explicitly, we do so by using the values of other numbers in the sequence, the relation is called a **recurrence relation**.

- Fibonacci sequence $F_n = F_{n-1} + F_{n-2}$ with $n \geq 2$;
  - $F_0 + F_1 + \cdots + F_n = F_{n+2} - 1$;
  - $F_n^2 + F_{n-1}^2 = F_{2n-1}$;
- The Tower of Hanoi

Dynamic programming and recurrence relation

Methods are applied to solve complex problems by breaking them down into simpler subproblems

1. Define subproblems;
2. Write down the recurrence that relates subproblems;
3. Recognize and solve the base cases.

LHR^2 and LNR^2

Given a recurrence relation

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

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

- It is a **linear homogeneous recurrence relation** (shorted in LHR^2) of degree k with constant coefficients if $F(n) = 0$.
- It is a **linear nonhomogeneous recurrence relation** (shorted in LNR^2) with constant coefficients of degree k is a recurrence relation if $F(n) \neq 0$.

Solving LHR^2 with constant coefficients

Let $c_1, c_2, \cdots, c_k$ be real numbers $c_k \neq 0$. Suppose that characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has t distinct roots r_i with multiplicities m_i (for $i = 1, 2, \cdots, t$), respectively. Then sequence $\{a_n\}$ is a solution of recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ if and only if

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

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

Solution for LNR^2

If $\{a_n^{(p)}\}$ is a particular solution of LNR^2 with constant coefficients

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

then every solution is of the form $\{a_n^{(p)} + a_n^{(h)}\}$, where $\{a_n^{(h)}\}$ is a solution of LHR^2 $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$.

Solution for LNR^2

If $\{a_n^{(p)}\}$ is a particular solution of LNR^2 with constant coefficients

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

then every solution is of the form $\{a_n^{(p)} + a_n^{(h)}\}$, where $\{a_n^{(h)}\}$ is a solution of LHR^2 $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$.

Forms of the particular solutions

In the above LNR^2, let $F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n$, where $b_0, b_1, \cdots, b_t$ and s are real numbers. $\{a_n^{(p)}\}$ can be

Solution for LNR^2

If $\{a_n^{(p)}\}$ is a particular solution of LNR^2 with constant coefficients

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

then every solution is of the form $\{a_n^{(p)} + a_n^{(h)}\}$, where $\{a_n^{(h)}\}$ is a solution of LHR^2 $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$.

Forms of the particular solutions

In the above LNR^2, let $F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n$, where $b_0, b_1, \cdots, b_t$ and s are real numbers. $\{a_n^{(p)}\}$ can be

- $(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n$ if s is not a root of the characteristic equation of the associated LHR^2

Solution for LNR^2

If $\{a_n^{(p)}\}$ is a particular solution of LNR^2 with constant coefficients

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

then every solution is of the form $\{a_n^{(p)} + a_n^{(h)}\}$, where $\{a_n^{(h)}\}$ is a solution of LHR^2 $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$.

Forms of the particular solutions

In the above LNR^2, let $F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n$, where $b_0, b_1, \cdots, b_t$ and s are real numbers. $\{a_n^{(p)}\}$ can be

- $(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n$ if s is not a root of the characteristic equation of the associated LHR^2
- $n^m (p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n$ if s is a root of multiplicity m.

Divide-and-Conquer recurrence relations

The divide-and-conquer strategy solves a problem P by:

1. Breaking P into subproblems that are themselves smaller instances of the same type of problem (Divide step);
2. Recursively solving these subproblems (Solve step);
3. Appropriately combining their answers (Conquer step).

Divide-and-Conquer recurrence relations

The divide-and-conquer strategy solves a problem P by:

1. Breaking P into subproblems that are themselves smaller instances of the same type of problem (Divide step);
2. Recursively solving these subproblems (Solve step);
3. Appropriately combining their answers (Conquer step).

The real work to implement Divide-and-Conquer strategy is done piecemeal, where the key works lay in three different places:

1. How to partition problem into subproblems;
2. At the very tail end of the recursion, how to solve the smallest subproblems outright;
3. How to glue together the partial answers.

Solution for DCR^2

Theorem

Let f be an increasing function that satisfies the recurrence relation

$$f(n) = af(n/b) + c$$

whenever n is divisible by b, where $a \geq 1$, b is an integer greater than 1, and c is a positive real number. Then

$$f(n) \text{ is } \begin{cases} O(n^{\log_b a}), & \text{if } a > 1; \\ O(\log n), & \text{if } a = 1. \end{cases}$$

Solution for DCR^2

Theorem

Let f be an increasing function that satisfies the recurrence relation

$$f(n) = af(n/b) + c$$

whenever n is divisible by b, where $a \geq 1$, b is an integer greater than 1, and c is a positive real number. Then

$$f(n) \text{ is } \begin{cases} O(n^{\log_b a}), & \text{if } a > 1; \\ O(\log n), & \text{if } a = 1. \end{cases}$$

Furthermore, when $n = b^k$ and $a \neq 1$, where k is a positive integer,

$$f(n) = C_1 n^{\log_b a} + C_2,$$

where $C_1 = f(1) + c/(a-1)$ and $C_2 = -c/(a-1)$.

Master theorem

Theorem

Let T be an increasing function that satisfies the recurrence relation

$$T(n) = aT(n/b) + cn^d$$

whenever n is divisible by b, where $a \geq 1$, b is an integer greater than 1, and c and d are real numbers with c positive and d nonnegative. Then

$$T(n) \text{ is } \begin{cases} O(n^d), & \text{if } a < b^d; \\ O(n^d \log n), & \text{if } a = b^d; \\ O(n^{\log_b a}), & \text{if } a > b^d; \end{cases}$$

Generating functions

Definition

The generating function for sequence $a_0, a_1, \cdots, a_k, \cdots$ of real numbers is the infinite series

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

Generating functions

Definition

The generating function for sequence $a_0, a_1, \cdots, a_k, \cdots$ of real numbers is the infinite series

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

Examples of power series

$\{a_k\}$	$g(x)$
$a_k = 1$	$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$ for $\lvert x\rvert < 1$
$a_k = a^k$	$\sum_{k=0}^{\infty} a^k x^k = \frac{1}{1-ax}$ for $\lvert ax\rvert < 1$
$a_k = k+1$	$\sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} 1\right) x^k = \frac{1}{(1-x)^2}$

Extended binomial coefficient

Definition

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

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

- Let n and r are two positive integers, the extended binomial coefficient can be expressed as

$$\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}.$$

- Let x be a real number with $|x| < 1$ and let u be a real number. Then

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k.$$

Applications of generating function

a. Counting
   - # solutions of $e_1 + e_2 + e_3 = 17$;
   - # k-combinations of a set with n elements;

b. Solve recurrence relations
   - $a_k = 3a_{k-1}$ with $a_0 = 2$;
   - $a_k = 3a_{k-1} + n$ with $a_0 = 1$;
   - $a_n = 8a_{n-1} + 10^{n-1}$ with $a_1 = 9$;

c. Proving identities
   - $\sum_{k=0}^{n} C(n,k)^2 = C(2n,n)$;
   - $C(n,r) = C(n-1,r) + C(n-1,r-1)$;

Probability axioms

- **Nonnegativity:** $P(A) \geq 0$;
- **Normalization:** $P(\Omega) = 1$ and $P(\emptyset) = 0$;
- **Additivity:** If $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$.

Probability axioms

- **Nonnegativity:** $P(A) \geq 0$;
- **Normalization:** $P(\Omega) = 1$ and $P(\emptyset) = 0$;
- **Additivity:** If $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$.

Finite probability

If S is a finite nonempty sample space of equally likely outcomes, and E is an event, that is, a subset of S, then the probability of E is

$$p(E) = \frac{|E|}{|S|}.$$

Probability axioms

- **Nonnegativity:** $P(A) \geq 0$;
- **Normalization:** $P(\Omega) = 1$ and $P(\emptyset) = 0$;
- **Additivity:** If $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$.

Finite probability

If S is a finite nonempty sample space of equally likely outcomes, and E is an event, that is, a subset of S, then the probability of E is

$$p(E) = \frac{|E|}{|S|}.$$

- Let all outcomes be equally likely;
- Computing probabilities $\equiv$ two countings;
  - Counting the successful ways of the event;
  - Counting the size of the sample space;

Probability operators

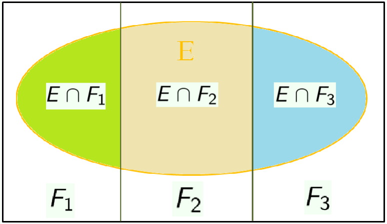
Operators

Let Ω be the sample space, A and B be two events:

1. If $A \cap B = \emptyset$, then
$$P(A \cup B) = P(A) + P(B);$$
2. $$P(\overline{A}) = P(\Omega) - P(A) = 1 - P(A);$$
3. If A and B are independent, then
$$P(A \cap B) = P(A) \cdot P(B);$$
4. The conditional probability of A given B, denoted by $P(A|B)$, is computed as
$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

Remarks for conditional probability

- $P(E|F) = P(E)$ if events E and F are independent;
- $P(E \cap F) = P(E) \cdot P(F|E) = P(F) \cdot P(E|F)$;



- $P(E) = P(F_1) \cdot P(E|F_1) + P(F_2) \cdot P(E|F_2) + P(F_3) \cdot P(E|F_3)$ if $F_1 \cup F_2 \cup F_3 = \Omega$ and $F_i \cap F_j = \emptyset$ for $i \neq j$ (**Total probability theorem**);
- $P(F_i|E) = \frac{P(F_i) \cdot P(E|F_i)}{P(E)} = \frac{P(F_i) \cdot P(E|F_i)}{\sum_i P(F_i) \cdot P(E|F_i)}$ (**Bayes rule**).

Random variables

- A **random variable** (r.v.) X is a function from sample space Ω of an experiment to the set of real numbers in R, i.e.,

$$\forall \omega \in \Omega, X(\omega) = x \in R.$$

- The **distribution** of a r.v. X on a sample space Ω is the set of pairs $(r, p(X = r))$ for all $r \in X(\Omega)$, where $P(X = r)$ is the probability that r.v. X takes value r.

Pair-wise independent

Let r.v.s X and Y are **pair-wise independent** if and only if for $\forall x, y \in R$, we have

$$P(X = x \wedge Y = y) = P(X = x)P(Y = y);$$

Independence of r.v.

Mutually independent

Let r.v.s $X_1, X_2, \cdots, X_n$ are **mutually independent** if and only if for $\forall x_{i_j} \in R$

$$P(X_{i_1} = x_{i_1} \wedge X_{i_2} = x_{i_2} \wedge \cdots \wedge X_{i_m} = x_{i_m})$$
$$= P(X_{i_1} = x_{i_1})P(X_{i_2} = x_{i_2}) \cdots P(X_{i_m} = x_{i_m}),$$

where $i_j, j = 1, 2, \cdots, m$, are integers with $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ and $m \geq 2$.

Let r.v.s X and Y are **independent** if and only if for $\forall x, y \in R$, s.t. $P(Y = y) \neq 0$, we have

$$P(X = x|Y = y) = \frac{P(X = x \wedge Y = y)}{P(Y = y)} = P(X = x).$$

Bernoulli trials and binomial distribution

Definition

- Each performance of an experiment with two possible outcomes is called a **Bernoulli trial**.
- The probability of exactly k successes in n independent Bernoulli trials, with probability of success p and probability of failure $q = 1 - p$, is

$$B(k; n, p) = P(X = k) = C(n, k)p^k q^{n-k},$$

  where this function is the **binomial distribution**.
- Let $G(k; p)$ denote the probability of failures before the $k-$th independent Bernoulli trials with probability of success p. This function is the **Geometric distribution**, i.e.,

$$G(k; p) = pq^{k-1}.$$

Expected value and variance

Let X be a r.v. on a sample space Ω, and $P(X = r)$ is the probability that $X = r$, so that $P(X = r) = \sum_{\omega \in \Omega, X(\omega)=r} P(\omega)$.

- The **expected value**, also called **expectation** or **mean**, of r.v. X on Ω is equal to

$$E(X) = \sum_{\omega \in \Omega} P(\omega)X(\omega).$$

- $E(X) = \sum_{r \in X(\Omega)} P(X = r) \cdot r$.
- The **deviation** of X at $\omega \in \Omega$ is $X(\omega) - E(X)$, the difference between the value of X and the mean of X.
- The **variance** of X, denoted by $V(X)$, is $V(X) = \sum_{\omega \in \Omega} (X(\omega) - E(X))^2 \cdot P(\omega)$.
- $V(X) = \sum_{x \in X(\Omega)} (x - E(X))^2 \cdot P(X = x) = E(X^2) - (E(X))^2$.

Properties of expectations and variance

If X_i, $i = 1, 2, \cdots, n$ with n a positive integer, are random variables on Ω, and if a and b are real numbers, then

- $E(\sum_{i=1}^n X_i) = \sum_{i=1}^n E(X_i)$;
- $E(aX_i + b) = aE(X_i) + b$.
- $V(aX + b) = a^2 V(X)$.
- If X_i, $i = 1, 2, \cdots, n$, with n a positive integer, are pairwise independent, then $V(\sum_{i=1}^n X_i) = \sum_{i=1}^n V(X_i)$.

Tail probability

Let X_i be a sequence of independent Bernoulli r.v.s with $P(X_i = 1) = p_i$ on a sample space Ω.

- Let X_i be a nonnegative. If a is a positive real number, then

$$P(X_i \geq a) \leq \frac{E(X_i)}{a}.$$

- If r is a positive real number, then

$$P(|X_i(\omega) - E(X_i)| \geq r) \leq \frac{V(X_i)}{r^2}.$$

- Assume that r.v. $X = \sum_{i=1}^{n} X_i$.
  - $P(X < (1-\delta)\mu) < \exp\left(-\mu\delta^2/2\right)$
  - $P(X > (1+\delta)\mu) < \exp\left(-\mu\delta^2/4\right)$

Relation

Let $A_1, A_2, \cdots, A_n$ be sets. An n-ary relation on these sets is a subset of $A_1 \times A_2 \times \cdots \times A_n$. The sets $A_1, A_2, \cdots, A_n$ are called the domains of the relation, and n is called its degree.

Representing relations

- A directed graph, or digraph, consists of (V, E), where V and E denote the sets of vertices (nodes) and edges (or arcs). In the edge (a, b), a and b are called the initial vertex and the terminal vertex.
- Suppose that R is a relation from $A = \{a_1, a_2, \cdots, a_m\}$ to $B = \{b_1, b_2, \cdots, b_n\}$. The relation R can be represented by $M_R = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1, & \text{if } (a_i, b_j) \in R; \\ 0, & \text{otherwise.} \end{cases}$$

Properties of relations

A relation R on a set A,

- It is **reflexive** if $\forall a((a, a) \in R)$.
- It is **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.
- A relation R on a set A such that for all $a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ is called **antisymmetric**.
- It is **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

Relation operators

Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4\}$.
The relations $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ and $R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$ can be combined to obtain

- $R_1 \cup R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\}$;
- $R_1 \cap R_2 = \{(1, 1)\}$;
- $R_1 - R_2 = \{(2, 2), (3, 3)\}$;
- $R_2 - R_1 = \{(1, 2), (1, 3), (1, 4)\}$.
- $R_1 \oplus R_2 = R_1 \cup R_2 - R_1 \cap R_2 = \{(1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\}$.
- Let R and S be a relation from A to B and from B to C. The **composite** of R and S, denoted as $S \circ R$, consists of ordered pairs (a, c), where $a \in A, c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$.
- $R^{n+1} = R^n \circ R$.

Matrix operations

Suppose that R_1 and R_2 are relations on a set A represented by the matrices M_{R_1} and M_{R_2}, respectively.

Matrix operations

Suppose that R_1 and R_2 are relations on a set A represented by the matrices M_{R_1} and M_{R_2}, respectively.
Thus, the matrices representing the union, intersection, composite and power of these relations are

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2},$$

$$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2},$$

$$M_{R_1 \circ R_2} = M_{R_1} \odot M_{R_2},$$

$$M_{R^n} = M_R^{[n]}.$$

Closures of relations

If there is a relation S with property P (such as reflexivity, symmetry, or transitivity) containing R such that S is a subset of every relation with property P containing R, then S is called the **closure** of R with respect to P.

- Reflexive closure
- Symmetry closure
- Transitivity closure
  - The *connectivity relation* R^* consists of the pairs (a, b) such that there is a path of length at least one from a to b in R.
  - The transitive closure of a relation R equals the connectivity relation R^*.
  - Let M_R be the zero-one matrix of the relation R on a set with n elements. Then the zero-one matrix of the transitive closure R^* is

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \cdots \vee M_R^{[n]}.$$

Equivalence relations

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

- 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. The equivalence class of a with respect to R is denoted by $[a]_R$.
- Let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:
  (i) aRb;
  (ii) $[a] = [b]$;
  (iii) $[a] \cap [b] \neq \emptyset$.
- Let R be an equivalence relation on S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i | i \in I\}$ of S, there is an equivalence relation R that has $A_i, i \in I$, as its equivalence classes.

Partial orderings

Definition

A relation R on a set S is called a **partial ordering** or **partial order** if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a **partially ordered set**, or poset, and is denoted by (S, R).

- is called a **totally ordered** or **linearly ordered set** if $(S, \preceq)$ is a poset and every two elements of S are comparable.
- Maximal VS. minimal
- Greatest element VS. least element
- Upper bound VS. lower bound
- Least upper bound VS. greatest lower bound

Graphs

Definition

A **graph** $G = (V, E)$ consists of V , a nonempty set of vertices (or nodes) and E, a set of edges. Each edge has either one or two vertices associated with it, called its endpoints. An edge is said to connect its endpoints.

- Neighbors, degree, subgraph and Induced subgraphs
- Undirected and directed graphs
- Special graphs: complete graph, $r-$regular graph, n-cube, cycles and wheels, etc.
- Graph operations:
  - Remove or adding edges of a graph
  - Adding a new edge e
  - Edge contraction
  - Graph union

Representing graphs

- Adjacency list
- Adjacency matrix
- Incidence matrices
- Random walk
- Laplacian
- Normalized Laplacian

Isomorphism of graphs

The simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are **isomorphic** if there exists a one to- one and onto function f from V_1 to V_2 with the property that a and b are adjacent in G_1 if and only if $f(a)$ and $f(b)$ are adjacent in G_2, for all a and b in V_1. Such a function f is called an isomorphism.

Graph invariant:

- The same number of vertices;
- The same number of edges;
- The same degree for the same vertex.
- The path and distance between vertices

Connectivity

- Path VS. circuit
- Counting pathes
- Connected component, giant connected component
- Strongly and weakly connected components
- Network robustness
  - Cut and bridge
  - Vertex and edge boundary
  - Vertex connectivity
  - Edge connectivity
  - Vertex expansion
  - Edge expansion
  - Cheeger ratio
  - Algebraic connectivity
  - R-energy

Euler circuit and Euler path

An **Euler circuit** in a graph G is a simple circuit containing every edge of G. An **Euler path** in G is a simple path containing every edge of G.

- A connected multigraph with at least two vertices has an Euler circuit if and only if each of its vertices has even degree.
- A connected multigraph has an Euler path but not an Euler circuit if and only if it has exactly two vertices of odd degree.

A simple path in a graph G that passes through every vertex exactly once is called a **Hamilton path**, and a simple circuit in a graph G that passes through every vertex exactly once is called a **Hamilton circuit**.

If G is a simple graph with n vertices with $n \geq 3$ such that the degree of every vertex in G is at least $n/2$, then G has a Hamilton circuit.

Planar graph

Definition

A graph is called **planar** if it can be drawn in the plane without any edges crossing.

- Let G be a connected planar simple graph with e edges and v vertices. Let r be the number of regions in a planar representation of G. Then $r = e - v + 2$.
- If G is a connected planar simple graph with e edges and v vertices, where $v \geq 3$, then $e \leq 3v - 6$ or G has a vertex of degree not exceeding five.
- If a connected planar simple graph has e edges and v vertices with $v \geq 3$ and no circuits of length three, then $e \leq 2v - 4$.
- K_5 and $K_{3,3}$ are not planar graphs.
- A graph is nonplanar if and only if it contains a subgraph homeomorphic to $K_{3,3}$ or K_5.

Graph coloring

A **coloring** of a simple graph is the assignment of a color to each vertex of the graph so that no two adjacent vertices are assigned the same color.

- The **chromatic number** of a graph is the least number of colors needed for a coloring of this graph. The chromatic number of a graph G is denoted by $\chi(G)$.
- The chromatic number of a planar graph is no greater than four.
- Nonplanar graphs can have arbitrarily large chromatic numbers.
- What are the chromatic numbers of graphs K_5, $K_{3,3}$, C_5 and C_6?

Take-home messages

- Introduction
- The Foundations of Logic and Proofs
- Basic Structures
- Counting
- Advanced Counting
- Discrete Probability
- Relations
- Graphs