COSC 311: Discrete Structures

Alex Zhang

November 21, 2022

Contents

1

Counting

Definition ▶ Permutation

A **permutation** is a grouping of elements where order **does** matter.

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

Permutation Formulae

Permutations of size r for n objects	$P(n,r)=\frac{n!}{(n-r)!}$
Must contain x elements	$P(r,x)\times P(n-x,r-x)$
Permutations with r indistinguishable types	$\frac{n!}{n_1!\times n_2!\times\cdots\times n_r!}$
Circular Arrangement	$\frac{n!}{n}$

Definition ▶ Combination

A **combination** is a grouping of elements where order **does not** matter.

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

We read $\binom{n}{r}$ as n choose r.

Theorem ▶ Binomial Theorem

Given variables x and y and a positive integer n, the repeated product of the term $(x+y)$ with itself can be expanded as the following sum:

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

Theorem ▶ Combination With Repetition

The number of combinations of r objects chosen from n distinct objects *with repetition* is

$$\binom{n+r-1}{r} = \frac{(n+r-1)!}{r!(n-1)!}$$

2 Logic

Logic is reasoning conducted or assessed according to strict principles of validity.

Definition ▸ Proposition/Statement

A **proposition** or **statement** is a declarative sentence that is exclusively either true or false.

$$p \coloneqq 2 + 5 = 7$$

p is a true proposition because $2 + 5 = 7$.

Definition ▸ Tautology

A compound proposition is referred to as a **tautology** if it is true for all truth value assignments.

Definition ▸ Contradiction

A compound proposition is referred to as a **contradiction** if it is false for all truth value assignments.

Definition ▸ Converse

The **converse** of an implication $p \Rightarrow Q$ is defined as the implication $q \Rightarrow p$

Definition ▸ Contrapositive

The **contrapositive** of an implication $p \Rightarrow q$ is defined as the implication proposition $\neg q \to \neg p$. It is logically equivalent to the original statement (i.e. has all same truth values).

Definition ▸ Dual

If S is a statement with no operations other than negation, $\vee$ and $\wedge$, then the dual of S (S^d) is a statement obtained from S by replacing $\wedge$ with $\vee$ and vice versa.

Theorem ▸ Principle of Duality

Assume S and T are statements with no other operations other than negation $\neg$. If $S \iff T$ then $S^d \iff T^d$

Substitution Rules

1. If the original statement is a tautology, we can replace every occurrence of p with q and still have a tautology
2. If $q \iff p$, we can replace any p with q and still have a logically equivalent statement.

Theorem ▸ Rule of Universal Specification

If a particular open statement becomes true for all replacements by elements of a given universe, the the open statement is true for each specific individual element in the universe.

$$(\forall x[m(x) \Rightarrow c(x)] \wedge m(l)) \Rightarrow c(l)$$

Theorem ▸ Rule of Universal Generalization

If open statement $p(x)$ is proved to be true when x is replaced by any arbitrarily chosen element c from the universe, then $\forall x\, p(x)$ is true.

Laws of Propositional Logic

Idempotent laws	$p \wedge p \iff p$	$p \vee p \iff p$
Associative Laws	$(p \vee q) \vee r \iff p \vee (q \vee r)$	$(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$
Commutative Laws	$p \vee q \iff q \vee p$	$p \wedge q \iff q \wedge p$
Distributive Laws	$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$
Identity Laws	$p \vee F \iff p$	$p \wedge T \iff p$
Domination Laws	$p \wedge F \iff F$	$p \vee T \iff T$
Double Negation Law	$\neg\neg p \iff p$	
Complement Laws	$p \wedge \neg p \iff F$	$p \vee \neg p \iff T$
De Morgan's Laws	$\neg(p \vee q) \iff \neg p \wedge \neg q$	$\neg(p \vee q) \iff \neg p \vee \neg q$
Absorption Laws	$p \vee (p \wedge q) \iff P$	$p \wedge (p \vee q) \iff p$
Conditional Identities	$(p \Rightarrow q) \iff (\neg p \vee q)$	$(p \iff q) \iff [(p \Rightarrow q) \wedge (q \Rightarrow p)]$
Contrapositive	$(p \Rightarrow q) \iff (\neg q \Rightarrow \neg p)$	

Proof by Contradiction

$$(p \Rightarrow q) \iff [(p \wedge \neg q) \Rightarrow F_0]$$

Definition ▶ Open Proposition

An **open proposition**

- has one or more variables belonging to a specified set of some universe
- is not a proposition on its own
- becomes a proposition when the variables are replaced by values

Definition ▶ Predicate

A **predicate** is a proposition that depends on a variable.

$$P(x): \text{ x is a prime number}$$

Definition ▸ Universal Quantifier

The **universal quantifier** ($\forall$) states that **for all** values of a quantified variable, the proposition holds.

$$\forall(x \in \mathbb{N})(P(x)) \iff P(1) \land P(2) \land P(3) \land \ldots$$

Definition ▸ Existential Quantifier

The **existential quantifier** ($\exists$) states **there exists** a value for a quantified variable such that the proposition holds.

$$\exists(x \in \mathbb{N})(P(x)) \iff P(1) \lor P(2) \lor P(3) \ldots$$

Negation of Quantified Statements

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

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

Rules of Inference

The following are all tautologies in logic:

Modus Ponens (Confirm)	$[(p) \wedge (p \Rightarrow q)] \Rightarrow q$
Modus Tollens (Contradict)	$[(\neg q) \wedge (p \Rightarrow q)] \Rightarrow \neg p$
Addition	$p \Rightarrow (p \vee q)$
Simplification	$(p \wedge q) \Rightarrow p$
Conjunction	$(p \wedge q) \Rightarrow (p \wedge q)$
Hypothetical Syllogism	$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$
Disjunctive Syllogism	$[(p \vee q) \wedge (\neg p)] \Rightarrow q$
Resolution	$[(p \vee q) \wedge (\neg p \vee r)] \Rightarrow (q \vee r)$

Let A be any non-empty set.

Universal Instantiation	$[(c \in A) \wedge \forall(x \in A)(P(x))] \Rightarrow P(c)$
Universal Generalization	$[(c \in A \text{ (arbitrary)}) \wedge P(c)] \Rightarrow \forall(x \in A)(P(x))$
Existential Instantiation	$\exists(x \in A)(P(x)) \Rightarrow [(c \in A \text{ (particular)}) \wedge P(c)]$
Existential Generalization	$[(c \in A) \wedge P(c)] \Rightarrow \exists(x \in A)(P(x))$

3

Proofs

3.1 Mathematical Definitions

Definition ▶ Parity

Parity describes whether an integer is even or odd.

Let $x \in \mathbb{Z}$

- $\exists(k \in \mathbb{Z})(x = 2k) \Rightarrow x$ is even
- $\exists(k \in \mathbb{Z})(x = 2k + 1) \Rightarrow x$ is odd

Definition ▶ Rational Numbers

$$\exists(x, y \in \mathbb{Z})\left(y \neq 0 \wedge r = \frac{x}{y}\right) \Rightarrow r \text{ is rational}$$

Definition ▶ Divides

An integer x **divides** an integer y if and only if $x \neq 0$ and $y = kx$ for some integer k.

$$x|y \iff [(x \in \mathbb{Z}) \wedge (x \neq 0) \wedge (y \in \mathbb{Z}) \wedge \exists(k \in \mathbb{Z})(y = kx)]$$

Example 3.1.1 ▶ Linear Combinations

Is it possible to sum 500 from any combination of elements from $A = \{144, 336, 30, 66, 138, 162, 318, 54, 84, 288, 126, 468\}$?

3 divides all elements of A. Therefore, 3 must divide any linear combination of the elements. But 3 does not divide 500, so it is impossible.

Definition ▶ Prime and Composite Numbers

An integer n is **prime** if and only if $n > 1$ and the only positive integers that divide n are 1 and n.

$$n \text{ is prime} \iff [(n > 1) \land \forall(x \in \mathbb{Z}^+)\,[(x = 1) \lor (x = n) \lor (x \nmid n)]]$$

$$n \text{ is prime} \iff |\{x : (x \in \mathbb{Z}^+) \land (x|n)\}| = 2$$

An integer n is **composite** if and only if $n > 1$ and there is an integer m such that $1 < m < n$ and m divides n.

$$n \text{ is composite} \iff [(n > 1) \land \exists(m \in \mathbb{Z})\,[(1 < m < n) \land (m|n)]]$$

$$n \text{ is composite} \iff |\{x : (x \in \mathbb{Z}^+) \land (x|n)\}| > 2$$

Definition ▶ Common Divisor

For $a, b \in \mathbb{Z}$, a positive integer c is said to be a **common divisor** of a and b if $c|a$ and $c|b$.
If either $a \neq 0$ or $b \neq 0$ then $c \in \mathbb{Z}^+$ is called the greatest common divisor (GCD) of a, b if:

- $c|a$ and $c|b$
- for any common divisor of a and b, say d, we have $d|c$

Definition ▶ Integers Modulo

The set of integers modulo p (denoted $\mathbb{Z}_p$) is defined as:

$$\mathbb{Z}_p = \{x : 0 \leq x < p\}$$

3.2 Introduction to Proofs

Definition ▶ Axiom

An **axiom** is a statement assumed to be true. It usually serves as a basis for many elementary theorems which, in turn, are used to prove other theorems.

Definition ▶ Theorem

A **theorem** is a statement that can be proven to be true.

Definition ▶ Proof

A **proof** consists of a series of steps, each of which follow logically from assumptions or from previously proven statements, whose final step should result in the statement of the theorem being proven.

In computer science, proofs are important for a multitude of things, including but not limited to:

- establishing that a program works as expected
- showing that a cryptosystem is secure
- validating a set of inferences in artificial intelligence

4 Mathematical Induction and Recursion

Definition ▸ Induction

Induction is a technique used to prove a proposition about any well-ordered set.
To prove a proposition $p(k)$ for any k in the well-ordered set A:

$$[p(n_0) \land \forall(k \geq n_0)(p(k) \Rightarrow p(k+1))] \Rightarrow \forall(n \in A)(p(n)$$

1. **Base Case** – Prove $p(n_0)$ where n_0 is the first element of the set
2. **Inductive Step** – Prove $p(k) \Rightarrow p(k+1)$. This recursively proves p for the rest of our set

Example 4.0.1 ▸ Sums of natural numbers

$\forall(n \in \mathbb{Z}^+)(p(n))$ where $p(n)$ is defined as:

$$p(n) := \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

1. **Base Case** – Let $n_0 = 1$. Then $p(n_0) = \frac{1(1+1)}{2}$, which is true.
2. **Induction Step** – We have proven $p(n)$ is already true. Now, we need to prove

$$p(n+1) := \sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$$

Definition ▸ RSA Encryption

Based on two algorithms:

1. Key Generation
2. RSA Function Evaluation: a function F that takes input data x and a key k and produces either an encrypted result or plain text

Steps to create secure RSA keys:

1. Select two large prime numbers p and q (preferably above 512 digits)
2. Generate modulus $n = p \cdot q$
3. Calculate the totient $\phi(n) = (p-1)(q-1)$
4. Generate a public key as a prime number calculated from the interval $[3, \phi(n)]$ that has a gcd of 1 with $\phi(n)$.
5. Generate a private key as the inverse of the prime number selected in the public key with respect to $\mod \phi(n)$

Summation

Definition ▸ Summation

Summation is used to express the sum of terms in a numerical sequence

$$\sum_{i=s}^{n} a_i = a_s + a_{s+1} + \ldots + a_n$$

Terms:

- i: index of summation
- s: lower limit of summation
- t: upper limit of summation
- $\sum_{i=s}^{n} a_1$: summation format
- $a_s + a_{s+1} + \ldots + a_n$: expanded form

Definition ▸ Closed Form Sum

A **closed form** for a sum is a finite expression used to calculate a sum.

Common Closed Forms

Arithmetic Sequence:

$$\forall (n \in \mathbb{N}) \sum_{k=0}^{n-1} (a + kd) = an + \frac{d(n-1)n}{2}$$

Geometric Sequence:

$$\forall (r \neq 1 \in \mathbb{R}) \forall (n \in \mathbb{N}) \sum_{k=0}^{n-1} a \cdot r^k = \frac{a(r^n - 1)}{r - 1}$$

6

Functions and Relations

Definition ▸ Onto Function

A function $f : A \to B$ is **onto** if every $b \in B$ has some $a \in A$ where $f(a) = b$.

Definition ▸ 1-to-1 Function

A function $f : A \to B$ is **1-to-1** if every $a \in A$ has a unique $f(a) \in B$.

$$[(a_1, a_2 \in A) \wedge (a_1 \neq a_2)] \Rightarrow f(a_1) \neq f(a_2)$$

Example 6.0.1 ▸ Onto Functions

Question: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Are all functions $f : A \to B$ onto? How many onto functions are there from A to B?

There are $|B|^{|A|} = 8$ functions $f : A \to B$.
All functions $f : A \to B$ are onto except:

- $f_1 = \{(x, 1), (y, 1), (z, 1)\}$
- $f_2 = \{(x, 2), (y, 2), (z, 2)\}$

Thus, there are only 6 onto functions $f : A \to B$.

Example 6.0.2 ▸ Choose

Let $A = \{w, x, y, z\}$ and $B = \{1, 2, 3\}$. There are 3^4 functinos from A to B. For subsets of size 2, there are 2^4 functions from A to $\{1, 3\}$. So, there are

$$3 \cdot 2^4 \text{ or } \binom{3}{2} \cdot 2^4$$

functinos from A to B that are not onto.

The constant functions such as $\{(w, 2), (x, 2)(y, 2), (z, 2)\}$ will be counted twice.
Thus, the total number of distinct onto functions is $3^4 - \binom{3}{2} \cdot 2^4 + 3 = 36$

For finite sets A and B, with $|A| = m$ and $|B| = n$, there are

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

onto functions from A to B.

Definition ▶ Bijective Function

A function $f : A \to B$ is **bijective** if it is both 1-to-1 and onto.

Definition ▶ Identity Function

A function $1_A : A \to A$ is defined by $1_A(a) = a \forall a \in A$ is called the identity function on the set A.

Definition ▶ Function Equality

For functions $f, g : A \to B$, we say that $f = g$ if $\forall (a \in A)\, [f(a) = g(a)]$

Example 6.0.3 ▶ asdf

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Q}$ such that $\forall (x \in \mathbb{Z})\, [f(x) = x = g(x)]$. Is $f = g$?

No, f is a 1-to-1 correspondence and g is a 1-to-1 function that is not onto.

Example 6.0.4 ▶ asdf

Consider $f, g : \mathbb{R} \to \mathbb{Z}$ where $\forall (x \in \mathbb{R})\, [g(x) = [x]]$.
If $x \in \mathbb{Z}$, then $f(x) = x$. If $x \in \mathbb{R} - \mathbb{Z}$, then $f(x) = |x| + 1$.

If $x \in \mathbb{Z}$ then $f(x) = x = [x] = g(x)$
If $x \in \mathbb{R} \setminus \mathbb{Z}$ then $x = n + r$ where $n \in \mathbb{Z}$ and $0 < r < 1$
So, $f(x) = [x] + 1 = n + 1 = [x] = g(x)$.
Therefore, $\forall (x \in \mathbb{R})\, [f(x) = g(x)]$

Definition ▸ Composition of Functions

Let $f : A \to B$ and $g : B \to C$. The **composition** of g with f (denoted as $g \circ f$) is a function $g \circ f : A \to C$ defined as:

$$\forall(a \in A)\,[(g \circ f)(a) = g(f(a))]$$

Example 6.0.5 ▸ Composition and Commutativity

Suppose $f, g : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ and $g(x) = x + 5$. Determine $(g \circ f)(x)$ and $(f \circ g)(x)$

$$(g \circ f)(x) = x^2 + 5$$

$$(f \circ g)(x) = (x + 5)^2$$

Thus, composition of functions does not commute (i.e. it's not a commutative operation).

Theorem ▸ Preservation of Onto/1-to-1

Theorem: Given $f : A \to B$ and $g : B \to C$

- If f and g are onto, then $(g \circ f)$ is onto
- If f and g are 1-to-1, then $(g \circ f)$ is 1-to-1

Theorem ▸ Associativity of Composition

Theorem: Given $f : A \to B$ and $g : B \to C$ and $h : C \to D$

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Definition ▸ Powers of Functions

Let $f : A \to A$.

- $f^1 = f$
- $f^{n+1} = f \circ f^n$ for $n \in \mathbb{N}$

Example 6.0.6 ▶ Simple Power Function

Suppose $A = \{1,2,3,4\}$ and $f : A \to A$ with $f = \{(1,2),(2,2),(3,1),(4,3)\}$. What is f^2 and f^3?

$$f^2 = f \circ f = \{(1,2),(2,2),(3,2),(4,1)\}$$

$$f^3 = f \circ f \circ f = \{(1,2),(2,2),(3,2),(4,2)\}$$

Definition ▶ Converse of a Relation

For a relation R from set A to B, the **converse** of R (R^c) is a relation from B to A defined as

$$R^c = \{(b,a) : (a,b) \in R\}$$

Definition ▶ Inverse

Let $f : A \to B$. f is invertible if:

$$\exists (g : B \to A)(g \circ f = 1_A \land f \circ g = 1_B)$$

We call g the **inverse** of f denoted as $g = f^{-1}$.

Example 6.0.7 ▶ Invertible Functions

Consider $f, g : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 5$ and $g(x) = \frac{x-5}{2}$. Show that both f and g are invertible functions.

Proof. $(g \circ f)(x) = g(f(x)) = g(2x+5) = \frac{(2x+5)-5}{2} = x$
$(f \circ g)(x)$
$g \circ f = f \circ g = 1_{\mathbb{R}}$
Thus, f and g are invertible functions. In addition, f and g are each other's inverses. □

Theorem ▶ Invertability

Theorem: A function $f : A \to B$ is invertible if and only if f is 1-to-1 and onto.

Theorem ▶ asdf

Theorem: If $f : A \to B$ and $g : B \to C$ are both invertible, then $g \circ f : A \to C$ is invertible, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Definition ▶ Preimage

If $f : A \to B$, and $B_1 \subseteq B$.

Theorem ▶ Equivalences

If $f : A \to B$ for finite sets A and B with $|A| = |B|$, then the following are equivalent:

- f is 1-to-1
- f is onto
- f is invertible

7

Computational Complexity

Definition ▶ Dominated Function

Let $f, g : \mathbb{Z}^+ \to \mathbb{R}$. We say g **dominates** f if

$$\exists(m \in \mathbb{R}^+, k \in \mathbb{Z}^+)\,[n \geq k \Rightarrow \forall(n \in \mathbb{Z}^+)\,(|f(n)| \leq m|g(n)|)]$$

When f is dominated by g, we say that f is of order (at most) g and write $f \in \mathcal{O}(g)$. We can think of $\mathcal{O}(g)$ as the set of all functions having domain $\mathbb{Z}^+$ and a co-domain $\mathbb{R}$ that are dominated by g.

Theorem ▶ asd

$g \notin \mathcal{O}(f)$
Assume $g \in \mathcal{O}(f)$. Then, $\forall(n \geq k)(n^2 = |g(n)| \leq m|f(n)| = 5mn)$. For $n \in \mathbb{Z}^+$, as n increases, $5m$ remains constant. So eventually, $5mn < n^2$ Hence, $g \notin \mathcal{O}(f)$.

Example 7.0.1 ▶ Dominance

Consider $f, g : \mathbb{Z}^+ \to \mathbb{R}$ with $f(n) = 5n^2 + 3n + 1$ and $g(n) = n^2$. Show that $f \in \mathcal{O}(g)$ and $g \in \mathcal{O}(f)$

Proof.

$$|f(n)| = |5n^2 + 3n + 1| = 5n^2 + 3n + 1 \leq 5n^2 + 3n^2 + n^2 = 9n^2 = 9|g(n)|$$

For all $n \geq 1$ and $n = k$, we have $|f(n) \leq m|g(n)| = 9|g(n)|$ for any $m \geq 9$. Hence, $f \in \mathcal{O}(g)$.

$$|g(n)| = n^2 \leq 5n^2 \leq 5n^2 + 3n + 1$$

For all $n \geq 1$ we have $|g(n)| \leq m|f(n)|$ for any $m \geq 1$ and $1 \leq k \leq n$. So $g \in \mathcal{O}(f)$. □

Example 7.0.2 ▸ Induction

Consider $f, g : \mathbb{Z}^+ \to \mathbb{R}$ with $f(n) = 1 + 2 + \ldots + n$ and $g(n) = 1^2 + 2^2 + \ldots + n^2$. How do we know that $f \in \mathcal{O}(n^2)$ and $g \in \mathcal{O}(n^3)$?

Proof. $f : \mathbb{Z}^+ \to \mathbb{R}$ where $f(n) = \frac{n(n+1)}{2}$. Hence, $f \in \mathcal{O}(n^2)$
$g(n) = \frac{(n(n+1)(2n+1))}{6}$. Hence, $g \in \mathcal{O}(n^3)$. □

8

Graph Theory

8.1 Introduction

Definition ▶ Graph

A **graph** is a set of objects with some relation between the objects.

Formally, a **graph** G is defined as a pair (V, E) where:

- V is a set of **vertices**
- E is a set of **edges**

We can think of a graph as a web of elements. When talking about graphs, we call the elements "vertices" and call the connections between elements "edges".

Definition ▶ Directed/Undirected Graph

A graph is **undirected** if every edge goes both ways. A graph is **directed** if some edges can only go one way.

- If a graph G is undirected, then $E \subseteq \{\{u, v\} : u, v \in V\}$
- If a graph G is directed, then $E \subseteq \{(u, v) : u, v \in V\}$

Notice the difference between a set $\{a, b\}$ and a tuple (a, b). The order of elements inside a set does not matter while the order of elements inside a tuple does matter.

Definition ▶ Walk

Let x, y be two vertices in an undirected graph $G = (V, E)$. An $x - y$ **walk** in G is a loop-free alternating sequence:

$$asdf$$

with $e_i = \{x_{i-1}, x_i\}, 1 \leq i \leq n$. The length of the walk is the number of edges traversed (n edges).

- If $n = 0$, we consider it a **trivial walk**
- If $x = y$ and $n > 1$, we consider it a **closed walk**
- If $x = y$ and $n \leq 0$, we consider it an **open walk**

Walk Variations

Name	Repeated Vertices	Repeated Edges	Open/Closed
Open Walk	Yes	Yes	Open
Closed Walk	Yes	Yes	Closed
Trail	Yes	No	Open
Circuit	Yes	No	Closed
Path	No	No	Open
Cycle	No	No	Closed

Theorem ▶ Trails are also paths

Theorem: Let $G = (V, E)$ be an undirected graph with $a, b \in \mathbb{V}$. If there is a trail from a to b, then there is also a path from a to b.

Definition ▶ Connected Graph

Let $G = (V, E)$ be an undirected graph. We say that G is **connected** if there is a path between any two distinct vertices of G. If G is not connected, then G is **disconnected**.

Definition ▶ Disconnected Graph

A graph $G = (V, E)$ is **disconnected** if and only if V can be partitioned in at least two subsets V_1 and V_2 such that (TODO FINISH THIS)

Definition ▶ Multigraph

A **multigraph** is a directed graph where there can exist more than one edge between two vertices. Also, more edges may then be removed.

8.2 Subgraphs

Definition ▶ Subgraph

Let $G = (V, E)$ be a graph of any kind. $G' = (V', E')$ is a subgraph of G if $V' \subseteq V$, $V' \neq \varnothing$, $E' \subseteq E$, and every edge $e = \{v_1, v_2\} \in E'$ satisfies $v_1, v_2 \in V'$.

In other words, we can create a subgraph by removing vertices and their respective edges.

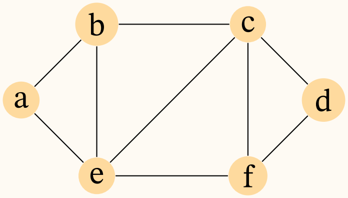
There are two types of subgraphs: induced subgraph and spanning subgraph.

- A subgraph is **induced** if vertices and their edges are removed.
- A subgraph is **spanning** if only edges are removed.

Example 8.2.1 ▶ Combinatorics

How may distinct spanning subgraphs can be created from the following graph?

$$V = \{a, b, c, d\}, E = \{(a, b), (a, c), (b, c), (c, d)\}$$



$$\underbrace{\binom{4}{0}}_{\text{remove 0}} + \underbrace{\binom{4}{1}}_{\text{remove 1}} + \underbrace{\binom{4}{2}}_{\text{remove 2}} + \underbrace{\binom{4}{3}}_{\text{remove 3}} + \underbrace{\binom{4}{4}}_{\text{remove 4}} = 2^4 = 16$$

Definition ▶ Complete Graph

Let V be a set of n vertices. The **complete graph** on V, denoted by K_n, is a loop-free undirected graph such that for all $a, b \in V$ where $a \neq b$, there exists an edge $\{a, b\} \in E$.

In other words, a graph is complete if every vertex is connected to all others by an edge. You can get from any vertex to any other vertex in one move.

Definition ▶ Complement Graph

Let $G = (V, E)$ be a loop-free undirected graph where $n = |V|$. The complement of G, denoted by $\overline{G}$, is the subgraph of K_n consisting of all n vertices of G and all edges $e = \{v_1, v_2\} \notin E$ that satisfy $v_1, v_2 \in V$. If $G = K_n$, then $\overline{G} = \varnothing$ (i.e. $\overline{G}$ is a null graph).

Note that for any graph G, $G + \overline{G}$ is a complete graph.

Definition ▶ Graph Isomorphism

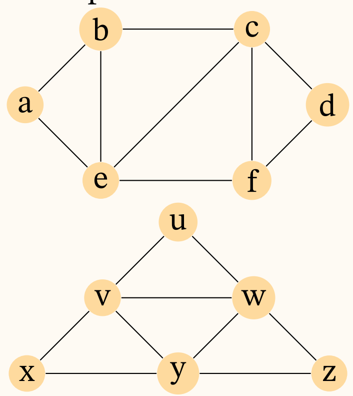
Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ where G_1 and G_2 are undirected graphs. A function $f : V_1 \to V_2$ is a **graph isomorphism** if:

1. f is 1-to-1 and onto
2. $\forall (a, b \in V_1)\, [\{a, b\} \in E \iff \{f(a), f(b)\} \in E_2]$

We say G_1 and G_2 are **isomorphic** if there exists a graph isomorphism between G_1 and G_2.

Example 8.2.2 ▶ Isomorphism

Are the two following graphs isomorphic?



Consider the following circuit in the second graph:

$$u \to w \to v \to y \to w \to z \to y \to x \to v \to u$$

No circuit of size 9 exists in the first graph. Thus, the two graphs are not isomorphic.

8.3 Planar Graphs

Definition ▶ Planar Graph

A graph is **planar** if its edges can be drawn without crossing lines.

Definition ▶ Bi-Partite Graph

$G = (V, E)$ is **bi-partite** if V can be split into two disjoint subsets, V_1 and V_2, and every edge connects a vertex in V_1 to a vertex in V_2 (or vice versa).

Definition ▶ Bi-Partite Complete Graph

A graph is **bi-partite complete** if it is bi-partite and has every possible edge that still satisfies the definition of bi-partite.

8.4 Elementary Subdivision and Homeomorphic Graphs

Definition ▸ Elementary Subdivision

Definition ▸ Homeomorphic Graph

G_1 and G_2 are **homeomorphic** if they can be obtained from the same loop-free undirected graph H by a sequence of elementary subdivisions.

Theorem ▸ Kuratowski's Theorem

A graph is nonplanar if and only if it contains a subgraph that is homeomorphic to either K_5 or $K_{3,3}$.

9

Hamiltonian Paths and Cycles

9.1 Introduction

Definition ▶ Hamiltonian Cycle

A Hamiltonian cycle is a cycle that visits each vertex of a graph only once (except for the vertex that is both the start and end, which is visited twice).

A Hamiltonian graph is a graph or multi-graph with 3 or more vertices that has a Hamiltonian cycle.

Definition ▶ Hamiltonian Path

A **Hamiltonian path** is a path in a graph or multigraph that contains each vertex only once.

Recall that in a path, we do not need to return to the beginning.

Surprisingly, we have not found any formal conditions that will guarantee that a graph will contain a Hamiltonian cycle or define a Hamiltonian path. Proving the existence of a Hamiltonian cycle and Hamiltonian path is a prime example of an NP-complete problem.

9.2 Properties

Let $G = (V, E)$ be a graph.

- If there exists a Hamiltonian cycle, then every vertex is degree 2 or more.
- If a vertex is degree 2, then the two edges that are incident with a must appear in every Hamiltonian cycle of the graph.
- If a vertex is degree more than 2, and you pass through that vertex when constructing a Hamiltonian cycle, then any unused edges incident with that vertex can be removed from further consideration.

Bi-Partite Labeling Strategy

If G has a Hamiltonian path, then it defines an alternating sequence between the two bi-partite graphs. If $|V_1| \neq |V_2|$, then no Hamiltonian path can exist.

9.3 Tournament Graphs

Definition ▶ Tournament

Let K_n^+ be a complete, directed graph with n vertices. For each distinct pair of vertices x and y, exactly one of the edges (x, y) or (y, x) is in K_n^+. We call K_n^+ a **tournament**, and it is guaranteed to contain a directed Hamiltonian path.

9.4 Useful Theorems

Theorem ▶ Paths

Let $G = (V, E)$ be a loop-free graph with $|V| = n \geq 2$. If $\deg(x) + \deg(y) \geq n - 1$ for all $x, y \in V$ where $x \neq y$, then G must have a Hamiltonian path.

Theorem ▶ Cycles

Let $G = (V, E)$ be a loop-free undirected graph with $|V| = n \geq 3$. If $\deg(x) + \deg(y) \geq n$ for all non-adjacent $x, y \in V$, then G must have a Hamiltonian cycle.

9.5 Graph Coloring

Definition ▶ Coloring