Types of Proofs

- Direct Proof
- Proof by Construction
- Disproof by Counter Example
- Proof by Exhaustion
- Proof by Deduction
- Proof by Contradiction
- Proof by Contraposition
- Proof by Mathematical Induction
- Combinatorial Proof

Logical Form and Logical Equivalence

1	Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2	Associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3	Distributive laws	$p \wedge (q \vee r)$ $\equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r)$ $\equiv (p \vee q) \wedge (p \vee r)$
4	Identity laws	$p \wedge \mathbf{true} \equiv p$	$p \vee \mathbf{false} \equiv p$
5	Negation laws	$p \vee \sim p \equiv \mathbf{true}$	$p \wedge \sim p \equiv \mathbf{false}$
6	Double negative law	$\sim(\sim p) \equiv p$	
7	Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
8	Universal bound laws	$p \vee \mathbf{true} \equiv \mathbf{true}$	$p \wedge \mathbf{false} \equiv \mathbf{false}$
9	De Morgan's laws	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10	Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11	Negation of **true** and **false**	$\sim\mathbf{true} \equiv \mathbf{false}$	$\sim\mathbf{false} \equiv \mathbf{true}$

5

- Conditional Statements and Implication Law: $p \to q \equiv \sim p \vee q$
- Negation of Conditional: $\sim (p \to q) \equiv \ p \wedge \sim q$
- Contrapositive: $\sim q \to \sim p$
- Converse: $q \to p$
- Inverse: $\sim p \to \sim q$
- Biconditional $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

Rule of inference	
Modus Ponens	$p \to q$, p • q
Modus Tollens	$p \to q$, $\sim q$ • $\sim p$
Generalization	p • $p \vee q$; q • $p \vee q$
Specialization	$p \wedge q$ • p ; $p \wedge q$ • q
Conjunction	p, q • $p \wedge q$

Rule of inference		
Elimination	$p \vee q$, $\sim q$ • p	$p \vee q$, $\sim p$ • q
Transitivity	$p \to q$, $q \to r$ • $p \to r$	
Proof by Division Into Cases	$p \vee q$, $p \to r$, $q \to r$ • r	
Contradiction Rule	$\sim p \to \mathbf{false}$ • p	

- Tutorial 2 Q8a: $(\forall x \in D\ P(x)) \wedge (\forall x \in D\ Q(x)) \leftrightarrow \forall x \in D(P(x) \wedge Q(x))$
- Tutorial 2 Q8b: $(\exists x \in D\ P(x)) \wedge (\exists x \in D\ Q(x))$ and $\exists x \in D(P(x) \wedge Q(x))$ are NOT equivalent.

Number Definitions and Theorems

- Even Numbers: $n = 2k$ for some $k \in \mathbb{Z}$
- Odd Numbers: $n = 2k + 1$ for some $k \in \mathbb{Z}$
- Rational Numbers: $r = \frac{a}{b}$ and $b \neq 0$
- Theorem 4.3.1: Every integer is a rational number.
- Theorem 4.3.2: The sum of any two rational numbers is rational.
- Corollary 4.2.3: The double of a rational number is rational.
- Theorem 4.6.1: There is no greatest integer.
- Proposition 4.7.4: For all integers n, if n^2 is even, then n is even.
- Theorem 4.8.1: $\sqrt{2}$ is irrational.
- Corollary 8.1.21: Let $n \in \mathbb{Z}$. Then n is either even or odd, but not both.
- Tutorial 1 Q9: The product of any 2 odd integers is an odd integer
- Tutorial 1 Q10: If a, b, c are integers such that $a^2 + b^2 = c^2$, then a, b cannot both be odd.
- Tutorial 2 Q3: $\forall a, b, c \in \mathbb{Z}$, if $a - b$ is even and $a - c$ is even, then $b - c$ is even
- Assignment 1 Q7: Let a be a rational number and b an irrational number. Then $a \neq 0 \rightarrow abisirrational$.
- Assignment 1 Q8: $\forall n \in \mathbb{Z}, n^2 + n$ is even.

Sets

- Definition 5.1.3: Roster Notation (listing out all elements of the set) $\{1, 2, 3\}$
- Definition 5.1.5: Set-Builder Notation $\{x \in U : P(x)\}$
- Definition 5.1.9: Two sets are equal if and only if they have the same elements.
- Definition 5.1.15: The set with no element is called the empty est. It is denoted by $\varnothing$.
- Definition 5.2.1: The set of all subsets of A, denoted $P(A)$, is called the power set of A.
- Theorem 5.2.4: Suppose A is a finite set. Then $|P(A)| = 2^{|A|}$.
- Definition 5.2.6: An ordered pair is an expression of the form (x, y). Let (x, y) and (x', y') be ordered pairs. Then $(x, y) = (x', y')$ if and only if $x = x'$ and $y = y'$.
- Definition 5.2.8: Let A, B be sets. The Cartesian product of A and B, denoted A $\times$ B, is defined to be $\{(x, y) : x \in A \text{ and } y \in B\}$
- Theorem 5.3.11: Let A, B be disjoint finite sets. Then $|A \cup B| = |A| + |B|$.
  Let $A_1, A_2, ..., A_n$ be pairwise disjoint finite sets. Then $|A_1| + |A_2| + ... + |A_n|$.

Set identities (Theorem 5.3.5)

For all set A, B, C in a context where U is the universal set, the following hold.

Identity Laws	$A \cup \varnothing = A$	$A \cap U = A$
Universal Bound Laws	$A \cup U = U$	$A \cap \varnothing = \varnothing$
Idempotent Laws	$A \cup A = A$	$A \cap A = A$
Double Complement Law	$\overline{(\overline{A})} = A$	
Commutative Laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
De Morgan's Laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Absorption Laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complement Laws	$A \cup \overline{A} = U$	$A \cap \overline{A} = \varnothing$
Set Difference Law	$A \setminus B = A \cap \overline{B}$	
	$\overline{\varnothing} = U$	$\overline{U} = \varnothing$

- Tutorial 3 Q4: Let A = {2n + 1 : $n \in \mathbb{Z}$} and B = {2n - 1 : $n \in \mathbb{Z}$}. Then A = B.
- Tutorial 3 Q7: $A \cap (B \backslash C) = (A \cap B) \backslash C$
- Tutorial 3 Q8: $(A \cup \overline{B}) \cap (\overline{A} \cup B) = (A \cap B) \cup (\overline{A} \cap \overline{B})$
- Tutorial 3 Q9: $A \subseteq B \leftrightarrow A \cup B = B$
- Assignment 1 Q11a: If $P(A \cup B) \subseteq P(A) \cup P(B)$, then either $A \subseteq B$ or $B \subseteq A$.

Functions

- Definition 6.1.1 (Function): A function or a map from A to B is an assignment to each element of A exactly one element of B. We write $f : A \to B$ for "f is a function from A to B"
- Terminology 6.1.18 (Well Definition): A function is well-defined if its definition ensures that every element of the domain is assigned exactly one element of the codomain
- Definition 6.1.19 (Equality of Functions): Two functions $f : A \to B$ and $g : C \to D$ are equal if:

$$\begin{array}{c}(1)\ A = C \text{ and } B = D; \text{ and} \\ (2)\ f(x) = g(x) \text{ for all } x \in A\end{array}$$

- Definition 6.1.22 (Function Composition): Let $f : A \to B$ and $g :\to C$. Then $g \circ f : A \to C$ such that for every $x \in A$, $(g \circ f)(x) = g(f(x))$
- Functions Compositions are non-commutative, but associative
- Definition 6.2.1 (Setwise image and preimage):
  Let $f : A \to B$.
  (1) If $X \subseteq A$, then let $f(X) = \{y \in B : y = f(x) \text{ for some } x \in X\} = \{f(x) : x \in X\}$
  (2) If $Y \subseteq B$, then let $f^{-1}(Y) = \{x \in A : y = f(x) \text{ for some } y \in Y\}$
  We call $f(X)$ the image of X, and $f^{-1}(Y)$ the preimage of Y under f
- Definition 6.2.5 (Surjection, Injection, Bijection):
  (1) f is *surjective* if $\forall y \in B\ \exists x \in A\ (y = f(x))$
  (2) f is *injective* if $\forall x, x' \in A\ (f(x) = f(x') \to x = x')$
  (3) f is *bijective* if it is surjective and injective, i.e., $\forall y \in B\ \exists! x \in A\ (y = f(x))$

- Prove Surjectivity:
  Example 6.2.6: The function $f : \mathbb{Q} \to \mathbb{Q}$, defined by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$, is surjective.

  Proof:
  1. Take any $y \in \mathbb{Q}$.
  2. Let $x = (y - 1)/3$.
  3. Then $x \in \mathbb{Q}$ and $f(x) = 3x + 1 = y$.

- Prove Non-surjectivity:
  - Remark 6.2.7(2): A function $f : A \to B$ is not surjective if and only if $\exists y \in B\ \forall x \in A\ (y \neq f(x))$

  Example 6.2.8: Define $g : \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then g is not surjective.

  Proof:
  1. Note $g(x) = x^2 \geq 0 > -1$ for all $x \in \mathbb{Z}$.
  2. So $g(x) \neq -1$ for all $x \in \mathbb{Z}$, although $-1 \in \mathbb{Z}$.

- Prove Injectivity:
  Example 6.2.9: The function $f : \mathbb{Q} \to \mathbb{Q}$, defined by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$, is injective.

  Proof:
  1. Let $x, x' \in \mathbb{Q}$ such that $f(x) = f(x')$.
  2. Then $3x + 1 = 3x' + 1$.
  3. So $x = x'$.

- Prove Non-injectivity:
  - Remark 6.2.10: A function $f : A \to B$ is not injective if $\exists x, x' \in A\ (f(x) = f(x') \wedge x \neq x')$.

  Example 6.2.11: Define $g : \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then g is not injective.

  Proof:
  Note $g(1) = 1^2 = (-1)^2 = g(-1)$, although $1 \neq -1$.

- Definition 6.2.13 (Inverse): Let $f : A \to B$. Then $g : B \to A$ is an inverse of f if $\forall x \in A\ \forall y \in B\ (y = f(x) \leftrightarrow x = g(y))$.

- Example 6.2.14 (Showing Inverse): Define $f : \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$.

  1. Note that for all $x, y \in \mathbb{Q}$, $y = 3x + 1 \leftrightarrow x = (y - 1)/3$.
  2. Let $g : \mathbb{Q} \to \mathbb{Q}$ such that $g(y) = (y - 1)/3$ for all $y \in \mathbb{Q}$.
  3. Then the equivalence above tells us $\forall x, y \in \mathbb{Q}\ (y = f(x) \leftrightarrow x = g(y))$.
  4. So g is an inverse of f.

- Proposition 6.2.16 (Uniqueness of inverses): If g, g' are inverses to $f : A \to B$, then $g = g'$.

- Theorem 6.2.18 (Bijection and Invertibility): A function $f : A \to B$ is bijective if and only if it has an inverse.

- Tutorial 4 Q4: Let $f : B \to C$.
  (a) Suppose f is injective. Then $g \circ f$ is injective whenever g is an injective function with domain C.
  (b) Suppose g is a function with domain C such that $g \circ f$ is injective. Then f is injective.

- Tutorial 4 Q5a: Let $f : B \to C$.
  (a) Suppose f is surjective. Then $f \circ h$ is surjective whenever h is an surjective function with codomain B.
  (b) Suppose h is a function with codomain B such that $f \circ h$ is surjective. Then f is surjective.

- Tutorial 4 Q9a: Let $f : A \to B$. Let $X \subseteq A$ and $Y \subseteq B$.
  (a) Then $X \subseteq f^{-1}(f(X))$, but $f^{-1}(f(X)) \subseteq X$ is NOT NECESSARILY true.
  (b) Then $f(f^{-1}(Y)) \subseteq Y$, but $Y \subseteq f(f^{-1}(Y))$ is NOT NECESSARILY true.

Mathematical Induction and Recursion

- Mathematical Induction Example:

Example 7.1.5. $n! > 2^n$ for all $n \in \mathbb{Z}_{\geqslant 4}$.

$n! = n \times (n-1) \times \cdots \times 1$.

To prove that $\forall n \in \mathbb{Z}_{\geqslant m}\ P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:
(base step) show that $P(m)$ is true;
(induction step) show that $\forall k \in \mathbb{Z}_{\geqslant m}\ \big(P(k) \Rightarrow P(k+1)\big)$ is true.

Proof

1. For each $n \in \mathbb{Z}_{\geqslant 4}$, let $P(n)$ be the proposition "$n! > 2^n$".
2. (Base step) $P(4)$ is true because $4! = 24 > 16 = 2^4$.
3. (Induction step)
   - 3.1. Let $k \in \mathbb{Z}_{\geqslant 4}$ such that $P(k)$ is true, i.e., such that $k! > 2^k$.
   - 3.2. Then $(k+1)! = (k+1) \times k!$ by the definition of !;
   - 3.3. $> (k+1) \times 2^k$ by the induction hypothesis $P(k)$;
   - 3.4. $> 2 \times 2^k$ as $k + 1 \geqslant 4 + 1 > 2$;
   - 3.5. $= 2^{k+1}$.
   - 3.6. So $P(k+1)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 4}\ P(n)$ is true by MI. □

Terminology 7.1.4. We call this an induction *on* n as n is the active variable in it.

- Strong Mathematical Induction Example:

1/2

Example 7.2.6 (again). $F_{n+1} \leqslant (7/4)^n$ for every $n \in \mathbb{Z}_{\geqslant 0}$.

To prove that $\forall n \in \mathbb{Z}_{\geqslant 0}\ P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:
(base step) show that $P(0), P(1)$ are true;
(induction step) show that $\forall k \in \mathbb{Z}_{\geqslant 0}\ \big(P(0) \wedge \cdots \wedge P(k+1) \Rightarrow P(k+2)\big)$ is true.

1. For each $n \in \mathbb{Z}_{\geqslant 0}$, let $P(n)$ be the proposition "$F_{n+1} \leqslant (7/4)^n$".
2. (Base step) $P(0)$ and $P(1)$ are true because
   $F_{0+1} = 1 \leqslant 1 = (7/4)^0$ and
   $F_{1+1} = 1 + 0 = 1 \leqslant 7/4 = (7/4)^1$.
3. (Induction step)
   - 3.1. Let $k \in \mathbb{Z}_{\geqslant 0}$ such that $P(0), P(1), \ldots, P(k+1)$ are true.
   - ⋮
   - 3.8. So $P(k+2)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 0}\ P(n)$ is true by Strong MI.

$F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \in \mathbb{Z}_{\geqslant 0}$.

2/2

Example 7.2.6 (again). $F_{n+1} \leqslant (7/4)^n$ for every $n \in \mathbb{Z}_{\geqslant 0}$.

To prove that $\forall n \in \mathbb{Z}_{\geqslant 0}\ P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:
(base step) show that $P(0), P(1)$ are true;
(induction step) show that $\forall k \in \mathbb{Z}_{\geqslant 0}\ \big(P(0) \wedge \cdots \wedge P(k+1) \Rightarrow P(k+2)\big)$ is true.

1. For each $n \in \mathbb{Z}_{\geqslant 0}$, let $P(n)$ be the proposition "$F_{n+1} \leqslant (7/4)^n$".
2. (Base step) $P(0)$ and $P(1)$ are true because ...
3. (Induction step)
   - 3.1. Let $k \in \mathbb{Z}_{\geqslant 0}$ such that $P(0), P(1), \ldots, P(k+1)$ are true.
   - 3.2. Then $F_{(k+2)+1} = F_{k+3}$
   - 3.3. $= F_{k+2} + F_{k+1}$ by the definition of F_{k+3};
   - 3.4. $\leqslant (7/4)^{k+1} + (7/4)^k$ as $P(k)$ and $P(k+1)$ are true;
   - 3.5. $= (7/4)^k(7/4 + 1)$
   - 3.6. $< (7/4)^k(7/4)^2$ as $7/4 + 1 < (7/4)^2$;
   - 3.7. $= (7/4)^{k+2}$.
   - 3.8. So $P(k+2)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 0}\ P(n)$ is true by Strong MI. □

$F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \in \mathbb{Z}_{\geqslant 0}$.

- Theorem 7.2.9 (Well-Ordering Principle): Every non-empty subset of $\mathbb{Z}_{\geqslant 0}$ has a smallest element.
- Recursive Definition consists of the base clause, recursion clause, and minimality clause.
- (Structural Induction over S, where S is a recursively defined set)
  To prove that $\forall n \in SP(n)$ is true, where each $P(n)$ is a proposition, it suffices to:
  (base step): show that $P(1)$ is true; and
  (induction step): show that $\forall x \in S\ (P(x) \to \{\text{recursive clause here}\})$ is true.

Divisibility, Primes and Base Expansion

- Definition 8.1.1 (Divisibility $d|n$): Let $n, d \in \mathbb{Z}$. Then d is said to divide n if $n = dk$ for some $k \in \mathbb{Z}$.
- Lemma 8.1.5: Let $n, d \in \mathbb{Z}$ with $d \neq 0$. Then $d|n$ if and only if $n/d \in \mathbb{Z}$.
- Lemma 8.1.9: Let $d, n \in \mathbb{Z}$. If $d|n$, then $-d|n$ and $d|-n$ and $-d|-n$.
- Proposition 8.1.10: Let $d, n \in \mathbb{Z}$. If $d|n$ and $n \neq 0$, then $|d| \leqslant |n|$.
- Theorem 8.1.12 (Transitivity of Divisibility): Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.
- Lemma 8.1.14 (Closure Lemma of Division): Let $a, b, d, m, n \in \mathbb{Z}$. If $d|m$ and $d|n$, then $d|am + bn$.
- Theorem 8.1.16 (Division Theorem): For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ such that $n = dq + r$ and $0 \leqslant r < d$.
  (Note: q, the quotient is denoted by n div d; r, the remainder is denoted by n mod d)
  - e.g. 11 div $5 = 2$ and 11 mod $5 = 1$ because $11 = 5 \times 2 + 1$ and $0 \leqslant 1 < 5$.
  - e.g. -16 div $3 = -6$ and -16 mod $3 = 2$ because $-16 = 3 \times -6 + 2$ and $0 \leqslant 2 < 3$.
- Definition 8.2.1 (Primes and Composites):
  (1) A positive integer is prime if it has exactly two positive divisors.
  (2) A positive integer is composite if it has (strictly) more than two positive divisors.
- Lemma 8.2.4: An integer n is composite if and only if n has a divisor d such that $1 < d < n$.
- Lemma 8.2.5 (Prime Divisor Lemma): Let $n \in \mathbb{Z}_{\geqslant 2}$. Then n has a prime divisor.
- Proposition 8.2.6: Let n be a composite positive integer. Then n has a prime divisor $p \leqslant \sqrt{n}$.
  (Note: We can use the contraposition of Proposition 8.2.6 to prove that a number is a prime)
- Theorem 8.2.8 (Euclid): There are infinitely many prime numbers.
- Base-b Representation:

Algorithm for finding base-b representation

Algorithm 8.3.8 ($b \in \mathbb{Z}_{\geqslant 2}$ fixed)

1. **input** $n \in \mathbb{Z}^+$
2. $q \coloneqq n$
3. $\ell \coloneqq 0$
4. **while** $q \neq 0$ **do**
5. $\quad a_\ell \coloneqq q$ mod b
6. $\quad q \coloneqq q$ div b
7. $\quad \ell \coloneqq \ell + 1$
8. **end do**
9. **output** $(a_{\ell-1}a_{\ell-2}\ldots a_1a_0)_b$

q div b and q mod b denote respectively the quotient and the remainder when q is divided by b.

Example 8.3.9. $(b, n) = (8, 1511)$

$8 \mid 1511$
$8 \mid 188$ — 7 $\to a_0$
$8 \mid 23$ — 4 $\to a_1$
$8 \mid 2$ — 7 $\to a_2$
0 — 2 $\to a_3$

So $1511 = (2747)_8$.

Example 8.3.10. $(b, n) = (16, 1511)$

$16 \mid 1511$
$16 \mid 94$ — 7 $\to a_0$
$16 \mid 5$ — $14 = \mathrm{E}$ $\to a_1$
0 — 5 $\to a_2$

So $1511 = (5\mathrm{E}7)_{16}$.

Example 8.3.6

(1) $(1231)_{10}$ is the decimal representation of 1231.

(2) $(1000011)_2$ is the binary representation of 67 because

$$1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 67.$$

(3) $(117)_8$ is the octal representation of 79 because $1 \times 8^2 + 1 \times 8^1 + 7 \times 8^0 = 79$.

(4) $(4D)_{16}$ is the hexadecimal representation of 77 because $4 \times 16^1 + 13 \times 16^0 = 77$.

- Tutorial 6 Q1: Let $a, b \in \mathbb{Z}$. If $a|b$ and $b|a$, then $a = b$ or $a = -b$.
- Tutorial 6 Q3: For all odd numbers $n \in \mathbb{Z}$, $n^2 div 4 = \frac{n^2-1}{4}$
- Tutorial 6 Q6: A positive integer n is a perfect square $\leftrightarrow$ n has an odd number of positive divisors
- Tutorial 6 Q9: Let $n \in \mathbb{Z}_{\geqslant 1}$ with decimal representation $(a_\ell a_{\ell-1} ... a_0)_{10}$. Then $9|n \leftrightarrow 9|(a_0 + a_1 + ... + a_\ell)$
- Assignment 2 Q2: Let $a \in \mathbb{Z}_{\geq 2}$. Suppose that $\forall m, n \in \mathbb{Z}^+$, if $a|mn$, then $a|m$ or $a|n$. Then a is prime.

Euclidean Algorithm, Fundamental Theorem of Arithmetic and Modular Arithmetic

- Definition 8.4.1 (gcd): Let $m, n \in \mathbb{Z}$.
  (1) A common divisor of m and n is divisor of both m and n.
  (2) The greatest common divisor of m and n is denoted $gcd(m, n)$.
- Exercise 8.4.3: Let $m, n \in \mathbb{Z}^+$. m mod $n = 0$ if and only if $gcd(m, n) = n$.
- Exercise 8.4.6: Let $m, n \in \mathbb{Z}^+$. If p is prime, then either $gcd(m, p) = 1$ or $p|m$.
- Euclidean Algorithm (the divisor that gives remainder 0 is the gcd):

The Euclidean Algorithm

Algorithm 8.4.8

1. **input** $m, n \in \mathbb{Z}^+$ with $m \geqslant n > 0$
2. $x := m$
3. $y := n$
4. **while** $y \neq 0$ **do**
5. $\quad r := x \bmod y$
6. $\quad x := y$
7. $\quad y := r$
8. **end do**
9. **output** x

Definitions 8.1.16 and 8.1.17.
$x \bmod y$ is the remainder when x is divided by y, and $0 \leqslant x \bmod y < y$.

To find gcd(m, n), where $m \geqslant n > 0$:

$$\begin{array}{ccccc} x & & y & & r \\ \downarrow & & \downarrow & & \downarrow \\ m & \bmod & n & = & r_1 \\ n & \bmod & r_1 & = & r_2 \\ r_1 & \bmod & r_2 & = & r_3 \\ r_2 & \bmod & r_3 & = & r_4 \\ & & \vdots & & \\ r_{k-2} & \bmod & r_{k-1} & = & r_k \\ r_{k-1} & \bmod & r_k & = & 0 \end{array}$$

$\therefore$ gcd$(m, n) = r_k$

Example 8.4.9. To find gcd(1076, 414):

$$\begin{array}{ccccc} x & & y & & r \\ \downarrow & & \downarrow & & \downarrow \\ 1076 & \bmod & 414 & = & 248 \\ 414 & \bmod & 248 & = & 166 \\ 248 & \bmod & 166 & = & 82 \\ 166 & \bmod & 82 & = & 2 \\ 82 & \bmod & 2 & = & 0 \end{array}$$

$\therefore$ gcd$(1076, 414) = 2$

- Lemma 8.4.11: If $x, y, z \in \mathbb{Z}$ such that x mod $y = r$, then $gcd(x, y) = gcd(y, r)$.
- Theorem 8.5.2 (Bezout's Lemma): For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $gcd(m, n) = ms + nt$. (Note: use the Euclidean Algorithm to backtrack and obtain this integer linear combination)
- Theorem 8.5.5 (Euclid's Lemma): Let $m, n, p \in \mathbb{Z}^+$. If p is prime and $p|mn$, then $p|m$ or $p|n$.
- Corollary 8.5.6: Let $n, m_0, m_1, ..., m_n, p \in \mathbb{Z}+$. If p is prime and $p \mid m_0 m_1 ... m_n$, then $p \mid m_i$ for some $i \in \{0, 1, ..., n\}$.
- Theorem 8.5.9 (Fundamental Theorem of Arithmetic; Prime Factorization Theorem):
  Every integer $n \geqslant 2$ has a unique prime factorization in which the prime factors are arranged in nondecreasing order.

- Definition 8.6.1 (Congruence): Let $a, b \in \mathbb{Z}^+$. Then a is congruent to b modulo n if $a \bmod n = b \bmod n$. In this case, we write $a \equiv b \pmod{n}$.
- Lemma 8.6.2: The following are equivalent for all $a, b \in \mathbb{Z}$ and all $n \in \mathbb{Z}^+$:
  (1) $a \equiv b \pmod{n}$
  (2) $a = nk + b$ for some $k \in \mathbb{Z}$
  (3) $n \mid (a - b)$
- Lemma 8.6.5: Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$:
  (1) (Reflexivity) $a \equiv a \pmod{n}$
  (2) (Symmetry) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
  (3) (Transitivity) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$
- Proposition 8.6.6 (Addition of Congruence): Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a + c \equiv b + d \pmod{n}$.
- Proposition 8.6.13 (Multiplication of Congruence): Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ such that $a \equiv b \pmod{\text{n}}$ and $c \equiv d \pmod{n}$. Then $ac \equiv bd \pmod{n}$.
- Definition 8.6.8 (Additive Inverse): Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. The integer b is an additive inverse of a modulo n if $a + b \equiv 0 \pmod{n}$.
- Proposition 8.6.10 (Additive Inverse): Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
  (1) $-a$ is an additive inverse of a modulo n.
  (2) b is an additive inverse of a modulo n if and only if $b \equiv -a \pmod{n}$.
- Definition 8.6.15 (Multiplicative Inverse): Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. A multiplicative inverse of a modulo n is an integer b such that $ab \equiv 1 \pmod{n}$.
- Proposition 8.6.16 (Multiplicative Inverse): Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
  (1) Let b, b' be multiplicative inverses of a. Then $b \equiv b' \pmod{n}$.
  (2) Let b be a multiplicative inverse of a and $b' \in \mathbb{Z}$ such that $b \equiv b' \pmod{n}$. Then b' is also a multiplicative inverse of a.
- Theorem 8.6.19 (Existence of Multiplicative Inverse):
  Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
  (Note: Apply Bezout's Lemma to find Multiplicative Inverse, if it exists)
- Tutorial 7 Q2: Let $a, b, c \in \mathbb{Z}$ If $a \mid c$ and $b \mid c$ and $gcd(a, b) = 1$, then $ab \mid c$.
- Tutorial 7 Q3: Let $a, b, s, t \in \mathbb{Z}$ such that $as + bt = 1$. Then $gcd(a, b) = 1$,
- Tutorial 7 Q4: Let $a, b, s, t \in \mathbb{Z}$ such that $as + bt = gcd(a, b)$. Then $gcd(s, t) = 1$,
- Tutorial 7 Q5: Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. Then $gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right) = 1$.
- Tutorial 7 Q6: Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. Then an integer n is an integer linear combination of a and $b \leftrightarrow gcd(a, b) \mid n$.

Relations, Equivalence Relations and Partitions, and Partial Orders

- Definition 9.1.1 (Relations):
  (1) A relation from A to B is a subset of $A \times B$.
  (2) Let R be a relation from A to B and $(x, y) \in A \times B$. Then we may write:

$$x \; R \; y \text{ for } (x, y) \in R \quad \text{and} \quad x \not R \; y \text{ for } (x, y) \notin R$$

  (3) R^{-1} is the inverse relation of R (i.e. $R^{-1} = \{(y, x) : (x, y) \in R\}$)
- Definition 9.2.1: A (binary) relation on a set A is a relation from A to A.

- Definition 9.2.2: Let A be a set and R be a relation on A.
  (1) R is reflexive if $\forall x \in A\ (x\ R\ x)$
  (2) R is symmetric if $\forall x, y \in A\ (x\ R\ y \to y\ R\ x)$
  (3) R is transitive if $\forall x, y, z \in A\ (x\ R\ y \wedge y\ R\ z \to x\ R\ z)$

- Definition 9.2.9 (Equivalence Relations): An equivalence relation is a relation that is reflexive, symmetric and transitive

- Definition 9.2.10 (Equivalence Class): Let A be a set and R be an equivalence relation on A. For each $x \in A$, the equivalence class of x with respect to R, denoted $[x]_R$, is defined by:

$$[x]_R = \{y \in A : x\ R\ y\}$$

- $A/R = \{[x]_R : x \in A\}$

- Proposition 9.2.13: Let R be an equivalence relation on a set A. The following are equivalent for all $x, y \in A$:
  (1) $x\ R\ y$
  (2) $[x] = [y]$
  (3) $[x] \cap [y] \neq \varnothing$

- Definition 9.3.1 (Partitions): A partition of a set A is a set C of nonempty subsets of A such that
  ($\geqslant 1$) $\forall x \in A\ \exists S \in C\ (x \in S)$ and
  ($\leqslant 1$) $\forall x \in A\ \forall S, S' \in C\ (x \in S \wedge x \in S' \to S = S')$
  (Note: elements of a partition are called components of the partition.)

- Theorem 9.3.4: Let R be an equivalence relation on a set A. Then A/R is a partition on A.

- Theorem 9.3.5: Let C be a partition of a set A. Then there is an equivalence relation R on A such that $A/R = C$.

- Definition 9.4.1 (Partial Orders): Let A be a set and R be a relation on A.
  (1) R is antisymmetric if $\forall x, y \in A\ (x\ R\ y \wedge y\ R\ x \to x = y)$
  (2) R is a (non-strict) partial order if R is reflexive, antisymmetric, and transitive
  (3) R is a (non-strict) total order if R is a partial order and $\forall x, y \in A\ (x\ R\ y \vee y\ R\ x)$

- Hasse Diagrams:

Positive divisors of 30

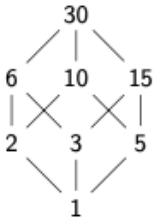
Notation 9.4.10
We often use $\preccurlyeq$ to denote a partial order. In this case, we write $x \prec y$ for $x \preccurlyeq y \wedge x \neq y$.

Definition 9.4.11
Let $\preccurlyeq$ be a partial order on a set A. A *Hasse diagram* of $\preccurlyeq$ satisfies the following condition for all $x, y \in A$:

If $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then x is placed below y and there is a line joining x to y.

Example 9.4.12
Consider $\{d \in \mathbb{Z}^+ : d \mid 30\}$ partially ordered by the divisibility relation $|$.

A Hasse diagram is as follows:



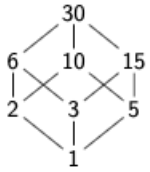
- Definition 9.5.1 Let $\preccurlyeq$ be a partial order on a set A, and $c \in A$:
  (1) c is a minimal element if $\forall x \in A\ (x \preccurlyeq c \to c = x)$
  (2) c is a maximal element if $\forall x \in A\ (c \preccurlyeq x \to c = x)$
  (3) c is the smallest element (or the minimum element) if $\forall x \in A\ (c \preccurlyeq x)$
  (4) c is the largest element (or the maximum element) if $\forall x \in A\ (x \preccurlyeq c)$

- Lemma 9.5.5: Consider a partial order $\preccurlyeq$ on a set A.
  (1) A smallest element. is minimal
  (2) There is at most one smallest element.

- Proposition 9.5.7: With respect to any partial order $\preccurlyeq$ on a finite set $A \neq \varnothing$, one can find a minimal element.
- Theorem 9.5.9: Let A be a set and $\preccurlyeq$ be a partial order on A. Then there exists a total order $\preccurlyeq^*$ on A such that for all $x, y \in A,\ x \preccurlyeq y \to x \preccurlyeq^* y$
- (Linearization) Just use the $\leqslant$ total order for linearization. But where $\leqslant$ is not possible:

Linearization

Want: *total* order $\preccurlyeq^*$ such that for all x, y,
$x \preccurlyeq y \quad \Rightarrow \quad x \preccurlyeq^* y$.



Example 9.5.10

Consider $\{d \in \mathbb{Z}^+ : d \mid 30\}$ partially ordered by the divisibility relation $|$.

- Set $A_0 := \{d \in \mathbb{Z}^+ : d \mid 30\}$.
- 1 is the only minimal element of A_0. Set $c_0 := 1$ and $A_1 := A_0 \setminus \{1\}$.
- $2, 3, 5$ are the minimal elements of A_1. Set $c_1 := 3$ and $A_2 := A_1 \setminus \{3\}$.
- $2, 5$ are the minimal elements of A_2. Set $c_2 := 2$ and $A_3 := A_2 \setminus \{2\}$.
- $5, 6$ is the only minimal element of A_3. Set $c_3 := 5$ and $A_4 := A_3 \setminus \{5\}$.
- $6, 10, 15$ are the minimal elements of A_4. Set $c_4 := 6$ and $A_5 := A_4 \setminus \{6\}$.
- $10, 15$ are the minimal elements of A_5. Set $c_5 := 15$ and $A_6 := A_5 \setminus \{15\}$.
- 10 is the only minimal element of A_6. Set $c_6 := 10$ and $A_7 := A_6 \setminus \{10\}$.
- 30 is the only (minimal) element of A_7. Set $c_7 := 30$ and $A_8 := A_7 \setminus \{30\}$.
- $A_8 = \varnothing$ and so we stop.
- A linearization is $1 \preccurlyeq^* 3 \preccurlyeq^* 2 \preccurlyeq^* 5 \preccurlyeq^* 6 \preccurlyeq^* 15 \preccurlyeq^* 10 \preccurlyeq^* 30$.

- Tutorial 8 Q2: Let R be a relation on a set A. R is symmetric $\leftrightarrow R = R^{-1}$
- Tutorial 8 Q5: Let A, B be non-empty sets and f be a surjection $A \to B$. Then $C = \{\{x \in A : f(x) = y\} : y \in B\}$ is a partition on A.
- Assignment 2 Q5: Let C be a partition on a set A. Then there exists a set B and a surjection $f : A \to B$ such that $C = \{\{x \in A : f(x) = y\} : y \in B\}$.

Counting and Probability I

- Theorem 9.1.1 (The Number of Elements in a List): If m and n are integers and $m \leqslant n$, then there are $n - m + 1$ integers from m t n inclusive.
- Theorem 9.2.1 (Multiplication/ Product Rule): If an operation consists of k steps and
  the first step can be performed in n_1 ways,
  the second step can be performed in n_2 ways (regardless of how the first step was performed),
  ...
  the k^{th} step can be performed in n_k ways (regardless of how the preceding steps were performed),
  Then the entire operation can be performed in $n_1 \times n_2 \times ... \times n_k$ ways.
- Theorem 9.2.2 (Permutations): The number of permutations of a set with n $(n \geqslant 1)$ elements is $n!$.
- Theorem 9.2.3 (r-permutations from a set of n elements): If n and r are integers and $1 \leqslant r \leqslant n$, then the number of r-permutations of a set of n elements is given by the formula:

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

- Theorem 9.3.1 (The Addition/ Sum Rule): Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, ..., A_k$. Then $|A| = |A_1| + |A_2| + ... + |A_k|$.
- Theorem 9.3.2 (The Difference Rule): If A is a finite set and $B \subseteq A$, then $|A \backslash B| = |A| - |B|$.
- Formula for the Probability of the Complement of an Event: $P(\bar{A}) = 1 - P(A)$

- Theorem 9.3.3 (The Inclusion/ Exclusion Rule): If A, B, and C are any finite sets, then:
  (1) $|A \cup B| = |A| + |B| - |A \cap B|$
  (2) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

- (Pigeonhole Principle): A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain.

- (Generalized Pigeonhole Principle): For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if $k < n/m$, then there is some $y \in Y$ such that y is the image of at least $k+1$ distinct elements of X.

  e.g. to fit 28 pigeons into 9 pigeonholes, it is guaranteed that some hole has 4 pigeons since $k = 3 < 28/9$ and $k + 1 = 4$

  (Contrapositive Form): For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each $y \in Y$, $f^{-1}(\{y\})$ has at most k elements, then X has at most km elements; in other words, $n \leqslant km$.

  e.g. If there are 10 modules, and each module is attended by at most 1000 students, then the total number of students is at most 10000

Counting and Probability II

- (Combinations): An r-combination of a set of n elements is a subset of r of the n elements. $\binom{n}{r}$ denotes the number of subsets of size r (r-combinations) that can be chosen from a set of n elements.

- Theorem 9.5.1 (Formula for $\binom{n}{r}$):

$$\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!} \text{ , where } n \text{ and } r \text{ are non-negative integers with } r \leqslant n.$$

- Theorem 9.5.2 (Permutations with Sets of Indistinguishable Objects):

$$\frac{n!}{n_1!n_2!...n_k!} \text{ , where } n_1, n_2, ..., n_k \text{ are the number of objects of type } 1, 2, ..., k$$

- Theorem 9.6.1 (Number of r-combinations with Repetition Allowed/ Number of multisets of size r):

$$\binom{r+n-1}{r} \text{ , where } r \text{ is the number of objects to be selected from a set of } n \text{ elements}$$

  (This equals the number of ways r objects can be selected from n categories of objects with repetitions allowed. Or similarly, r number of objects, and $n-1$ 'category dividers')

- Theorem 9.7.1 (Pascal's Formula):

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r} \text{ , where } n, r \in \mathbb{Z}^+ \text{ and } r \leqslant n$$

- Lecture Example 8: $\binom{n}{r} = \binom{n}{n-r}$

- Lecture Example 10: $k\binom{n}{k} = n\binom{n-1}{k-1}$

- Theorem 9.7.2 (Binomial Theorem): Given any real numbers a and b and any non-negative integer n,

$$(a+b)^n = \Sigma_{k=0}^{n} \binom{n}{k} a^{n-k}b^k = a^n + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + ... + \binom{n}{n-1}a^1b^{n-1} + b^n$$

- (Probability Axioms):
  (1) $0 \leqslant P(A) \leqslant 1$, where A is an event in sample space S
  (2) $P(\varnothing) = 0$ and $P(S) = 1$
  (3) If A and B are disjoint events ($A \cap B = \varnothing$), then $P(A \cup B) = P(A) + P(B)$

- (Probability of the Complement of an Event): If A is any event in a sample space S, then $P(\bar{A}) = 1 - P(A)$
- (Probability of a General Union of Two Events): If A and B are any events in a sample space S, then $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.
- (Expected Value): Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, ..., a_n$ which occur with probabilities $p_1, p_2, ..., p_n$ respectively. The expected value of the process is:

$$\Sigma_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + ... + a_n p_n$$

- (Linearity of Expectation): The expected value of the sum of random variables is equal to the sum of their individual expected values, regardless of whether they are independent.

  For random variables X and Y (which may be dependent), $E[X + Y] = E[X] + E[Y]$

  e.g. Using linearity of expectation, the expected value for the sum of two dice $= 3.5 + 3.5 = 7$, where 3.5 is the expected value for a fair dice

- (Conditional Probability): Let A and B be events in a sample space S. If $P(A) \neq 0$, then the conditional probability of B given A is:
  (1) $P(B|A) = \frac{P(A \cap B)}{P(A)}$
  (2) $P(A \cap B) = P(B|A) \cdot P(A)$
  (3) $P(A) = \frac{P(A \cap B)}{P(B|A)}$
- Theorem 9.9.1 (Bayes' Theorem):

$$P(B_k|A) = \frac{P(A|B_k) \cdot P(B_k)}{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + ... + P(A|B_n) \cdot P(B_n)} ,$$

  where $B_1, B_2, ...B_n$ are mutually disjoint events, and A and all the B_i have non-zero probabilities

- (Independent Events): If A and B are events in a sample space S, then A and B are independent if and only if:

$$P(A \cap B) = P(A) \cdot P(B)$$

- (Pairwise Independent and Mutually Independent) Three events A, B, and C are pairwise independent, if and only if, they satisfy conditions 1-3 below. They are mutually independent, if and only if, they satisfy all four conditions below:
  (1) $P(A \cap B) = P(A) \cdot P(B)$
  (2) $P(A \cap C) = P(A) \cdot P(C)$
  (3) $P(B \cap C) = P(B) \cdot P(C)$
  (4) $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

  (Note: Events can be pairwise independent without satisfying the condition $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$. Conversely, they can satisfy the condition $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$ without being pairwise independent.)
- (Generalized Definition of Mutually Independent): Events $A_1, A_2, ..., A_n$ in a sample space S are mutually independent, if and only if, the probability of the intersection of any subset of the events is the product of the probabilities of the events in the subset.

Graphs

- (Simple Graph): A simple graph is an undirected graph that does not have any loops or parallel edges. (That is, there is at most one edge between each pair of distinct vertices.)
- (Complete Graphs): A complete graph on n vertices, $n > 0$, denoted K_n, is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.
- (Bipartite Graph): A bipartite graph (or bigraph) is a simple graph whose vertices can be divided into two disjoint sets U and V such that every edge connects a vertex in U to one in V.

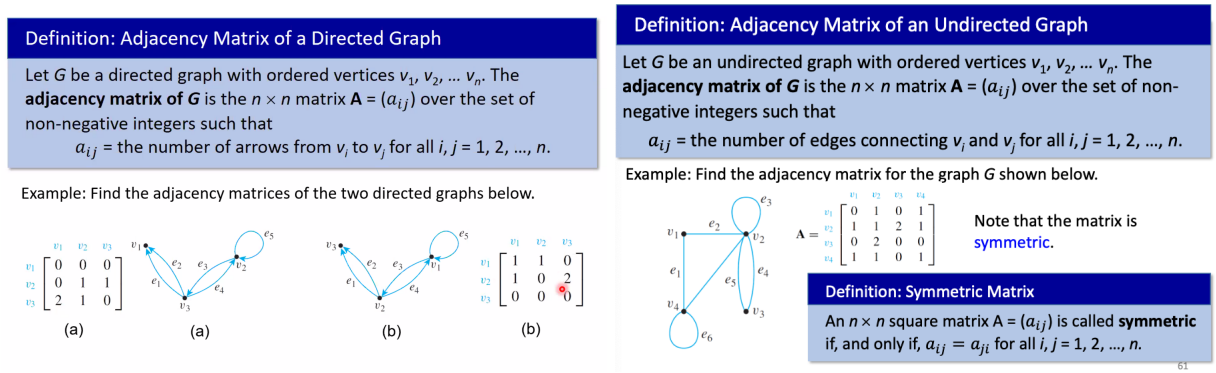
- (Complete Bipartite Graph): A complete bipartite graph is a bipartite graph on two disjoint sets U and V such that every vertex in U connects to every vertex in V.
  (Note: If $|U| = m$ and $|V| = n$, the complete bipartite graph is denoted as $K_{m,n}$)
- (Subgraph of a Graph): A graph H is said to be a subgraph of graph G if and only if every vertex in H is also a vertex in G, every edge in H is also an edge in G, and every edge in H has the same endpoints as it has in G.
- (Degree of a Vertex and Total Degree of an Undirected Graph):
  (1) Let G be an undirected graph and v a vertex of G. The degree of v, denoted $\deg(v)$, equals the number of edges that are incident on v, with an edge that is a loop counted twice.
  (2) The total degree of G is the sum of the degrees of all the vertices of G.
- Theorem 10.1.1 (The Handshake Theorem): The total degree of a graph $G = 2\times$ (the number of edges of G)
- Corollary 10.1.2: The total degree of a graph is even.
- Proposition 10.1.3: In any graph there are an even number of vertices of odd degree.
- (Walk): A walk from v to w is a finite alternating sequence of adjacent vertices and edges of G.
- (Trivial Walk): The trivial walk from v to v consists of the single vertex v.
- (Trail): A trail from v to w is a walk from v to w that does not contain a repeated edge.
- (Path): A path from v to w is a trail that does not contain a repeated vertex.
- (Closed Walk): A closed walk is a walk that starts and ends at the same vertex.
- (Circuit/ Cycle): Let $n \in \mathbb{Z}_{\geqslant 3}$. An undirected graph $G(V, E)$ where

  $$V = \{x_1, x_2, ..., x_n\} \text{ and } E = \{\{x_1, x_2\}, \{x_2, x_3\}, ..., \{x_{n-1}, x_n\}, \{x_n, x_1\}\}$$

  is called a circuit/ cycle. (AKA: a circuit is a closed walk that does not contain a repeated edge)
- (Simple Circuit): A simple circuit (or simple cycle) is a circuit that does not have any other repeated vertex except the first and last.
- An undirected graph is cyclic if it contains a loop or a cycle; otherwise, it is acyclic.
- (Connectedness): A graph G is connected if and only if given any two vertices v and w in G, there is a walk from v to w.
- Lemma 10.2.1: Let G be a graph.
  (1) If G is connected, then any two distinct vertices of G can be connected by a path.
  (2) If vertices v and w are part of a circuit in G and one edge is removed from the circuit, then there still exists a trail from v to w in G.
  (3) If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G.
- (Connected Component): A graph H is a connected component of a graph G if and only if
  (1) The graph H is a subgraph of G.
  (2) The graph H is connected.
  (3) No connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H.
  (AKA: a connected component of a graph is a connected subgraph of largest possible size)
- (Euler Circuit): Let G be a graph. An Euler Circuit for G is a circuit that contains every vertex and traverses every edge of G exactly once.
- (Eulerian Graph): An Eulerian Graph is a graph that contains an Euler Circuit.
- Theorem 10.2.2: If a graph has an Euler Circuit, then every vertex of the graph has positive even degree.
  (Contrapositive): If some vertex of a graph has odd degree, then the graph does not have an Euler Circuit.

- Theorem 10.2.3: If a graph G is connected and the degree of every vertex of G is a positive even integer, then G has an Euler Circuit.
- Theorem 10.2.4: A graph G has an Euler Circuit if and only if G is connected and every vertex of G has positive even degree.
- (Euler Trail): An Euler Trail from v to w is a sequence of adjacent edges and vertices that starts at v, ends at w, passes through every vertex of G at least once, and traverses every edge of G exactly once.
- Corollary 10.2.5: There is an Euler Trail from v to w if and only if G is connected, v and w have odd degree, and all other vertices of G have positive even degree.
- (Hamiltonian Circuit): A Hamiltonian Circuit for G is a simple circuit that includes every vertex of G. (That is, every vertex appears exactly once, except for the first and the last, which are the same.)
- (Hamiltonian Graph): A Hamiltonian Graph is a graph that contains a Hamiltonian Circuit.
- (Differences between Euler Circuit and Hamiltonian Circuit):
  (1) Euler Circuit may visit some vertices more than once while Hamiltonian Circuit can only visit each vertex exactly once (both visit all vertices in G)
  (2) Euler Circuit traverses every edge in G exactly once, while Hamiltonian Circuit does not need to traverse all edges.
- Proposition 10.2.6: If a graph G has a Hamiltonian Circuit, then G has a subgraph H with the following properties:
  (1) H contains every vertex of G
  (2) H is connected
  (3) H has the same number of edges as vertices
  (4) Every vertex of H has degree 2

  (Contraposition): If a graph G does not have a subgraph H with properties (1)-(4), then G does not have a Hamiltonian Circuit
- Adjacency Matrix (Directed and Undirected Graphs):



- Theorem 10.3.2 (n-th power of adjacency matrix): The ij-th entry of A^n = the number of walks of length n from v_i to v_j
- (Isomorphic Graph): Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs.
  G is isomorphic to G' if and only if there exists a permutation $\pi : V_G \to V_{G'}$ such that $\{u, v\} \in E_G \leftrightarrow \{\pi(u), \pi(v)\} \in E_{G'}$.
- Theorem 10.4.1: Let S be a set of graphs and let $\cong$ be the relation of graph isomorphism on S. Then $\cong$ is an equivalence relation on S.
- (Planar Graph): A planar graph is a graph that can be drawn on a (two-dimensional) plane without edges crossing.
- Kuratowski's Theorem: A finite graph is planar if and only if it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$.

- Euler's Formula: For a connected planar simple graph $G = (V, E)$ with $e = |E|$ and $v = |V|$, if we let f be the number of faces, then $f = e - v + 2$
- Tutorial 11 Q2: Every simple graph with at least two vertices has two vertices of the same degree.
- Tutorial 11 Q4: For any simple graph with 6 vertices, G or its complementary graph contains a triangle.
- Tutorial 11 Q6: There are $v - k$ edges in a forest (where v is the number of vertices and k is the number of components).
- Tutorial 11 Q8a: If G is a complete graph with n vertices, the total number of spanning trees in G is n^{n-2}.

Trees

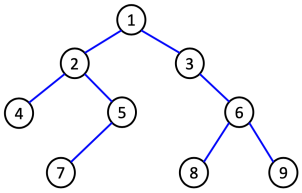
- (Tree): A graph is called a tree if and only if it is circuit-free and connected.
- (Trivial Tree): A trivial tree is a graph that consists of a single vertex.
- (Forest): A graph is called a forest if and only if it is circuit-free and not connected.
- Lemma 10.5.1: Any non-trivial tree has at least one vertex of degree 1.
- (Terminal Vertex/ leaf and internal vertex):
  (1) If T has only one or two vertices, then each is called a terminal vertex (or leaf).
  (2) If T has at least three vertices, then a vertex of degree 1 in T is called a terminal vertex (or leaf), and a vertex of degree greater than 1 in T is called an internal vertex.
- Theorem 10.5.2: Any tree with n vertices ($n > 0$) has $n - 1$ edges.
- Lecture Example: A non-trivial tree has at least 2 vertices of degree 1.
- Lemma 10.5.3: If G is any connected graph, C is any circuit in G, and one of the edges of C is removed from G, then the graph that remains is still connected.
- Theorem 10.5.4: If G is a connected graph with n vertices and $n - 1$ edges, then G is a tree.
- (Rooted Trees): A rooted tree is a tree in which there is one vertex that is distinguished from the others and is called the root.
  (Level): The level of a vertex is the number of edges along the unique path between it and the root.
  (Height): The height of a rooted tree is the maximum level of any vertex of the tree.
  (Also know: children, parent, siblings, ancestor, descendant)
- (Binary Tree): A binary tree is a rooted tree in which every parent has at most two children (a left child, a right child or both)
- (Full Binary Tree): A full binary tree is a binary tree in which each parent has exactly two children.
  (Also know what is Left Subtree and Right Subtree of a (Full) Binary Tree)
- Theorem 10.6.1 (Full Binary Tree Theorem): If T is a full binary tree with k internal vertices, then T has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices (leaves).
- Theorem 10.6.2: For non-negative integers h, if T is any binary tree with height h and t terminal vertices (leaves), then $t \leqslant 2^h$. Equivalently, $log_2 t \leqslant h$

- Binary Tree Traversal:

Breadth-First Search

In breadth-first search (by E.F. Moore), it starts at the root and visits its adjacent vertices, and then moves to the next level.

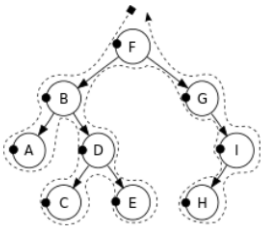
The figure shows the order of the vertices visited.



Depth-First Search

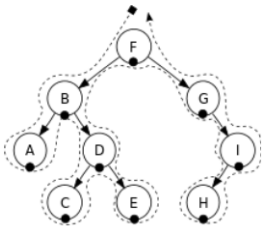
There are three types of depth-first traversal:

- Pre-order
  - Print the data of the root (or current vertex)
  - Traverse the left subtree by recursively calling the pre-order function
  - Traverse the right subtree by recursively calling the pre-order function
- In-order
  - Traverse the left subtree by recursively calling the in-order function
  - Print the data of the root (or current vertex)
  - Traverse the right subtree by recursively calling the in-order function
- Post-order
  - Traverse the left subtree by recursively calling the post-order function
  - Traverse the right subtree by recursively calling the post-order function
  - Print the data of the root (or current vertex)



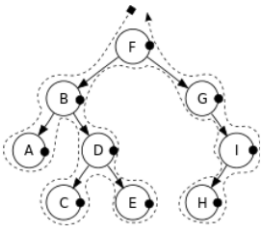
Pre-order:

F, B, A, D, C, E, G, I, H



In-order:

A, B, C, D, E, F, G, H, I



Post-order:

A, C, E, D, B, H, I, G, F

- (Spanning Tree): A spanning tree for a graph G is a subgraph of G that contains every vertex of G and is a tree.
- Proposition 10.7.1:
  (1) Every connected graph has a spanning tree.
  (2) Any two spanning trees for a graph have the same number of edges.
- (Minimum Spanning Tree): A minimum spanning tree for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph.
- (Algorithms to get Minimum Spanning Tree):

Algorithm 10.7.1 Kruskal

Input: G [a connected weighted graph with n vertices]

Algorithm:

1. Initialize T to have all the vertices of G and no edges.
2. Let E be the set of all edges of G, and let $m = 0$.
3. While ($m < n - 1$)
   3a. Find an edge e in E of least weight.
   3b. Delete e from E.
   3c. If addition of e to the edge set of T does not produce a circuit, then add e to the edge set of T and set $m = m + 1$
   End while

Output: T [T is a minimum spanning tree for G]

Algorithm 10.7.2 Prim

Input: G [a connected weighted graph with n vertices]

Algorithm:

1. Pick a vertex v of G and let T be the graph with this vertex only.
2. Let V be the set of all vertices of G except v.
3. For $i = 1$ to $n - 1$
   3a. Find an edge e of G such that (1) e connects T to one of the vertices in V, and (2) e has the least weight of all edges connecting T to a vertex in V. Let w be the endpoint of e that is in V.
   3b. Add e and w to the edge and vertex sets of T, and delete w from V.

Output: T [T is a minimum spanning tree for G]