CS1231S Discrete Structures
AY23/24, Y1S1
Definitions and Lemmas

Sim Ray En Ryan

December 3, 2025

Contents

1 Speaking Mathematically

1.1 Definitions in Number Theory

1.1.1 Even and Odd Integers

- n is **even** $\leftrightarrow \exists k \in Z$ s.t. $n = 2k$
- n is **odd** $\leftrightarrow \exists k \in Z$ s.t. $n = 2k + 1$
- **Assumption 1:** Every integer is even or odd, but not both.
- **Example:** Product of two consecutive odd numbers is odd (Lecture 1 Example #1).

1.1.2 Divisibility

- d **divides** n, written $d|n$, $\leftrightarrow \exists k \in Z$ s.t. $n = dk$, where $n, d \in Z$, $d \neq 0$.
- **Example:** Difference of two consecutive squares is always odd (Lecture 1 Example #5).
- **Division Algorithm (Theorem 4.4.1):** Given any integers n and d with $d > 0$, there exist unique integers q (quotient) and r (remainder) such that $n = dq + r$ and $0 \leq r < d$.

1.1.3 Rational and Irrational Numbers

- r is **rational** $\leftrightarrow \exists a, b \in Z$ s.t. $r = a/b$, where $b \neq 0$.
- r is **irrational** $\leftrightarrow r$ is not rational.

1.1.4 Fraction in Lowest Term

- A fraction a/b is in **lowest term** if the largest integer that divides both a and b is 1 (i.e., $\gcd(a, b) = 1$).
- **Assumption 2:** Every rational number can be reduced to a fraction in lowest term.

1.1.5 Colorful Numbers

- n is **colorful** $\leftrightarrow n = 3k$ for some integer k.

1.2 Properties of Divisibility (Chapter 4, Section 3)

- **Theorem 4.3.1:** If $a|b$ and $b > 0$, then $a \leq b$.
- **Theorem 4.3.2:** The only divisors of 1 are 1 and -1.
- **Theorem 4.3.3 (Transitivity of Divisibility):** If $a|b$ and $b|c$, then $a|c$.

2 Logic of Compound Statements

2.1 Connectives and Statement Forms

- **Negation ($\sim$, not):** (Definition 2.1.2)
- **Conjunction ($\wedge$, and):** (Definition 2.1.3)
- **Disjunction ($\vee$, or):** (Definition 2.1.4)
- **Statement Form (Definition 2.1.5):** An expression made up of statement variables and logical connectives.

2.2 Equivalence and Tautology/Contradiction

- **Logical Equivalence (Definition 2.1.6):** Two statement forms are logically equivalent if they have identical truth values for every possible substitution of statements.
- **Tautology (Definition 2.1.7):** A statement form that is always true.
- **Contradiction (Definition 2.1.8):** A statement form that is always false.

2.3 Conditional and Biconditional Statements

2.3.1 Conditional Statement ($p \to q$) (Definition 2.2.1)

- p is the **hypothesis** (antecedent).
- q is the **conclusion** (consequent).
- The statement is **vacuously true** if the hypothesis p is false.
- **Implication Law:** $p \to q \leftrightarrow \sim p \vee q$.
- **Contrapositive (Definition 2.2.2):** $\sim q \to \sim p$. (Logically equivalent to the conditional).
- **Converse (Definition 2.2.3):** $q \to p$.
- **Inverse (Definition 2.2.4):** $\sim p \to \sim q$.
- **"Only If" (Definition 2.2.5):** p only if q means $p \to q$.

2.3.2 Biconditional Statement ($p \leftrightarrow q$) (Definition 2.2.6)

- Equivalent to $(p \to q) \wedge (q \to p)$.

2.3.3 Necessary and Sufficient Conditions (Definition 2.2.7)

- r is **sufficient** for $s \to (r \to s$, "if r then s").
- r is **necessary** for $s \to (s \to r$, "if not r then not s").
- r is **necessary and sufficient** for $s \to (r \leftrightarrow s)$.

2.4 Logical Equivalences (Theorem 2.1.1)

- Commutative Laws
- Associative Laws
- Distributive Laws
- Identity Laws
- Negation Laws
- Double Negative Law

2.5 Arguments and Soundness

- **Argument (Definition 2.3.1):** A sequence of statements (premises) followed by a final statement (conclusion).
- **Valid Argument:** An argument is valid if and only if whenever statements are substituted that make all the premises true, the conclusion is also true.
- **Sound Argument (Definition 2.3.2):** An argument that is valid and all its premises are true.
- **Fallacies:**
  - Converse Error (2.3.5.1)
  - Inverse Error (2.3.5.2)

3 Logic of Quantified Statements

3.1 Predicates and Quantifiers

- **Predicate (Definition 3.1.1):** A sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables.
- **Truth Set (Definition 3.1.2):** The set of elements that make $P(x)$ true.
- **Universal Statement (Definition 3.1.3):** Uses the quantifier $\forall$ (for all).

- **Existential Statement (Definition 3.1.4):** Uses the quantifier $\exists$ (there exists).
- **Unique Existential Quantifier:** $\exists!$ (There exists only one).

3.2 Negations and Relations of Quantified Statements

- **Negation of a Universal Statement (Theorem 3.2.1):** $\sim (\forall x, P(x)) \leftrightarrow \exists x, \sim P(x)$.
- **Negation of an Existential Statement (Theorem 3.2.1):** $\sim (\exists x, P(x)) \leftrightarrow \forall x, \sim P(x)$.
- **Relations (Definition 3.2.1, 3.2.2):** The concepts of **Contrapositive**, **Converse**, **Inverse**, **Necessary**, **Sufficient**, and **Only if** apply to quantified statements in the same manner as to conditional statements.

4 Methods of Proof

4.1 Definitions of Integers

- **Prime Number:** n is **prime** $\leftrightarrow (n > 1) \wedge (\forall r, s \in Z((r > 1) \wedge (s > 1) \rightarrow rs \neq n))$.
- **Composite Number:** A positive integer n is **composite** $\leftrightarrow n$ is not prime.

4.2 Theorems and Propositions

- **Theorem 4.2.1:** Every integer is a rational number.
- **Theorem 4.2.2:** The sum of any two rational numbers is rational.
- **Theorem 4.6.1:** There is no greatest integer.
- **Proposition 4.6.4 (Parity):** If n^2 is even, then n is even.
- **Proposition (Tutorial 1 Q11b):** If n^2 is odd, then n is odd.
- **Inequality (Tutorial 2 Q8b):** $n^2 > n \rightarrow (x < 0)$ or $(x > 1)$.
- **Divisor Bound:** If $n = ab$, where a, b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- **Theorem 4.7.1 (Proof by Contradiction):** $\sqrt{2}$ is irrational.
- **Conjecture:** There is no integer n greater than 3 such that $n, n+2$ and $n+4$ are all prime.

5 Set Theory

5.1 Set Notations and Definitions

- **Set Roster Notation:** E.g., $\{1, 2, 3, \ldots\}$.
- **Membership (Definition of):** $\in$ denotes an element belonging to a set.
- **Cardinality (Definition of):** $|S|$ is the number of elements in a set S.
- **Set Builder Notation:** $\{x \in U : P(x)\}$.
- **Replacement Notation:** $\{P(x) : x \in A\}$.

5.2 Set Relations and Operations

5.2.1 Subset and Equality

- **Subset (Definition of):** $A \subseteq B$ if and only if $\forall x(x \in A \to x \in B)$. B is a **superset** of A.
- **Proper Subset:** $A \subset B$ if $A \subseteq B$ and $A \neq B$.
- **Theorem 6.2.4:** The empty set ($\emptyset$) is a subset of every set.
- **Equivalence (Tutorial 3 Q8):** $A \subseteq B \iff A \cap B = A \iff A \cup B = B$.
- **Set Equality (Definition of):** $A = B \iff A \subseteq B \wedge B \subseteq A$, or equivalently $\forall x(x \in A \iff x \in B)$.

5.2.2 Ordered Pair and Cartesian Product

- **Ordered Pair (Definition of):** (a, b).
- **Cartesian Product (Definition of):** $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.

5.2.3 Union, Intersection, Difference, and Complement

- **Union:** $A \cup B = \{x \in U : x \in A \vee x \in B\}$.
- **Intersection:** $A \cap B = \{x \in U : x \in A \wedge x \in B\}$.
- **Set Difference:** $B \setminus A = \{x \in U : x \in B \wedge x \notin A\}$.
- **Complement:** $\bar{A} = A^c = \{x \in U : x \notin A\}$.
- **Symmetric Difference:** $A \oplus B = (A \cup B) \setminus (A \cap B)$.

5.2.4 Set Properties

- **Disjoint Sets (Definition of):** A and B are disjoint $\iff A \cap B = \emptyset$. Sets are **mutually disjoint** if this is true for all pairs of sets in a collection.
- **Partition (Definition of):** A collection of non-empty subsets C of A is a partition of A if:
  - The subsets in C are mutually disjoint.
  - The union of all subsets in C equals A.
  - Equivalent condition: $\forall x \in A \exists! S \in C (x \in S)$.
- **Real Number Notation:** Parentheses (,) mean the endpoint is **not included**. Brackets [,] mean the endpoint **is included**.

5.3 Power Set

- **Power Set (Definition of):** $\mathcal{P}(A)$ is the set of all subsets of A.
- **Cardinality (Theorem 6.3.1):** If $|A| = n$ (finite), then $|\mathcal{P}(A)| = 2^n$.

5.4 Set Identities

- **Subset Relations (Theorem 6.2.1):**
  - Inclusion of Intersection: $A \cap B \subseteq A$ and $A \cap B \subseteq B$.
  - Inclusion in Union: $A \subseteq A \cup B$ and $B \subseteq A \cup B$.
  - Transitive Property of Subsets: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
- **Set Identities (Theorem 6.2.2):** Includes Commutative, Associative, Distributive, Identity, Complement, Double Complement, Idempotent, De Morgan's Laws, etc.
- **Tutorial 3 Q5:** $A \cap (B \setminus C) = (A \cap B) \setminus C$.
- **Tutorial 3 Q6:** $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

6 Relations

6.1 Basic Definitions

- **Relation (Definition of):** A relation R from a set A to a set B is a subset of the Cartesian product $A \times B$. x is related to y by R, written xRy, iff $(x, y) \in R$.
- **Domain, Co-domain, and Range:**
  - **Domain** is A.

- **Co-domain** is B.
- **Range** is $\{y \in B \mid \exists x \in A \text{ s.t. } (x, y) \in R\}$.

6.2 Inverse and Composition

- **Inverse of Relation (Definition of):** $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$.
- **Symmetry and Inverse (Tutorial 4 Q2):** R is symmetric $\rightarrow R = R^{-1}$.
- **Composition of Relations (Definition of):** Let R be a relation from A to B, and S be a relation from B to C. The composition $S \circ R$ is a relation from A to C defined as: $\forall x \in A, \forall z \in C(x(S \circ R)z \iff \exists y \in B(xRy \wedge ySz))$.
- **Associativity (Tutorial 4 Q6):** Composition of relations is associative.
- **Inverse of Composition:** $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

6.3 Properties of Relations on a Set A

- **Reflexive:** R is reflexive $\iff \forall x \in A(xRx)$.
- **Symmetric:** R is symmetric $\iff \forall x, y \in A(xRy \Rightarrow yRx)$.
- **Transitive:** R is transitive $\iff \forall x, y, z \in A(xRy \wedge yRz \Rightarrow xRz)$.
- **Antisymmetric:** R is antisymmetric $\iff \forall x, y \in A(xRy \wedge yRx \Rightarrow x = y)$.
- **Asymmetric:** R is asymmetric $\iff \forall x, y \in A(xRy \Rightarrow \sim (yRx))$.
- **Asymmetry Implies Antisymmetry (Tutorial 5 Q6c):** If R is asymmetric, then R is antisymmetric.

6.4 Transitive Closure

- **Transitive Closure (R^t):** The least (smallest) relation on A that contains R and is transitive. R^t is transitive.

6.5 Equivalence Relations

- **Equivalence Relation (Definition of):** A relation R on a set A that is **Reflexive**, **Symmetric**, and **Transitive**.
- **Equivalence Class:** For an equivalence relation $\sim$ on A, the equivalence class of $a \in A$ is $[a]_\sim = \{x \in A \mid x \sim a\}$.
- **Property of Equivalence Classes:** $x \sim y \iff [x] = [y] \iff [x] \cap [y] \neq \emptyset$.

- **Relation Induced by a Partition (Set A, Partition $\mathcal{T}$):** $xRy \iff$ there is a component $S \in \mathcal{T}$ such that $x \in S$ and $y \in S$. This induced relation is an equivalence relation.
- **Congruence Modulo n (Definition of):** $a \equiv b \pmod{n} \iff n|(a-b)$. This is an equivalence relation.

6.6 Partial and Total Orders

6.6.1 Partial Order

- **Partial Order (Definition of):** A relation $\preceq$ on a set A that is **Reflexive**, **Anti-symmetric**, and **Transitive**.
- **Common Partial Orders:** Subset relation ($\subseteq$) on the power set of a set (Tutorial 5 Q3).
- **Hasse Diagram:** A diagram representing a partial order. $x \prec y$ means x is "curly less than" y (i.e., $x \preceq y$ and $x \neq y$).
- **Comparability:** Two elements $x, y \in A$ are comparable if $x \preceq y$ or $y \preceq x$.
- **Compatibility (Upper Bound):** Two elements $x, y \in A$ are compatible if there is another element $z \in A$ such that $x \preceq z$ and $y \preceq z$.
- **Relation between Comparability and Compatibility (Tutorial 5 Q10):** Any two comparable elements are compatible, but the reverse is not true.

6.6.2 Extremal Elements

- **Maximal Element c:** For all $x \in A$, if $c \preceq x$, then $c = x$. (Nothing is strictly greater than c).
- **Minimal Element c:** For all $x \in A$, if $x \preceq c$, then $c = x$. (Nothing is strictly smaller than c).
- **Largest Element c (Greatest Element):** For all $x \in A$, $x \preceq c$. (Must be comparable to and greater/equal to everything).
- **Smallest Element c (Least Element):** For all $x \in A$, $c \preceq x$. (Must be comparable to and smaller/equal to everything).
- **Relation:** All largest/smallest elements are also maximal/minimal, respectively.

6.6.3 Total Order and Well Ordered Sets

- **Total Order (Definition of):** A partial order in which every pair of elements is comparable with each other. Also called a **linear order**.

- **Linearization ($\preceq^*$):** A total order $\preceq^*$ that is an extension of a partial order $\preceq$ such that $\forall x, y \in A, x \preceq y \to x \preceq^* y$.
- **Vacuously True Note:** If x is not R-related to y ($\sim (xRy)$), then x and y can be "anywhere" relative to each other in the context of transitivity, etc.
- **Well Ordered Set (Definition of):** A totally ordered set A such that every non-empty subset $S \subseteq A$ contains a smallest element. $\forall S \in \mathcal{P}(A), S \neq \emptyset \Rightarrow \exists x \in S \forall y \in S(x \preceq y)$.

7 Functions

7.1 Definition and Notation

- **Function $f : X \to Y$ (Definition of):** A relation from X (domain) to Y (co-domain) that satisfies:
  1. **Existence:** $\forall x \in X \exists y \in Y((x, y) \in f)$. (Every element in X is mapped).
  2. **Uniqueness:** $\forall x \in X \forall y_1, y_2 \in Y(((x, y_1) \in f \wedge (x, y_2) \in f) \to y_1 = y_2)$. (Each element in X maps to exactly one element in Y).
- **Equivalently:** $\forall x \in X \exists! y \in Y((x, y) \in f)$.

7.2 Terminology

- x is the **argument** or **input**.
- $f(x)$ is the **output**, the **image** of x under f.
- x is a **preimage** of y.
- **Domain** is X (All inputs).
- **Co-domain** is Y (All possible outputs).
- **Range** is the setwise image of X under f, $\{f(x) : x \in X\}$. It is a subset of the co-domain.

7.3 Setwise Image and Preimage

- **Setwise Image (Definition of):** If $A \subseteq X$, $f(A) = \{f(x) : x \in A\}$.
- **Setwise Preimage (Definition of):** If $B \subseteq Y$, $f^{-1}(B) = \{x \in X : f(x) \in B\}$.

7.4 Special Types of Functions

7.4.1 Sequences and Strings

- **Sequence:** A function $a : Z^{\geq 0} \to Y$, usually written a_n for $a(n)$.
- **Fibonacci Sequence:** $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for $n \in Z^{\geq 0}$.
- **String:** A finite sequence of elements (characters) over an alphabet set A. The **empty string** is ϵ (length 0).
- **Equality:**
  - Two sequences a and b are equal if $a(n) = b(n)$ for all n.
  - Two strings are equal if they have the same length and the characters $a_i = b_i$ for all i.

7.4.2 Injective, Surjective, and Bijective

- **Function Equality (Theorem 7.1.1):** $f = g$ iff (Domains are the same) $\wedge$ (Co-domains are the same) $\wedge$ ($f(x) = g(x)$ for all x in the domain).
- **Injective (One-to-One):** $\forall x_1, x_2 \in X(f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$. (One input to one output).
  - **Not Injective:** $\exists x_1, x_2 \in X(f(x_1) = f(x_2) \wedge x_1 \neq x_2)$.
  - **Property (Assignment 2 Q2):** A function is injective iff it has a left inverse.
- **Surjective (Onto):** $\forall y \in Y \exists x \in X(y = f(x))$. (Range = Co-domain).
  - **Not Surjective:** $\exists y \in Y \forall x \in X(y \neq f(x))$.
  - **Property (Assignment 2 Q2):** A function is surjective iff it has a right inverse.
- **Bijective:** $\forall y \in Y \exists! x \in X(y = f(x))$. (Injective and Surjective).

7.5 Inverse and Composition

- **Inverse Function (f^{-1}):** A function $g : Y \to X$ is the inverse of $f : X \to Y$ if $\forall x \in X \forall y \in Y(y = f(x) \iff x = g(y))$.
- **Uniqueness:** f^{-1} is unique.
- **Existence (Theorem 7.2.3):** f^{-1} exists $\iff$ f is bijective.
- **Identity Function (id):** $id(x) = x$ for all x.
- **Composition ($g \circ f$):** $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

- **Composition with Inverse (Theorem 7.3.2):** $f^{-1} \circ f = id_X$ and $f \circ f^{-1} = id_Y$.
- **Composition with Identity (Theorem 7.3.1):** $f \circ id_X = f$ and $id_Y \circ f = f$.
- **Associativity:** Function composition is associative.
- **Commutativity:** Function composition is generally not commutative.
- **Properties of Composition:**
  - **Injective Composition (Theorem 7.3.3):** If f and g are injective, then $g \circ f$ is injective.
  - **Injective Components (Tutorial 6 Q7):** If g is injective and $g \circ f$ is injective, then f is injective.
  - **Surjective Composition (Theorem 7.3.4):** If f and g are surjective, then $g \circ f$ is surjective.
  - **Inverse of Composition (Tutorial 6 Q4):** $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
- **Well-Defined Operations:** Addition and multiplication of Z_n (integers modulo n) are well-defined functions.

8 Mathematical Induction

8.1 Notations (Theorem 5.1.1)

- **Summation Notation ($\sum$):**
  - $\sum a_k + \sum b_k = \sum (a_k + b_k)$.
- **Product Notation ($\prod$):**
  - $c \prod a_k = \prod (c a_k)$. (Generalised Distributive law only for c an expression depending on k).
  - $\prod a_k \times \prod b_k = \prod (a_k b_k)$.

8.2 Sequences

- **Arithmetic Progression (AP):** $a_n = a_0 + dn$.
- **Geometric Progression (GP):** $a_n = a_0 r^n$.
- **Closed Form:** An expression that does not use summation or $\ldots$.
- **Recurrence Relation:** Each term in the sequence is based on the previous terms (e.g., Fibonacci).

8.3 Principle of Mathematical Induction (MI) Format

1. **Base Case:** Show that $P(a)$ is true (where a is the starting integer).
2. **Inductive Hypothesis:** Assume that for an arbitrary integer $k \geq a$, $P(k)$ is true. (For Strong Induction, assume $P(i)$ is true for all i such that $a \leq i \leq k$).
3. **Inductive Step:** Show that $P(k+1)$ is true using the Inductive Hypothesis.
4. **Conclusion:** By the Principle of Mathematical Induction, $P(n)$ is true for all integers $n \geq a$.

8.4 Summation Formulas and Examples

- **Sum of First n Integers (Theorem 5.2.2):** $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
- **Sum of First n Squares (Tutorial 7 Q2):** $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.
- **Sum of Geometric Sequence (Theorem 5.2.3):** $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$, for $r \neq 1$.
- **Bernoulli's Inequality (Tutorial 7 Q3):** Let $x \in R^{\geq -1}$. Then $1 + nx \leq (1+x)^n$ for all positive integers n.
- **Divisibility (Theorem 5.3.1):** For all non-negative integers n, $2^{2n} - 1$ is divisible by 3.
- **Inequality (Theorem 5.3.2):** For all integers $n \geq 3$, $2n + 1 < 2^n$.
- **Divisibility (Tutorial 7 Q5):** $2^{n+1} | a^{2^n} - 1$, where a is an odd, positive integer.
- **Coinage Problem (Tutorial 7 Q6):** Any integer-valued transaction of at least \$8 can be carried out using only \$3 and \$5 notes.
- **Binary Representation (Tutorial 7 Q7):** Every positive integer can be written as a sum of distinct non-negative integer powers of 2.
- **Fibonacci Identity (Tutorial 7 Q8):** $F_{n+4} = 3F_{n+2} - F_n$.

9 Cardinality

9.1 Finite and Infinite Sets

- **Finite Set (Definition of):** A set S is finite if $S = \emptyset$ or if there is a bijection from S to $Z_n = \{1, 2, \ldots, n\}$ for some non-negative integer n.
- **Infinite Set (Definition of):** A set that is not finite. A set A is infinite if there exists a proper subset $B \subset A$ such that $|B| = |A|$.
- **Cardinality of Finite Set:**

- 0 if $S = \emptyset$.
- n if $f : S \to Z_n$ is a bijection.

9.2 The Pigeonhole Principle (PHP)

- **Standard PHP:** If $f : A \to B$ is a function and $|A| > |B|$, then f is not injective (i.e., there must be at least two elements in A that have the same image in B).
- **Injective Implication:** If $f : A \to B$ is injective, then $|A| \le |B|$.
- **Dual PHP:** If $f : A \to B$ is surjective, then $|A| \ge |B|$.
- **Bijective Implication:** If $f : A \to B$ is injective and surjective (bijective), then $|A| = |B|$.
- **Generalized PHP (First Form):** For any function $f : X \to Y$ where $|X| = n$ and $|Y| = m$, 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.
- **Generalized PHP (Second Form):** For any function $f : X \to Y$ where $|X| = n$ and $|Y| = m$, and for any positive integer k, if for each $y \in Y$, $f^{-1}(\{y\})$ has at most k elements, then $|X| \le km$.

9.3 Countability

- **Cardinal Number $\aleph_0$ (Aleph-null):** $|Z^+|$.
- **Countably Infinite:** A set is countably infinite if it has the same cardinality as $\aleph_0$.
- **Countable:** A set is countable if it is finite or countably infinite.
- **Uncountable:** A set is uncountable if it is not countable.
- **Countability of Products (Lecture 9 Slide 30):** If A and B are both countably infinite, then $A \times B$ is countable. This works for any finite number of countably infinite sets.
- **Countability of Unions (Lemma 9.4):** If A and B are countable, then $A \cup B$ is countable.
- **Countability of Union with Finite Set (Tutorial 8 Q2):** If B is countably infinite and C is finite, $B \cup C$ is countable.
- **Uncountability of Reals (Theorem 7.4.2):** The set of real numbers (R) is uncountable.
- **Countability and Sequences (Lemma 9.2):** An infinite set B is countably infinite iff there is a sequence $b_0, b_1, b_2, \ldots$ in which every element of B appears.

- **Subset of Countable Set (Theorem 7.4.3):** Any subset of a countable set is countable.
- **Uncountable Subset Implies Uncountable Set (Corollary 7.4.4):** Any set with an uncountable subset is uncountable.
- **Infinite Sets and Countably Infinite Subsets (Proposition 9.3):** Every infinite set has a countably infinite subset.
- **Power Set of Countably Infinite Set (Tutorial 8 Q7):** If A is countably infinite, $\mathcal{P}(A)$ is uncountable.

10 Counting 1

10.1 Probability Basics

- **Sample Space (S):** The set of all possible outcomes.
- **Event (E):** A subset of the sample space.
- **Probability:** $P(E) = |E|/|S|$ (for uniform sample space).

10.2 Counting Principles

- **Number of Integers (Theorem 9.1.1):** There are $n - m + 1$ integers between m and n inclusive.
- **Multiplication Rule (Theorem 9.2.1):** If a procedure can be broken down into a sequence of k steps, and the first step can be performed in n_1 ways, the second in n_2 ways, $\ldots$, and the k-th step in n_k ways, then the total procedure can be performed in $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ ways.
- **Number of Permutations (Theorem 9.2.2):** The number of permutations (orderings) of a set with n elements is $n!$.
- **r-Permutations (Theorem 9.2.3):** The number of r-permutations of a set of n elements (number of ways to choose r elements and permute them) is $P(n,r) = {}_nP_r = \frac{n!}{(n-r)!}$.

10.3 Addition and Subtraction Rules

- **Addition Rule (Theorem 9.3.1):** If sets $A_1, A_2, \ldots$ are all mutually disjoint, then $|A_1 \cup A_2 \cup \ldots| = |A_1| + |A_2| + \ldots$.
- **Difference Rule (Theorem 9.3.2):** $|A \setminus B| = |A| - |A \cap B|$. If $B \subseteq A$, then $|A \setminus B| = |A| - |B|$.

- **Probability of Complement:** $P(\sim A) = 1 - P(A)$.
- **Principle of Inclusion and Exclusion (PIE):**
  - **Two Sets (Theorem 9.3.2):** $|A \cup B| = |A| + |B| - |A \cap B|$.
  - **Three Sets:** $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.
  - **General PIE:** Sum of single set sizes - Sum of double intersection sizes + Sum of triple intersection sizes - ...

11 Counting 2

11.1 Combinations

- **r-Combinations (Theorem 9.5.1):** The number of r-combinations of a set of n elements (number of ways to choose r elements without regard to order) is $C(n,r) = \binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}$.
- **Symmetry (Lecture 11 Slide 29):** $\binom{n}{r} = \binom{n}{n-r}$.
- **Pascal's Identity (Theorem 9.7.1):** $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$, for $1 \leq r \leq n$.

11.2 Permutations and Combinations with Repetition

- **Permutations with Indistinguishable Objects (Theorem 9.5.2):** The number of distinct permutations of n objects where there are n_1 indistinguishable objects of type 1, n_2 of type 2, ..., is $\frac{n!}{n_1!n_2!n_3!\dots}$.
- **r-Combinations with Repetition (Stars and Bars) (Theorem 9.6.1):** The number of ways to select r objects from n categories (with repetition allowed) is $\binom{r+n-1}{r}$.

11.3 Binomial Theorem

- **Binomial Theorem (Theorem 9.7.2):** $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

11.4 Probability Theory

11.4.1 Axioms and Rules

- **Probability Axioms (Lecture 11 Slide 39):**
  1. $0 \leq P(A) \leq 1$.
  2. $P(\emptyset) = 0$ and $P(S) = 1$.
  3. If $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$.

- **General Addition Rule:** $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

11.4.2 Expected Value

- **Expected Value $E(X)$:** For a discrete random variable X, $E(X) = \sum_x xP(X = x)$.

11.4.3 Conditional Probability and Independence

- **Conditional Probability (Definition 9.9.1):** $P(B|A) = \frac{P(A \cap B)}{P(A)}$, provided $P(A) > 0$.
- **Multiplication Rule (Theorem 9.9.2):** $P(A \cap B) = P(B|A)P(A)$.
- **Bayes' Theorem (Theorem 9.9.1):** Used to compute a posterior probability $P(H|E)$ from a prior probability $P(H)$ and likelihood $P(E|H)$.
- **Independence (Definition of):** Events A and B are independent if $P(A \cap B) = P(A)P(B)$.
- **Mutual Independence:** A set of events is mutually independent if the probability of the intersection of any subset of the events is the product of their individual probabilities.

12 Graphs

12.1 Graph Definitions

- **Graph $G = (V, E)$:** V is the set of **vertices** (points, nodes), E is the set of **edges** (lines connecting vertices).
- **Undirected Edge:** $e = \{v_1, v_2\}$ (a set).
- **Directed Edge:** $e = (v_1, v_2)$ (an ordered pair).
- **Simple Graph:** No loops (self-related edges) and no parallel edges (multiple edges between the same two vertices).
- **Complete Graph (K_n):** A simple undirected graph with n vertices where every pair of distinct vertices is connected by a unique edge. Has $\binom{n}{2}$ edges.
- **Bipartite Graph:** A graph whose vertices can be divided into two disjoint and independent sets V_1 and V_2 such that every edge connects a vertex in V_1 to one in V_2.
- **Complete Bipartite Graph ($K_{m,n}$):** A bipartite graph where every vertex in V_1 (size m) is connected to every vertex in V_2 (size n).
- **Subgraph:** $H = (V', E')$ is a subgraph of $G = (V, E)$ if $V' \subseteq V$, $E' \subseteq E$, and every edge in E' connects vertices in V'.

- **Four Colour Theorem:** Any map can be coloured using no more than four colours, such that no two adjacent regions have the same colour. (Equivalent to saying any planar graph can be 4-coloured).

12.2 Degrees and Handshake Theorem

- **Degree of a Vertex (**$\deg(v)$**):** The number of edges incident to v. (Loop edges count twice).
- **Indegree (**$\deg^{-}(v)$**):** The number of edges going **in** to v (for directed graphs).
- **Outdegree (**$\deg^{+}(v)$**):** The number of edges going **out** from v (for directed graphs).
- **Handshake Theorem (Theorem 10.1.1):** The total degree of a graph G is $\sum_{v \in V} \deg(v) = 2 \times |E|$.
- **Corollary 10.1.2:** The total degree of any graph is an even number.
- **Proposition 10.1.3:** There is an even number of vertices with odd degrees in any graph.

12.3 Paths and Circuits

- **Walk:** A sequence of alternating vertices and edges $v_0 e_1 v_1 e_2 v_2 \ldots e_n v_n$. n is the **length**. A walk of length 0 is a **trivial walk**.
- **Trail:** A walk with no repeated edges.
- **Path:** A trail with no repeated vertices.
- **Closed Walk:** A walk that starts and ends with the same vertex ($v_0 = v_n$).
- **Circuit (Cycle):** A closed walk of length ≥ 3 with no repeated edges.
- **Simple Circuit (Simple Cycle):** A circuit with no repeated vertices other than the first and last ($v_0 = v_n$).
- **Cyclicity:** A graph is **cyclic** if it contains a cycle (circuit); **acyclic** otherwise.

12.4 Connectedness

- **Connected Graph:** A graph G is connected if there is a walk (or path) between every pair of distinct vertices v and w.
- **Edge Removal (Lemma 10.5.3):** If G is connected and contains a circuit, then an edge in the circuit can be removed without disconnecting G.
- **Connected Component:** A subgraph H of G such that:
  1. H is connected.

2. H is maximal: No connected subgraph of G has H as a subgraph and contains vertices or edges not in H.

12.5 Euler and Hamiltonian

- **Euler Circuit:** A circuit that contains every vertex and traverses each edge exactly once. An **Eulerian Graph** contains an Euler circuit.
- **Euler Circuit Condition (Theorem 10.2.4):** A connected graph G has an Euler circuit if and only if every vertex has an even degree.
- **Euler Trail:** A trail that contains every vertex and traverses each edge exactly once.
- **Euler Trail Condition (Corollary 10.2.5):** A connected graph G has an Euler trail if and only if it has at most two vertices of odd degree (start and end at the odd-degree vertices).
- **Hamiltonian Circuit:** A simple circuit that contains every vertex exactly once (except for the start/end vertex).
- **Hamiltonian Circuit Properties (Proposition 10.2.6):** Must be connected, have the same number of edges as vertices, and $\deg(v) = 2$ for all vertices in the circuit.
- **Complete Graphs and Hamiltonian Circuits:** All complete graphs K_n, where $n > 2$, contain a Hamiltonian circuit.
- **Travelling Salesman Problem (TSP):** The problem of finding the shortest Hamiltonian circuit in a weighted complete graph.

12.6 Matrix Representation and Isomorphism

- **Adjacency Matrix (A):** A_{ij} is the number of edges from vertex i to vertex j.
- **Property:** The adjacency matrix is symmetric if the graph is undirected.
- **Power of Adjacency Matrix (Theorem 10.3.2):** $(A^n)_{ij}$ is the number of walks of length n from vertex i to vertex j.
- **Isomorphism:** Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there exist bijections $g : V_1 \to V_2$ and $h : E_1 \to E_2$ such that v is an endpoint of e in G_1 if and only if $g(v)$ is an endpoint of $h(e)$ in G_2. (The graphs "look the same").
- **Equivalence Relation (Theorem 10.4.1):** The relation "is isomorphic to" on the set of all graphs is an equivalence relation.

12.7 Planar Graphs

- **Planar Graph (Definition of):** A graph that can be drawn on a 2D plane without any edges crossing.
- **Faces, Edges, and Vertices:** A planar graph partitions the plane into regions called **faces** (including the "outside" face).
- **Euler's Formula:** For a connected planar graph: $|V| - |E| + |F| = 2$, where $|V|$ is the number of vertices, $|E|$ the number of edges, and $|F|$ the number of faces.
- **Kuratowski's Theorem:** A graph is planar if and only if it does not contain a subgraph that is a subdivision of K_5 (complete graph on 5 vertices) or $K_{3,3}$ (complete bipartite graph with 3 vertices in each partition).

13 Trees

13.1 Definitions and Properties

- **Tree (Definition of):** A connected, acyclic graph (no circuits).
- **Trivial Tree:** A tree consisting of a single vertex.
- **Forest:** A circuit-free graph that is not necessarily connected (a collection of disjoint trees).
- **Leaf (Terminal Vertex):** A vertex with degree 1.
- **Internal Vertex:** A vertex with degree greater than 1.
- **Property (Lemma 10.5.1):** Every non-trivial tree has at least one vertex of degree 1 (a leaf). A tree with $n \geq 2$ vertices has at least 2 leaves.
- **Edge Count (Theorem 10.5.2):** A tree with n vertices has exactly $n - 1$ edges.
- **Equivalence (Theorem 10.5.3):** If a graph G has n vertices and $n - 1$ edges, and G is connected, then G is a tree.

13.2 Rooted and Binary Trees

- **Binary Tree (Definition of):** A rooted tree where every parent has at most two children, designated as a **left child** and a **right child**.
- **Full Binary Tree:** A binary tree where every internal vertex has exactly two children. Arithmetic expressions can be represented by a full binary tree.
- **Property of Full Binary Tree (Theorem 10.6.1):** A full binary tree with k internal vertices has $k + 1$ leaves.

- **Height and Leaves (Theorem 10.6.2):** The maximum number of leaves is 2^h, where h is the height of the tree. Equivalently, $\log_2(\text{leaves}) \leq h$.
- **Traversal Methods:**
  - **Breadth-First Search (BFS):** Explore all nodes at the present depth level before moving on to the nodes at the next depth level.
  - **Depth-First Search (DFS):** Explore as far as possible down each branch before backtracking.
  - **Pre-Order Traversal (Root, Left, Right):** Print $\rightarrow$ Go Left $\rightarrow$ Go Right.
  - **In-Order Traversal (Left, Root, Right):** Go Left $\rightarrow$ Print $\rightarrow$ Go Right.
  - **Post-Order Traversal (Left, Right, Root):** Go Left $\rightarrow$ Go Right $\rightarrow$ Print.

13.3 Spanning Trees

- **Spanning Tree (Definition of):** A subgraph of G that includes every vertex of G and is a tree. It uses the minimal amount of edges to keep G connected.
- **Existence (Proposition 10.7.1):** Every connected graph has a spanning tree.
- **Size:** Any two spanning trees for a graph have the same number of edges ($|V| - 1$).
- **Number of Spanning Trees:** There are n^{n-2} spanning trees in a complete graph K_n, where $n \geq 2$ (Cayley's Formula).

13.4 Minimal Spanning Trees and Shortest Paths

- **Minimal Spanning Tree (MST):** A spanning tree of a weighted graph that has the minimum possible total edge weight.
- **Kruskal's Algorithm (Algorithm 10.7.1):**
  1. Find the edge with the lowest weight.
  2. If adding the edge does not create a circuit, add it to the MST set.
  3. Repeat until $n - 1$ edges are in the MST set.
- **Prim's Algorithm (Algorithm 10.7.2):**
  1. Start from an arbitrary vertex.
  2. Add the edge that connects a vertex **not yet** in the current tree to one **in** the current tree with the lowest weight.
  3. Repeat until all vertices are included.

- **Dijkstra's Algorithm (Algorithm 10.7.3):** Finds the shortest path between a starting node and all other nodes in a weighted graph with non-negative edge weights.