1 - Set Theory

Set

- $A \cup B = \{x | x \in A \text{ or } x \in B\}$
- $A \cap B = \{x | x \in A \text{ and } x \in B\}$
- $A \backslash B = \{x | x \in A \text{ and } x \notin B\}$
- $A \subseteq B \leftrightarrow x \in B \; \forall \; x \in A$
- For universe $U, \bar{S} = U \backslash S$

*complement of S -> U\S

Double Containment Proof

To prove that $S = T$, we need to show that both sets contain the same elements. This involves proving:

1. $S \subseteq T$: Every element in S is also in T.
2. $T \subseteq S$: Every element in T is also in S.

This method is known as a **double containment proof**.

2 - Sets, Functions and Sequences

Cartesian Product of Sets

Definition

For two sets A and B, the **Cartesian product** $A \times B$ is the set of **ordered pairs**:

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

Counting Elements

If $|A| = n$ and $|B| = m$, then:

$$|A \times B| = n \cdot m$$

Function Terminology

Let $f : X \to Y$ be a function. Then:

1. **Domain**: X is called the **domain** of f.
2. **Codomain**: Y is called the **codomain** of f.
3. **Image of an Element**: For an element $x \in X$, $f(x) \in Y$ is called the **image** (or value) of x under f.
4. **Image of a Set**: If $A \subseteq X$, the **image of A** under f is the set:

   $$f(A) = \{f(a) \mid a \in A\} \subseteq Y$$

   We also call $f(X)$ the **range** of f (the actual values in Y that f maps to).
5. **Preimage of an Element**: For an element $y \in Y$, the **preimage** of y is the set:

   $$f^{-1}(y) = \{x \in X \mid f(x) = y\} \subseteq X$$
6. **Preimage of a Set**: If $B \subseteq Y$, the **preimage of B** under f is the set:

   $$f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subseteq X$$

Types of Functions

1. Surjective (Onto) Functions

A function $f : X \to Y$ is called **surjective** or **onto** if **every element** in Y has a **preimage** in X.

- **Definition**: For every $y \in Y$, there exists an $x \in X$ such that $f(x) = y$.

2. Injective (One-to-One) Functions

A function $f : X \to Y$ is called **injective** or **one-to-one** if **different elements in X** have **different images** in Y.

- **Definition**: If $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for all $x_1, x_2 \in X$.

3. Bijective (One-to-One Correspondence) Function

A function $f : X \to Y$ is called **bijective** or a **one-to-one correspondence** if it is **both injective and surjective**.

- **Definition**: Every element in X maps to a unique element in Y, and every element in Y is mapped to by an element in X.

Proving or Disproving Properties of f: X→Y

	Prove	Disprove
Onto:	Take arbitrary $y \in Y$. Show/construct some $x \in X$ so that $f(x) = y$	Find an explicit $y \in Y$ and show $y \neq f(x)$ for any $x \in X$.
One-to-one:	Assume $f(x_1) = f(x_2)$. Deduce that $x_1 = x_2$.	Find an explicit pair $x_1, x_2 \in X$ with $x_1 \neq x_2$ but $f(x_1) = f(x_2)$

Functions and Finite Sets

- If f is one-to-one, then $|X| \leq |Y|$
- If f is onto, then $|X| \geq |Y|$.
- If f is a one-to-one correspondence, then $|X| = |Y|$

3 - Divisibility, Prime numbers, Euclidean Algorithm

Divisibility Definition

For two integers a and b, we say that:

- a **divides** b, or
- b **is divisible by** a, or
- a **is a divisor of** b,

if there exists some integer $k \in \mathbb{Z}$ such that:

$$b = a \cdot k$$

Quotient Remainder Theorem

Theorem

For two integers n and d with $d > 0$:

- There exist **unique integers** q (quotient) and r (remainder) such that:

$$n = q \cdot d + r$$

  where $0 \leq r < d$.

Modular Arithmetic

For two integers n and m, and a positive integer d:

- We say that n and m are **congruent modulo** d if they have the **same remainder** when divided by d.
- This is written as:

$$n \equiv m \pmod{d}$$

  which reads "n is congruent to m modulo d."

For $d > 0$:

- If $a \equiv b \pmod{d}$ and $n \equiv m \pmod{d}$, then:
  - **Addition**: $a + n \equiv b + m \pmod{d}$
  - **Multiplication**: $a \cdot n \equiv b \cdot m \pmod{d}$

Fundamental Theorem of Arithmetic (FTA)

Statement

The theorem states that:

- **Every integer $n > 1$ can be uniquely written as a product of primes.**

Mathematical Expression

For any integer $n > 1$, we can express n as:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s} = \prod_{i=1}^{s} p_i^{k_i}$$

where:

- Each p_i is a prime number.
- Each $k_i > 0$ is an integer exponent.
- The representation is **unique**, up to the order of the prime factors.

Greatest Common Divisor (GCD)

For two integers a and b (not both zero), the **greatest common divisor** (denoted as $\gcd(a, b)$) is defined as the **largest integer** $d \in \mathbb{N}$ such that:

- $d \mid a$ (meaning d divides a), and
- $d \mid b$ (meaning d divides b).

Least Common Multiple (LCM)

For two **positive** integers a and b, the **least common multiple** (denoted as $\operatorname{lcm}(a, b)$) is defined as the **smallest positive integer** $n \in \mathbb{N}$ such that:

- $a \mid n$ (meaning a divides n), and
- $b \mid n$ (meaning b divides n).

Euclidean Algorithm

The **Euclidean Algorithm** is a method to compute $\gcd(a, b)$ by repeatedly applying the Division Algorithm.

Steps:

1. For two integers a and b (where $a > b > 0$):
   - Use the Division Algorithm to write $a = q \cdot b + r$, where q is the quotient and r is the remainder.
2. Check the remainder r:
   - If $r = 0$, then $\gcd(a, b) = b$.
   - If $r \neq 0$, replace (a, b) with (b, r) and repeat the process.

- Example: Find $\gcd(60, 36)$.
  - $60 = \underbrace{1}_{q} \cdot 36 + \underbrace{24}_{r} \rightarrow \gcd(60,36) = \gcd(36, 24)$
  - $36 = 1 \cdot 24 + 12 \rightarrow \gcd(36,24) = \gcd(24, 12)$
  - $24 = 2 \cdot 12 + 0 \rightarrow \gcd(24,12) = \gcd(12,0) = 12.$

$\Rightarrow \gcd(60, 36) = 12.$

Base b Expansions

Let $b > 1$ be a positive integer. Then **every positive integer** n can be uniquely expressed in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where:

- Each a_i (for $i = 0, 1, \ldots, k$) is a nonnegative integer.
- $a_i < b$ (each coefficient a_i is less than the base b).
- $a_k \neq 0$ (the leading coefficient is not zero to ensure uniqueness).

Notation:

We represent n in base b as:

$$n = (a_k a_{k-1} \ldots a_1 a_0)_b$$

- Example: $(245)_8 = 5\cdot 8^0 + 4\cdot 8^1 + 2\cdot 8^2 = 165 = (165)_{10}$.

- Example: $51 = (51)_{10} = 2\cdot 5^2 + 0\cdot 5^1 + 1\cdot 5^0$
$= (201)_5$.

- Example: What is 79 in base 6? (Want: $79 = a_0\cdot 1 + a_1\cdot 6$
$+ a_2 + 6^2 + \ldots$)

$$79 = \underbrace{13}_{q_0}\cdot 6 + \underbrace{1}_{r_0} \to a_0$$

$$13 = \underbrace{2}_{q_1}\cdot 6 + \underbrace{1}_{r_1} \to a_1 \quad \Rightarrow 79 = (211)_6$$

$$2 = \underbrace{0}_{q_2}\cdot 6 + \underbrace{2}_{r_2} \to a_2$$

Stop; q_2

- Check: $(211)_6 = 1\cdot 6^0 + 1\cdot 6 + 2\cdot 6^2 = 1 + 6 + 72 = 79$ ✓

- Example: $(11101)_2 \times (11)_2$

$$
\begin{array}{r}
(11101)_2 \\
\times \quad (11)_2 \\
\hline
11101 \\
111010 \\
\hline
(1010111)_2
\end{array}
$$

4 - Counting, choosing k items from n

Summary

Summary: Choosing k objects from a set of n

	Order Matters	Order Doesn't Matter
Repetition Allowed	n^k	$\binom{k+n-1}{n-1}$
Repetition Not Allowed	$P(n,k) = \frac{n!}{(n-k)!}$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

5 - Binomial Theorem, Inclusion-Exclusion and Catalan numbers

Inclusion-Exclusion principle

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

Pigeonhole Principle

If you have n pigeons sitting in k pigeonholes, and $k < n$, then at least one pigeonhole must contain at least two pigeons.

Proof

Example

Let X and Y be finite sets such that $|X| > |Y|$. Show that there are no injective (one-to-one) functions $f : X \to Y$.

Proof

1. **Define Sets**: Let
   - $X = \{x_1, x_2, \ldots, x_n\}$
   - $Y = \{y_1, y_2, \ldots, y_m\}$
     where $n > m$.
2. **Consider any function** $f : X \to Y$ and examine the image of X under f:
   $$f(x_1), f(x_2), \ldots, f(x_n) \in Y$$
3. **Mapping of Elements**: Each $f(x_i) = y_j$ for some $1 \leq j \leq m$.
4. **Apply the Pigeonhole Principle**:
   - **Pigeons**: The elements $f(x_1), f(x_2), \ldots, f(x_n)$.
   - **Pigeonholes**: The elements $y_1, y_2, \ldots, y_m$.
   - Since $n > m$, there are more "pigeons" (elements of X) than "pigeonholes" (elements of Y).
   - By the Pigeonhole Principle, at least two elements of X, say x_r and x_s, must map to the same element in Y, meaning $f(x_r) = f(x_s) = y_j$ for some j.
5. **Conclusion**: Since $f(x_r) = f(x_s)$ for distinct x_r and x_s, f is not injective. Therefore, there are no injective functions from X to Y when $|X| > |Y|$.

The Binomial Theorem

For variables x, y, and a natural number $n \geq 0$:

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

Pascal's Identity

For any integers n and k where $0 \leq k \leq n$:

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

This identity shows that each entry in Pascal's Triangle is the sum of the two entries directly above it.

Catalan Numbers

The sequence $(C_n)_{n \geq 0}$ is defined recursively as follows:

1. **Base Case**: $C_0 = 1$
2. **Recursive Case**:

$$C_n = \sum_{i=1}^{n} C_{i-1} \cdot C_{n-i}$$

The **general formula** for the n-th Catalan number C_n is:

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!\,n!}$$

Proof

6: Probability

Distributions of Random Variables

The **distribution** of a random variable X is defined as the set of pairs:

$$(r, p(X = r))$$

where r represents a possible value of X and $p(X = r)$ is the probability that X takes the value r.

Conditional Probability

For two events E and F with $p(F) > 0$, the **conditional probability** of E given F is:

$$p(E|F) = \frac{p(E \cap F)}{p(F)}$$

Independent Events

We say that E and F are **independent events** if either of the following equivalent conditions is true:

1. The probability of E does not change given F:

$$p(E) = p(E|F)$$

2. The probability of both E and F occurring is the product of their individual probabilities:

$$p(E \cap F) = p(E) \cdot p(F)$$

Complementary Events

For an event $F \subset S$ in the sample space S, the **complementary event** $\overline{F}$ is defined as:

$$\overline{F} = S \setminus F$$

This represents all outcomes in S that are **not** in F.

Bayes' Theorem (in cheatsheet)

$$p(F|E) = \frac{p(F) \cdot p(E|F)}{p(E|F) \cdot p(F) + p(E|\overline{F}) \cdot p(\overline{F})}$$

Expected Value

The **expected value** (or **expectation** or **mean**) of a random variable X is given by:

$$E(X) = \sum_{s \in S} p(s) \cdot X(s)$$

Variance

The formula for variance is:

$$V(X) = \sum_{s \in S} (X(s) - E(X))^2 \cdot p(s)$$

The variance $V(X)$ of a random variable X can be calculated as:

$$V(X) = E(X^2) - (E(X))^2$$

For a random variable X and constants $a, b \in \mathbb{R}$:

$$E(aX + b) = a \cdot E(X) + b$$

Standard Deviation

The **standard deviation** of X, denoted $\sigma(X)$, is the square root of the variance. It provides a measure of the spread of X in the same units as X itself:

$$\sigma(X) = \sqrt{V(X)}$$

Properties for Independent Random Variables

If X and Y are **independent random variables**, then:

- The expected value of their product is the product of their expected values:
$$E(XY) = E(X) \cdot E(Y)$$
- The variance of their sum is the sum of their variances:
$$V(X + Y) = V(X) + V(Y)$$

7 - Basics on Graph Theory

Simple Graph

A **simple graph** is a graph that has no loops (edges connecting a vertex to itself) and no parallel edges (multiple edges connecting the same pair of vertices).

Degrees of Vertices

Incidence

- An edge e and a vertex v are said to be **incident** if v is an endpoint of e.

Adjacency

- Two vertices v and w are **adjacent** if $\{v, w\}$ is an edge of the graph.
- A vertex v is **adjacent to itself** if $\{v, v\}$ is a loop.

Handshake Theorem

Let Γ be a graph with n vertices, denoted $V(\Gamma) = \{v_1, \ldots, v_n\}$. Then:

$$\sum_{i=1}^{n} \deg(v_i) = 2|E(\Gamma)|$$

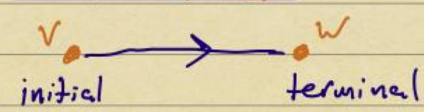
where $|E(\Gamma)|$ represents the number of edges in the graph.

Corollary

For any graph Γ, there must be an **even number of vertices with odd degree**.

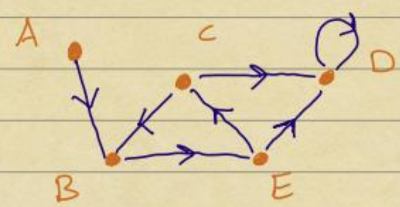
Directed Graphs

- An initial vertex
- A terminal vertex



- The in-degree 入度 $\deg^-(v)$ to be the number of edges terminating at v.
- The out-degree 出度 $\deg^+(v)$ to be the number of edges initializing at v.

- Example:



$\deg^-(A) = 0$ $\deg^-(B) = 2$ $\deg^-(C) = 1$ $\deg^-(D) = 3$ $\deg^-(E) = 1$

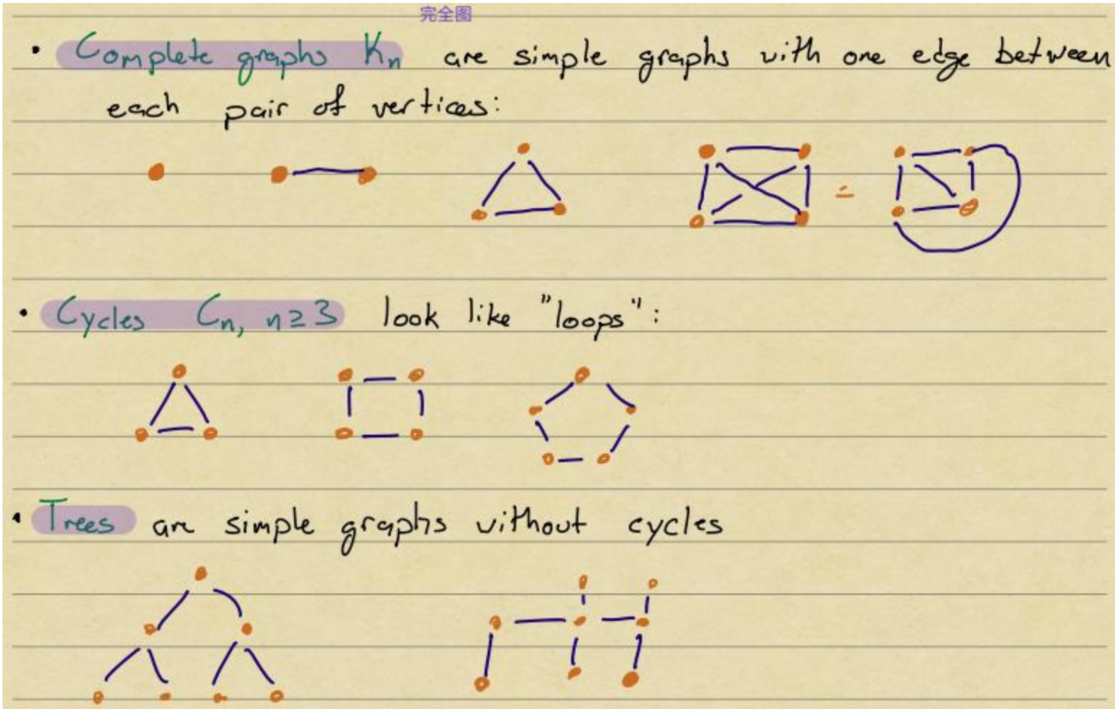
$\deg^+(A) = 1$ $\deg^+(B) = 1$ $\deg^+(C) = 2$ $\deg^+(D) = 1$ $\deg^+(E) = 2$

Handshake Theorem for Directed Graphs

Let Γ be a directed graph with vertices $\{v_1, v_2, \ldots, v_n\}$. Then:

$$\sum_{i=1}^{n} \deg^-(v_i) = \sum_{i=1}^{n} \deg^+(v_i) = |E(\Gamma)|$$

Complete graphs



Euler Circuit

A **path** of nonzero length (having at least one edge) is called:

1. **Simple**: if it does not repeat any edge. 每条边恰好一次
2. **Circuit**: if it begins and ends at the same vertex. 闭合路径
3. **Euler Circuit**: if it is a simple circuit that contains every edge of the graph.

Let Γ be a **connected** graph. Then Γ has an **Euler circuit** if and only if every vertex has an even degree.

Isomorphic Graphs

Two graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ are said to be **isomorphic**, denoted $\Gamma_1 \cong \Gamma_2$, if there exists a **bijection** $\phi : V_1 \to V_2$ such that:

$$\{v, u\} \in E_1 \text{ if and only if } \{\phi(v), \phi(u)\} \in E_2$$

Graph Invariants

Definition

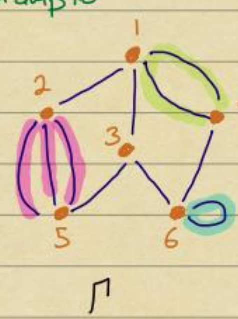
A **graph invariant** is a property or piece of data associated with a graph Γ that remains the same for any graph Γ' that is **isomorphic** to Γ (i.e., $\Gamma' \cong \Gamma$).

Examples of Graph Invariants

1. The **number of vertices** of a graph.
2. The **number of edges** of a graph.
3. The **list of degrees of the vertices** in a graph.

Adjacency Matrices

• Example:



• Theorem: Two graphs Γ_1 and Γ_2 are isomorphic ($\Gamma_1 \cong \Gamma_2$) if and only if there is a labeling of their vertices so that $A_{\Gamma_1} = A_{\Gamma_2}$.

$$A_\Gamma = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{pmatrix} \end{array}$$

Note: $a_{ij} = a_{ji}$

With our conventions, $\deg(i) =$ sum of all numbers in row i = sum of col. i.

Path on Graphs

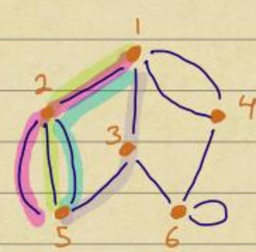
Let Γ be a graph with vertices $\{1,2,\dots,n\}$ and adjacency matrix A_Γ.

A path of length k from vertex i to j is a path consisting of k (not necessarily distinct) edges.

- Theorem: The number of paths from vertex i to vertex j in Γ of length k is the (i,j) entry of the matrix

$$A_\Gamma^k := \underbrace{A_\Gamma \cdot A_\Gamma \cdot \cdots \cdot A_\Gamma}_{k \text{ times.}}$$

- Example:



Γ

\# Paths from 5 to 1 of length 2.

$= 4$

$$A_\Gamma^2 = \begin{pmatrix} 0 & 1 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

The $(5,1)$ entry of A_Γ^2 is

$$0\cdot 0 + 3\cdot 1 + 1\cdot 1 + 0\cdot 2 + 0\cdot 0 + 0\cdot 0 = 4.$$

8 - Equivalence Relations, Closures

Relation

A relation R on a set X is said to have the following properties:

1. **Reflexive**: R is reflexive if every element is related to itself. That is,

$$x \, R \, x \quad \text{for all } x \in X.$$

2. **Symmetric**: R is symmetric if whenever x is related to y, then y is also related to x. That is,

$$x \, R \, y \implies y \, R \, x.$$

3. **Transitive**: R is transitive if whenever x is related to y and y is related to z, then x is also related to z. That is,

$$x \, R \, y \text{ and } y \, R \, z \implies x \, R \, z.$$

Equivalence Class

For an equivalence relation R on X and an element $x \in X$, the **equivalence class** of x, denoted by $[x]$, is the set of all elements in X that are related to x under R. Formally,

$$[x] = \{y \in X \mid xRy\}.$$

Complementary Relation (not important)

Let R be a relation from set X to set Y. The **complementary relation** to R, denoted by $\overline{R}$, is defined as:

$$\overline{R} = (X \times Y) \setminus R$$

Composition of Relations (not important)

Let R be a relation from set X to set Y, and let S be a relation from set Y to set Z. The **composition relation** $S \circ R$ is defined as a relation from X to Z, given by:

$$S \circ R = \{(x, z) \in X \times Z \mid \exists y \in Y \text{ such that } xRy \text{ and } ySz\}$$

In other words, $(x, z) \in S \circ R$ if there exists some $y \in Y$ such that x is related to y by R, and y is related to z by S.

Example

Let R be a relation where xRy means that x is a parent of y.

- $R^2 = R \circ R$: Represents the relationship where x is a grandparent of z (since xRy and yRz implies xR^2z).
- $R^3 = R \circ R^2$: Represents the great-grandparent relationship.
- $R^4 = R \circ R^3$: Represents the great-great-grandparent relationship.

• Exercise: Let R be the relation on $\mathbb{R}$ given by

$$xRy \text{ if and only if } x < y.$$

Show that $R \circ R = R$.

Solution

We need to show xR^2y implies xRy and conversely.

Assume xR^2y. Then by definition for some $z \in \mathbb{R}$,

$$xRz \text{ and } zRy.$$

This says $x<z$ and $z<y$. But this implies $x<y$, or xRy.

Now assume xRy, so $x<y$. We need to show xR^2y; that is, $x<z$ and $z<y$ for some $z \in \mathbb{R}$. Now,

$$x<y$$
$$\Rightarrow x+x < x+y < y+y$$
$$\Rightarrow x < \frac{x+y}{2} < y.$$

So, let $z = \frac{x+y}{2}$. Then $x<z<y \Rightarrow xR^2y$. ∎

Partitions of Sets

Let X be a nonempty set. A **partition** of X is a collection of subsets $S_1, S_2, S_3, \ldots$ that satisfies the following conditions:

1. **Nonempty Subsets**: Each subset $S_i \neq \emptyset$.
2. **Pairwise Disjoint**: For any two distinct subsets S_i and S_k (where $i \neq k$), their intersection is empty: $S_i \cap S_k = \emptyset$.
3. **Union Covers** X: The union of all subsets S_i equals X: $X = \bigcup S_i$.

① $S_i \neq \emptyset$ for all i.

② $S_i \cap S_k = \emptyset$ for $i \neq k$ ("pairwise disjoint") 成对不相交

③ $X = \bigcup_i S_i$

*Z = S1 U S2 U S3

Equivalence Classes and Partitions

Let X be a nonempty set, and let R be an equivalence relation on X. Then the set of equivalence classes $\{[x]\}$ forms a **partition** of X.

- **Theorem**: Given a partition $\{S_i\}$ of a set X, we can define an equivalence relation R on X as follows:

$$xRy \text{ if and only if } x, y \in S_i \text{ for some } i.$$

Anti-Symmetric

Definition: Anti-Symmetric Relation

- A relation is called **anti-symmetric** if, whenever both aRb and bRa hold, it must be that $a = b$.

Partial Order

- Reflexive
- Anti-symmetric
- Transitive

Partially Ordered Set (Poset)

- A set X with a partial order R is called a **partially ordered set**, or **poset**.

Exercise

- Examples of posets:
  - $(\mathbb{R}, \leq)$: The set of real numbers with the usual "less than or equal to" relation.
  - $(\mathcal{P}(X), \subseteq)$: The power set of X with the subset relation.

Total Order

Definition: Total Order

- A **total order** on a set X is a partial order R with an additional property:
  - **Comparability**: For any $x, y \in X$, either xRy or yRx.

  This means every pair of elements in X can be compared with each other according to R.

Exercise

- Examples:
  - $(\mathbb{R}, \leq)$ is a **total order**: Every pair of real numbers can be compared.
  - $(\mathcal{P}(X), \subseteq)$ need not be a total order: Not all subsets of a set X are comparable under subset inclusion.

Reflexive Closure

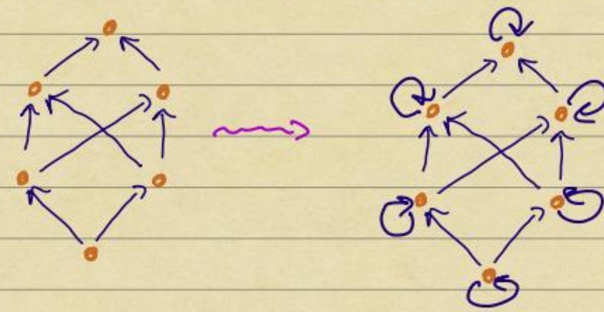
• Example: Let $X = \mathbb{R}$ with relation xRy given by $x > y$.
What is $\text{ref}(R)$?

- By definition, $\text{ref}(R) = \overset{R}{\{(x,y) \mid x > y\}} \cup \{(x,x) \mid x \in \mathbb{R}\}$
$= \{(x,y) \mid x \geq y\}$

So, in effect, reflexive closure of $>$ is $\geq$.

• Example: For a relation given by a directed graph, reflexive closure adds a loop at each vertex.

R



ref(R).

Symmetric Closure

• Example: The relation $x > y$ on $\mathbb{R}$ is not symmetric. What is its symmetric closure?

- By def.,

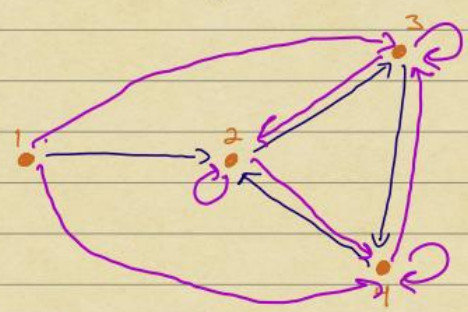
$$\begin{aligned} sym(R) &= R \cup \{(y,x) \mid (x,y) \in R\} \\ &= \{(x,y) \mid x > y\} \cup \{(y,x) \mid x > y\} \\ &= \{(x,y) \mid x > y\} \cup \{(x,y) \mid x < y\} \\ &= \{(x,y) \mid x \neq y\}. \end{aligned}$$

• Example: For a relation given by a directed graph, symmetric closure adds edges in opposite directions for all edges (can ignore loop).

Transitive Closure

• For a relation R given by a directed graph, the transitive closure tra(R) does the following:

if there is a path of length 1 or more from x to y in R, add in the edge $x \to y$



1R2
2R3
Want to add in 1R3

Connectivity Relation

• Definition: For a relation R, the connectivity relation R^* is given by

$$R^* = \bigcup_{k=1}^{\infty} R^k$$

• Theorem: $\operatorname{tra}(R) = R^*$

• Fact: If R is a relation on X and $|X| = n$, then

$$R^* = \operatorname{tra}(R) = \bigcup_{k=1}^{n} R^k$$

9 - Propositional Logic

Negation, Conjunction, Disjunction

① Negation: $\neg p$ (sometimes see $\sim p$) "not p"
② Conjunction: $p \wedge q$ "p and q"
③ Disjunction: $p \vee q$ "p or q"

• Order of operations: $\neg$ comes first
$\wedge$ and $\vee$ are equal seconds

Contradictions and Tautologies

• Definition: A contradiction is a proposition whose only truth value is False: $P \equiv F$

A tautology is a proposition whose only truth value is True: $Q \equiv T$. 重言式或恒真命题

Conditionals

- For two propositions p, q, the conditional $p \to q$ is defined by the truth table

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

- We call p the hypothesis or antecedent and q the conclusion or consequent

Constructions on Conditionals

- Definition: Given a conditional $p \to q$, the
  - Converse is the conditional $q \to p$
  - Inverse is the conditional $\neg p \to \neg q$
  - Contrapositive is the conditional $\neg q \to \neg p$

Biconditional

- Definition: Given propositional variables p, q, the biconditional $p \leftrightarrow q$ is defined by the truth table

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

- Read as "p if and only if q", most commonly.

Satisfiability

A compound proposition is **satisfiable** if there exists at least one assignment of truth values to its variables that makes the entire proposition true. If no such assignment exists (meaning it is always false), the proposition is considered **unsatisfiable** (a **contradiction**).

Example

The given example expression:

$$((p \to r) \lor (\neg r \leftrightarrow q)) \land (\neg q \to (\neg s \land p))$$

is **satisfiable**.

An assignment of truth values that makes it true is provided:

- $p, s \equiv \text{False}$
- $q, r \equiv \text{True}$

Predicates

- **Definition of a Predicate**: A statement that contains a finite number of variables, which becomes a proposition when the values of the variables are specified.
  - Example: $P(x, y) = x^2 \geq y$
- **Domain**: The set of values that can be assigned to the variables in a predicate.
- **Truth Set**: The set of all values in the domain for which the predicate is true.
  - Example: If $P(x) = "x^2 = 4"$, with the domain being integers, the truth set of $P(x)$ is $\{2, -2\}$.

Universal quantifier

Existential quantifier

Negating Multiple Quantifiers

$$\neg(\forall x \in D\ \exists y \in D\ \forall z \in D\ (P(x) \to (R(y,z) \land Q(x)))$$

$$\equiv \exists x \in D\ \forall y \in D\ \exists z \in D\ (\underbrace{P(x) \land (\neg R(y,z) \lor \neg Q(x))}_{\neg(P(x) \to (R(y,z) \land Q(x)))})$$

Valid and Invalid Arguments

- An argument is **valid** if, when all premises are true, the conclusion must also be true. Otherwise, it is **invalid**.

10 - Quantifiers, Predicates, and Proofs

Basic Logical Inferences

Modus Ponens
$p,\ p \to q,\ \therefore q$

Modus Tollens
$p \to q,\ \neg q,\ \therefore \neg p$

Addition
$p,\ \therefore p \vee q$

Simplification
$p \wedge q,\ \therefore p$

Conjunction
$p,\ q,\ \therefore p \wedge q$

Resolution
$p \vee q,\ \neg p \vee r,\ \therefore q \vee r$

Hypothetical Syllogism
$p \to q,\ q \to r,\ \therefore p \to r$

Disjunctive Syllogism
$p \vee q,\ \neg p,\ \therefore q$

*Premise

Logical Inferences for Quantifiers

Universal Instantiation
$\forall x \in D\ (P(x))$
$\therefore P(A)$ for any $A \in D$.

Existential Instantiation
$\exists x \in D\ (P(x))$
$\therefore P(A)$ for some $A \in D$.

Universal Generalization
$P(A)$ for all $A \in D$
$\forall x \in D\ (P(x))$

Existential Generalization
$P(A)$ for some $A \in D$
$\therefore \exists x \in D\ (P(x))$

Direct Proof

Proof by Contrapositive

- Model: $p \to q \equiv \neg q \to \neg p$, $\forall x(P(x) \to Q(x)) \equiv \forall x(\neg Q(x) \to \neg P(x))$.

- Method: Assume the negation of the conclusion you want, and show that you can deduce the negation of your assumptions.

- Example: Prove that if $n \in \mathbb{Z}$ and n^2 is even, then n is even.

Prove by contrapositive: Assume that $n \in \mathbb{Z}$ is odd.

Proof by Contradiction

- Model: $p \wedge \neg p \equiv F$, $p \wedge T \equiv F \leftrightarrow p \equiv F$, $\neg p \equiv F \leftrightarrow p \equiv T$.

- Method: To show a statement is true, first assume it is false and prove using this assumption (and perhaps other true propositions!) that you conclude a contradiction, hence we were wrong about our assumption.

• Example: Show that $\sqrt{2}$ is irrational.

Assume for contradiction that $\sqrt{2}$ is rational.
Then we can write
$$\sqrt{2} = a/b, \quad b \neq 0.$$
Assume that a/b is in lowest terms: $\gcd(a,b)=1$.
Then we get
$$2 = a^2/b^2 \Rightarrow a^2 = 2b^2$$
Then $2 \mid 2b^2$, thus $2 \mid a^2$, so a^2 is even. Thus, a is even.
Write $a=2k$, $k \in \mathbb{Z}$. Then $a^2 = 4k^2 = 2b^2$.
$$\Rightarrow b^2 = 2k^2$$
Now, $2 \mid b^2$, so b^2 is even, thus b is even.
But this means a/b is not in lowest terms!
Contradiction! Thus $\sqrt{2} \notin \mathbb{Q}$. $\square$

11 - Induction, Recursion, and O-notation

Induction Example

Base case: for …

Inductive step: Assume … Then…

Conclude: Thus…, by induction

Strong Induction

Base case: Prove $P(0)$ directly.
Inductive case: Prove $\forall n \geq 0\ P(0) \land P(1) \land \ldots \land P(n)) \rightarrow P(n+1)$
Conclude: $\forall n \geq 0\ P(n)$

Example: Prove that $\forall n \geq 0$ n can be written as a product of primes
Base case: n = 2 has a decomposition into a product of primes: 2 = 2
For strong induction, assume that we can find prime decompositions for all of 2,3,4,..,n
Consider (n+1)

- If (n+1) is prime, we are done: n+1 = n+1
- If (n+1) is not prime: $n+1 = ab\ (a, b \geq 2) \rightarrow a, b \leq n$

By strong induction hypothesis, since $2 \leq a, b \leq n$, we have prime factorizations for a and b.
$\rightarrow n+1 = ab$ is a product of prime factorizations, which is a prime factorization
Example: Prove that every positive integer is a sum of distinct powers of 2
Base case n=1: $n = 2^0$
Is a sum of exactly one (therefore distinct) power of 2
For strong induction, assume this holds for 1,2,...,n.
Consider n+1. We have 2 cases:

- Case 1: n+1 is even
  We write n+1 = 2m for some $m \in N$
  Using strong induction hypothesis for $m \leq n \rightarrow m = \sum_{i=1}^{l} 2^{k_i}$
- Case 2: n+1 is odd, then n is even...

Big-O Notation

Definition

We say that $f(x)$ is in $O(g(x))$, or $f(x) \in O(g(x))$, or "f is Big-O of g," if there exist constants C and k such that for all $x \geq k$,

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

12 - Running times, Complexity Theory, and Models of Computations

1. **Polynomials**:
   - If $f(n)$ is a polynomial of degree k, then $f(n) \in O(n^k)$.
2. **Logarithmic Functions**:
   - $\log(n) \in O(n)$
   - $\log_b(n) \in O(n)$, where $b > 1$.
3. **Factorial Growth**:
   - $n! \in O(n^n)$
4. **Polynomial vs. Exponential Growth**:
   - $n^d \in O(b^n)$ if $d > 0$ and $b > 1$.
5. **Exponential Functions Comparison**:
   - If $c > b > 1$, then $b^n \in O(c^n)$ and $c^n \notin O(b^n)$.

Phrase-Structure Grammar

Definition

A **phrase-structure grammar** is a collection of data, denoted by

$$G = (V, T, S, P)$$

where:

- V is the **vocabulary**, a set of symbols used in the grammar.
- $T \subset V$ is the set of **terminal symbols** (symbols that appear in the final output).
- $S \in V$ is the **starting symbol** (the initial symbol from which derivations begin).
- P is a set of **production rules** (rules that define how symbols can be transformed).

Finite-State Machine

Definition

A **finite-state machine with output** (sometimes called a **finite-state transducer**) is a collection

$$M = (S, I, O, f, g, s_0)$$

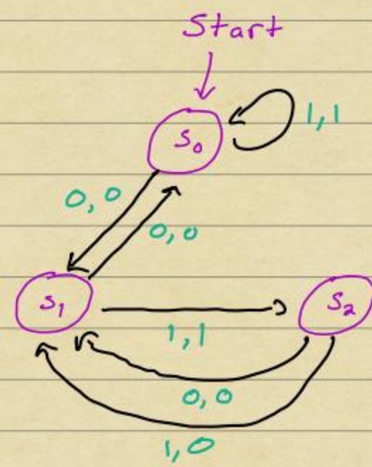
where:

- S is a finite set of **states**.
- I is a finite **input alphabet** (the set of symbols that the machine can process as input).
- O is a finite **output alphabet** (the set of symbols that the machine can produce as output).
- f is the **transition function**: $(\text{state}, \text{input}) \to \text{state}$.
- g is the **output function**: $(\text{state}, \text{input}) \to \text{output}$.
- $s_0 \in S$ is the **initial state**.

State Diagrams

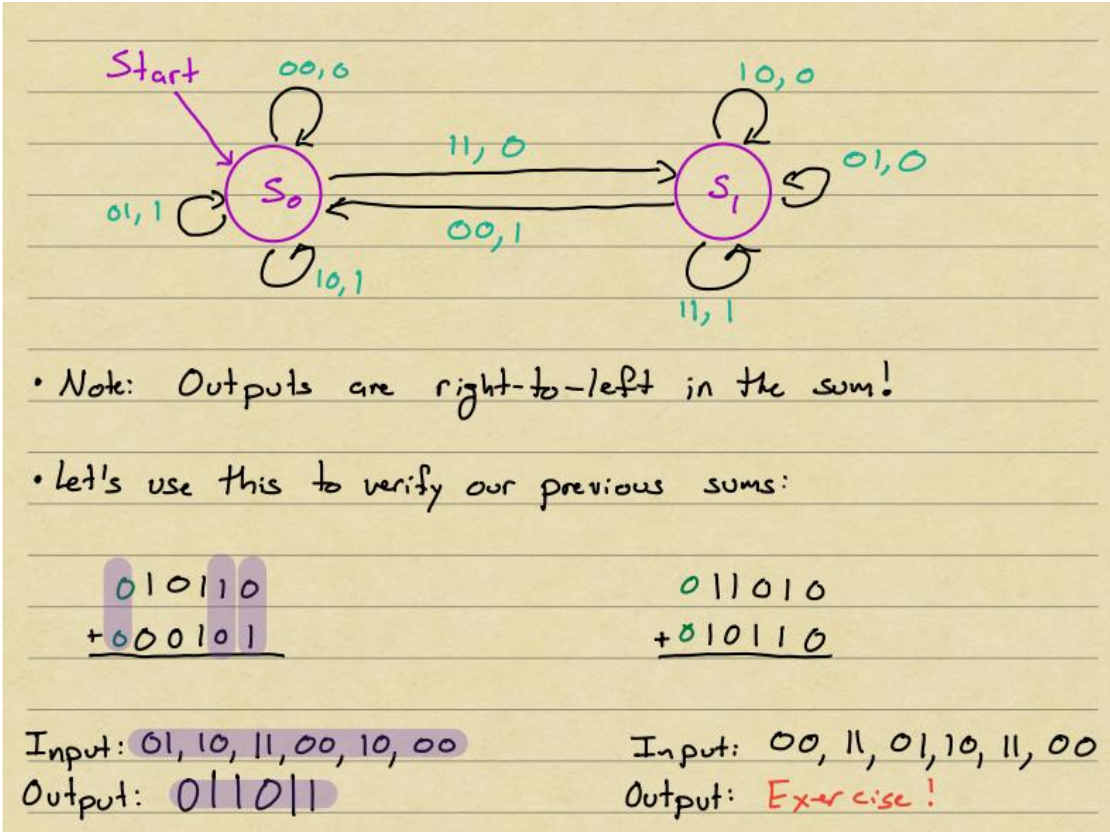
We encode this data in a directed graph with extra data called a state diagram

	f		g	
	Input		Input	
State	0	1	0	1
s_0	s_1	s_0	0	1
s_1	s_0	s_2	0	1
s_2	s_1	s_1	0	0



The first label is the input, determines the state to move to.
The second label is the output.

- Example: Input: 10110 $\rightarrow$ Output: 10100



13 - Finite State Automata and Regular Languages

Finite-state Automaton

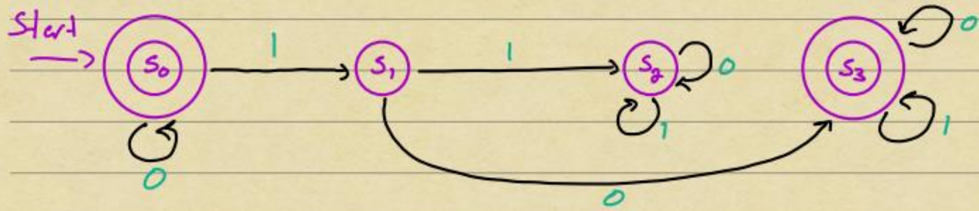
A **finite-state machine without output**, or a **finite-state automaton**, is given by the tuple

$$M = (S, I, f, s_0, F)$$

where:

- S is a finite set of **states**.
- I is a finite **input alphabet** (the set of symbols the machine can process as input).
- f is the **transition function**: $(\text{state}, \text{input}) \to \text{state}$.
- s_0 is the **initial state**.
- $F \subseteq S$ is the set of **final** or **accepting states**.

• Example: What language is recognized by the following finite-state automaton?



• s_0, s_3 only final states. How can we get to these?

• s_0: Only way to end here is via input 0^n

• s_3: $0^n 1 0 x$, x is any string in 0, 1

$$\Rightarrow L(M) = \left\{ 0^n,\ 0^n 1 0 x \;\middle|\; n \geq 0,\ x \text{ any string} \right\}.$$