# Discrete Structures (DS)

Rupak R. Gupta (RRG)
Aaditya Joil (Jojo)

2024

# Contents

Chapter 1

# Foundations

## 1.1 Set Theory

A *set* is an unordered collection of distinct objects. A set is denoted as follows:

$$\underset{\text{Name of the set}}{A} \coloneqq \{\underbrace{a_1, a_2, a_3, \dots}_{\text{Set elements}}\}$$

Membership of an element $a$ in a set $A$ is denoted as $a \in A$.

**Empty set**

The empty set is defined as the set with no elements. It is denoted as $\varnothing$ or $\{\ \}$.

### 1.1.1 Notation

A set can be represented using the following notations:

**Roster notation**

The *roster* form of a set is said to be used when all of the elements of the set are listed out. For example, $\{1, 2, 3, 4, 5\}$ or $\{2, 4, 6, 8, \dots\}$ are sets in roster notation.

**Set-builder notation**

The *set-builder* form of a set is said to be used when the membership of an element is defined by a rule rather than simply listing. For example, $\{x \mid 1 \leq x \leq 5\}$ and $\{2k \mid k \in \mathbb{N}\}$ are sets in set-builder notation.

### 1.1.2 Subsets and Supersets

A set $A$ is said to be a *subset* of $B$ if every element of $A$ also belongs in $B$. Consequently, B is called the *superset* of $A$. It is denoted as $A \subseteq B$ or $B \supseteq A$. This is illustrated in fig. 1.1.

$$A \subseteq B \iff \forall x\,(x \in A \implies x \in B) \tag{1.1}$$

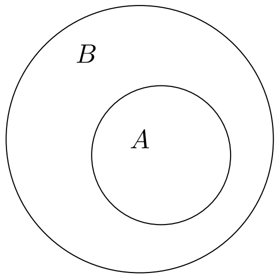



Figure 1.1: Subsets and supersets

### Proper subset

Set $A$ is said to be a *proper subset* of $B$ if $A$ is a subset of B but $A$ is not equal to $B$. It is denoted as $A \subset B$ or $B \supset A$.

$$A \subset B \iff \forall x\,(x \in A \implies x \in B) \land \exists x\,(x \in B \land x \notin A) \tag{1.2}$$

*or,*

$$A \subset B \iff \forall x\,(x \in A \implies x \in B) \land \neg\forall x\,(x \in B \implies x \in A) \tag{1.3}$$

**Q.1.** Consider the sets $A$, $B$ and $C$ defined as follows:

$$\begin{aligned}
A &\coloneqq \{x \mid x \text{ is a positive integer } \leq 8\} \\
B &\coloneqq \{x \mid x \text{ is a positive even integer } < 10\} \\
C &\coloneqq \{2, 4, 6, 8, 10\}
\end{aligned}$$

State whether each set is a subset or not of every set.

Converting $A$ and $B$ into their respective roster forms, we get

$$\begin{aligned}
A &= \{1, 2, 3, 4, 5, 6, 7, 8\} \\
B &= \{2, 4, 6, 8\}
\end{aligned}$$

Therefore, we can deduce that:

$$\boxed{\begin{array}{ccc}
A \subseteq A & A \not\subset B & A \not\subset C \\
B \subset A & B \subseteq B & B \subset C \\
C \not\subset A & C \not\subset B & C \subseteq C
\end{array}}$$

**(Ans.)**

### Properties of subsets

- $A = B \iff (A \subseteq B) \land (B \subseteq A)$
- $(A \subseteq B) \land (B \subseteq C) \implies A \subseteq C$
- $\forall A\,(\varnothing \subseteq A)$

### 1.1.3 Cardinality

The *cardinality* of a subset is defined as the number of elements in the set. The cardinality of a set $A$ is denoted as $|A|$.

**Q.2.** Consider $D \coloneqq \{n \in \mathbb{N} \,|\, n \leq 7000\}$. Find $|D|$.

Now, $D$ in roster form is $\{1, 2, 3, \ldots, 7000\}$. Therefore, $\boxed{|D| = 7000}$. **(Ans.)**

**Q.3.** Consider $E \coloneqq \{n \in \mathbb{N} \,|\, n \geq 7000\}$. Find $|E|$.

Now, $E$ in roster form is $\{7000, 7001, 7002, \ldots\}$. Therefore, the set $E$ is $\boxed{\textit{countably infinite}}$ and hence its cardinality is defined as $\boxed{\aleph_0}$. **(Ans.)**

### 1.1.4 Power Set

The *power set* of a set $A$ is the set of all of its subsets. It is denoted as $\mathcal{P}(A)$ or $2^A$.

$$\mathcal{P}(A) \coloneqq \{B \,|\, B \subseteq A\} \tag{1.4}$$

#### Cardinality of the Power Set

The cardinality of the power set $\mathcal{P}(A)$ is given by $2^{|A|}$. Here are two intuitions to justify this:

- For every element in $A$, the inclusion of that element in a subset is a boolean result. Therefore, by theorem 3, $|\mathcal{P}(A)| \coloneqq \underbrace{2 \times 2 \times \cdots \times 2}_{|A| \text{ times}} = 2^{|A|}$.
- We can construct any subset of $A$ by choosing to include any $k$ elements at a time. Therefore, by theorem 2, $|\mathcal{P}(A)| \coloneqq {}^{|A|}\mathrm{C}_0 + {}^{|A|}\mathrm{C}_1 + \cdots + {}^{|A|}\mathrm{C}_{|A|} = 2^{|A|}$.

#### Cantor's Theorem

**Theorem 1.** *The cardinality of the power set of any set is strictly greater than the cardinality of the set itself.*

$$\forall A \, |\mathcal{P}(A)| > |A| \tag{1.5}$$

### 1.1.5 Cartesian Product

The ordered $n$-tuple $(a_1, a_2, a_3, \ldots, a_n)$ is an ordered collection of $n$ objects.

Two ordered $n$-tuples $(a_1, a_2, a_3, \ldots, a_n)$ and $(b_1, b_2, b_3, \ldots, b_n)$ are equal iff they contain exactly the same elements in the same order, *i.e.* $a_i = b_i \forall i \in [\![1, n]\!]$.

The *Cartesian product* of sets $A$ and $B$ is defined as,

$$A \times B \coloneqq \{(a, b) \,|\, a \in A, b \in B\} \tag{1.6}$$

The Cartesian product is **not commutative**.

**Q.4.** Find the Cartesian product of the sets $\{\text{good}, \text{bad}\}$ and $\{\text{student}, \text{professor}\}$.

$$\{\text{good}, \text{bad}\} \times \{\text{student}, \text{professor}\} \coloneqq \boxed{\begin{matrix} \{(\text{good}, \text{student}), & (\text{good}, \text{professor}), \\ (\text{bad}, \text{student}), & (\text{bad}, \text{professor})\} \end{matrix}}$$

**(Ans.)**

More generally, the Cartesian product for $n$ sets $A_1, A_2, \ldots, A_n$ is defined as,

$$A_1 \times A_2 \times \cdots \times A_n \coloneqq \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in A_i \ \forall i \in [\![1, n]\!]\} \tag{1.7}$$

**Properties of the Cartesian product**

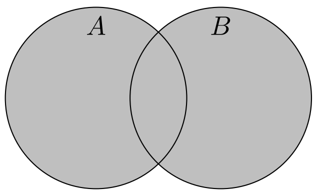
- $|A \times B| = |A||B|$
- $A \times \varnothing = \varnothing \times A = \varnothing$
- $\forall A \neq \varnothing \ \forall B \neq \varnothing \ A \neq B \iff A \times B \neq B \times A$

### 1.1.6 Set Operations

**Union**

The *union* of two sets $A$ and $B$ is defined as the set comprising all elements from $A$ and $B$.

$$A \cup B \coloneqq \{x \,|\, x \in A \vee x \in B\} \tag{1.8}$$




| $A$ | $B$ | $A \cup B$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

Figure 1.2: Union

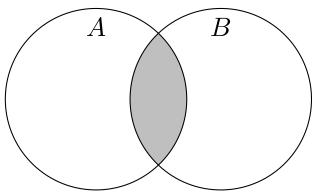
For example, $\{a, b\} \cup \{b, c, d\} = \{a, b, c, d\}$.

For the union of the sets $A_1, A_2, \ldots, A_n$ the shorthand notation is $\bigcup_{i=1}^{n} A_i$.

**Intersection**

The *intersection* of two sets $A$ and $B$ is defined as the set comprising all the elements common in $A$ and $B$.

$$A \cap B \coloneqq \{x \,|\, x \in A \wedge x \in B\} \tag{1.9}$$




| $A$ | $B$ | $A \cap B$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

Figure 1.3: Intersection

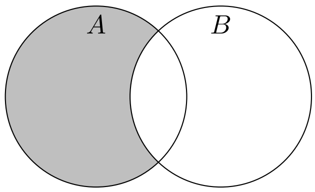
For example, $\{a, b\} \cap \{b, c, d\} = \{b\}$.

For the intersection of the sets $A_1, A_2, \ldots, A_n$ the shorthand notation is $\bigcap_{i=1}^{n} A_i$.

**Difference**

The *difference* of sets $A$ and $B$ is defined as the set comprising all elements from $A$ that are not also in $B$.

$$A \setminus B \coloneqq \{x \mid x \in A \wedge x \notin B\} \tag{1.10}$$




| $A$ | $B$ | $A \setminus B$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

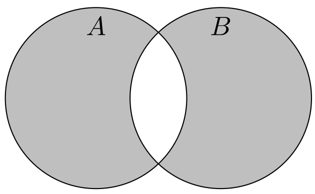
Figure 1.4: Difference

For example, $\{a, b\} \setminus \{b, c, d\} = \{a\}$.

**Symmetric difference**

The *symmetric difference* of sets $A$ and $B$ is defined as the set comprising all elements that belong in either $A$ or $B$ but not both.

$$A \triangle B \coloneqq \{x \mid (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\} = (A \setminus B) \cup (B \setminus A) \tag{1.11}$$




| $A$ | $B$ | $A \triangle B$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Figure 1.5: Symmetric difference

For example, $\{a, b\} \triangle \{b, c, d\} = \{a, c, d\}$.

### 1.1.7 Inclusion-Exclusion Principle

For sets $A$ and $B$, the cardinalities of their union and intersection are related by the following equality:

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{1.12}$$

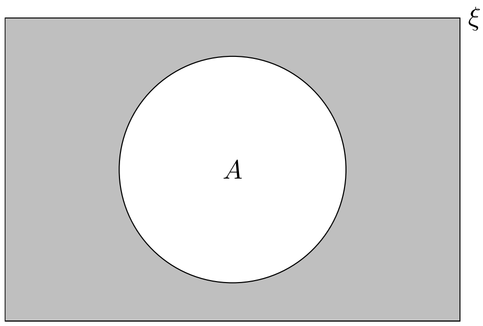
### 1.1.8 Universal Set

The superset of all objects of current interest is called the *universe of discourse* or the *universal set*. It is denoted as $U$ or $\xi$.

#### Complement

The complement of a set $A$ is defined as the set of all elements in $\xi$ not contained in $A$.

$$A^{\complement} \coloneqq \xi \setminus A \coloneqq \{x \mid x \notin A\} \tag{1.13}$$




| $A$ | $A^{\complement}$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

Figure 1.6: Complement

### 1.1.9 Set Identity Laws

- $A \cup \varnothing = A$, $A \cap \xi = A$ (Identity)
- $A \cup \xi = \xi$, $A \cap \varnothing = \varnothing$ (Domination)
- $A \cup A = A$, $A \cap A = A$ (Idempotence)
- $\left(A^{\complement}\right)^{\complement} = A$ (Complementation)
- $A \cup B = B \cup A$, $A \cap B = B \cap A$ (Commutativity)
- $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ (Associativity)
- $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$, $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$ (De Morgan)
- $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$ (Absorption)
- $A \cup A^{\complement} = \xi$, $A \cap A^{\complement} = \varnothing$ (Complement)

### 1.1.10 Number Sets

Following are some of the standard number sets used throughout mathematics:

$$\text{Natural numbers, } \mathbb{N} := \{1, 2, 3, \dots\} := \{n \mid n \text{ is a natural number}\} \tag{1.14}$$

$$\text{Integers, } \mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\} := \{n \mid n \text{ is an integer}\} \tag{1.15}$$

$$\text{Rational numbers, } \mathbb{Q} := \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbb{Z} \wedge q \neq 0 \right\} \tag{1.16}$$

$$\text{Real numbers, } \mathbb{R} := \{x \mid x \text{ is a real number}\} \tag{1.17}$$

$$\text{Complex numbers, } \mathbb{C} := \{x + iy \mid x, y \in \mathbb{R}\} \tag{1.18}$$

## 1.2 Logic

Logic is the branch of philosophy concerned with analysing the patterns of reasoning by which a conclusion is drawn from a set of premises, without relevance to meaning or object.

Logic requires two key skills: **Abstraction** and **Formalisation**.

### 1.2.1 Propositional Logic

#### Negation

The *negation* of a proposition refers to the inversion of its truth value.

| $p$ | $\neg p$ |
|---|---|
| $T$ | $F$ |
| $F$ | $T$ |

Table 1.1: Negation

#### Conjunction

The *conjunction* of two propositions is true when both the propositions are true, otherwise it is false.

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $F$ |

Table 1.2: Conjunction

In the expression $p \wedge q$, $p$ and $q$ are called *conjuncts*.

For the conjunction of the propositions $p_1, p_2, \dots, p_n$ the shorthand notation is $\bigwedge_{i=1}^{n} p_i$.

### Disjunction

The *disjunction* of two propositions is false when both the propositions are false, otherwise it is true.

| $p$ | $q$ | $p \lor q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $T$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $F$ |

Table 1.3: Disjunction

In the expression $p \lor q$, $p$ and $q$ are called *disjuncts*.

For the disjunction of the propositions $p_1, p_2, \ldots, p_n$ the shorthand notation is $\bigvee_{i=1}^{n} p_i$.

### Exclusive disjunction

*Exclusive disjunction* is a special type of disjunction where the truth value is true when only one of the propositions is true, otherwise it is false.

| $p$ | $q$ | $p \veebar q$ |
|---|---|---|
| $T$ | $T$ | $F$ |
| $T$ | $F$ | $T$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $F$ |

Table 1.4: Exclusive disjunction

### Implication

*Implication* is an operation between two propositions where it results in false when the first proposition is true and the second one is false, otherwise it is true. It is also known as a *conditional operator*.

| $p$ | $q$ | $p \implies q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $T$ |

Table 1.5: Implication

In the expression $p \implies q$, $p$ is called the *hypothesis* or *antecedent*, while $q$ is called the *consequent*.

For an implication $p \implies q$,

- Its **converse** is $q \implies p$.
- Its **inverse** is $\neg p \implies \neg q$.
- Its **contrapositive** is $\neg q \implies \neg p$.

| $p$ | $q$ | $\neg p$ | $\neg q$ | $p \implies q$ | $q \implies p$ | $\neg p \implies \neg q$ | $\neg q \implies \neg p$ |
|---|---|---|---|---|---|---|---|
| $T$ | $T$ | $F$ | $F$ | $T$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $T$ | $F$ | $T$ | $T$ | $F$ |
| $F$ | $T$ | $T$ | $F$ | $T$ | $F$ | $F$ | $T$ |
| $F$ | $F$ | $T$ | $T$ | $T$ | $T$ | $T$ | $T$ |

Table 1.6: Converse, Inverse and Contrapositive

From the truth table, it can be observed that,

$$p \implies q \equiv \neg q \implies \neg p \qquad \text{(Implication} \equiv \text{Contrapositive)}$$

$$q \implies p \equiv \neg p \implies \neg q \qquad \text{(Converse} \equiv \text{Inverse)}$$

**Equivalence**

*Equivalence* is a type of implication where both statements act as the antecedent as well as consequent. This means that the implication is true only when the statements have the same truth value. This is what it means for two propositions to be logically equivalent.

| $p$ | $q$ | $p \iff q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $T$ |

Table 1.7: Equivalence

In the expression $p \iff q$, $p$ and $q$ are called *equivalents*.

### 1.2.2 Logical Equivalence Laws

- $p \wedge T \equiv p$, $p \vee F \equiv p$ (Identity)
- $p \wedge F \equiv F$, $p \vee T \equiv T$ (Domination)
- $p \wedge p \equiv p$, $p \vee p \equiv p$ (Idempotence)
- $\neg(\neg p) \equiv p$ (Double negation)
- $p \wedge q \equiv q \wedge p$, $q \vee q \equiv q \vee p$ (Commutativity)
- $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$, $p \vee (q \vee r) \equiv (p \vee q) \vee r$ (Associativity)
- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$, $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (Distributivity)
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$, $\neg(p \vee q) \equiv \neg p \wedge \neg q$ (De Morgan)
- $p \implies q \equiv \neg p \vee q$, $p \iff q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ (Implication)

### 1.2.3 Predicate logic

#### Existential quantifier

The existential quantifier $\exists$ (read as "there exists") states that there exists an element in the given set that follows the stated rule or has the specified property. In some contexts, the notation $\exists!$ is used to denote the existence of **exactly one** element.

#### Universal quantifier

The universal quantifier $\forall$ (read as "for all") states that all elements in the given set that follow the stated rule or have the specified property.

### 1.2.4 Rules of Inference

The validity of an argument is determined using the rules of inference.

| Inference Rule | Form | Equivalent Implication |
|---|---|---|
| **Modus Ponens** | $\begin{array}{rl} & p \implies q \\ & \underline{p \qquad\quad} \\ \therefore & q \end{array}$ | $((p \implies q) \land p) \implies q$ |
| **Modus Tollens** | $\begin{array}{rl} & p \implies q \\ & \underline{\neg q \qquad\quad} \\ \therefore & \neg p \end{array}$ | $((p \implies q) \land \neg q) \implies \neg p$ |
| **Addition** | $\begin{array}{rl} & \underline{p \qquad} \\ \therefore & p \lor q \end{array}$ | $p \implies (p \lor q)$ |
| **Simplification** | $\begin{array}{rl} & \underline{p \land q} \\ \therefore & p \end{array}$ | $(p \land q) \implies p$ |
| **Conjunction** | $\begin{array}{rl} & p \\ & \underline{q \qquad} \\ \therefore & p \land q \end{array}$ | $(p \land q) \implies (p \land q)$ |
| **Resolution** | $\begin{array}{rl} & p \lor q \\ & \underline{\neg p \lor r} \\ \therefore & q \lor r \end{array}$ | $((p \lor q) \land (\neg p \lor r)) \implies (q \lor r)$ |
| **Hypothetical Syllogism** | $\begin{array}{rl} & p \implies q \\ & \underline{q \implies r} \\ \therefore & p \implies r \end{array}$ | $((p \implies q) \land (q \implies r)) \implies (p \implies r)$ |
| **Disjunctive Syllogism** | $\begin{array}{rl} & p \lor q \\ & \underline{\neg p \qquad} \\ \therefore & q \end{array}$ | $((p \lor q) \land \neg p) \implies q$ |
| **Constructive Dilemma** | $\begin{array}{rl} & p \implies q \\ & r \implies s \\ & \underline{p \lor r \qquad} \\ \therefore & q \lor s \end{array}$ | $((p \implies q) \land (r \implies s) \land (p \lor r)) \implies (q \lor s)$ |
| **Destructive Dilemma** | $\begin{array}{rl} & p \implies q \\ & r \implies s \\ & \underline{\neg q \lor \neg s} \\ \therefore & \neg p \lor \neg r \end{array}$ | $((p \implies q) \land (r \implies s) \land (\neg q \lor \neg s))$ $\implies (\neg p \lor \neg r)$ |

Table 1.8: Propositional rules of inference

These rules are useful for formulating *proofs* in §1.2.5.

**Rules of inference for quantified statements**

| Inference Rule | Form | Equivalent Implication |
|---|---|---|
| **Universal instantiation** | $\dfrac{\forall x P(x)}{\therefore\ P(c)}$ | $(\forall x P(x)) \implies P(c)$ |
| **Universal generalization** | $\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x P(x)}$ | $(P(c) \text{ for an arbitrary } c) \implies \forall x P(x)$ |
| **Existential instantiation** | $\dfrac{\exists x P(x)}{\therefore\ P(c) \text{ for some element } c}$ | $\exists x P(x) \implies P(c) \text{ for some element } c$ |
| **Existential generalization** | $\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x P(x)}$ | $(P(c) \text{ for some element } c) \implies \exists x P(x)$ |

Table 1.9: Rules of inference for quantified statements

### 1.2.5 Methods of Proofs

**Direct proof**

A direct proof proves a given statement using a sequence of true implications derived from previous results. A direct proof applies the inference rule of **hypothetical syllogism**.

$$p \implies q \equiv p \implies r_1 \implies r_2 \implies \cdots \implies r_n \implies q$$

**Q.5.** Prove $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$.

**Method 1**: Hypothetical syllogism

$$\begin{aligned} X \cup (Y \cap Z) &:= \{p \,|\, p \in X\} \cup \{p \,|\, p \in Y \wedge p \in Z\} \\ &= \{p \,|\, p \in X \vee (p \in Y \wedge p \in Z)\} \\ &= \{p \,|\, (p \in X \vee p \in Y) \wedge (p \in X \vee p \in Z)\} \quad \textit{Distributivity} \\ &= \{p \,|\, p \in X \vee p \in Y\} \cap \{p \,|\, p \in X \vee p \in Z\} \\ &:= (X \cup Y) \cap (X \cup Z) \end{aligned}$$

Therefore, $\boxed{X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)}$. □

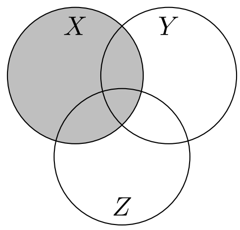
**Method 2**: Membership tables

| $X$ | $Y$ | $Z$ | $Y \cap Z$ | $X \cup Y$ | $X \cup Z$ | $\mathbf{X} \cup (\mathbf{Y} \cap \mathbf{Z})$ | $(\mathbf{X} \cup \mathbf{Y}) \cap (\mathbf{X} \cup \mathbf{Z})$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| 0 | 0 | 1 | 0 | 0 | 1 | **0** | **0** |
| 0 | 1 | 0 | 0 | 1 | 0 | **0** | **0** |
| 0 | 1 | 1 | 1 | 1 | 1 | **1** | **1** |
| 1 | 0 | 0 | 0 | 1 | 1 | **1** | **1** |
| 1 | 0 | 1 | 0 | 1 | 1 | **1** | **1** |
| 1 | 1 | 0 | 0 | 1 | 1 | **1** | **1** |
| 1 | 1 | 1 | 1 | 1 | 1 | **1** | **1** |

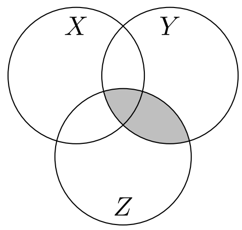
It can be observed that the columns under $X \cup (Y \cap Z)$ and $(X \cup Z) \cap (X \cup Z)$ are identical. Therefore, $\boxed{X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)}$. □

**Method 3**: Venn diagrams

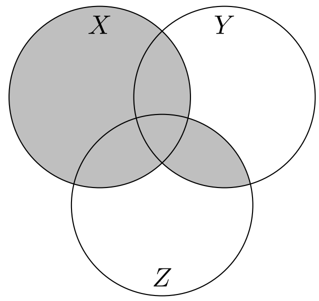
Venn diagram for $X \cup (Y \cap Z)$:




$X$

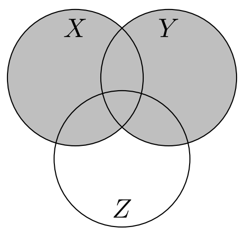



$Y \cap Z$

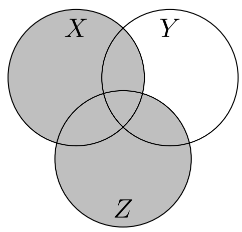



$\mathbf{X} \cup (\mathbf{Y} \cap \mathbf{Z})$

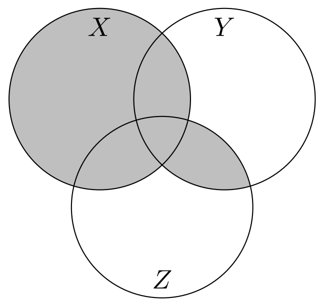
Venn diagram for $(X \cup Y) \cap (X \cup Z)$:




$X \cup Y$




$X \cup Z$




$(\mathbf{X} \cup \mathbf{Y}) \cap (\mathbf{X} \cup \mathbf{Z})$

It can be observed that the Venn diagrams of $X \cup (Y \cap Z)$ and $(X \cup Z) \cap (X \cup Z)$ are identical. Therefore, $\boxed{X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)}$. $\square$

**Proof by contraposition**

We know that an implication $p \implies q$ is equivalent to its contrapositive implication $\neg\, q \implies \neg\, p$ from §1.2.1.

Therefore, an implication could be proven by first assuming its consequent as false and then proving its antecedent to be false.

**Proof by contradiction**

**Q.6.** Prove if $n$ is an integer, then $n^2 + 2$ is not divisible by 4.

*Proof.* For contradiction, assume $\exists n \in \mathbb{Z} : 4|n^2 + 2 \implies n^2 + 2 \equiv 0 \pmod 4$.

Let $n$ be an even integer, *i.e.* $n \coloneqq 2k_1$ for some integer $k_1$.

$$\begin{aligned}\therefore n^2 + 2 &= (2k_1)^2 + 2\\ &= 4k_1^2 + 2\\ &\equiv 2 \pmod 4 \implies 4 \nmid n^2 + 2 \text{ for even } n.\end{aligned}$$

Let $n$ be an odd integer, *i.e.* $n \coloneqq 2k_2 + 1$ for some integer $k_2$.

$$\begin{aligned}\therefore n^2 + 2 &= (2k_2 + 1)^2 + 2\\ &= 4k_2^2 + 4k_2 + 1 + 2\\ &= 4(k_2^2 + k_2) + 3\\ &\equiv 3 \pmod 4 \implies 4 \nmid n^2 + 2 \text{ for odd } n.\end{aligned}$$

This implies that $n$ must be an integer that is neither even nor odd, which is a contradiction ($\implies \impliedby$).

Therefore, our assumption is incorrect and $\boxed{n^2 + 2 \text{ is not divisible by 4 if } n \in \mathbb{Z}}$. $\square$

**Proof by exhaustion**

Proof by exhaustion or proof by cases is a proof method in which we prove a statement $P(n)$ for all individual and exhaustive $k$ cases.

$$P(n) \coloneqq \bigwedge_{i=1}^{k} P(n_i)$$

**Mathematical induction**

Let $P(n)$ be a propositional function ($P : \mathbb{N} \to \{T, F\}$).

The proof that $\forall n\, P(n) \equiv T$ by mathematical induction has the following steps:

- **Basis step**: State $P(n) \equiv T$ for $n = 1$ (or any other starting $n$).
- **Inductive step**: Assume the *inductive hypothesis* $P(k) \equiv T$ for some $n = k$. Then, prove $P(k) \implies P(k+1)$.
- **Conclusion**: Therefore, $\forall n\, P(n) \equiv T$.

**Q.7.** Prove $n < 2^n \ \forall n > 1$.

*Proof.* Let $P(n) \equiv n < 2^n$, $n \in \{2, 3, 4, \dots\}$.

- **Basis step**: $P(2) \equiv \left(2 < 2^2\right) \equiv (2 < 4) \equiv T$.
- **Inductive step**: Consider $P(k) \equiv T$ for some $k > 1$.

$$\begin{aligned}\therefore k &< 2^k\\ \therefore 2k &< 2 \cdot 2^k\\ \therefore k + k &< 2^{k+1}\\ \therefore (k+1) + (k-1) &< 2^{k+1} \longrightarrow (1)\end{aligned}$$

*Multiplying both sides by 2*

$$
\begin{aligned}
\text{Now, } k &> 1 \\
\implies k - 1 &> 0 \\
\therefore (k+1) + (k-1) &> k + 1 \quad \textit{Adding } k+1 \textit{ to both sides} \\
\implies k + 1 &< (k+1) + (k-1) \implies (2)
\end{aligned}
$$

From (1) and (2),

$$k + 1 < (k+1) + (k-1) < 2^{k+1} \implies \boxed{k + 1 < 2^{k+1}} \text{ by transitivity.}$$

$\therefore \boxed{P(k) \implies P(k+1)}$.

- **Conclusion**: Therefore, $\boxed{n < 2^n \; \forall n > 1}$ by induction.

□

**Q.8.** Prove $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$ for all positive integers $n$.

*Proof.* Let $P(n) \equiv 1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$ for $n \in \mathbb{N}$.

- **Basis step**: $P(1) \equiv \left(1 = \frac{1(1+1)}{2}\right) \equiv \left(1 = \frac{2}{2}\right) \equiv T$.
- **Inductive step**: Consider $P(k) \equiv T$ for some $k \in \mathbb{Z}^+$.

$$
\begin{aligned}
\therefore 1 + 2 + 3 + \cdots + k &= \frac{k(k+1)}{2} \quad \textit{Adding } k+1 \textit{ to both sides} \\
\therefore 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\
\therefore 1 + 2 + 3 + \cdots + (k+1) &= \frac{k^2 + k + 2(k+1)}{2} \\
\therefore 1 + 2 + 3 + \cdots + (k+1) &= \frac{k^2 + 3k + 2}{2} \\
\therefore 1 + 2 + 3 + \cdots + (k+1) &= \frac{(k+1)(k+2)}{2} \\
\therefore 1 + 2 + 3 + \cdots + (k+1) &= \frac{(k+1)((k+1)+1)}{2} \implies \boxed{P(k) \implies P(k+1)}
\end{aligned}
$$

- **Conclusion**: Therefore, $\boxed{1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}}$ by induction.

□

## 1.3 The Five Most Asked Questions in Computer Science

1. Can a problem be solved by a computer program?
2. If not, then can the problem be modified so that it can be solved by a computer program?
3. If so, can *you* write a program to solve the problem?
4. Can you convince another person that your program is correct?
5. Can you prove that the program is efficient?

# Chapter 2

# Combinatorics and Discrete Probability

## 2.1 Combinatorics

### 2.1.1 Fundamental Principle of Counting

**Fundamental Theorem of Addition**

**Theorem 2.** *If a task $T$ can be subdivided into subtasks $T_1$ and $T_2$, then the total number of ways to perform task $T$ is equal to the sum of the number of ways of performing subtask $T_1$ and the number of ways of performing subtask $T_2$, if task $T$ is dependent on the completion of both the subtasks together* disjunctively*.*

**Fundamental Theorem of Multiplication**

**Theorem 3.** *If a task $T$ can be subdivided into subtasks $T_1$ and $T_2$, then the total number of ways to perform subtask $T$ is equal to the product of the number of ways of performing subtask $T_1$ and the number of ways of performing subtask $T_2$, if task $T$ is dependent on the completion of both the subtasks together* conjunctively*.*

**Permutations**

The number of ways to permute or arrange $r$ objects out of $n$ objects is denoted by ${}^n\mathrm{P}_r$, such that

$$ {}^n\mathrm{P}_r \coloneqq \frac{n!}{(n-r)!} \tag{2.1} $$

**Corollary 1.** *The number of ways to permute or arrange $n$ objects is equal to*

$$ {}^n\mathrm{P}_n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n! $$

**Theorem 4.** *The number of distinguishable permutations that can be performed from a collection of $n$ objects, consisting of $r$ distinct objects, where the first object appears $k_1$ times, second object appears $k_2$ times and so on is:*

$$ \frac{n!}{k_1!k_2!\cdots k_r!} = \frac{n!}{\prod_{i=1}^{r} k_i!} $$

**Combinations**

The number of ways to select or choose $r$ objects out of $n$ objects is denoted by ${}^{n}\mathrm{C}_r$[1], such that

$$ {}^{n}\mathrm{C}_r := \frac{n!}{r!(n-r)!} \tag{2.2} $$

**Corollary 2.** *The number of ways to select $r$ objects out of $n$ objects is equal to the number of ways to not select the remaining $n-r$ objects of the $n$ objects.*

$$ {}^{n}\mathrm{C}_r = {}^{n}\mathrm{C}_{n-r} $$

**Q.1.** There are 5 ways to move from $A$ to $B$, 2 ways to move from $B$ to $C$ and 2 ways to move from $A$ to $C$. How many total ways exist from $A$ to $C$?

Number of ways to move from $A$ to $C$ without moving through $B = 2$
By theorem 3, number of ways to move from $A$ to $C$ through $B = 5 \times 2 = 10$

By theorem 2, $\boxed{\text{Total number of ways from } A \text{ to } C = 2 + 10 = 12}$ **(Ans.)**

**Q.2.** Find the total number of all license plates consisting of 7 letters of the English alphabet.

Each of the 7 spaces of the license plate can have one of the 26 letters of the English alphabet, so the total number of ways by theorem 3 is $\boxed{\underbrace{26 \times 26 \times \cdots \times 26}_{7 \text{ times}} = 26^7}$ **(Ans.)**

**Q.3.** Find the number of passwords consisting of 5 or less letters,

i) With repetition

For each character, there are 26 possible letters.
For a password of length $n$, there are $\underbrace{26 \times 26 \times \cdots \times 26}_{n \text{ times}} = 26^n$ possible passwords.

$\therefore$ Number of passwords $= \boxed{26^5 + 26^4 + 26^3 + 26^2 + 26 = \dfrac{26(26^5 - 1)}{25}}$ **(Ans.)**

ii) Without repetition

For a password of length $n$, we need to permute $n$ letters out of the 26 letters.

$$ \begin{aligned} \therefore \text{Number of passwords} &= {}^{26}\mathrm{P}_5 + {}^{26}\mathrm{P}_4 + {}^{26}\mathrm{P}_3 + {}^{26}\mathrm{P}_2 + {}^{26}\mathrm{P}_1 \\ &= \boxed{\frac{26!}{21!} + \frac{26!}{22!} + \frac{26!}{23!} + \frac{26!}{24!} + \frac{26!}{25!}} \end{aligned} $$

**(Ans.)**

**Q.4.** Set $A$ contains 2 elements and set $B$ contains 5 elements. How many

i) functions can exist from set $A$ to set $B$?

By the definition of a function, each element of the domain ($A$) should map to exactly one element of the codomain ($B$).

$\therefore$ $\boxed{\text{Number of functions} = 5^2 = 25}$ **(Ans.)**

ii) injective functions can exist from set $A$ to set $B$?

For an injective function, select any two elements of the codomain and map them to

[1] An alternative notation for ${}^{n}\mathrm{C}_r$ is $\binom{n}{r}$, which is used to denote a binomial coefficient.

the elements of the domain.

$\therefore$ $\boxed{\text{Number of injective functions} = {}^5C_2 \times 2! = 20}$ **(Ans.)**

**Q.5.** If there are 5 shirts and 3 pants, how many ways are there to dress up?

By theorem 3, there are $5 \times 3 =$ $\boxed{\text{15 ways to dress up.}}$ **(Ans.)**

**Q.6.** Set $A$ has 5 elements and set $B$ has 3 elements. How many relations exist from set $A$ to set $B$?

Cardinality of Cartesian product $=|A \times B| = 3 \times 5 = 15$
By definition, a relation is a subset of the Cartesian product.

$$\begin{aligned} \therefore \text{Number of relations} &= \text{Number of subsets of } |A \times B| \\ &= 2^{|A \times B|} \\ &= \boxed{2^{15}} \end{aligned}$$

**(Ans.)**

**Q.7.** From 9 Maths faculty members and 11 IT faculty members, a committee consisting of 3 Maths faculty members and 4 IT faculty members is to be created to decide the question paper. How many total committees can be created?

We need to choose 3 faculty members out of 9 from Maths and 4 faculty members out of 11 from IT.

$\therefore$ By theorem 3, $\boxed{\text{total number of committees} = {}^9C_3 \times {}^{11}C_4}$ **(Ans.)**

**Q.8.** How many distinguishable permutations are there of the letters of the word

i) BANANA?

The word BANANA consists of 6 letters out of which letter B appears once, letter A appears 3 times and letter N appears 2 times.

By theorem 4, number of distinguishable permutations $= \dfrac{6!}{1!3!2!} = \boxed{60}$

$\boxed{\text{There are 60 distinguishable permutations.}}$ **(Ans.)**

ii) BOOLEAN?

The word BOOLEAN consists of 7 letters out of which every letter appears once except O, which appears twice.

By theorem 4, number of distinguishable permutations $= \dfrac{7!}{2!} = \boxed{2520}$

$\boxed{\text{There are 2520 distinguishable permutations.}}$ **(Ans.)**

**Q.9.** In how many ways can 7 people be seated in a circle?

The number of ways 7 people can be seated in a line $= 7!$

For a circular arrangement, the same permutation can be rotated 7 times and there would be no change to the arrangement.
$\Longrightarrow$ 7 linear arrangements correspond to one circular arrangement.

$\therefore$ Number of circular permutations $= \dfrac{7!}{7} = 6! = \boxed{720}$

$\boxed{\text{There are 720 ways 7 people can be seated in a circle.}}$ **(Ans.)**

**Q.10.** 6 men and 6 women are to be seated in a row. How many ways are there to seat them, if

i) there is no restriction?

With no restriction, we can simply permute 12 people in a row.
$\therefore$ $\boxed{\text{There are } 12! \text{ ways to seat the people.}}$ **(Ans.)**

ii) men and women occupy alternate positions?

To seat the men and women in alternate positions, we need to permute the 6 men in 6 of the alternate positions and permute the 6 women in the remaining 6 positions, and consider the arrangements where the men and women could swap their positions.

$\therefore$ Number of permutations $= \boxed{6! \times 6! \times 2!}$
$\boxed{\text{There are } 6! \times 6! \times 2! \text{ ways the men and women can be seated.}}$ **(Ans.)**

**Q.11.** How many 5 letter words can be made using the 4 letters A, B, C and D such that the string "ADC" does not appear?

Consider 5 spots for each letter of the 5 letter word.

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

There are $4^5 = 1024$ possible 5 letter words that can be formed with the letters A, B, C and D.

Now consider the string "ADC" as a single unit, which could appear at spots 123, 234 or 345.
The remaining 2 letters could be any of the given 4 letters.

$\therefore$ Number of words containing the string "ADC" $= (1 \times 4 \times 4) \times 3 = 48$

$\therefore$ Number of required words $= 1024 - 48 = \boxed{976}$

$\boxed{\text{There are 976 words that do not contain the string “ADC”.}}$ **(Ans.)**

### Derangements

The number of ways to arrange $n$ objects such that no objects are present in their original position is denoted by $!n$ (read as "$n$ subfactorial") or $D_n$, the number of *derangements* of $n$. It is defined as,

$$!n := n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right) \tag{2.3}$$

**Theorem 5.** *The sum of all partial derangements of $n$ distinct elements is the equal to the total number of permutations of those $n$ elements.*

$$\binom{n}{0}(!0) + \binom{n}{1}(!1) + \binom{n}{2}(!2) + \cdots + \binom{n}{n}(!n) = n! \tag{2.4}$$

*Proof.* Consider permuting $n$ objects. There are $n!$ ways to do this.

Now consider the following cases:

- Fix no elements in place and derange all elements, *i.e.* no elements are in the correct position. The number of ways to do this is $!n$ or ${}^n\mathrm{C}_0(!n)$.
- Fix any one element in its correct place and derange the remaining $(n - 1)$ elments. The

number of ways to do this is ${}^{n}\mathrm{C}_1(!(n-1))$.

- Fix any two elements in their correct place and derange the remaining $(n-2)$ elements. The number of ways to do this is ${}^{n}\mathrm{C}_2(!(n-2))$.

$$\vdots$$

- Fix all elements in their correct place and derange no elements. The number of ways to do this is ${}^{n}\mathrm{C}_n(!0)$.

It can be observed all the cases are *mutually exclusive*, since there is at least one element that is not in its correct place in any two of the cases simultaneously.

The above cases are also *exhaustive*, since there is no arrangement of the $n$ elements that does not fit under any of the above cases.

Therefore by theorem 2,

$$\begin{aligned}
\binom{n}{0}(!n) + \binom{n}{1}(!(n-1)) + \binom{n}{2}(!(n-2)) + \cdots + \binom{n}{n}(!0) &= n! \\
\therefore \binom{n}{n}(!0) + \binom{n}{n-1}(!1) + \binom{n}{n-2}(!2) + \cdots + \binom{n}{0}(!n) &= n! \\
\therefore \binom{n}{0}(!0) + \binom{n}{1}(!1) + \binom{n}{2}(!2) + \cdots + \binom{n}{n}(!n) &= n!
\end{aligned}$$

*By corollary 2*

$\square$

### 2.1.2 Inclusion-Exclusion Principle

For sets $A$ and $B$, the cardinalities of their union and intersection are related by the following equality,

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{2.5}$$

The same can be generalised to three sets $A$, $B$ and $C$.

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| \tag{2.6}$$

And to $n$ sets.

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\varnothing \neq J \subseteq [\![1,n]\!]} (-1)^{|J|+1} \left|\bigcap_{j \in J} A_j\right| \tag{2.7}$$

**Q.12.** A software development company employs 100 computer programmers such that

45 programmers are proficient in Java,

30 programmers are proficient in C#,

20 programmers are proficient in Python,

6 programmers are proficient in C# and Java,

1 programmer is proficient in Java and Python,

5 programmers are proficient in C# and Python,

and 1 programmer is proficient in all three.

Find the number of programmers not proficient in any of the above languages.

Let set $J$ denote the set of programmers proficient in Java, set $C$ denote those proficient in C# and set $P$ denote those proficient in Python.

From equation 2.6,

$$\begin{aligned} |J \cup C \cup P| &= |J| + |C| + |P| - |J \cap C| - |C \cap P| - |J \cap P| + |J \cap C \cap P| \\ &= 45 + 30 + 20 - 6 - 5 - 1 + 1 \\ \therefore |J \cup C \cup P| &= 84 \end{aligned}$$

$J \cup C \cup P$ denotes the set of programmers proficient in at least one of the three languages.

$$\begin{aligned} \therefore \text{No. of programmers not proficient in any language} &= |\neg (J \cup C \cup P)| \\ &= 100 - |J \cup C \cup P| \\ &= 100 - 84 \\ &= \boxed{16} \end{aligned}$$

**(Ans.)**

**Q.13.** A class contains 75 students, such that 50 students like Cricket and 15 students like Cricket and Volleyball. If every student likes at least one of Cricket or Volleyball, how many students like Volleyball?

Let set $C$ denote the set of students who like Cricket and set $V$ denote those who like Volleyball.

From equation 2.5,

$$\begin{aligned} |C \cup V| &= |C| + |V| - |C \cap V| \\ \therefore 75 &= 50 + |V| - 15 \\ \therefore |V| &= 75 - 35 = 40 \end{aligned}$$

$\therefore$ $\boxed{\text{40 students like Volleyball.}}$ **(Ans.)**

### 2.1.3 The Pigeonhole Principle

**Theorem 6.** *If there are $n$ pigeons and $m$ pigeonholes such that $n > m$, then each of the pigeons can be put on a pigeonhole iff there exists at least one hole with more than one pigeon.*

For example, if there are 367 people in a room, it is guaranteed that at least two of them share a birthday.

**Q.14.** Show that if any five numbers from 1 to 8 are chosen, then two of them will add to 9.

*Proof.* There are 4 possible pairs of numbers that add up to 9:

$$\{1, 8\}, \{2, 7\}, \{3, 6\}, \{4, 5\}$$

Let each of these sets represent a pigeonhole, and each of the 5 chosen numbers represent a pigeon.

By theorem 6, two numbers will belong to the same set.

$\Longrightarrow$ $\boxed{\text{Two of the chosen numbers will add to 9.}}$ □

**Q.15.** Shirts numbered consecutively from 1 to 20 are worn by the 20 member of a bowling league. When any three of these members are chosen to be a team, sum of their numbers are used as a code number for the team. Show that if any 8 of the 20 members are selected then from these eight, one must form at least two different teams having the same code.

The question can be interpreted purely in a mathematical way as follows:

From integers 1 to 20, eight numbers are selected at random. From these eight numbers if we form groups of three then we have to prove that at least two groups have the same sum.

*Proof.* From 8 numbers, 3 numbers can be selected in ${}^8\mathrm{C}_3 = \frac{8\times7\times6}{3\times2} = 56$ ways. If three numbers are taken from 1 to 20, then the smallest sum is $1+2+3=6$ and the largest sum is $18+19+20=57$.

If we choose any other three numbers, their sum will be between 6 and 57. Thus, there are $57-6+1=52$ different sums. These 52 sums can be considered as pigeonholes and the selected 56 group can be considered as pigeons.

Therefore by theorem 6, $\boxed{\text{two groups will have the same sum.}}$ □

**Extended Pigeonhole Principle**

**Theorem 7.** *If $n$ pigeons are assigned to $m$ pigeonholes such that $n > m$, then one of the pigeonholes must contain at least* $\left\lfloor \dfrac{n-1}{m} \right\rfloor + 1$ *pigeons.*

*Proof.* Consider $m$ pigeonholes and $n$ pigeons. By the pigeonhole principle (theorem 6), each pigeonhole will contain at least two or more pigeons for at least $m+1$ pigeons.
Similarly, it will require at least $2m+1$ pigeons to guarantee that at least one pigeonhole contains three or more pigeons.

Hence, it can be generalized that we require at least $(h-1)m+1$ pigeons in order to guarantee that there is at least one pigeonhole contains $h$ or more pigeons.

$$\Longrightarrow n \geq (h-1)m+1$$
$$\therefore n-1 \geq (h-1)m$$
$$\therefore \left\lfloor \frac{n-1}{m} \right\rfloor = h-1 \qquad \text{(Taking the quotient upon dividing by } m\text{)}$$
$$\therefore \left\lfloor \frac{n-1}{m} \right\rfloor + 1 = h$$

$\Longrightarrow$ Each pigeonhole contains at least $\left\lfloor \dfrac{n-1}{m} \right\rfloor + 1$ pigeons. □

**Q.16.** Show that if any 30 people are selected and one may choose a subset of 5 people, then all five people were born on the same day of the week.

*Proof.* Let each of the 7 days of the week represent pigeonholes and the 30 people represent pigeons.

By the extended pigeonhole principle, each pigeonhole must contain at least $\left\lfloor \frac{30-1}{7} \right\rfloor + 1$ pigeons.

$$\begin{aligned}
\therefore \text{ Number of people born on the same day of the week} &= \left\lfloor \frac{30-1}{7} \right\rfloor + 1 \\
&= \left\lfloor \frac{29}{7} \right\rfloor + 1 \\
&= 4 + 1 = \boxed{5}
\end{aligned}$$

Thus, there must be at least 5 people that are born on the same day of the week. ☐

### 2.1.4 Binomial Theorem

**Theorem 8.** *Let $x$ and $y$ be two variables and $n$ be any non-negative integer, then*

$$\begin{aligned}
(x+y)^n &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n}y^n \\
&= \sum_{r=0}^{n} \binom{n}{r} x^{n-r}y^r
\end{aligned}$$

*where $\binom{n}{r}$ is called a* binomial coefficient.

**Corollary 3.** *Let $n$ be a non-negative integer, then*

$$\text{i) } \sum_{r=0}^{n} \binom{n}{r} = 2^n \tag{2.8}$$

$$\text{ii) } \sum_{r=0}^{n} (-1)^r \binom{n}{r} = 0 \tag{2.9}$$

$$\text{iii) } \sum_{r=0}^{n} 2^r \binom{n}{r} = 3^n \tag{2.10}$$

**Pascal's Identity**

**Theorem 9.** *Let $n$ and $k$ be positive integers with $n \geq k$. Then*

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \tag{2.11}$$

*Proof.* Let $S$ be a set of cardinality $n+1$ and $a \in S$.

Now, consider the number of ways one can select $k$ elements out of the $n+1$ elements of set $S$. This is equal to $\binom{n+1}{k}$.

$\because S = \{a\} \cup (S - \{a\})$,

$$\begin{aligned}
\binom{n+1}{k} = &\text{ (number of ways to select } k \text{ elements including element } a) + \\
&\text{ (number of ways to select } k \text{ elements excluding element } a)
\end{aligned}$$

Now, the number of ways to select $k$ elements from $S$ *including* element $a$ = number of ways to select $a$ and $k-1$ elements from the remaining $n$ elements, which is equal to $\binom{n}{k-1}$.

Moreover, the number of ways to select $k$ elements from $S$ *excluding* element $a$ = number of ways to select $k$ elements from the remaining $n$ elements, which is equal to $\binom{n}{k}$.

Therefore,

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

□

### 2.1.5 Modular Arithmetic

A modulo class of a natural number $n$ is a set consisting of all possible remainders when a natural number is divided by $n$. It is denoted by $[n]$.

$$[n] \coloneqq \{0, 1, 2 \ldots, n\} \coloneqq [\![0, n]\!]$$

**Q.17.** How many one-one functions exist from

$$f : [6] \to \{A, B, C, \ldots, Z\}?$$

Cardinality of domain = Cardinality of the set $\{0, 1, 2, 3, 4, 5\} = 6$
Cardinality of codomain = Cardinality of the set $\{A, B, C, \ldots, Z\} = 26$

For a one-one function, select any two elements of the codomain and map them to the elements of the domain.

$\therefore$ $\boxed{\text{Number of one-one functions} = {}^{26}\mathrm{P}_6 = \frac{26!}{20!}}$ **(Ans.)**

### 2.1.6 Newton's Identity

**Theorem 10.** *If $n \geq r \geq k$ are natural numbers, then*

$$^{n}\mathrm{C}_r \times {}^{r}\mathrm{C}_k = {}^{n}\mathrm{C}_k \times {}^{n-k}\mathrm{C}_{r-k}$$

*Proof.* Consider selecting $r$ objects from a set of $n$ objects and further selecting $k$ objects from the selected $r$ objects.

Thus we have a set of selected $r - k$ objects and a set of further selected $k$ objects. The number of ways of creating these sets is $^{n}\mathrm{C}_r \times {}^{r}\mathrm{C}_k$.

The same sets can be constructed by first selecting the $k$ objects from the set of $n$ objects and then selecting the remaining $r - k$ objects from the remaining $n - k$ objects. The number of ways of accomplishing this is $^{n}\mathrm{C}_k \times {}^{n-k}\mathrm{C}_{r-k}$.

Therefore,

$$\boxed{^{n}\mathrm{C}_r \times {}^{r}\mathrm{C}_k = {}^{n}\mathrm{C}_k \times {}^{n-k}\mathrm{C}_{r-k}}$$

□

### 2.1.7 Non-Negative Integral Solutions

**Theorem 11.** *Number of non-negative integral solutions of the equation* $x_1 + x_2 + \cdots + x_r = n$ *is* ${}^{n+r-1}\mathrm{C}_{r-1}$.

For example, the number of non-negative integral solutions of the equation $x_1 + x_2 + x_3 = 7$ is ${}^{7+3-1}\mathrm{C}_{3-1} = {}^{9}\mathrm{C}_2 = 36$, which can be verified by enumeration.

*Proof.* Consider the equation $x_1 + x_2 + \cdots + x_r = n$.

The given problem can be interpreted as creating $r$ groups from $n$ identical objects by using $r - 1$ identical partitions.

$$\bullet \quad | \quad \bullet \quad \bullet \quad \bullet \quad \cdots\cdots \quad \bullet \quad | \quad \bullet \quad \bullet \quad |$$

$n$ identical objects and $r-1$ partitions

Now, the number of ways to create $r$ groups from $n$ identical objects using $r - 1$ identical partitions is simply equal to the number of distinguishable permutations of the total $n + r - 1$ objects.

$\therefore$ From theorem 4, number of permutations $= \dfrac{(n + r - 1)!}{n!(r - 1)!} := \boxed{{}^{n+r-1}\mathrm{C}_{r-1}}$

*Alternatively,*

We could consider selecting any $r-1$ spots out of the total $n+r-1$ spots to place the partitions in, and then placing the $n$ objects in the remaining $n$ spots, giving the same result as $\boxed{{}^{n+r-1}\mathrm{C}_{r-1}}$.

Therefore, the number of non-negative integral solutions of the equation $x_1 + x_2 + \cdots + x_r = n$ is equal to ${}^{n+r-1}\mathrm{C}_{r-1}$. $\square$

**Q.18.** 15 friends are buying ice cream from 5 different flavors, such that each friend gets one ice cream. How many ways are there to buy ice cream?

Let variables $x_1, x_2, x_3, x_4$ and $x_5$ represent the number of ice cream bought for each of the 5 flavors.

According to the given condition, $x_1 + x_2 + x_3 + x_4 + x_5 = 15$. $\therefore$ Number of non-negative solutions of the above equation is given by ${}^{15+5-1}\mathrm{C}_{5-1} = \boxed{{}^{19}\mathrm{C}_4}$.

$\boxed{\text{There are } {}^{19}\mathrm{C}_4 \text{ ways to buy the ice cream.}}$ **(Ans.)**

**Q.19.** How many non-negative integral solutions are there to $x+y+z = 60$ such that $x \geq 3, y \geq 4$ and $z \geq 5$?

Let $x := x' + 3, y := y' + 4$ and $z := z' + 5 \implies x', y', z' \geq 0$.

$$\begin{aligned} x + y + z &= 60 \\ \therefore (x' + 3) + (y' + 4) + (z' + 5) &= 60 \\ \therefore x' + y' + z' &= 48 \end{aligned}$$

Number of non-negative solutions of the above equation is given by ${}^{48+3-1}\mathrm{C}_{3-1} = {}^{50}\mathrm{C}_2 = \boxed{1225}$

$\boxed{\text{There are 1225 solutions to the given equation.}}$ **(Ans.)**

## 2.2 Discrete Probability

### 2.2.1 Definition

#### Sample Space

The set of all possible possible outcomes is called the sample space, which is analogous to the universe of discourse $\xi$ in set theory. Every event in discourse is a subset of the sample space.

#### Experiment

An *experiment* refers to a process that when repeated under the same conditions has a well-defined set of possible outcomes. An experiment has the following properties:

- It can be repeated under the same conditions.
- It produces one outcome at a time.
- The outcome is uncertain before conducting the experiment.

A single execution or instance of an experiment is called a *trial*. Each trial produces exactly one outcome from the sample space.

#### Defining Probability

*Probability* is the study of numerically assigning the chance of occurrence of an event. Probability can also be understood as the proportion of the success of a given event out of all trials in the sample space.

The probability of an event $A$ is denoted as $P(A)$ and defined as,

$$P(A) \coloneqq \frac{|A|}{|S|} \tag{2.12}$$

### 2.2.2 Axioms of Probability

#### Axiom of Non-Negativity

**Theorem 12.** *For any event $A$, the probability of $A$ is always non-negative.*

$$\forall A \, P(A) \geq 0$$

#### Axiom of Normalization

**Theorem 13.** *The probability of the sample space $S$ is 1, since something within the sample space must occur.*

$$P(S) = 1$$

#### Axiom of Additivity

**Theorem 14.** *The probability of the union of two disjoint events $A$ and $B$ is equal to the sum of their individual probabilities.*

$$P(A \cup B) = P(A) + P(B) \ \textit{if} \ A \cap B = \varnothing$$

**Corollary 4.** *If $A \cap B \neq \varnothing$, then we can use the Inclusion-Exclusion principle:*

$$
\begin{aligned}
|A \cup B| &= |A| + |B| - |A \cap B| && \textit{Divide both sides by } |S| \\
\therefore \frac{|A \cap B|}{|S|} &= \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|A \cap B|}{|S|} && \textit{By eq. } (2.12) \\
\therefore P(A \cap B) &= P(A) + P(B) - P(A \cap B)
\end{aligned}
$$

---

Chapter 3

# Relations and Functions

## 3.1 Relations

A relation $R$ is a subset of the Cartesian product of two sets. $a$ is said to be *related* to $b$ by $R$ iff $(a, b) \in R$. this is denoted as $aRb$. If $(a, b) \notin R$, then $a$ is not related to $b$ by $R$. This is denoted as $a\overline{R}b$.

The converse relation $R^{-1}$ to a relation $R$ is defined as follows:

$$R^{-1} \coloneqq \{(b, a) \mid aRb\} \tag{3.1}$$

### 3.1.1 Properties of Relations

**Symmetric relations**

A symmetric relation is one where the presence of one pair $(a, b)$ implies that the pair $(b, a)$ is also present in the given relation.

$$\forall a \, \forall b \, (aRb \implies bRa) \tag{3.2}$$

**Antisymmetric relations**

An antisymmetric relation is one where the presence of $(a, b)$ and $(b, a)$ in the relation implies $a = b$. In other words, an antisymmetric relation does not allow symmetric pairs of ordered pairs except those which contain the same elements.

$$\forall a \, \forall b \, (aRb \wedge bRa \implies a = b) \tag{3.3}$$

**Asymmetric relations**

An asymmetric relation is one where the presence of $(a, b)$ implies that the pair $(b, a)$ is absent from the given relation. In other words, NO symmetric pairs of ordered pairs are allowed.

$$\exists a \, \exists b \left(aRb \wedge b\overline{R}a\right) \tag{3.4}$$

**Q.1.** Determine the symmetricity of the following relations:

(i) $R_1 = \{(1,1), (1,2), (2,1), (3,3), (4,4)\}$
The given relation is symmetric as all the symmetric pairs of ordered pairs are present in the relation.

(ii) $R_2 = \{(1,1)\}$
The given relation is symmetric and antisymmetric at the same time.

(iii) $R_3 = \{(1,3), (3,2), (2,1)\}$
The given relation is antisymmetric and asymmetric at the same time.

(iv) $R_4 = \{(4,4), (3,3), (1,4)\}$
The given relation is antisymmetric as the only symmetric pairs of ordered pairs present are of the type $(a, a)$.

### Reflexive relations

A relation from a set $A$ to *itself* is reflexive if the ordered pairs of the form $(a, a)$ for all elements $a \in A$ are present in the relation.

$$\forall a \, (aRa) \tag{3.5}$$

**Q.2.** Determine the reflexivity of the following relations for the set $A = \{1, 2, 3, 4\}$.

(i) $R_1 \coloneqq \{(1,1), (2,2), (1,3), (4,4)\}$
The given relation is not reflexive as the element $(3,3)$ is not a part of the relation.

(ii) $R_2 \coloneqq \{(1,1), (2,2), (3,3), (1,2), (4,4)\}$
The given relation is reflexive since all reflexive pairs belong in it.

### Transitive relations

A relation from a set $A$ to $B$ where $A \supseteq B$ is transitive if for all the ordered pairs $(a, b)$ and $(b, c)$ present in the relation, the ordered pair $(a, c)$ is also present in the relation.

$$\forall a \, \forall b \, \forall c \, (aRb \land bRc \implies aRc) \tag{3.6}$$

**Q.3.** Determine the transitivity of the given relations for the set $A = \{1, 2, 3, 4\}$.

(i) $R_1 = \{(1,1), (1,2), (2,2), (2,1), (3,3)\}$
The given relation is transitive in nature.

(ii) $R_2 = \{(1,3), (3,2), (2,1)\}$
The given relation is not transitive as the ordered pair $(1,2)$ is not present despite the presence of $(1,3)$ and $(3,2)$.

(iii) $R_3 = \{(2,4), (4,3), (2,3), (4,1)\}$
The given relation is not transitive as the ordered pair $(2,1)$ is not present despite the presence of $(2,4)$ and $(4,1)$.

### 3.1.2 Equivalence Relations

A relation which is reflexive, symmetric and transitive is said to be an *equivalence* relation.

#### Equivalence classes

For an equivalence relation $R$ from $A$ to $B$, the equivalence class $[a]_R$ is the set $\{b \in B \mid aRb\}$.

**Q.4.** Prove that the relation $R \coloneqq \{(a, b) \mid a \equiv b \pmod 3\}$ is equivalence on the set of integers. Find all of its equivalence classes.

For any integer $a$, $a \bmod 3 = a \bmod 3 \iff a \equiv a \pmod 3 \implies R$ is reflexive.

For any two integers $a$ and $b$, $a \equiv b \pmod 3 \iff a \bmod 3 = b \bmod 3 \iff b \equiv a \pmod 3 \implies R$ is symmetric.

Consider $a \bmod 3 = b \bmod 3 \coloneqq r$ and $b \bmod 3 = c \bmod 3 \coloneqq s$ for some integers $a$, $b$, $c$.

$\because r = b \bmod 3 = s$, $a \equiv b \pmod 3 \wedge b \equiv c \pmod 3 \implies a \equiv c \pmod 3$. Therefore, $R$ is transitive.

$\because R$ is reflexive, symmetric and transitive, $\boxed{\text{it is an equivalence relation}}$. $\square$

Modulo 3, the possible remainders are 0, 1 and 2. Therefore, the equivalence classes are:

$$\boxed{\begin{aligned} [0]_R &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ [1]_R &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ [2]_R &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}}$$

**(Ans.)**

#### Partitions of a set

A partition of a set is a subset of the elements of a set such that each element of the original set is a part of one and only one such subset.

#### Rules for partitions of a set

A given set $S$ is said to have $n$ partitions $A_1, A_2, \ldots, A_n$ if and only if the following conditions are satisfied:

1. $\forall A_i,\ A_i \neq \varnothing$; The partitions are non-empty.
2. $\bigcup_{i=1}^{n} A_i = S$; The union of the partition should be the original set.
3. $A_i \cap A_j = \varnothing, \forall i \neq j$; The partitions should be disjoint.

**Q.5.** Determine whether the following sets contain valid partitions for the set $S = \{\mathrm{u, m, b, r, o, c, k, s}\}$.

(i) $\{\{\mathrm{m, o, c, k}\}, \{\mathrm{r, u, b, s}\}\}$

Since all subsets are non-empty, disjoint and they unite to form $S$, $\boxed{\text{they are valid partitions.}}$ **(Ans.)**

(ii) $\{\{\mathrm{c, o, m, b}\}, \{\mathrm{u, s}\}, \{\mathrm{r}\}\}$

The above subsets $\boxed{\text{are not valid partitions}}$, as there is no subset containing the element k. **(Ans.)**

(iii) $\{\{\mathrm{b, r, o, c, k}\}, \{\mathrm{m, u, s, t}\}\}$

The above subsets $\boxed{\text{are not valid partitions}}$, as their union consists of an additional element $\mathrm{t} \notin S$. **(Ans.)**

(iv) $\{\{\mathrm{u, m, b, r, o, c, k, s}\}\}$

Since the set itself is non-empty, $\boxed{\text{it forms a partition}}$ by itself. **(Ans.)**

(v) $\{\{\mathrm{b, o, o, k}\}, \{\mathrm{r, u, m}\}, \{\mathrm{c, s}\}\}$

Since all subsets are non-empty, disjoint and they unite to form $S$, $\boxed{\text{they are valid partitions.}}$ **(Ans.)**

(vi) $\{\{\mathrm{u, m, b}\}, \{\mathrm{r, o, k}\}, \varnothing\}$

$\varnothing$ cannot be a partition, therefore the given subsets $\boxed{\text{are not valid partitions.}}$ **(Ans.)**

**Equivalence partitions**

A partition of a set $S$ being 'equivalent' means that for a particular equivalence relation $R_{eq} : S \to S$, the set of equivalence classes is a subset of the given partition.

For an equivalence relation $R$ with the partitions $R_1, R_2, \ldots, R_n$, the equivalence relation is given by $R = \bigcup_{i=1}^{n} R_i \times R_i$.

*E.g.,* Let $\{0\}, \{1, 2\}$ be partitions of the set $\{0, 1, 2\}$ under an equivalence relation $R$.

The equivalence classes are: $[0]_R = \{0\},\ [1]_R = [2]_R = \{1, 2\}$
The equivalence relation is: $R = \{(0, 0), (1, 1), (1, 2), (2, 1), (2, 2)\}$

### 3.1.3 Representing Relations

**Adjacency Matrices**

We can represent the relations using boolean adjacency matrices, also called zero-one matrices. The matrix element has a non-zero entry $a_{ij}$ if $iRj$.

$$\mathbf{M}_R \coloneqq [m_{ij}] \,:\, m_{ij} = \begin{cases} 0, & i\overline{R}j \\ 1, & iRj \end{cases}$$

**Operations on Adjacency Matrices**

The various operations which can be applied to sets can also be applied to the matrix form of relations. They are as follows:

- **Join**: The union ($\cup$) of two relations is also called the *join* ($\vee$) operation. We take the 'join' of two relations by disjoining corresponding elements of the matrices.

$$[p_{ij}]_{m \times n} \vee [q_{ij}]_{m \times n} = [p_{ij} \vee q_{ij}]_{m \times n}$$

- **Meet**: The intersection ($\cap$) of two relations is also called the *meet* ($\wedge$) operation. We take the 'meet' of two relations by conjoining corresponding elements of the matrices.

$$[p_{ij}]_{m \times n} \wedge [q_{ij}]_{m \times n} = [p_{ij} \wedge q_{ij}]_{m \times n}$$

- **Composition**: We can compose two relations by performing a pseudo-matrix multiplication of the zero-one matrices of the given relations, where any element which is greater than one is replaced by 1 itself.

$$[p_{ij}]_{m\times r} \circ [q_{ij}]_{r\times n} = \left[\bigvee_{k=1}^{r} (p_{ik} \wedge q_{kj})\right]_{m\times n}$$

**Properties of zero-one matrices**

- A relation $R$ is **reflexive** iff the leading diagonal of its matrix is all 1's.
- A relation $R$ is **symmetric** iff the matrix is symmetric (*i.e.*, $\mathbf{M}_R = \mathbf{M}_R^\top$).
- A relation $R$ is **antisymmetric** iff $\mathbf{M}_R \wedge \mathbf{M}_R^\top$ is a diagonal matrix.
- The **converse** relation $R^{-1}$ corresponds to the matrix $\mathbf{M}_R^\top$
- The **complement** relation $\overline{R}$ corresponds to the matrix $[\overline{m}_{ij}]$.

**Directed Graphs**

A relation can also be represented by using a directed graph (digraph). A digraph is denoted by $G(V, E)$ where $V$ is the set of vertices and $E$ is the set of edges from one vertex to another. We can say that $E \subseteq V \times V$. These graphs are 'directed' as they represent *ordered* pairs. The ordered pair $(a, b)$ in the relation $R$ can be represented as an edge from vertex $a$ to vertex $b$.

*E.g.,* Find the adjacency matrix and digraph of the relation $\{(1,1),(1,2),(2,1),(3,3),(4,4)\}$ for the set $A = \{1, 2, 3, 4\}$.

$$\mathbf{M}_R := \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \end{array} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Figure 3.1: Zero-one matrix

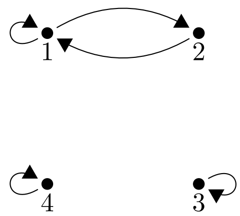



Figure 3.2: Digraph

### 3.1.4 Composition of Relations

Suppose, we have been given two relations $R = \{(a, b) \mid a \in A,\ b \in B\}$ and $S = \{(b, c) \mid b \in B,\ c \in C\}$, then the composition of the two relations is defined as $S \circ R = \{(a, c) \mid aRb \wedge bSc\}$.

Think of a relation as applying a transformation (foreshadowing?) to the first element with the second element being the result of that transformation. Then a composition $S \circ R$ is defined as the transformation which first takes in $a$, applies $R$ on it and then applies $S$ on the output of $R$.

A composition of a relation to itself is denoted using exponent notation *i.e.* $R \circ R = R^2$, $R^k \circ R = R^{k+1}$.

### 3.1.5 Closure

A closure of a relation is the smallest set which contains the provided relation and satisfies the specified property of binary relations. The closure of a relation is denoted as $R^*$. The set of least elements required for the closure is denoted as $\Delta$.

$$R^* \coloneqq R \cup \Delta \tag{3.7}$$

#### Reflexive closure

The reflexive closure $R^*$ of a relation $R$ is the smallest possible relation containing $R$ while being reflexive. For a relation $R$ defined on the set $A$, the reflexive closure:

$$R^* = R \cup \left\{(a, a) \,\middle|\, a\overline{R}a\right\}, \implies \Delta = \left\{(a, a) \,\middle|\, a\overline{R}a\right\} \tag{3.8}$$

#### Symmetric closure

The symmetric closure $R^*$ of a relation $R$ is the smallest possible relation containing $R$ while being symmetric. For a relation $R$ defined on the set $A$, the symmetric closure:

$$R^* = R \cup \left\{(b, a) \,\middle|\, aRb \wedge b\overline{R}a\right\} \implies \Delta = R^{-1} \setminus R \tag{3.9}$$

#### Transitive closure

The transitive closure $R^*$ of a relation $R$ is the smallest possible relation containing $R$ while being transitive.

#### Warshall's algorithm

**Lemma 1.** *Let $R$ be a relation on $S \coloneqq \{v_1, v_2, \ldots, v_n\}$ and let $\mathbf{W}^{(k)} \coloneqq \left[w_{ij}^{(k)}\right]$ be the zero-one matrix s.t. $w_{ij}^{(k)} = 1 \iff \exists$ a path from $v_i$ to $v_j$ with interior vertices $\in \{v_1, v_2, \ldots, v_k\}$.*

Warshall's algorithm is an algorithm in graph theory used to find the shortest path, or transitive closure in a digraph. It is as follows:

**Algorithm 1:** Warshall's algorithm to find transitive closure

**Input:** Adjacency matrix $\mathbf{M}_R$ of a relation $R$ of size $n$

**Output:** Transitive closure of the graph, represented by the matrix $\mathbf{W}^{(n)}$

$\mathbf{W}^{(0)} \coloneqq \mathbf{M}_R$;<br>
**for** $k \coloneqq 1$ ***to*** $n$ **do**<br>
    **for** $i \coloneqq 1$ ***to*** $n$ **do**<br>
        **for** $j \coloneqq 1$ ***to*** $n$ **do**<br>
            $\mathbf{W}_{ij}^{(k)} \coloneqq \mathbf{W}_{ij}^{(k-1)} \vee \left(\mathbf{W}_{ik}^{(k-1)} \wedge \mathbf{W}_{kj}^{(k-1)}\right)$;<br>
        **end**<br>
    **end**<br>
**end**<br>
**return** $\mathbf{W}^{(n)}$;

The result $\mathbf{W}^{(n)}$ of the above relation is the required **transitive closure** of $R$.

Transitivity can be understood as every transitive triplet of ordered pairs sort of following the 'polygon law of vector addition'. *E.g.*, if the ordered pairs $(a, b)$, $(b, c)$ and $(c, d)$ are present in the relation then by transitivity there should exist a direct path from $a$ to $c$ and $b$ to $d$. However, now the addition of $(b, d)$ means that $aRb$ AND $bRd$[1] exist, which implies a path from $a$ to $d$ must also exist for the relation to be considered transitive.

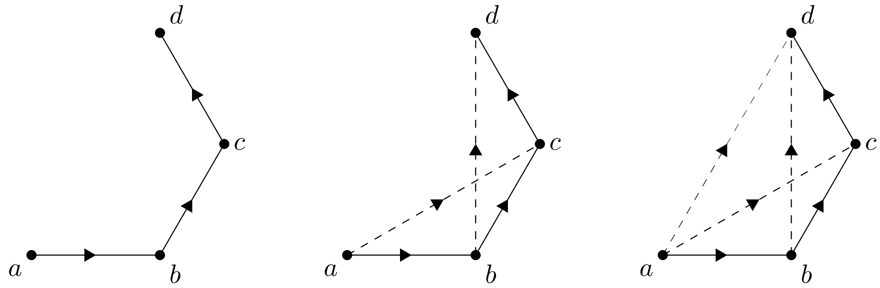



Figure 3.3: Transitivity

### 3.1.6 Partially-Ordered Set

Formally, a Partially-ordered set (poset) is a homogeneous binary relation that is reflexive, antisymmetric and transitive. In order theory, a partial ordering on a set is an arrangement such that, for certain pair of elements, one precedes ($\preceq$) or succeeds ($\succeq$) the other.

#### Notation

A poset $P$ is denoted as $(S, \text{ඩ})$, where $S$ is the ground set and ඩ is the relation which determines the ordering. A poset is *partial* because not every element needs to be related to to every other element by ඩ. Two elements that are related by the partial ordering are called *comparable*, while those unrelated are called *incomparable*.

$$\text{For } a \neq b,\ a \text{ and } b \text{ are comparable} \iff ((a, b) \in \text{ඩ}) \veebar ((b, a) \in \text{ඩ}) \tag{3.10}$$

#### Total Ordering

A total ordering is a partial ordering where every pair of elements in $S$ is comparable by the partial order ඩ.

#### Hasse diagrams

A Hasse diagram is a special type of digraph which is used to commonly represent a poset. It has a few special properties.

1. Self relations are not represented.
2. For $n$ ordered pairs which are transitive in nature, i.e. $aRb_1 \wedge b_1Rb_2 \wedge b_2Rb_3 \wedge \cdots \wedge b_{n-1}Rc \implies aRc$, the relation $aRc$ is not represented but the connecting relations from $a$ to $b_1$, $b_1$ to $b_2$, and so on are represented.
3. The actual physical placement of nodes matters since the arrowsheads representing the direction are not usually drawn. This is done to drive home the idea of "ordering".

[1]The same argument could also have been made about $aRc$ and $cRd$.

Some terminologies related to posets are as follows:

**Minimal elements** An element is said to be *minimal* if there is no comparable element in the poset $(S, \preceq)$ that preceeds it except itself, *i.e.* the element is at a "valley" of the Hasse diagram.

$$a \text{ is minimal} \iff \forall b \in S\,(b \preceq a \implies a = b) \tag{3.11}$$

**Least elment** If a poset $(S, \preceq)$ consists of exactly one minimal element, then that element is said to be the *least*.

$$a \text{ is least} \iff \forall b \in S\,(a \preceq b) \tag{3.12}$$

**Maximal elements** An element is said to be *maximal* if there is no comparable element in the poset $(S, \preceq)$ that succeeds it except itself, *i.e.* the element is at a "peak" of the Hasse diagram.

$$a \text{ is maximal} \iff \forall b \in S\,(a \preceq b \implies a = b) \tag{3.13}$$

**Greatest elment** If a poset $(S, \preceq)$ consists of exactly one minimal element, then that element is said to be the *greatest*.

$$a \text{ is greatest} \iff \forall b \in S\,(b \preceq a) \tag{3.14}$$

**Lower bound** An element $c$ is said to be a *lower bound* of two elements $a$ and $b$ in the poset $(S, \preceq)$ if $c \preceq a \land c \preceq b$. If every pair of elements has a unique greatest lower bound, then the Hasse diagram is said to be a *meet semilattice*.

**Upper bound** An element $c$ is said to be a *upper bound* of two elements $a$ and $b$ in the poset $(S, \preceq)$ if $a \preceq c \land b \preceq c$. If every pair of elements has a unique least upper bound, then the Hasse diagram is said to be a *join semilattice*.

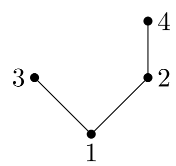
### Lattices

A *lattice* is an algebraic structure derived from posets in which every pair of elements has a unique greatest lower bound and a unique least upper bound. Therefore, a Hasse diagram that is a meet semilattice as well as a join semilattice is called a lattice.

*E.g.,* Find the partially ordered relation, draw the Hasse diagram and determine the total ordering and latticity of the following:

(i) $(\{1, 2, 3, 4\}, |)$ where $a|b$ means $a$ divides $b$.

$$\begin{aligned} P &= (\{1, 2, 3, 4\}, |) \\ &\equiv \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\} \end{aligned}$$

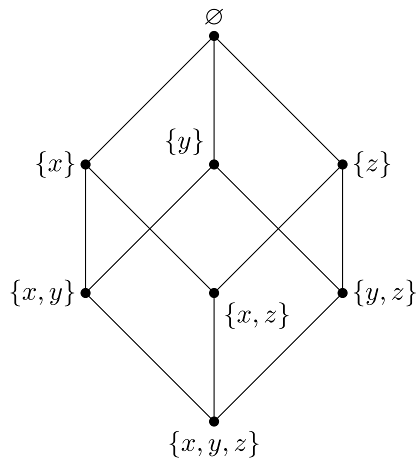



Hasse diagram

The given poset is not totally ordered as the elements 2 and 3 are incomparable by the | relation. It is also not a lattice as the least upper bound for elements 3 and 2 does not exist.

(ii) $(\mathcal{P}(\{x,y,z\}), \supseteq)$, where $\mathcal{P}(S)$ denotes the power set of $S$.

$$
\begin{aligned}
P &= (\mathcal{P}(\{x,y,z\}), \supseteq) \\
&\equiv \{(\{x,y,z\},\{x,y,z\}), (\{x,y,z\},\{x,y\}), (\{x,y,z\},\{y,z\}), (\{x,y,z\},\{x,z\}), (\{x,y,z\},\{x\}), \\
&\quad (\{x,y,z\},\{y\}), (\{x,y,z\},\{z\}), (\{x,y,z\},\varnothing), (\{x,y\},\{x,y\}), (\{x,y\},\{x\}), (\{x,y\},\{y\}), \\
&\quad (\{x,y\},\varnothing), (\{y,z\},\{y,z\}), (\{y,z\},\{y\}), (\{y,z\},\{z\}), (\{y,z\},\varnothing), (\{x,z\},\{x,z\}) \\
&\quad (\{x,z\},\{x\}), (\{x,z\},\{z\}), (\{x\},\{x\}), (\{x\},\varnothing), (\{y\},\{y\}), (\{y\},\varnothing), (\{z\},\{z\}), (\{z\},\varnothing)\}
\end{aligned}
$$

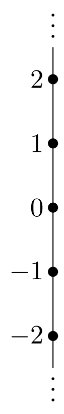



Hasse diagram

The given poset is not a total ordering because $\{x\}$ and $\{y\}$ are incomparable by the $\supseteq$ relation. It is however a lattice, as each pair of comparable elements have a greatest lower bound and a least upper bound.

(iii) $(\mathbb{Z}, \leq)$, where $\mathbb{Z}$ denotes the set of integers.

$$
\begin{aligned}
P &= (\mathbb{Z}, \leq) \\
&\equiv \{(n,m) \mid n, m \in \mathbb{Z} \wedge n \leq m\}
\end{aligned}
$$




Hasse diagram

The given poset is a **total ordering** since by transitivity, every two elements are comparable. It is also a lattice since it is a meet semilattice as well as a join semilattice.

### 3.1.7 Lattice Job Scheduling Problem

Consider you have 5 jobs to complete: $A$, $B$, $C$, $D$ and $E$. Some jobs are dependent on others as follows:

- $A$ must be completed before $B$ and $C$ can start.
- $B$ and $C$ both must be completed before $D$ can start.
- $D$ must be completed before $E$ can start.

Suppose you have **2 processors** to complete these jobs, and each job takes one unit of time on each processor. The goal is to schedule jobs in such a way that all the dependencies are respected and the total completion time is minimized.

This is an example of an $\mathcal{NP}$-hard problem. Its solution is as follows:

The given dependencies are partially ordered and they form a directed acyclic graph. Therefore, they can be represented by the following lattice:

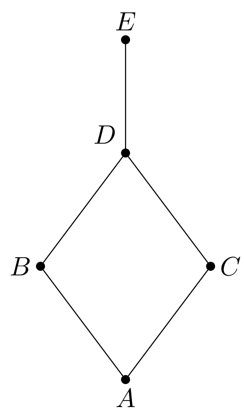



Figure 3.4: Lattice Job Scheduling Problem

Traversing up the lattice, we can schedule the jobs in the following way:

| **Time** | **Processor 1** | **Processor 2** |
|---|---|---|
| 0 | $A$ | $\varnothing$ |
| 1 | $B$ | $C$ |
| 2 | $D$ | $\varnothing$ |
| 3 | $E$ | $\varnothing$ |

Thus, this version of the job scheduling problem takes 3 units of time. Contact Abhay Upadhyay to solve this for a general case.

## 3.2 Functions

### 3.2.1 Definition

A function $f$ from a set $A$ to a set $B$ is an assignment of exactly one element of $B$ to each element of $A$. We denote this as,

$$f : \underset{\text{Domain}\uparrow}{A} \to \underset{\uparrow\text{Co-domain}}{B}$$

$f(a) = b$, if $b$ is the unique element in $B$ assigned by the function $f$ to the element $a$ of $A$. We denote this as,

$$\underset{\text{Preimage}\uparrow}{a} \mapsto \underset{\uparrow\text{Image}}{b}$$

A function is also called a *mapping* from the domain to the codomain.

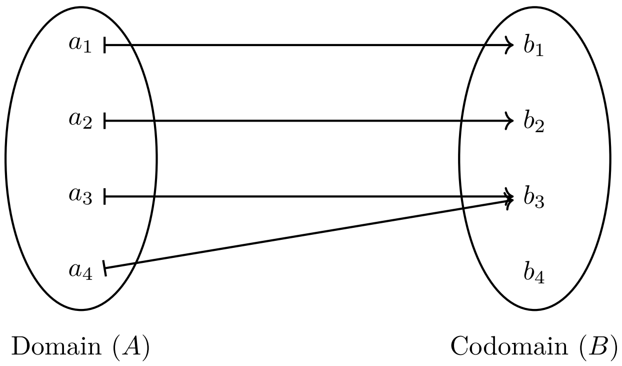



Figure 3.5: Function as a mapping

**Range**

The range of a function $f$ is defined as the set of all images mapped by the function.

If $f : A \to B$, then the range of $f$ is $f(A) \coloneqq \{f(a) \,|\, a \in A\}$.

**Q.6.** $f : P \to C$ where $P \coloneqq \{\text{Linda}, \text{Max}, \text{Hathy}, \text{Peter}\}$ and $C \coloneqq \{\text{Boston}, \text{New York}, \text{Hong Kong}, \text{Moscow}\}$.

$$\begin{aligned} f(\text{Linda}) &\coloneqq \text{Moscow} \\ f(\text{Max}) &\coloneqq \text{Boston} \\ f(\text{Kathy}) &\coloneqq \text{Hong Kong} \\ f(\text{Peter}) &\coloneqq \text{Boston} \end{aligned}$$

Find the range of $f$.

The range of $f$ is the set of images for all preimages in the domain. It is equal to: $\boxed{\{\text{Moscow}, \text{Boston}, \text{Hong Kong}\}}$. **(Ans.)**

### 3.2.2 Properties of Functions

#### Injectivity

A function is said to be *one-one* or *injective* if every image in the range corresponds to a unique image in the domain.

$$\forall x \in A\, \forall y \in A\, (f(x) = f(y) \implies x = y) \tag{3.15}$$

#### Surjectivity

A function is said to be *onto* or *surjective* if every element in the codomain has a corresponding image in the domain. In other words, the codomain equals the range.

$$\forall y \in B\ \exists x \in A : f(x) = y \tag{3.16}$$

#### Monotonicity

A function $f$ is said to be *monotonically increasing* if greater elements in the domain correspond to greater elements in the range. It is denoted as $f\uparrow$.

$$f\uparrow \iff \forall x_1 \in A\, \forall x_2 \in A\, (x_1 > x_2 \implies f(x_1) > f(x_2)) \tag{3.17}$$

A function $f$ is said to be *monotonically decreasing* if greater elements in the domain correspond to lesser elements in the range. It is denoted as $f\downarrow$.

$$f\downarrow \iff \forall x_1 \in A\, \forall x_2 \in A\, (x_1 > x_2 \implies f(x_1) < f(x_2)) \tag{3.18}$$

#### Bijections

A function that is injective as well as surjective is said to be *bijective*. Such a mapping is called a *bijection*.

If $f$ is a bijection from $A$ to $B$ and $A$ and $B$ are finite, then $|A| = |B|$.

### 3.2.3 Function Operations

#### Addition

The sum of two functions is defined as the sum of the corresponding images for each element in the domain.

$$(f+g)(x) = f(x) + g(x)$$

#### Multiplication

The product of two functions is defined as the product of the corresponding images for each element in the domain.

$$(fg)(x) = f(x)g(x)$$

#### Composition

Consider $g : A \to B$ and $f : B \to C$.

The composition $f \circ g$ is defined as follows:

$$f \circ g : A \to C,\ (f \circ g)(x) = f(g(x))$$

### 3.2.4 Identity Function

The identity function $i(x)$ is defined as the input to the function itself.

$$i(x) \coloneqq x \tag{3.19}$$

### 3.2.5 Inverse Functions

If $f : A \to B$, then $f^{-1} : B \to A$ and $f(a) = b \iff f^{-1}(b) = a$. A function is said to be *invertible* iff it is a bijection. Therefore, $f$ is also an inverse for the function $f^{-1}$.

The composition of a function and its inverse always produce the identity function.

$$\left(f \circ f^{-1}\right)(x) = \left(f^{-1} \circ f\right)(x) = i(x)$$

---

# Appendix A

# Assignments

## A.1 Assignment 1

**1.** Let $P(m,n)$ be the statement "$m$ divides $n$", where the domain for both variables consists of all positive integers. Determine the truth values of each of these statements.

**(a)** $\forall m\ \forall n\, P(m,n)$

**(b)** $\exists m\ \forall n\, P(m,n)$

**(c)** $\exists n\ \forall m\, P(m,n)$

**(d)** $\forall n\, P(1,n)$

**2.** Let $p$, $q$ and $r$ be the propositions

$$\begin{aligned} p &: \text{Ghruank has been seen in the area.}\\ q &: \text{Hiking is safe on the trail.}\\ r &: \text{Onions are ripe along the trail.} \end{aligned}$$

Write these propositions using $p$, $q$ and $r$ and logical connectives.

**(a)** It is not safe to hike on the trail, but Ghruank has not been seen in the area and the onions along the trail are ripe.

**(b)** For hiking on the trail to be safe, it is necessary but not sufficient that onions not be ripe along the trail and for Ghruank to not have been seen in the area.

**(c)** Hiking is not safe on the trail whenever Ghruank has been seen in the area and onions are ripe along the trail.

**3.** Let $\mathbb{E}$ denote the set of even integers and $\mathbb{O}$ denote the set of odd integers. As usual, let $\mathbb{Z}$ denote the set of all integers. Determine each of these sets.

**(a)** $\mathbb{E} \cup \mathbb{O}$

**(b)** $\mathbb{E} \cap \mathbb{O}$

**(c)** $\mathbb{Z} \setminus \mathbb{E}$

**(d)** $\mathbb{Z} \setminus \mathbb{O}$

4. Let $A = \{a, b\}$. Let $A^+$ be the successor of set $A$ defined as $A \cup \{A\}$ and $\mathcal{P}(A)$ be the power set of $A$.

   Determine the following sets:

   **(a)** $\{A^+\} \setminus \{A\}$

   **(b)** $\mathcal{P}(A) \cap A^+$

   **(c)** $\{A\} \cap \mathcal{P}(A^+)$

   **(d)** $\mathcal{P}(A^+) \setminus \{A\}$

5. Let $A$, $B$ and $C$ be sets. Show that $(A \setminus B) \setminus C$ is not necessarily equal to $A \setminus (B \setminus C)$.

6. Let $A$ and $B$ be subsets of the finite universal set $U$. Show that $|\overline{A} \cap \overline{B}| - |A \cap B| = |U| - |A| - |B|$.

7. Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$ if for each integer $i$,

   **(a)** $A_i = (0, i)$

   **(b)** $A_i = \{-i, i\}$

   **(c)** $A_i = [-i, i]$

   **(d)** $A_i = [i, \infty)$

   Here $(a, b)$, $[a, b]$ and $[a, b)$ represent interval notation for real numbers.

8. Inductively prove the generalization of De Morgan's laws:

$$\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j}$$

9. Use mathematical induction to show that $(\cos x + i \sin x)^n = \cos nx + i \sin nx$ whenever $n$ is a positive integer. (Here $i$ is the square root of $-1$.)

10. Let $P(n)$ be the statement that

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n},$$

   where $n$ is an integer greater than 1. Show that $\forall n \, P(n)$.

11. Justify why $f$ is not a function from $\mathbb{R}$ to $\mathbb{R}$ if

   **(a)** $f(x) = 1/x$.

   **(b)** $f(x) = \sqrt{x}$.

   **(c)** $f(x) = \pm\sqrt{x^2 + 1}$.

12. Determine whether the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is surjective if

   **(a)** $f(m, n) = m^2 + n^2$.

   **(b)** $f(m, n) = m$.

   **(c)** $f(m, n) = |n|$.

   **(d)** $f(m, n) = m - n$.

13. Let $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2 + 2x + 2$, $g : \mathbb{Z} \to \mathbb{Z}$ and $g(x) = x - 1$.

Find out the following functions:

**(a)** $f \circ f$

**(b)** $g \circ g$

**(c)** $g \circ f$

**(d)** $f \circ g$

**14.** Let $f(x) = 2x$ where the domain is the set of real numbers. What is

**(a)** $f(\mathbb{Z})$?

**(b)** $f(\mathbb{N})$?

**(c)** $f(\mathbb{R})$?

**15.** Suppose that $a$ and $b$ are odd integers with $a \neq b$. Show that there is a unique integer $c$ such that $|a - c| = |b - c|$.

**16.** Prove that there is no positive integer $n$ such that $n^2 + n^3 = 100$.

**17.** Show that if $n$ is an integer, then $n = \lceil n/2 \rceil + \lfloor n/2 \rfloor$.

**18.** Show that $n$ lines separate the plane into $\left(n^2 + n + 2\right)/2$ regions if no two of these lines are parallel and no three pass through a common point.

**19.** Suppose that five ones and four zeros are arranged around a circle.

**(a)** Find the total number of such arrangements.

**(b)** Suppose between any two equal bits you insert a 0 and between any two unequal bits you insert a 1 to produce nine new bits. Then you erase the nine original bits. Show that when you iterate this procedure, you can never get nine zeros.

**20.** Darsh writes the numbers $1, 2, \ldots, 2n$ on a blackboard, where $n$ is an odd integer. He picks any two of the numbers, $j$ and $k$, writes $|j - k|$ on the board and erases $j$ and $k$. He continues this process until only one integer is left on the board. Prove that this integer will be odd.

---

## A.2 Assignment 2

**1.** Which of these relations on the set of all functions from $\mathbb{Z}$ to $\mathbb{Z}$ are equivalence relations? Determine the properties of an equivalence relation that the others lack.

**(a)** $\{(f, g) \mid f(1) = g(1)\}$

**(b)** $\{(f, g) \mid f(0) = g(0) \text{ or } f(1) = g(1)\}$

**(c)** $\{(f, g) \mid \text{for some } C \in \mathbb{Z}, \text{ for all } x \in \mathbb{Z}, f(x) - g(x) = C\}$

**(d)** $\{(f, g) \mid f(0) = g(1) \text{ and } f(1) = g(0)\}$

**2.** **(a)** Let $n$ be a positive integer. Show that the relation $R$ on the set of all polynomials with real-valued coefficients consisting of all pairs $(f, g)$ such that $f^{(n)}(x) = g^{(n)}(x)$ is an equivalence relation. [Here $f^{(n)}(x)$ is the $n^{th}$ derivative of $f(x)$.]

**(b)** Which functions are in the same equivalence class as the function $f(x) = x^4$, where $n = 3$?

**3.** A relation $R$ is called *circular* if $aRb$ and $bRc$ imply that $cRa$. Show that $R$ is reflexive and circular if and only if it is an equivalence relation.

**4.** Which of these are partitions of the set of real numbers?

**(a)** the the negative real numbers, $\{0\}$, the positive real numbers

**(b)** the set of irrational numbers, the set of rational numbers

**(c)** the set of intervals $[k, k + 1]$, $k = \ldots, -2, -1, 0, 1, 2, \ldots$

**(d)** the set of intervals $(k, k + 1)$, $k = \ldots, -2, -1, 0, 1, 2, \ldots$

**(e)** the set of intervals $(k, k + 1]$, $k = \ldots, -2, -1, 0, 1, 2, \ldots$

**5.** List the ordered pairs in the equivalence relations produced by these partitions of $\{0, 1, 2, 3, 4, 5\}$.

**(a)** $\{0\}$, $\{1, 2\}$, $\{3, 4, 5\}$

**(b)** $\{0, 1\}$, $\{2, 3\}$, $\{4, 5\}$

**(c)** $\{0, 1, 2\}$, $\{3, 4, 5\}$

**(d)** $\{0\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{5\}$

**6.** Let $R$ be a binary relation from $A$ to $B$.

**(a)** If $R$ is reflexive, is $R^{-1}$ necessarily reflexive?

**(b)** If $R$ is symmetric, is $R^{-1}$ necessarily symmetric?

**(c)** If $R$ is transitive, is $R^{-1}$ necessarily transitive?

**7.** Let $R$ be the relation represented by the matrix

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

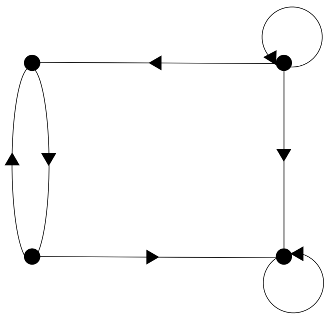
Find the matrix representing

**(a)** $R^{-1}$.

**(b)** $\overline{R}$.

**(c)** $R^2$.

**8.** Draw the digraph of the transitive closure of the relation represented by the following digraph.



**9.** Which of these are posets?

**(a)** $(\mathbb{Z}, =)$

**(b)** $(\mathbb{Z}, \neq)$

**(c)** $(\mathbb{Z}, \geq)$

**(d)** $(\mathbb{Z}, \nmid)$

**10.** Answer these questions for the poset $(\{2, 4, 6, 9, 12, 18, 27, 36, 48, 54, 60, 72\}, |)$.

**(a)** Find the maximal elements.

**(b)** Find the minimal elements.

**(c)** Is there a greatest element?

**(d)** Is there a least element?

**(e)** Find all the upper bounds of $\{2, 9\}$.

**(f)** Find the least upper bound of $\{2, 9\}$, if it exists.

**(g)** Find all lower bounds of $\{60, 72\}$.

**(h)** Find the greatest lower bound of $\{60, 72\}$, if it exists.

**11.** A fortune cookie company makes 213 different fortunes. Aditya eats at a restaurant that uses fortunes from this company. What is the largest possible number of times that he can eat at the restaurant without getting the same fortune six times?

**12.** Suppose I study for 7 days, and during each day, the number of hours spent studying ranges from 1 hour to 5 hours. The total study hours over the 7 days is 21 hours. I study for 4 hours on the first day and only 2 hours on the last day. Show that there must be at least one period of two consecutive days during which I study at least 7 hours.

**13.** Four students of FY IT are playing with a standard deck of 52 cards in the VJTI quadrangle during lecture. How many ways are there to distribute hands of five cards to each of the four players?

**14.** How many different combinations of pennies, nickels, dimes, quarters and half dollars can a piggy bank contain if it has 20 coins in it?

**15.** Once a computer worm infects a personal computer via an infected e-mail message, it sends a copy of itself to 100 e-mail addresses it finds in the electronic message mailbox on this personal computer. What is the maximum number of different computers this one computer can infect in the time it takes for the infected message to be forwarded five times?

**16.** How many ways are there to travel in $xyzw$ space from the origin $(0, 0, 0, 0)$ to the point $(4, 3, 5, 4)$ by taking steps one unit in the positive $x$, positive $y$, positive $z$, or positive $w$ direction?

**17.** Suppose that $S$ is a set with cardinality $n$. How many ordered pairs $(A, B)$ are there such that $A$ and $B$ are subsets of $S$ with $A \subseteq B$?

**18.** What is the probability of these events when we randomly select a permutation of $\{1, 2, \ldots, n\}$ where $n \geq 4$?

**(a)** 1 precedes 2.

**(b)** 1 immediately precedes 2.

**(c)** $n$ precedes 1 and $n - 1$ precedes 2.

**(d)** $n$ precedes 1 and $n$ precedes 2.

**19.** In poker,

- a **flush** is a hand of five cards of the same suit.
- a **straight** is a hand of five cards of consecutive[1] kinds.

What is the probability that a five-card poker hand contains

**(a)** a straight?

**(b)** a flush?

**(c)** a straight flush?

**(d)** neither a flush nor a straight?

**(e)** a royal[2] flush?

[1] An ace can be considered either the lowest card of an A-2-3-4-5 straight or the highest card of a 10-J-Q-K-A straight.

[2] 10, jack, queen, king, ace of one suit.

**20.** A player in the Mega Millions lottery picks five different integers between 1 and 56, inclusive, and a sixth integer between 1 and 46, which may duplicate one of the earlier five integers. The player wins the jackpot if the first five numbers picked match the first five numbers drawn and the sixth number matches the sixth number drawn.

**(a)** What is the probability that a player wins the jackpot?

**(b)** What is the probability that a player wins \$250,000, which is the prize for matching the first five numbers, but not the sixth number, drawn?

**(c)** What is the probability that a player wins \$150 by matching exactly three of the first five numbers and the sixth number or by matching four of the first five numbers but not the sixth number?

**(d)** What is the probability that a player wins a prize, if a prize is given when the player matches at least three of the first five numbers or the last number?

---

# Acronyms

**digraph** directed graph 33–35

**DS** Discrete Structures 1

**Jojo** Aaditya Joil 1

**poset** Partially-ordered set 35–38

**RRG** Rupak R. Gupta 1

$$\boxed{\begin{bmatrix} \mathbb{R} & \mathfrak{R} \\ \mathcal{g} & \infty \end{bmatrix} \begin{pmatrix} 0 \\ \mathbb{j} \end{pmatrix}^2}$$

The End.