

Diploma

**Mathematical Foundation For
Cyber Security**

ITBS 102

**Basic Structures:
Sets, and Matrices**

Unit 1

Objectives



Dear student, at the end of this unit you are expected to be able to:

- Definition of sets
- Describing Sets
- Explain Set Operations
- Determine Matrix Arithmetic
- Distinguish between Some Important Sets in Mathematics

Content

Introduction

Sets

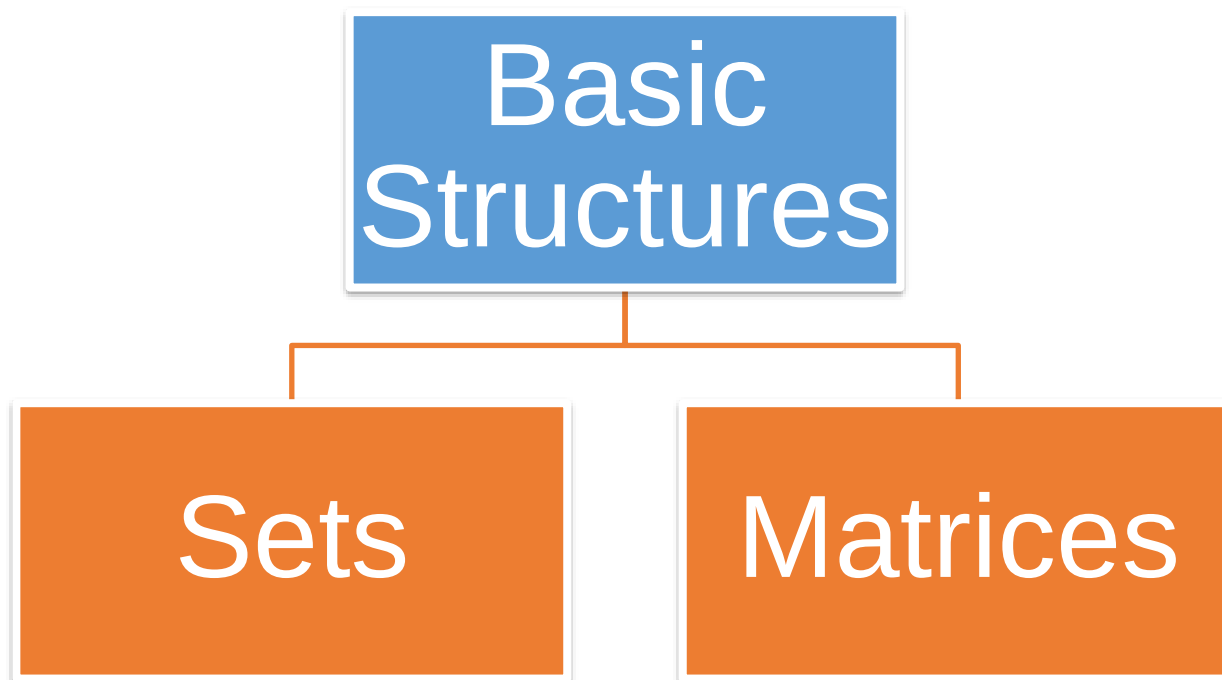
Set Operations

Matrices

Conclusion

Resources

Mind Map



Chapter Summary

- Sets
 - The Language of Sets
 - Set Operations
 - Set Identities
- Matrices
 - Matrix Arithmetic

Activity

1- whether $\{1, 3, 5, 7, 9, \dots, 599\}$ is finite or infinite set.

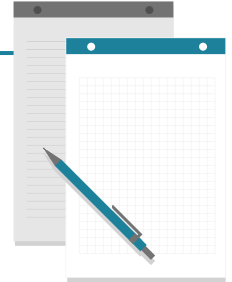
*A. Finite

B. Infinite

2- The sets $\{1,3,5\}$ and $\{3,5,1\}$ are equal.

*A. True

B. False



Section 1.1: Sets

Section Summary

- Definition of sets
- Describing Sets
 - Roster Method
 - Set-Builder Notation
- Some Important Sets in Mathematics
- Empty Set and Universal Set
- Subsets and Set Equality
- Cardinality of Sets
- Tuples
- Cartesian Product

Introduction

- Sets are one of the basic building blocks for the types of objects considered in discrete mathematics.
 - Important for counting.
 - Programming languages have set operations.
- Set theory is an important branch of mathematics.
 - Many different systems of axioms have been used to develop set theory.
 - Here we are not concerned with a formal set of axioms for set theory. Instead, we will use what is called naïve set theory.

Sets

- A *set* is an unordered collection of objects.
 - the students in this class
 - the chairs in this room
- The objects in a set are called the *elements*, or *members* of the set. A set is said to *contain* its elements.
- The notation $a \in A$ denotes that a is an element of the set A .
- If a is not a member of A , write $a \notin A$

Describing a Set: Roster Method

- $S = \{a, b, c, d\}$
- Order not important

$$S = \{a, b, c, d\} = \{b, c, a, d\}$$

- Each distinct object is either a member or not; listing more than once does not change the set.

$$S = \{a, b, c, d\} = \{a, b, c, b, c, d\}$$

- Ellipses (...) may be used to describe a set without listing all of the members when the pattern is clear.

$$S = \{a, b, c, d, \dots, z\}$$

Roster Method

- Set of all vowels in the English alphabet:
 $V = \{a, e, i, o, u\}$
- Set of all odd positive integers less than 10:
 $O = \{1, 3, 5, 7, 9\}$
- Set of all positive integers less than 100:
 $S = \{1, 2, 3, \dots, 99\}$
- Set of all integers less than 0:
 $S = \{\dots, -3, -2, -1\}$

Some Important Sets

$\mathbf{N}$ = *natural numbers* = $\{0,1,2,3,\dots\}$

$\mathbf{Z}$ = *integers* = $\{\dots,-3,-2,-1,0,1,2,3,\dots\}$

$\mathbf{Z}^+$ = *positive integers* = $\{1,2,3,\dots\}$

$\mathbf{R}$ = *set of real numbers*

$\mathbf{R}^+$ = *set of positive real numbers*

$\mathbf{C}$ = *set of complex numbers.*

$\mathbf{Q}$ = *set of rational numbers*

Set-Builder Notation

- Specify the property or properties that all members must satisfy:

$$S = \{x \mid x \text{ is a positive integer less than } 100\}$$

$$O = \{x \mid x \text{ is an odd positive integer less than } 10\}$$

$$O = \{x \in \mathbf{Z}^+ \mid x \text{ is odd and } x < 10\}$$

- A predicate may be used:

$$S = \{x \mid P(x)\}$$

- Example: $S = \{x \mid \text{Prime}(x)\}$

- Positive rational numbers:

$$\mathbf{Q}^+ = \{x \in \mathbf{R} \mid x = p/q, \text{ for some positive integers } p, q\}$$

Interval Notation

$$[a,b] = \{x \mid a \leq x \leq b\}$$

$$[a,b) = \{x \mid a \leq x < b\}$$

$$(a,b] = \{x \mid a < x \leq b\}$$

$$(a,b) = \{x \mid a < x < b\}$$

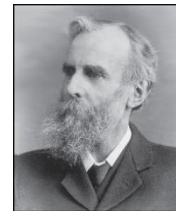
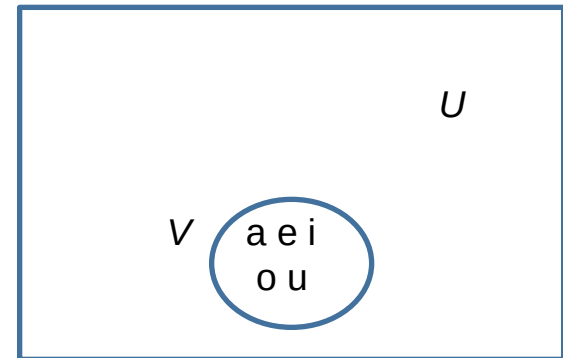
closed interval $[a,b]$

open interval (a,b)

Universal Set and
Empty Set

- The *universal set* U is the set containing everything currently under consideration.
 - Sometimes implicit
 - Sometimes explicitly stated.
 - Contents depend on the context.
- The empty set is the set with no elements. Symbolized $\emptyset$, but $\{\}$ also used.

Venn Diagram

John Venn (1834-1923)
Cambridge, UK

Introduction

Russell's Paradox

- Let S be the set of all sets which are not members of themselves. A paradox results from trying to answer the question “Is S a member of itself?”
- Related Paradox:
 - Henry is a barber who shaves all people who do not shave themselves. A paradox results from trying to answer the question “Does Henry shave himself?”



Bertrand Russell (1872-1970)
Cambridge, UK
Nobel Prize Winner

Some things to remember

- Sets can be elements of sets.

$$\{\{1,2,3\}, a, \{b,c\}\}$$

$$\{\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}\}$$

- The empty set is different from a set containing the empty set.

$$\emptyset \neq \{ \emptyset \}$$

Set Equality

Definition: Two sets are *equal* if and only if they have the same elements.

- Therefore if A and B are sets, then A and B are equal if and only if $\forall x (x \in A \leftrightarrow x \in B)$
- We write $A = B$ if A and B are equal sets.

$$\{1, 3, 5\} = \{3, 5, 1\}$$

$$\{1, 5, 5, 5, 3, 3, 1\} = \{1, 3, 5\}$$

Subsets

Definition: The set A is a *subset* of B , if and only if every element of A is also an element of B .

- The notation $A \subseteq B$ is used to indicate that A is a subset of the set B .
- $A \subseteq B$ holds if and only if $\forall x(x \in A \rightarrow x \in B)$ is true.
 1. Because $a \in \emptyset$ is always false, $\emptyset \subseteq S$, for every set S .
 2. Because $a \in S \rightarrow a \in S$, $S \subseteq S$, for every set S .

Showing a Set is or is
not a Subset of

- **Showing that A is a Subset of B:** To show that $A \subseteq B$, show that if x belongs to A , then x also belongs to B .
- **Showing that A is not a Subset of B:** To show that A is not a subset of B , $A \not\subseteq B$, find an element $x \in A$ with $x \notin B$. (Such an x is a counterexample to the claim that $x \in A$ implies $x \in B$.)

Examples:

1. The set of all computer science majors at your school is a subset of all students at your school.
2. The set of integers with squares less than 100 is not a subset of the set of nonnegative integers.

Another look at
Equality of Sets

- Recall that two sets A and B are *equal*, denoted by $A = B$, iff

$$\forall x (x \in A \leftrightarrow x \in B)$$

- Using logical equivalences we have that $A = B$ iff

$$\forall x [(x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)]$$

- This is equivalent to

$$A \subseteq B \quad \text{and} \quad B \subseteq A$$

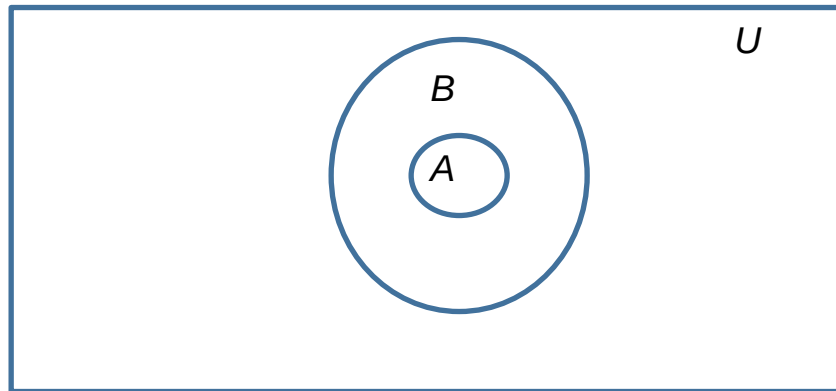
Proper Subsets

Definition: If $A \subseteq B$, but $A \neq B$, then we say A is a *proper subset* of B , denoted by $A \subset B$. If $A \subset B$, then

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A)$$

is true.

Venn Diagram



Set Cardinality

Definition: If there are exactly n distinct elements in S where n is a nonnegative integer, we say that S is *finite*. Otherwise it is *infinite*.

Definition: The *cardinality* of a finite set A , denoted by $|A|$, is the number of (distinct) elements of A .

Examples:

1. $|\emptyset| = 0$
2. Let S be the letters of the English alphabet. Then $|S| = 26$
3. $|\{1,2,3\}| = 3$
4. $|\{\emptyset\}| = 1$
5. The set of integers is infinite.

Power Sets

Definition: The set of all subsets of a set A , denoted $\mathcal{P}(A)$, is called the *power set* of A .

Example: If $A = \{a, b\}$ then

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

- If a set has n elements, then the cardinality of the power set is 2^n .

Tuples

- The *ordered n -tuple* $(a_1, a_2, \dots, a_n)$ is the ordered collection that has a_1 as its first element and a_2 as its second element and so on until a_n as its last element.
- Two n -tuples are equal if and only if their corresponding elements are equal.
- 2-tuples are called *ordered pairs*.
- The ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$.

Cartesian Product

Definition: The *Cartesian Product* of two sets A and B , denoted by $A \times B$ is the set of ordered pairs (a,b) where $a \in A$ and $b \in B$.

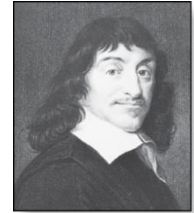
$$A \times B = \{(a,b) | a \in A \wedge b \in B\}$$

Example:

$$A = \{a,b\} \quad B = \{1,2,3\}$$

$$A \times B = \{(a,1),(a,2),(a,3), (b,1),(b,2),(b,3)\}$$

- **Definition:** A subset R of the Cartesian product $A \times B$ is called a *relation* from the set A to the set B .



René Descartes
(1596-1650)

Cartesian Product

Definition: The cartesian products of the sets $A_1, A_2, \dots, A_n$, denoted by $A_1 \times A_2 \times \dots \times A_n$, is the set of ordered n -tuples $(a_1, a_2, \dots, a_n)$ where a_i belongs to A_i for $i = 1, \dots, n$.

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \dots, n\}$$

Example: What is $A \times B \times C$ where $A = \{0,1\}$, $B = \{1,2\}$ and $C = \{0,1,2\}$

Solution: $A \times B \times C = \{(0,1,0), (0,1,1), (0,1,2), (0,2,0), (0,2,1), (0,2,2), (1,1,0), (1,1,1), (1,1,2), (1,2,0), (1,2,1), (1,2,2)\}$

Truth Sets of Quantifiers

- Given a predicate P and a domain D , we define the *truth set* of P to be the set of elements in D for which $P(x)$ is true. The truth set of $P(x)$ is denoted by

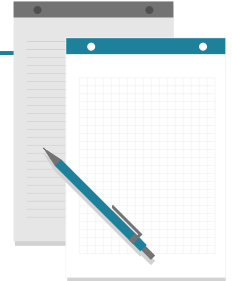
$$\{x \in D \mid P(x)\}$$

- **Example:** The truth set of $P(x)$ where the domain is the integers and $P(x)$ is “ $|x| = 1$ ” is the set $\{-1, 1\}$

Activity

List the members of these sets.

- a) $\{x \mid x \text{ is a real number such that } x^2 = 1\}$
- b) $\{x \mid x \text{ is a positive integer less than } 12\}$
- c) $\{x \mid x \text{ is the square of an integer and } x < 100\}$
- d) $\{x \mid x \text{ is an integer such that } x^2 = 2\}$



Section 1.2: Set Operations

Section Summary

- Set Operations
 - Union
 - Intersection
 - Complementation
 - Difference
- More on Set Cardinality
- Set Identities
- Proving Identities
- Membership Tables

Boolean Algebra

- Propositional calculus and set theory are both instances of an algebraic system called a *Boolean Algebra*. This is discussed in Chapter 6.
- The operators in set theory are analogous to the corresponding operator in propositional calculus.
- As always there must be a universal set U . All sets are assumed to be subsets of U .

Union

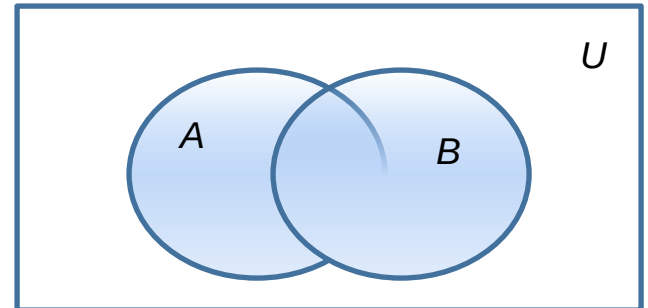
- **Definition:** Let A and B be sets. The *union* of the sets A and B , denoted by $A \cup B$, is the set:

$$\{x \mid x \in A \vee x \in B\}$$

- **Example:** What is $\{1,2,3\} \cup \{3,4,5\}$?

Solution: $\{1,2,3,4,5\}$

Venn Diagram for $A \cup B$



Intersection

- **Definition:** The *intersection* of sets A and B , denoted by $A \cap B$, is

$$\{x | x \in A \wedge x \in B\}$$

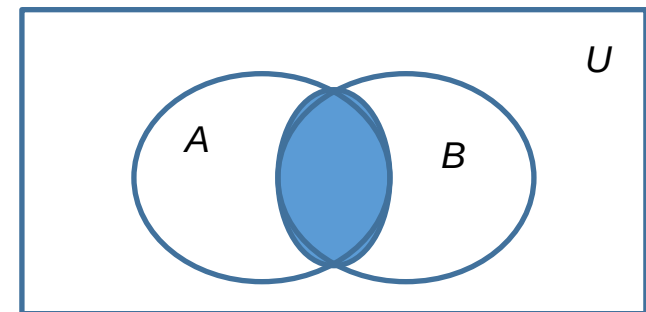
- Note if the intersection is empty, then A and B are said to be *disjoint*.
- **Example:** What is? $\{1,2,3\} \cap \{3,4,5\}$?

Solution: $\{3\}$

- **Example:** What is?
 $\{1,2,3\} \cap \{4,5,6\}$?

Solution: $\emptyset$

Venn Diagram for $A \cap B$



Complement

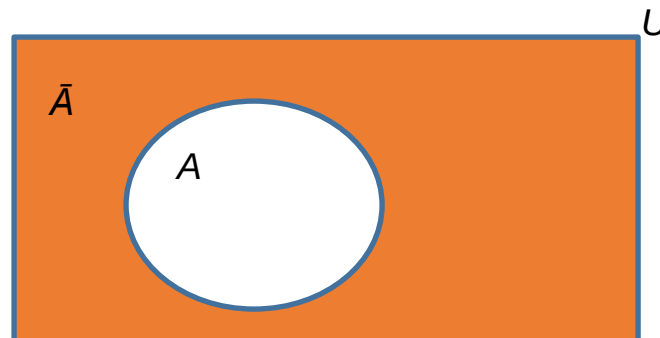
Definition: If A is a set, then the complement of the A (with respect to U), denoted by $\bar{A}$ is the set $U - A$

$$\bar{A} = \{x \in U \mid x \notin A\}$$

(The complement of A is sometimes denoted by A^c .)

Example: If U is the positive integers less than 100, what is the complement of $\{x \mid x > 70\}$

Solution: $\{x \mid x \leq 70\}$

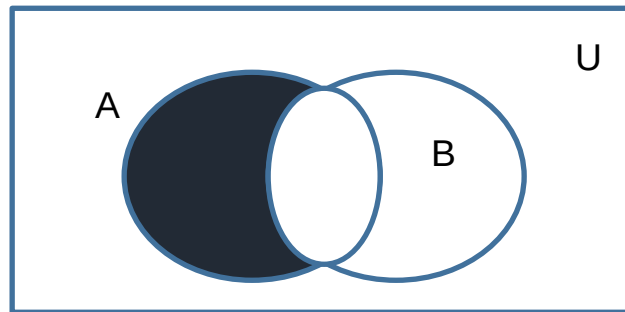


Venn Diagram for Complement

Difference

- **Definition:** Let A and B be sets. The *difference* of A and B , denoted by $A - B$, is the set containing the elements of A that are not in B . The difference of A and B is also called the complement of B with respect to A .

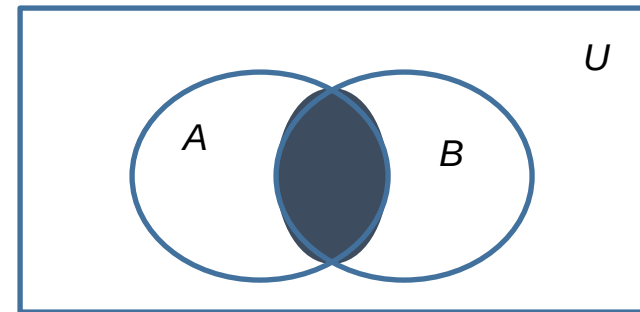
$$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \bar{B}$$

Venn Diagram for $A - B$

The Cardinality of the Union of Two Sets

- Inclusion-Exclusion

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



Venn Diagram for $A, B, A \cap B, A \cup B$

- **Example:** Let A be the math majors in your class and B be the CS majors. To count the number of students who are either math majors or CS majors, add the number of math majors and the number of CS majors, and subtract the number of joint CS/math majors.
- We will return to this principle in Chapter 6 and Chapter 8 where we will derive a formula for the cardinality of the union of n sets, where n is a positive integer.

Review Questions

Example: $U = \{0,1,2,3,4,5,6,7,8,9,10\}$ $A = \{1,2,3,4,5\}$, $B = \{4,5,6,7,8\}$

1. $A \cup B$

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

2. $A \cap B$

Solution: $\{4,5\}$

3. $\bar{A}$

Solution: $\{0,6,7,8,9,10\}$

4.

$\bar{B}$ **Solution:** $\{0,1,2,3,9,10\}$

5. $A - B$

Solution: $\{1,2,3\}$

6. $B - A$

Solution: $\{6,7,8\}$

Symmetric Difference
(optional)

Definition: The *symmetric difference* of **A** and **B**, denoted by $A \oplus B$ is the set

$$(A - B) \cup (B - A)$$

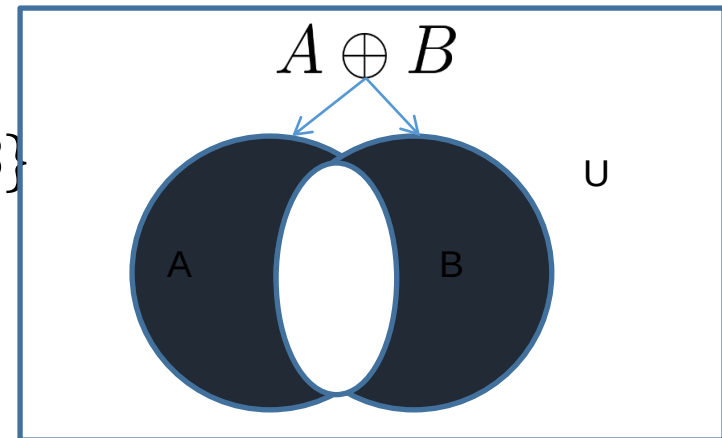
Example:

$$U = \{0,1,2,3,4,5,6,7,8,9,10\}$$

$$A = \{1,2,3,4,5\} \quad B = \{4,5,6,7,8\}$$

What is $A \oplus B$:

- **Solution:** $\{1,2,3,6,7,8\}$



Venn Diagram

Set Identities

- Identity laws

$$A \cup \emptyset = A \quad A \cap U = A$$

- Domination laws

$$A \cup U = U \quad A \cap \emptyset = \emptyset$$

- Idempotent laws

$$A \cup A = A \quad A \cap A = A$$

- Complementation law

$$\overline{(\overline{A})} = A$$

Continued on next slide →

Set Identities

- Commutative laws

$$A \cup B = B \cup A \quad A \cap B = B \cap A$$

- Associative laws

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

- Distributive laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Continued on next slide →

Set Identities

- De Morgan's laws

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$$

- Absorption laws

$$A \cup (A \cap B) = A \quad A \cap (A \cup B) = A$$

- Complement laws

$$A \cup \overline{A} = U \quad A \cap \overline{A} = \emptyset$$

Proving Set Identities

- Different ways to prove set identities:
 1. Prove that each set (side of the identity) is a subset of the other.
 2. Use set builder notation and propositional logic.
 3. Membership Tables: Verify that elements in the same combination of sets always either belong or do not belong to the same side of the identity. Use 1 to indicate it is in the set and a 0 to indicate that it is not.

Proof of Second De
Morgan Law

Example: Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Solution: We prove this identity by showing that:

$$1) \overline{A \cap B} \subseteq \overline{A} \cup \overline{B} \quad \text{and}$$

$$2) \overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$$

Continued on next slide →

Proof of Second De Morgan Law

These steps show that: $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$

$$x \in \overline{A \cap B}$$

by assumption

$$x \notin A \cap B$$

defn. of complement

$$\neg((x \in A) \wedge (x \in B))$$

defn. of intersection

$$\neg(x \in A) \vee \neg(x \in B)$$

1st De Morgan Law for Prop Logic

$$x \notin A \vee x \notin B$$

defn. of negation

$$x \in \overline{A} \vee x \in \overline{B}$$

defn. of complement

$$x \in \overline{A} \cup \overline{B}$$

defn. of union

Continued on next slide →

Proof of Second De Morgan Law

These steps show that: $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$

$$x \in \overline{A \cap B}$$

by assumption

$$(x \in \overline{A}) \vee (x \in \overline{B})$$

defn. of union

$$(x \notin A) \vee (x \notin B)$$

defn. of complement

$$\neg(x \in A) \vee \neg(x \in B)$$

defn. of negation

$$\neg((x \in A) \wedge (x \in B))$$

by 1st De Morgan Law for Prop Logic

$$\neg(x \in A \cap B)$$

defn. of intersection

$$x \in \overline{A \cap B}$$

defn. of complement

Set-Builder Notation:
Second De Morgan Law

$$\begin{aligned}\overline{A \cap B} &= \{x | x \notin A \cap B\} && \text{by defn. of complement} \\ &= \{x | \neg(x \in (A \cap B))\} && \text{by defn. of does not belong symbol} \\ &= \{x | \neg(x \in A \wedge x \in B)\} && \text{by defn. of intersection} \\ &= \{x | \neg(x \in A) \vee \neg(x \in B)\} && \text{by 1st De Morgan law} \\ &&& \text{for Prop Logic} \\ &= \{x | x \notin A \vee x \notin B\} && \text{by defn. of not belong symbol} \\ &= \{x | x \in \overline{A} \vee x \in \overline{B}\} && \text{by defn. of complement} \\ &= \{x | x \in \overline{A} \cup \overline{B}\} && \text{by defn. of union} \\ &= \overline{A} \cup \overline{B} && \text{by meaning of notation}\end{aligned}$$

Membership Table

Example: Construct a membership table to show that the distributive law holds.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Solution:

A	B	C	$B \cap C$	$A \cup (B \cap C)$	$A \cup B$	$A \cup C$	$(A \cup B) \cap (A \cup C)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

Generalized Unions and Intersections

- Let $A_1, A_2, \dots, A_n$ be an indexed collection of sets.

We define:

$$\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup \dots \cup A_n$$

$$\bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap \dots \cap A_n$$

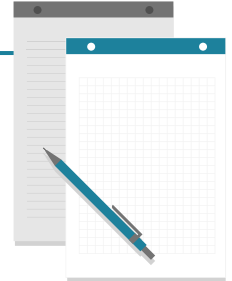
These are well defined, since union and intersection are associative.

- For $i = 1, 2, \dots$, let $A_i = \{i, i + 1, i + 2, \dots\}$. Then,

$$\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n \{i, i + 1, i + 2, \dots\} = \{1, 2, 3, \dots\}$$

$$\bigcap_{i=1}^n A_i = \bigcap_{i=1}^n \{i, i + 1, i + 2, \dots\} = \{n, n + 1, n + 2, \dots\} = A_n$$

Activity



Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{0, 3, 6\}$. Find

a) $A \cup B$.

b) $A \cap B$.

c) $A - B$.

d) $B - A$.

Section 1.3: Matrices

Section Summary

- Definition of a Matrix
- Matrix Arithmetic
- Transposes and Powers of Arithmetic
- Zero-One matrices

Matrices

- Matrices are useful discrete structures that can be used in many ways. For example, they are used to:
 - describe certain types of functions known as linear transformations.
 - Express which vertices of a graph are connected by edges (see Chapter 10).
- In later chapters, we will see matrices used to build models of:
 - Transportation systems.
 - Communication networks.
- Algorithms based on matrix models will be presented in later chapters.
- Here we cover the aspect of matrix arithmetic that will be needed later.

Matrix

Definition: A *matrix* is a rectangular array of numbers. A matrix with m rows and n columns is called an $m \times n$ matrix.

- The plural of matrix is *matrices*.
- A matrix with the same number of rows as columns is called *square*.
- Two matrices are *equal* if they have the same number of rows and the same number of columns and the corresponding entries in every position are equal.

3×2 matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$$

Notation

- Let m and n be positive integers and let

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

- The i th row of $\mathbf{A}$ is the $1 \times n$ matrix $[a_{i1}, a_{i2}, \dots, a_{in}]$. The j th column of $\mathbf{A}$ is the $m \times 1$ matrix:

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \cdot \\ \cdot \\ a_{mj} \end{bmatrix}$$

- The (i,j) th *element* or *entry* of $\mathbf{A}$ is the element a_{ij} . We can use $\mathbf{A} = [a_{ij}]$ to denote the matrix with its (i,j) th element equal to a_{ij} .

Matrix Arithmetic:
Addition

Defintion: Let $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ be $m \times n$ matrices. The sum of $\mathbf{A}$ and $\mathbf{B}$, denoted by $\mathbf{A} + \mathbf{B}$, is the $m \times n$ matrix that has $a_{ij} + b_{ij}$ as its (i,j) th element. In other words, $\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}]$.

Example:

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}$$

Note that matrices of different sizes can not be added.

Matrix Multiplication

Definition: Let $\mathbf{A}$ be an $m \times k$ matrix and $\mathbf{B}$ be a $k \times n$ matrix. The *product* of $\mathbf{A}$ and $\mathbf{B}$, denoted by $\mathbf{AB}$, is the $m \times n$ matrix that has its (i,j) th element equal to the sum of the products of the corresponding elements from the i th row of $\mathbf{A}$ and the j th column of $\mathbf{B}$. In other words, if $\mathbf{AB} = [c_{ij}]$ then $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj}$.

Example:

$$\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{bmatrix}$$

The product of two matrices is undefined when the number of columns in the first matrix is not the same as the number of rows in the second.

Illustration of Matrix Multiplication

- The Product of $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \textcolor{red}{a_{i1}} & \textcolor{red}{a_{i2}} & \dots & \textcolor{red}{a_{ik}} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{m1} & a_{m2} & \dots & a_{mk} \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} b_{11} & b_{12} & \dots & \textcolor{red}{b_{1j}} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & \textcolor{red}{b_{2j}} & \dots & b_{2n} \\ \cdot & \cdot & & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & & \cdot \\ b_{k1} & b_{k2} & \dots & \textcolor{red}{b_{kj}} & \dots & b_{kn} \end{bmatrix}$$

$$\mathbf{AB} = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \textcolor{red}{c_{ij}} & \cdot \\ \cdot & \cdot & & \cdot \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{bmatrix}$$

$$\textcolor{red}{c_{ij}} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj}$$

Matrix Multiplication is
not Commutative

Example: Let

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$$

$$\mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Does $\mathbf{AB} = \mathbf{BA}$?

Solution:

$$\mathbf{AB} = \begin{bmatrix} 2 & 2 \\ 5 & 3 \end{bmatrix}$$

$$\mathbf{BA} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$$

$$\mathbf{AB} \neq \mathbf{BA}$$

Identity Matrix and
Powers of Matrices

Definition: The *identity matrix of order n* is the $m \times n$ matrix $\mathbf{I}_n = [\delta_{ij}]$, where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$.

$$\mathbf{I}_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$\mathbf{A}\mathbf{I}_n = \mathbf{I}_m\mathbf{A} = \mathbf{A}$$

when $\mathbf{A}$ is an $m \times n$ matrix

Powers of square matrices can be defined. When $\mathbf{A}$ is an $n \times n$ matrix, we have:

$$\mathbf{A}^0 = \mathbf{I}_n \quad \mathbf{A}^r = \underbrace{\mathbf{A}\mathbf{A}\mathbf{A}\cdots\mathbf{A}}_{r \text{ times}}$$

Transposes of Matrices

Definition: Let $\mathbf{A} = [a_{ij}]$ be an $m \times n$ matrix. The *transpose* of $\mathbf{A}$, denoted by $\mathbf{A}^t$, is the $n \times m$ matrix obtained by interchanging the rows and columns of $\mathbf{A}$.

If $\mathbf{A}^t = [b_{ij}]$, then $b_{ij} = a_{ji}$ for $i = 1, 2, \dots, n$
and $j = 1, 2, \dots, m$.

The transpose of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ is the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$.

Transposes of Matrices

Definition: A square matrix $\mathbf{A}$ is called symmetric if $\mathbf{A} = \mathbf{A}^t$. Thus $\mathbf{A} = [a_{ij}]$ is symmetric if $a_{ij} = a_{ji}$ for i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$.

The matrix $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ is square.

Square matrices do not change when their rows and columns are interchanged.

Zero-One Matrices

Definition: A matrix all of whose entries are either 0 or 1 is called a *zero-one matrix*.

Algorithms operating on discrete structures represented by zero-one matrices are based on Boolean arithmetic defined by the following Boolean operations:

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{if } b_1 = b_2 = 1 \\ 0 & \text{otherwise} \end{cases} \quad b_1 \vee b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

Zero-One Matrices

Definition: Let $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ be an $m \times n$ zero-one matrices.

- The *join* of $\mathbf{A}$ and $\mathbf{B}$ is the zero-one matrix with (i,j) th entry $a_{ij} \vee b_{ij}$. The *join* of $\mathbf{A}$ and $\mathbf{B}$ is denoted by $\mathbf{A} \vee \mathbf{B}$.
- The *meet* of $\mathbf{A}$ and $\mathbf{B}$ is the zero-one matrix with (i,j) th entry $a_{ij} \wedge b_{ij}$. The *meet* of $\mathbf{A}$ and $\mathbf{B}$ is denoted by $\mathbf{A} \wedge \mathbf{B}$.

Joins and Meets of Zero-One Matrices

Example: Find the join and meet of the zero-one matrices

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Solution: The join of **A** and **B** is

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The meet of **A** and **B** is

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Boolean Product of Zero-One Matrices

Definition: Let $\mathbf{A} = [a_{ij}]$ be an $m \times k$ zero-one matrix and $\mathbf{B} = [b_{ij}]$ be a $k \times n$ zero-one matrix. The *Boolean product* of $\mathbf{A}$ and $\mathbf{B}$, denoted by $\mathbf{A} \odot \mathbf{B}$, is the $m \times n$ zero-one matrix with (i,j) th entry

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \dots \vee (a_{ik} \wedge b_{kj}).$$

Example: Find the Boolean product of $\mathbf{A}$ and $\mathbf{B}$, where

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix},$$

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

Continued on next slide $\rightarrow$

Boolean Product of Zero-One Matrices

Solution: The Boolean product $\mathbf{A} \odot \mathbf{B}$ is given by

$$\begin{aligned}\mathbf{A} \odot \mathbf{B} &= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix} \\ &= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.\end{aligned}$$

Boolean Powers of Zero-One Matrices

Definition: Let $\mathbf{A}$ be a square zero-one matrix and let r be a positive integer. The r th Boolean power of $\mathbf{A}$ is the Boolean product of r factors of $\mathbf{A}$, denoted by $\mathbf{A}^{[r]}$. Hence,

$$\mathbf{A}^{[r]} = \underbrace{\mathbf{A} \odot \mathbf{A} \odot \dots \odot \mathbf{A}}_{r \text{ times}}.$$

We define $\mathbf{A}^{[r]}$ to be $\mathbf{I}_n$.

(The Boolean product is well defined because the Boolean product of matrices is associative.)

Boolean Powers of Zero-One Matrices

Example: Let $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$.

Find A^n for all positive integers n .

Solution:

$$A^{[2]} = A \odot A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad A^{[3]} = A^{[2]} \odot A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

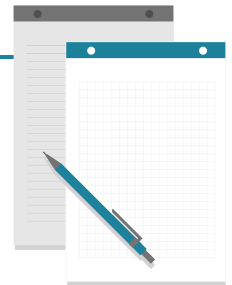
$$A^{[4]} = A^{[3]} \odot A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A^{[5]} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad A^{[n]} = A^5 \quad \text{for all positive integers } n \text{ with } n \geq 5.$$

Activity

Let $A = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 2 & 0 & 4 & 6 \\ 1 & 1 & 3 & 7 \end{bmatrix}$.

- a) What size is A ?
- b) What is the third column of A ?
- c) What is the second row of A ?
- d) What is the element of A in the $(3, 2)$ th position?
- e) What is A^t ?



Conclusion



In this unit we discussed:

- Sets
- Set Operations
- Matrix Arithmetic

Resources



- Rosen, Kenneth H. [Discrete Mathematics and Its Applications](#). New York: McGraw-Hill, 2019. Print.