Chapter 1 Fundamental

1.1 Sets

1.2 Subsets

1.3 Operations on Sets

1.4 Algebraic Properties of Set Operations

1.5 Sequences

1.6 Induction and Recursion

1.7 Division in the Integers

1.8 Matrices

1.9 Boolean Matrix Operations

1.1 Sets

- A set is any well-defined collection of objects called the elements or members of the set.
  - E.g. the collection of integers between zero to nine and mathematics operators;

    the collection of all first four even integers;

    the collection of real numbers between zero and one.

1.1 Sets (cont)

- We use uppercase letters such as A, B, C to denote sets, and lowercase letters such as a, b, c, x, y, z, t to denote the members (or elements) of sets.
- $x \in A$ means x is an element of the set A, $x \notin A$ means x is not an element of A.
  - Let $A = \{1, 3, 5, 7\}$. Then $1 \in A$, $3 \in A$ but $2 \notin A$.
- We use P(x) to denote a sentence or statement P concerning the variable object x.

1.1 Sets (cont)

- The set defined by P(x), written $\{x \mid P(x)\}$, is just the collection of all objects for which P is sensible and true.
  - $Z^+ = \{x \mid x \text{ is a positive integer}\} = \{1, 2, 3, \ldots\}$ (consists of the numbers used for counting)
  - $N = \{x \mid x \text{ is a positive integer or zero}\}$

    $= \{x \mid x \text{ is a natural number}\} = \{0, 1, 2, \ldots\}$
  - $Z = \{x \mid x \text{ is an integer}\}$

    $= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

1.1 Sets (cont)

- Q = {x | x is a rational number} (consists of numbers that can be written as , where a and b are integers and $b \neq 0$)
- R = {x | x is a real number}

1.1 Sets (cont)

- The set with no elements in it is denoted either by { } or the symbol $\varnothing$ and is called the empty set.
- Sets are completely known when their members are all known. Thus we say two sets A and B are equal if they have the same elements, and we write $A = B$.

E.g.1

$\{x \mid x \text{ is a positive integer less than } 4\}$

=

E.g.2

The set consisting of all the letters in the word ‘byte’ can be denoted by

E.g.2

The set consisting of all the letters in the word ‘byte’ can be denoted by

E.g.3

$\{x \mid x$ is a real number and $x^2 = -1\}$

$=$

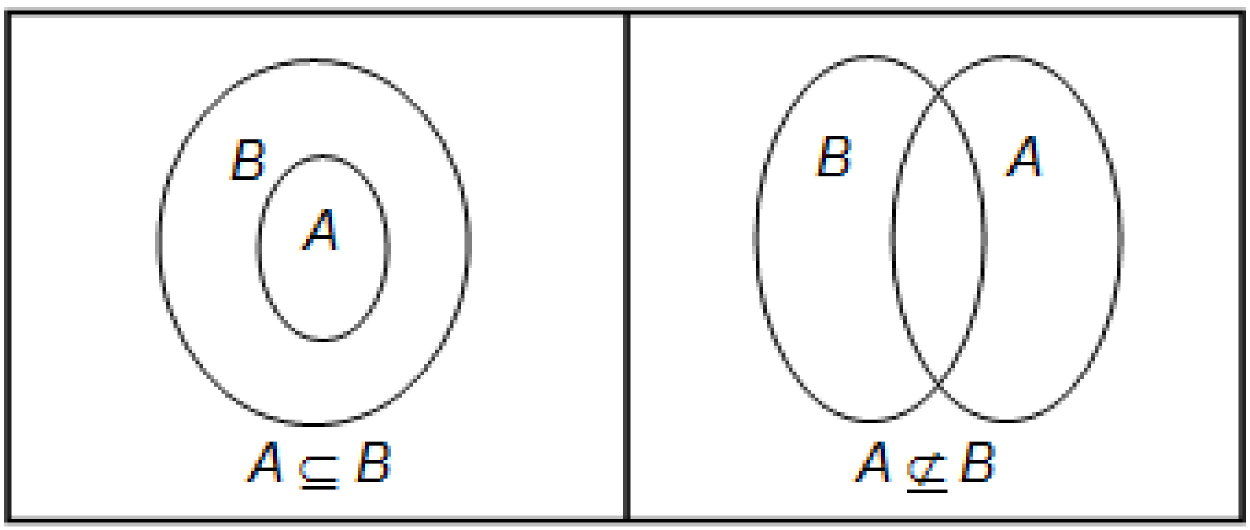
E.g.4

If $A = \{1, 2, 3\}$ and

$B = \{x \mid x$ is a positive integer and $x^2 < 12\}$,

then

1.2 Subsets

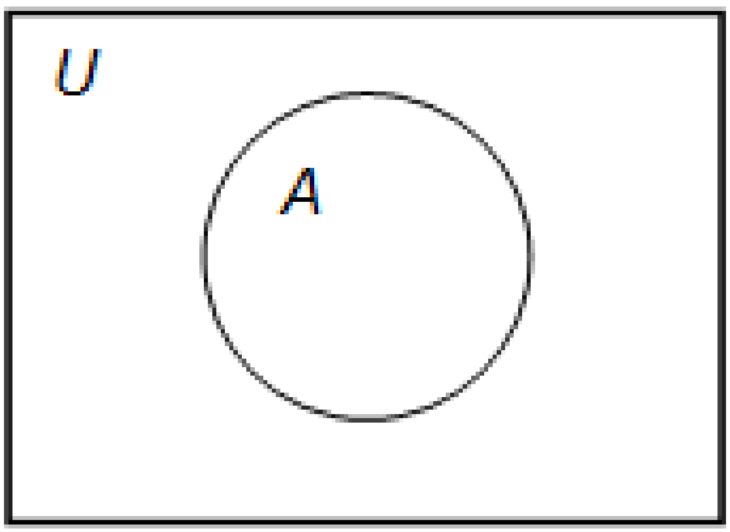
- If every element of A is also an element of B, that is, if whenever $x \in A$ then $x \in B$, we say that A is a subset of B or that A is contained in B, write as $A \subseteq B$. If A is not a subset of B, we write $A \not\subseteq B$.
- 

1.2 Subsets (cont)

- $Z^+ \subseteq Z$ and $Z \subseteq Q$.
- If A is any set, then $A \subseteq A$. That is, every set is a subset of itself.
- For any set A, since there are no elements of $\varnothing$ that are not in A, we have $\varnothing \subseteq A$.
- $A = B \Leftrightarrow A \subseteq B$ and $B \subseteq A$.
- A universal set U is a set consisting of all the objects under study so that every set is a subset of U.

1.2 Subsets (cont)

- In Venn diagrams, the universal set U will be denoted by a rectangle, while sets within U will be denoted by circles.



1.2 Subsets (cont)

- A set A is called finite if it has n distinct elements, where $n \in$ N. In this case, n is called the cardinality of A and is denoted by $|A|$.
  - The sets in E.g. 1, 2, 3, and 4 are finite.
- A set that is not finite is called infinite.
  - Z^+, N, Z, Q, and R are infinite sets.
- If A is a set, then the set of all subsets of A is called the power set of A and is denoted by $\wp(A)$.

E.g.5

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

E.g.6

Let A be a set and let $B = \{A, \{A\}\}$. Then

E.g.7

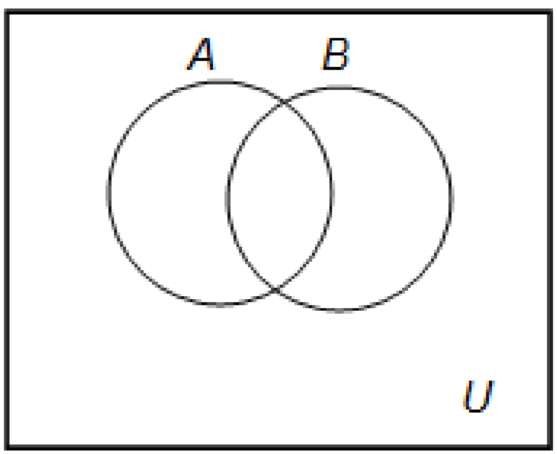
Let A = {1, 2, 3}. Then $\wp(A)$ consists of the following subsets of A:

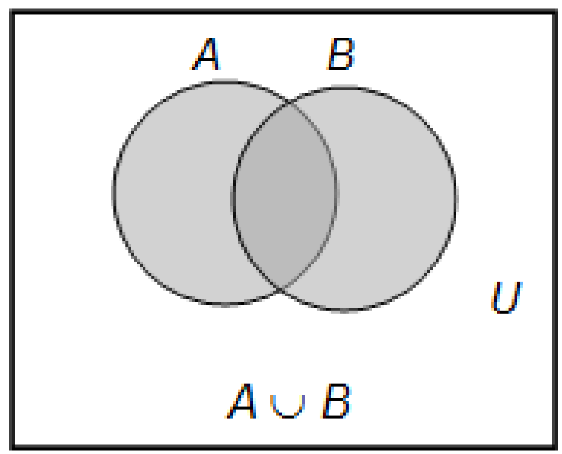
1.3 Operations on Sets

- If A and B are sets, we define their union as the set consisting of all elements that belong to A or B and denote it by $A \cup B$. Thus

  $$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

  - $x \in A \cup B$ if $x \in A$ or $x \in B$ or x belongs to both A and B.

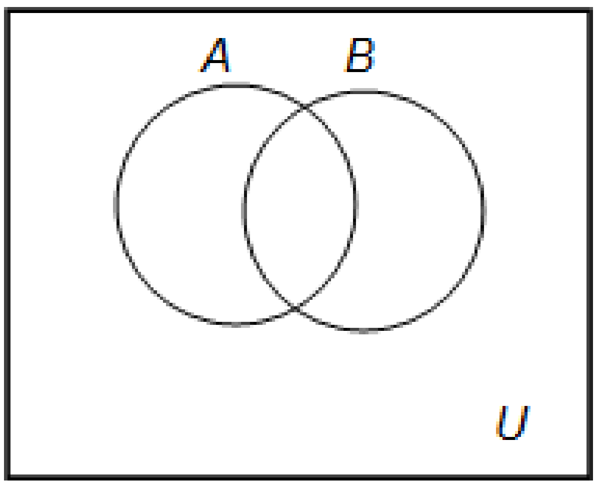


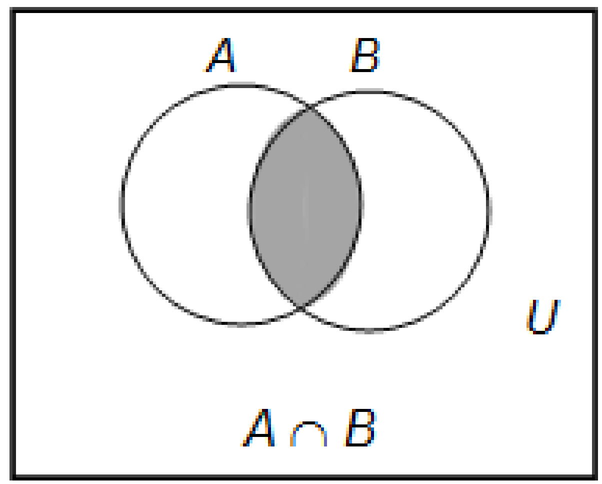


1.3 Operations on Sets (cont)

- If A and B are sets, we define their intersection as the set consisting of all elements that belong to both A and B and denote it by $A \cap B$. Thus

$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

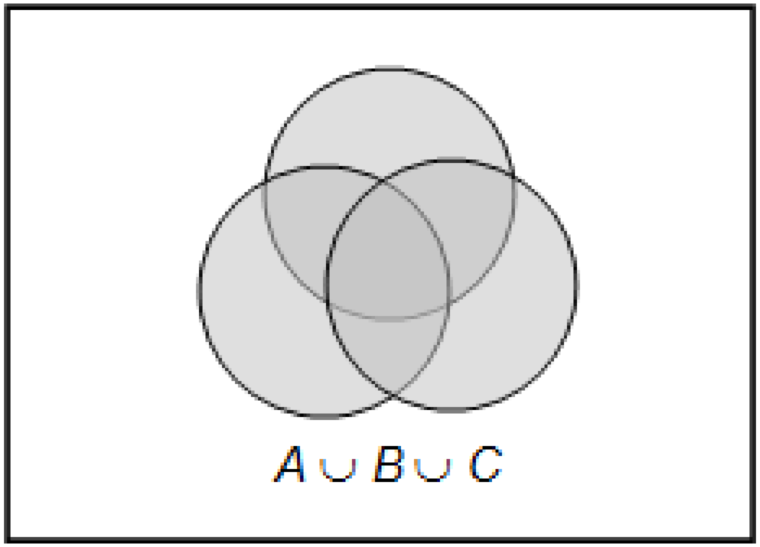


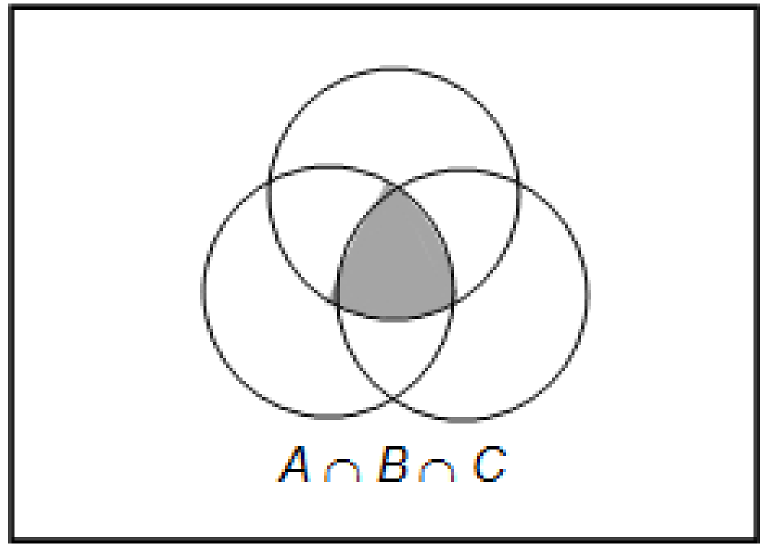


1.3 Operations on Sets (cont)

- Two sets that have no common elements are called disjoint sets.
- The operations of union and intersection can be defined for three or more sets in an obvious manner:
  - $A \cup B \cup C = \{x \mid x \in A \text{ or } x \in B \text{ or } x \in C\}$
  - $A \cap B \cap C$
    $= \{x \mid x \in A \text{ and } x \in B \text{ and } x \in C\}$

1.3 Operations on Sets (cont)



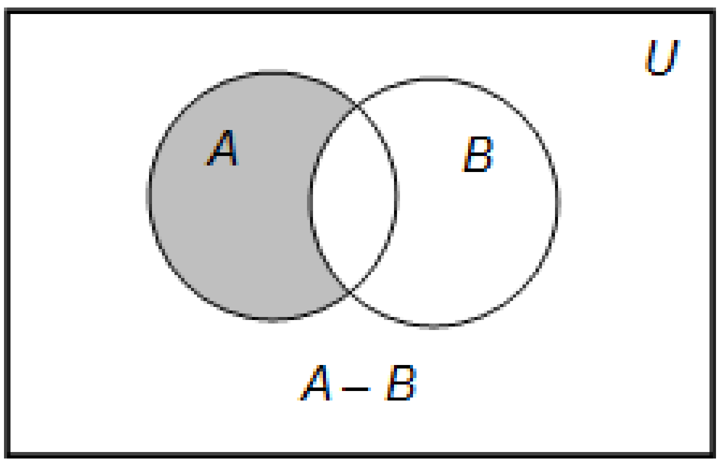


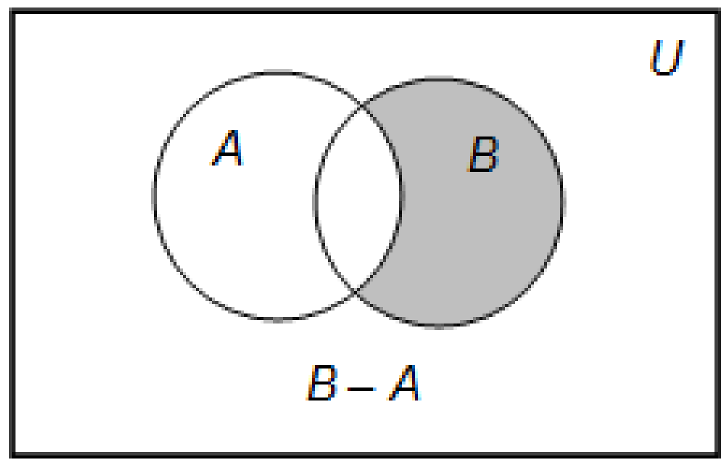
- In general, if $A_1, A_2, \ldots, A_n$ are subsets of U, then $\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \ldots \cup A_n$ (the union from 1 to *n* of *A* sub *k*)
and $\bigcap_{k=1}^{n} A_k = A_1 \cap A_2 \cap \ldots \cap A_n$
(the intersection from 1 to *n* of *A* sub *k*)

1.3 Operations on Sets (cont)

- If A and B are two sets, we define the complement of B with respect to A as the set of all elements that belong to A but not to B, and we denote it by $A - B$. Thus

  $A - B = \{x | x \in A \text{ and } x \notin B\}$.

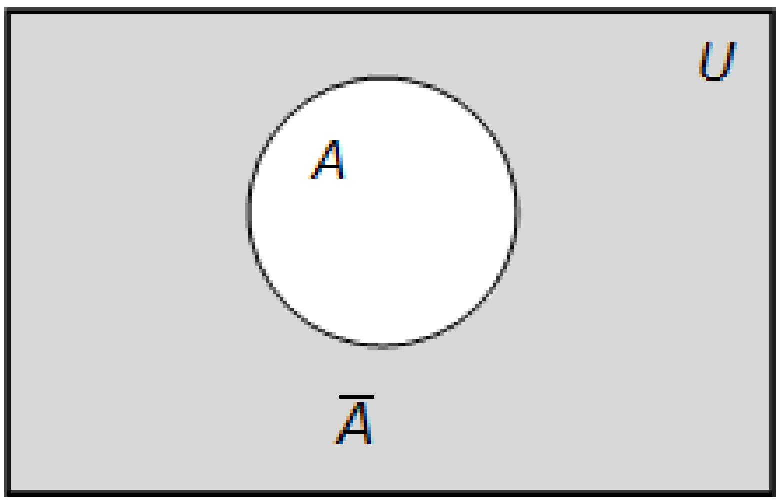




1.3 Operations on Sets (cont)

- If U is a universal set containing A, then $U - A$ is called the complement of A and is denoted by . Thus

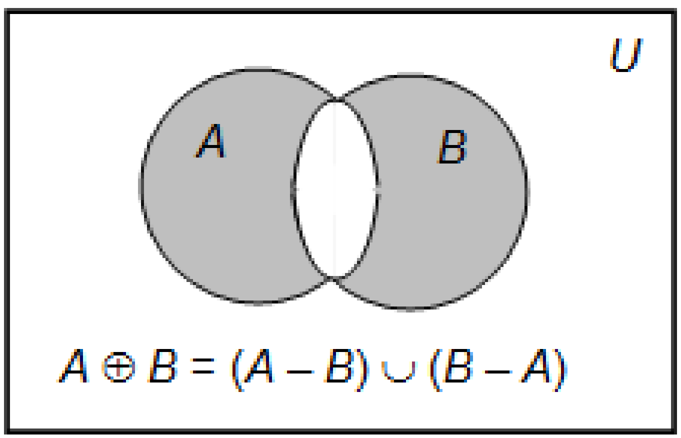
$$\overline{A} = \{x \mid x \notin A\}.$$



1.3 Operations on Sets (cont)

- If A and B are two sets, we define their symmetric difference as the set of all elements that belong to A or B, but not to both A and B, and we denote it by $A \oplus B$. Thus $A \oplus B$

$= \{x \mid (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A)\}$.



E.g.8

Let $A = \{a, b, c, d, e, f\}$ and $B = \{b, d, r, s\}$.

Find $A \cup B$.

E.g.9

Let $A = \{a, b, c, e, f\}$, $B = \{b, e, f, r, s\}$, and $C = \{a, t, u, v\}$. Find $A \cap B$, $B \cap C$, and $A \cap B \cap C$.

E.g.10

Let A = {1, 2, 3, 4, 5, 7}, B = {1, 3, 8, 9}, and C = {1, 3, 6, 8}. Find $A \cap B \cap C$.

E.g.11

Let $A = \{a, b, c\}$ and $B = \{b, c, d, e\}$. Find $A - B$ and $B - A$.

E.g.12

Let $A = \{x \mid x \text{ is an integer and } x \leq 4\}$ and $U = \mathbb{Z}$. Determine $\overline{A}$.

E.g.13

Let $A = \{a, b, c, d\}$ and $B = \{a, c, e, f, g\}$. Find $A \oplus B$.

1.4 Algebraic Properties of Set Operations

- Theorem 1

  The operations defined on sets satisfy the following properties:

  - Commutative Properties
    - $A \cup B = B \cup A$
    - $A \cap B = B \cap A$

1.4 Algebraic Properties of Set Operations (cont)

- Associative Properties
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $A \cap (B \cap C) = (A \cap B) \cap C$
- Distributive Properties
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- Idempotent Properties
  - $A \cup A = A$
  - $A \cap A = A$

1.4 Algebraic Properties of Set Operations (cont)

- Properties of the Complement
  - $\overline{(\overline{A})} = A$
  - $A \cup \overline{A} = U$
  - $A \cap \overline{A} = \varnothing$
  - $\overline{\varnothing} = U$
  - $\overline{U} = \{\ \}$
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (De Morgan's law)
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (De Morgan's law)

1.4 Algebraic Properties of Set Operations (cont)

- Properties of a Universal Set
  - $A \cup U = U$
  - $A \cap U = A$
- Properties of the Empty Set
  - $A \cup \varnothing = A$
  - $A \cap \varnothing = \varnothing$ or $A \cap \{\,\} = \{\,\}$

1.4 Algebraic Properties of Set Operations (cont)

- Theorem 2 (Addition Principle, Inclusion-exclusion Principle)
  - If A and B are finite sets, then

    $|A \cup B| = |A| + |B| - |A \cap B|$.
  - If A and B are disjoint sets, $A \cap B = \varnothing$ and

    $|A \cap B| = 0$, then $|A \cup B| = |A| + |B|$.

1.4 Algebraic Properties of Set Operations (cont)

- Theorem 3
  - Let A, B, and C are finite sets. Then

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

E.g.14

A survey must be taken on methods of commuter travel. Each respondent was asked to check BUS, TRAIN, or AUTOMOBILE as a major method of travelling to work. More than one answer was permitted. The results reported was as follows: BUS, 30 people; TRAIN, 35 people; AUTOMOBILE, 100 people; BUS and TRAIN, 15 people; BUS and AUTOMOBILE, 15 people; TRAIN and AUTOMOBILE, 20 people; and all three methods, 5 people. How many people completed the survey?

Let A: set of people who take bus to work

B: set of people who take train to work

C: set of people who take automobile to work

Let A: set of people who take bus to work

B: set of people who take train to work

C: set of people who take automobile to work

$|A| = 30$, $|B| = 35$, $|C| = 100$, $|A \cap B \cap C| = 5$

$|A \cap B| = 15$, $|A \cap C| = 15$, $|B \cap C| = 20$,

1.5 Sequences

- A sequence is simply a list of objects arranged in a definite order; a first element, second element, third element, and so on.
- The list may stop after n steps, $n \in \mathbb{N}$ (finite sequence); or it may go on forever (infinite sequence).
- The elements may all be different, or some may be repeated.
  - The sequence 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1 is a finite sequence with repeated items. The digit zero, for example, occurs as the second, third, fifth, seventh, and eighth elements of the sequences.

1.5 Sequences (cont)

- The list 3, 8, 13, 18, 23, … is an infinite sequence.
  - The three dots in the expression mean "and so on," that is, continue the pattern established by the first few elements.

    The sequence can be described as $a_1 = 3$, $a_n = a_{n-1} + 5$, $2 \le n < \infty$.
  - The formula that refers to previous terms to define the next term is called recursive.
  - Every recursive formula must include a starting place.

1.5 Sequences (cont)

- 1, 4, 9, 16, 25, …, the list of squares of all positive integers, is an infinite sequence.
  - The sequence can be described using only its position number, $b_n = n^2$, $1 \leq n < \infty$.
  - This type of formula is called explicit because it tells us exactly what value any particular item has.

E.g.15

The recursive formula

$c_1 = 5,\ c_n = 2c_{n-1},\ 2 \leq n \leq 6,$

defines the finite sequence

E.g.16

The infinite sequence 3, 7, 11, 15, 19, 23, …
can be defined by the recursive formula

E.g.17

The explicit formula $s_n = (-4)^n$, $1 \leq n < \infty$, describes the infinite sequence

E.g.18

The finite sequence 87, 82, 77, 72, 67 can be defined by the explicit formula

E.g.19

An ordinary English word such as “sturdy” can be viewed as the finite sequence

Note:

- Sequences of letters or other symbols, written without commas, are also referred to as strings.

E.g.20

An infinite string such as *abababab*… may be regarded as the

E.g.21

The sentence “now is the time for the test” can be regarded as

Note:

- The set corresponding to a sequence is simply the set of all distinct elements in the sequence.

E.g.22

The set corresponding to the sequence 1, 4, 9, 16, 25, … is

E.g.23

The set corresponding to the sequence in E.g.20 is

1.6 Induction and Recursion

- The principle of mathematical induction is:
  - Let P(n) be a predicate that is defined for all $n \geq 1$.
  - If 1. P(1) is true, and

    2. $\forall k \geq 1$ (P(k) $\Rightarrow$ P($k + 1$)) is true

  then P(n) is true for all $n \geq 1$.

E.g.24

Prove, by induction, that

$1 + 2 + \ldots + n = \frac{1}{2}n(n + 1)$ for all $n \geq 1$.

$$P(n): 1 + 2 + \ldots + n = \frac{1}{2}n(n + 1) \text{ for all } n \geq 1.$$

E.g.25

Prove, by induction, that $7^n - 1$ is divisible by 6 for all $n \geq 1$.

P(n): $7^n - 1$ is divisible by 6 for all $n \geq 1$.

E.g.26

A sequence of integers x_1, x_2, …, x_n is defined recursively as follows:

$x_1 = 1$ and $x_{k+1} = x_k + 8k$ for $k \geq 1$.

Prove that $x_n = (2n - 1)^2$ for all $n \geq 1$.

P(n): $x_n = (2n - 1)^2$ for all $n \geq 1$.

1.7 Division in the Integers

- Theorem 1

  If n and m are integers and $n > 0$, we can write $m = qn + r$ for integers q and r with $0 \leq r < n$. Moreover, there is just one way to do this.

- If $r = 0$, so that m is a multiple of n, write as $n \mid m$, which is "n divides m".
- If $n \mid m$, then $m = qn$ and $n < |m|$.
- If m is not a multiple of n, write as $n \nmid m$, which is read "n does not divide m".

E.g.27

Write the following in the form of $m = qn + r$, $0 \leq r < n$.

i. $m = 16$, $n = 3$

ii. $m = 3$, $n = 10$

iii. $m = -11$, $n = 5$

1.7 Division in the Integers (cont)

- Theorem 2

  Let a, b, and c be integers.
  - If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  - If $a \mid b$ and $a \mid c$, where $b > c$, then $a \mid (b - c)$.
  - If $a \mid b$ and $a \mid c$, then $a \mid bc$.
  - If $a \mid b$ and $b \mid c$, then $a \mid c$.
- Note: If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$, for any integers m and n.

1.7 Division in the Integers (cont)

- A number $p > 1$ in Z^+ is called prime if the only positive integers that divide p are p and 1.
  - 2, 3, 5, 7, 11, and 13 are prime, while 4, 10, 16 and 21 are not prime.

1.7 Division in the Integers (cont)

- Algorithm to test whether an integer $N > 1$ is prime:
  - Step 1: Check whether N is 2. If so, N is prime. If not, proceed to
  - Step 2: Check whether $2|N$. If so, N is not prime; otherwise, proceed to
  - Step 3: Compute the largest integer $K \leq \sqrt{N}$. Then
  - Step 4: Check whether $D \mid N$, where D is any prime number such that $1 < D \leq K$. if $D \mid N$ then N is not prime; otherwise, N is prime.

1.7 Division in the Integers (cont)

- Theorem 3

  Every positive integer $n > 1$ can be written uniquely as $p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, where $p_1 < p_2 < \dots < p_s$ are distinct primes that divides n and the k's are positive integers giving the number of times each prime occurs as a factor of n.

  - 9 =

    24 =

    30 =

1.7.1 Greatest Common Divisor

- If a, b, and k are in Z^+, and $k|a$ and $k|b$, we say that k is a common divisor of a and b. If d is the largest such k, d is called the greatest common divisor, or GCD, of a and b, and written as $d = \text{GCD}(a, b)$.
- Theorem 4

  If $d = \text{GCD}(a, b)$, then
  - $d = sa + tb$ for some integers s and t. (These are not necessary positive)
  - If c is any other common divisor of a and b, then $c \mid d$.

1.7.1 Greatest Common Divisor (cont)

- From the definition of greatest common divisor and Theorem 4, we have the following result:

  Let a, b, and d be in Z^+. The integer d is the greatest common divisor of a and b if and only if
  - $d \mid a$ and $d \mid b$.
  - Whenever $c \mid a$ and $c \mid b$, then $c \mid d$.

1.7.1 Greatest Common Divisor (cont)

- If GCD(a, b) = 1, we say a and b are relatively prime.
- Theorem 5

  If a and b are in Z^+, then

  GCD(a, b) = GCD(b, $b \pm a$).

E.g.28

Find the greatest common divisor of the following and then rewrite them in the form of $sa + tb$.

i. 12 and 30

Method 1: (Euclidean algorithm)

Method 2:

$30 = 12(2) + 6$

GCD $(12, 30) = 6$

ii. 17 and 95

(ii) GCD (17, 95) = 1

iii. 98 and 273

iii. GCD (98, 273) = 7

1.7.2 Least Common Multiple

- If a, b, and k are in Z^+, and $a|k$, $b|k$, we say k is a common multiple of a and b. The smallest such k, say c, is called the least common multiple, or LCM, of a and b, and we write c = LCM (a, b).
- Theorem 6

  If a and b are two positive integers, then $\mathrm{GCD}(a, b) \cdot \mathrm{LCM}(a, b) = ab$.

E.g.29

Verify Theorem 6 for $a = 540$ and $b = 504$.

$540 = 2^2\, 3^3\, 5^1$; $504 =$

GCD (504, 540) =

LCM (504, 540) =

Note:

- If n and m are integers and $n > 1$, from Theorem 1, $m = qn + r$, $0 \le r < n$. Sometimes the remainder r is more important than the quotient q.

E.g.30

If the time is now 4 o'clock, what time will it be 101 hours from now?

1.8 Matrices

- A matrix is a rectangular array of numbers arranged in m horizontal rows and n vertical columns:

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

- The ith row of **A** is , $1 \leq i \leq m$, and the jth column of **A** is $\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$, $1 \leq j \leq n$.

1.8 Matrices (cont)

- We say **A** is *m* by *n*, written $m \times n$.
  - E.g. $\mathbf{A} = \begin{bmatrix} 3 & 2 & 5 \\ 0 & -1 & 2 \end{bmatrix}$ is

    $\mathbf{B} = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}$ is

    $\mathbf{C} = \begin{bmatrix} 1 & -1 & 3 & 4 \end{bmatrix}$ is

    $\mathbf{D} = \begin{bmatrix} -1 \\ 2 \\ 0 \end{bmatrix}$ is

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

1.8 Matrices (cont)

- If $m = n$, **A** is a square matrix of order n and that the numbers $a_{11}, a_{22}, \ldots, a_{nn}$ form the main diagonal of **A**.
  - E.g. The following matrix gives the airline distances between the cities indicated.

$$\begin{array}{c c}
 & \begin{array}{cccc} \text{London} & \text{Madrid} & \text{New York} & \text{Tokyo} \end{array} \\
\begin{array}{c} \text{London} \\ \text{Madrid} \\ \text{New York} \\ \text{Tokyo} \end{array} & \begin{bmatrix} 0 & 785 & 3469 & 5959 \\ 785 & 0 & 3593 & 6706 \\ 3469 & 3693 & 0 & 6757 \\ 5959 & 6706 & 6757 & 0 \end{bmatrix}
\end{array}$$

1.8 Matrices (cont)

- We refer to the number a_{ij}, which is in the ith row and jth column of **A** as the i, j element of **A** or as the (i, j) entry of **A**, and we often write $\mathbf{A} = [a_{ij}]$.
- A square matrix $\mathbf{A} = [a_{ij}]$ for which every entry off the main diagonal is zero, that is $a_{ij} = 0$ for $i \neq j$, is called a diagonal matrix.
  - E.g. $\mathbf{F} = \begin{bmatrix} 4 & 0 \\ 0 & 3 \end{bmatrix}$, $\mathbf{G} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$, and $\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 6 \end{bmatrix}$ are diagonal matrices.

1.8 Matrices (cont)

- The $n \times n$ diagonal matrix $\begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}$, all of whose diagonal elements are 1, is called the identity matrix of order n, written as $\mathbf{I}_n$.
- A matrix all of whose entries are zero is called a zero matrix and is denoted by **O**.
  - E.g. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ are zero matrices.

1.8 Matrices (cont)

- If $\mathbf{A} = [a_{ij}]$ is an $m \times n$ matrix, then the $n \times m$ matrix $\mathbf{A}^{T} = [a_{ij}^{T}]$ where $a_{ij}^{T} = a_{ji}$, $1 \le i \le m$, $1 \le j \le n$, is called the transpose of $\mathbf{A}$. Thus the transpose of $\mathbf{A}$ is obtained by interchanging the rows and columns of $\mathbf{A}$.
  - The transpose of $\mathbf{A} = \begin{bmatrix} 2 & -3 & 5 \\ 6 & 1 & 3 \end{bmatrix}$ is

    and the transpose of $\mathbf{B} = \begin{bmatrix} 3 & 4 & 5 \\ 2 & -1 & 0 \\ 1 & 6 & -2 \end{bmatrix}$ is

1.8 Matrices (cont)

- A matrix **A** = [a_{ij}] is symmetric if $\mathbf{A}^T = \mathbf{A}$, i.e. $a_{ij} = a_{ji}$, the entries of **A** are symmetric with respect to the main diagonal of **A**. Thus, if **A** is symmetric, it must be a square matrix.
  - E.g. $\mathbf{A} = \begin{bmatrix} 1 & 2 & -3 \\ 2 & 4 & 5 \\ -3 & 5 & 6 \end{bmatrix}$ is symmetric and $\mathbf{B} = \begin{bmatrix} 1 & 2 & -3 \\ 2 & 4 & 0 \\ 3 & 2 & 1 \end{bmatrix}$ is not symmetric.

1.8 Matrices (cont)

- Two $m \times n$ matrices $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ are said to be equal if $a_{ij} = b_{ij}$, $1 \leq i \leq m$, $1 \leq j \leq n$; that is, if corresponding elements are the same.
- If $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ are $m \times n$ matrices, then the sum of $\mathbf{A}$ and $\mathbf{B}$ is the matrix $\mathbf{C} = [c_{ij}]$ defined by $c_{ij} = a_{ij} + b_{ij}$, $1 \leq i \leq m$, $1 \leq j \leq n$. That is, $\mathbf{C}$ is obtained by adding the corresponding elements of $\mathbf{A}$ and $\mathbf{B}$.
  - The sum of matrices **A** and **B** is defined only when **A** and **B** have the same number of rows and the same number of columns.

1.8 Matrices (cont)

- Basic Properties of Matrix Addition

  Theorem 1

  - $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$
  - $(\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$
  - $\mathbf{A} + \mathbf{O} = \mathbf{O} + \mathbf{A} = \mathbf{A}$

1.8 Matrices (cont)

- If $\mathbf{A} = [a_{ij}]$ is an $m \times p$ matrix and $\mathbf{B} = [b_{ij}]$ is a $p \times n$ matrix, then the product of **A** and **B**, denoted by **AB**, is the $m \times n$ matrix $\mathbf{C} = [c_{ij}]$ defined by

  $c_{ij} = a_{i1}\, b_{1j} + a_{i2}\, b_{2j} + \ldots + a_{ip}\, b_{pj}$,

  $1 \leq i \leq m$, $1 \leq j \leq n$,

1.8 Matrices (cont)

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \cdots & a_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ip} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mp} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \boxed{c_{ij}} & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

$$\begin{array}{ccc} a_{i1} & \longleftrightarrow & b_{1j} \\ a_{i2} & \longleftrightarrow & b_{2j} \\ \vdots & & \vdots \\ a_{ip} & \longleftrightarrow & b_{pj} \end{array}$$

Multiply corresponding elements together and add the results to form c_{ij}.

1.8 Matrices (cont)

- If **A** is an $m \times p$ matrix and **B** is a $p \times n$ matrix, then **AB** can be computed and is $m \times n$ matrix. As for **BA**, we have the following possibilities:
  - **BA** may not be defined; we may have $n \neq m$.
  - **BA** may be defined and then **BA** is $p \times p$, while **AB** is $m \times m$ and $p \neq m$. Thus **AB** and **BA** are not equal.
  - **AB** and **BA** may both be the same size, but not be equal as matrices.
  - **AB** = **BA**.

1.8 Matrices (cont)

- Theorem 2
  - $\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}$
  - $\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$
  - $(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$
- $\mathbf{I}_m \mathbf{A}_{m \times n} = \mathbf{A}_{m \times n} \mathbf{I}_n = \mathbf{A}_{m \times n}$, for identity matrix $\mathbf{I}_m$ or $\mathbf{I}_n$.
- If $\mathbf{A}$ is an $n \times n$ matrix and p is a positive integer, we define

  $\mathbf{A}^p = \underbrace{\mathbf{A} \cdot \mathbf{A} \cdot \mathbf{A} \cdot \ldots \cdot \mathbf{A}}_{p \text{ factors}}$ and $\mathbf{A}^0 = \mathbf{I}$.

1.8 Matrices (cont)

- If p and q are nonnegative integers, we can prove the following laws of exponents for matrices:
  - $\mathbf{A}^p\mathbf{A}^q = \mathbf{A}^{p+q}$
  - $(\mathbf{A}^p)^q = \mathbf{A}^{pq}$
- The rule $(\mathbf{AB})^p = \mathbf{A}^p\mathbf{B}^p$ does not hold for square matrices. However, if $\mathbf{AB} = \mathbf{BA}$, then $(\mathbf{AB})^p = \mathbf{A}^p\mathbf{B}^p$.

1.8 Matrices (cont)

- Theorem 3

  If **A** and **B** are matrices, then
  - $(\mathbf{A}^T)^T = \mathbf{A}$.
  - $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$.
  - $(\mathbf{AB})^T = \mathbf{B}^T\mathbf{A}^T$.

E.g.31

Let $\mathbf{A} = \begin{bmatrix} 2 & -3 & -1 \\ 0 & 5 & 2 \\ 4 & -4 & 6 \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} 2 & x & -1 \\ y & 5 & 2 \\ 4 & -4 & z \end{bmatrix}$.

Determine the values of x, y, and z if $\mathbf{A} = \mathbf{B}$.

E.g.32

Let $\mathbf{A} = \begin{bmatrix} 3 & 4 & -1 \\ 5 & 0 & -2 \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} 4 & 5 & 3 \\ 0 & -3 & 2 \end{bmatrix}$.

Find $\mathbf{A} + \mathbf{B}$ and $\mathbf{AB}^T$.

1.9 Boolean Matrix Operations

- A Boolean matrix is an $m \times n$ matrix whose entries either zero or one.
- Let **A** = $[a_{ij}]$ and **B** = $[b_{ij}]$ be $m \times n$ Boolean matrices. We define $\mathbf{A} \vee \mathbf{B} = \mathbf{C} = [c_{ij}]$, the join of **A** and **B**, by

  $$c_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 1 \text{ or } b_{ij} = 1. \\ 0 & \text{if } a_{ij} \text{ and } b_{ij} \text{ are both } 0. \end{cases}$$

  and $\mathbf{A} \wedge \mathbf{B} = \mathbf{D} = [d_{ij}]$, the meet of **A** and **B**, by

  $$d_{ij} = \begin{cases} 1 & \text{if } a_{ij} \text{ and } b_{ij} \text{ are both } 1. \\ 0 & \text{if } a_{ij} = 0 \text{ or } b_{ij} = 0. \end{cases}$$

1.9 Boolean Matrix Operations (cont)

- These operations are only possible when **A** and **B** have the same size, just as in the case of matrix addition.
- Suppose that **A** = $[a_{ij}]$ is an $m \times p$ Boolean matrix and **B** = $[b_{ij}]$is a $p \times n$ Boolean matrix. We define the Boolean product of **A** and **B**, denoted **A** ⊙ **B**, is the $m \times n$ Boolean matrix **C** = $[c_{ij}]$ defined by

$$c_{ij} = \begin{cases} 1 & \text{if } a_{ik} = 1 \text{ and } b_{kj} = 1 \text{ for some } k, 1 \le k \le p. \\ 0 & \text{otherwise.} \end{cases}$$

1.9 Boolean Matrix Operations (cont)

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \cdots & a_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ \boxed{a_{i1} \quad a_{i2} \quad \cdots \quad a_{ip}} & & & \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mp} \end{bmatrix} \odot \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \boxed{c_{ij}} & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

$$\begin{matrix} a_{i1} & \longleftrightarrow & b_{1j} \\ a_{i2} & \longleftrightarrow & b_{2j} \\ \vdots & & \vdots \\ a_{ip} & \longleftrightarrow & b_{pj} \end{matrix}$$

If any corresponding pair of entries are both equal to 1, then $c_{ij} = 1$; otherwise $c_{ij} = 0$

E.g.33

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

Compute $\mathbf{A} \vee \mathbf{B}$ and $\mathbf{A} \wedge \mathbf{B}$.

E.g.34

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

Compute $\mathbf{A} \odot \mathbf{B}$.

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

$$= \begin{bmatrix} \\ \\ \\ \end{bmatrix}$$

$$A \odot B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

$$=$$

1.9 Boolean Matrix Operations (cont)

- Theorem 1

If $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ are Boolean matrices of compatible sizes, then

1. (a) $\mathbf{A} \vee \mathbf{B} = \mathbf{B} \vee \mathbf{A}$.

   (b) $\mathbf{A} \wedge \mathbf{B} = \mathbf{B} \wedge \mathbf{A}$.

2. (a) $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C} = \mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$.

   (b) $(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C} = \mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})$.

3. (a) $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$.

   (b) $\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$.

4. $(\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C} = \mathbf{A} \odot (\mathbf{B} \odot \mathbf{C})$.