Thus, we have to show $a_{k+1} = 3^{k+2} - 2^{k+1}$.

Given that

$$a_n = 5a_{n-1} - 6a_{n-2}.$$

Therefore, $a_{k+1} = 5a_k - 6a_{k-1}$.

As $P(k)$ and $P(k-1)$ are true, $a_k = 3^{k+1} - 2^k$ and $a_{k-1} = 3^k - 2^{k-1}$.

Thus,

$$\begin{aligned} a_{k+1} &= 5a_k - 6a_{k-1} \\ &= 5(3^{k+1} - 2^k) - 6(3^k - 2^{k-1}) \\ &= 15 \times 3^k - 10 \times 2^{k-1} - 6 \times 3^k + 6 \times 2^{k-1} \\ &= (15-6)3^k - (10-6)2^{k-1} \\ &= 9 \times 3^k - 4 \times 2^{k-1} \\ &= 3^{k+2} - 2^{k+1} \end{aligned}$$

i.e.

$$a_{k+1} = 3^{k+2} - 2^{k+1}.$$

i.e. $P(k+1)$ is true.

Thus, the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true.

Step 4. (Conclusion) As we have already shown $P(0)$, $P(1)$ and $P(2)$ are true, and the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true, by method of strong induction $P(n)$ is true for all $n \in \mathbb{N}$. That is $a_n = 3^{n+1} - 2^n$ for all $n \in \mathbb{N}$.

## Unit II---- Set, Relation and Function

Set

A *set* is an unordered collection of objects, called *elements* or *members* of the set. A set is said to *contain* its elements. We write $a \in A$ to denote that $a$ is an element of the set $A$. The notation $a \notin A$ denotes that $a$ is not an element of the set $A$.

It is common for sets to be denoted using uppercase letters. Lowercase letters are usually used to denote elements of sets. There are several ways to describe a set. One way is to list all the members of a set, when this is possible. We use a notation where all members of the set are listed between braces. For example, the notation $\{a, b, c, d\}$ represents the set with the four elements $a, b, c$, and $d$. This way of describing a set is known as the **roster method**.

Representation of Set — Set Builder Form — Roster

**Example:** The set $V$ of all vowels in the English alphabet can be written as $V = \{a, e, i, o, u\}$.

**Example:** The set $O$ of odd positive integers less than $10$ can be expressed by $O = \{1, 3, 5, 7, 9\}$.

Although sets are usually used to group together elements with common properties, there is nothing that prevents a set from having seemingly unrelated elements. For instance, {a, 2, Fred, New Jersey} is the set containing the four elements a, 2, Fred, and New Jersey.

Sometimes the roster method is used to describe a set without listing all its members. Some members of the set are listed, and then *ellipses* (. . .) are used when the general pattern of the elements is obvious.

**Example:** The set of positive integers less than 100 can be denoted by $\{1, 2, 3, \ldots, 99\}$.

Another way to describe a set is to use **set builder** notation. We characterize all those elements in the set by stating the property or properties they must have to be members. For instance, the set $O$ of all odd positive integers less than 10 can be written as

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

or, specifying the universe $\mathbb{N}$ as the set of positive integers, as

$$O = \{x \in \mathbb{N} : x \text{ is odd and } x < 10\}.$$

Equal sets: 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.

**Example:** The sets $\{1, 3, 5\}$ and $\{3, 5, 1\}$ are equal, because they have the same elements.

Note that the order in which the elements of a set are listed does not matter. Note also that it does not matter if an element of a set is listed more than once, so $\{1, 3, 3, 3, 5, 5, 5, 5\}$ is the same as the set $\{1, 3, 5\}$ because they have the same elements.

* ignore order of the set
* ignore repetation

There is a special set that has no elements. This set is called the **empty set**, or **null set**, and is denoted by ∅. The empty set can also be denoted by { } (that is, we represent the empty set with a pair of braces that encloses all the elements in this set). Often, a set of elements with certain properties turns out to be the null set. For instance, the set of all positive integers that are greater than their squares is the null set. A set with one element is called a **singleton set**.

A common error is to confuse the empty set $\emptyset$ with the set $\{\emptyset\}$, which is a singleton set. The single element of the set $\{\emptyset\}$ is the empty set itself!

It is common to encounter situations where the elements of one set are also the elements of a second set. We now introduce some terminology and notation to express such relationships between sets.

Subset: The set *A* is a *subset* of *B* if and only if every element of *A* is also an element of *B*. We use the notation $A \subseteq B$ to indicate that *A* is a subset of the set *B*.

We see that $A \subseteq B$ if and only if the quantification $\forall x(x \in A \rightarrow x \in B)$ is true. Note that to show that *A* is not a subset of *B* we need only find one element $x \in A$ with $x \notin B$. Such an *x* is a counterexample to the claim that $x \in A$ implies $x \in B$.

**Example:** For every set $S$, (i) $\emptyset \subseteq S$ and (ii) $S \subseteq S$.

***Solution:*** To show that $\emptyset \subseteq S$, we must show that $\forall x(x \in \emptyset \rightarrow x \in S)$ is true. Because the empty set contains no elements, it follows that $x \in \emptyset$ is always false. It follows that the conditional statement $x \in \emptyset \rightarrow x \in S$ is always true, because its hypothesis is always false and a conditional statement with a false hypothesis is true. Therefore, $\forall x(x \in \emptyset \rightarrow x \in S)$ is true. Thus, $\emptyset \subseteq S$. Since $\forall x(x \in S \rightarrow x \in S)$ is true, $S \subseteq S$.

Note that this is an example of a vacuous proof. To show that two sets $A$ and $B$ are equal, show that $A \subseteq B$ and $B \subseteq A$.

Vacuous proof is a proof in which the implication p  q is true based on the fact that p is false.

Sets may have other sets as members. For instance, we have the sets $A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ and $B = \{x \mid x \text{ is a subset of the set } \{a, b\}\}$. Note that these two sets are equal, that is, $A = B$. Also note that $\{a\} \in A$, but $a \notin A$.

Sets are used extensively in counting problems, and for such applications we need to discuss the sizes of sets.

The Size of a Set: Let $S$ be a set. If there are exactly $n$ distinct elements in $S$ where $n$ is a nonnegative integer, we say that $S$ is a *finite set* and that $n$ is the *cardinality* of $S$. The cardinality of $S$ is denoted by $|S|$.

size of the set = cardinality

**Example:** Let *A* be the set of odd positive integers less than 10. Then $|A| = 5$.

**Example:** Let $S$ be the set of letters in the English alphabet. Then $|S| = 26$.

**Example:** Because the null set has no elements, it follows that $|\emptyset| = 0$.

Infinite set: A set is said to be *infinite* if it is not finite.

**Example:** The set of positive integers is infinite.

Many problems involve testing all combinations of elements of a set to see if they satisfy some property. To consider all such combinations of elements of a set *S*, we build a new set that has as its members all the subsets of *S*.

Power Sets: Given a set $S$, the *power set* of $S$ is the set of all subsets of the set $S$. The power set of $S$ is denoted by $P(S)$.

**Example:** What is the power set of the set $\{0, 1, 2\}$?

*Solution:* The power set $P(\{0, 1, 2\})$ is the set of all subsets of $\{0, 1, 2\}$. Hence,

$$P(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

$n = 3$

$2^n = 2^3 = 8$

Note that the empty set and the set itself are members of this set of subsets.

**Example:** What is the power set of the empty set? What is the power set of the set $\{\emptyset\}$?

*Solution:* The empty set has exactly one subset, namely, itself. Consequently, $P(\emptyset) = \{\emptyset\}$.

The set $\{\emptyset\}$ has exactly two subsets, namely, $\emptyset$ and the set $\{\emptyset\}$ itself. Therefore,

$$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$

Note: If a set has $n$ elements, then its power set has $2^n$ elements.

## Set Operations

Two, or more, sets can be combined in many different ways. For instance, starting with the set of mathematics majors at your school and the set of computer science majors at your school, we can form the set of students who are mathematics majors or computer science majors, the set of students who are joint majors in mathematics and computer science, the set of all students not majoring in mathematics, and so on.

Union of the sets: Let *A* and *B* be sets. The *union* of the sets *A* and *B*, denoted by $A \cup B$, is the set that contains those elements that are either in *A* or in *B*, or in both. An element $x$ belongs to the union of the sets *A* and *B* if and only if $x$ belongs to *A* or $x$ belongs to *B*. This tells us that

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

**Example:** The union of the sets $\{1, 3, 5\}$ and $\{1, 2, 3\}$ is the set $\{1, 2, 3, 5\}$; that is, $\{1, 3, 5\} \cup \{1, 2, 3\} = \{1, 2, 3, 5\}$.

**Example:** The union of the set of all computer science majors at your school and the set of all mathematics majors at your school is the set of students at your school who are majoring either in mathematics or in computer science (or in both).

Intersection of the sets: Let *A* and *B* be sets. The *intersection* of the sets *A* and *B*, denoted by $A \cap B$, is the set containing those elements in both *A* and *B*. An element $x$ belongs to the intersection of the sets *A* and *B* if and only if $x$ belongs to *A* and $x$ belongs to *B*. This tells us that

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

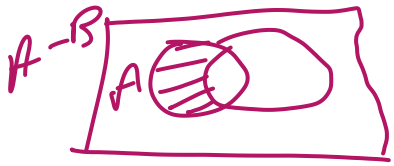
**Example:** The intersection of the sets $\{1, 3, 5\}$ and $\{1, 2, 3\}$ is the set $\{1, 3\}$; that is, $\{1, 3, 5\} \cap \{1, 2, 3\} = \{1, 3\}$.

Disjoint sets: Two sets are called *disjoint* if their intersection is the empty set.

**Example:** Let $A = \{1, 3, 5, 7, 9\}$ and $B = \{2, 4, 6, 8, 10\}$. Because $A \cap B = \emptyset$, $A$ and $B$ are disjoint. $A \cap B = \emptyset$

Difference of sets: Let *A* and *B* be sets. The *difference* of *A* and *B,* denoted by $A - B$, is the set containing those elements that are in $A$ but not in $B$. The difference of *A* and *B* is also called the *complement of B with respect to A*. An element $x$ belongs to the difference of $A$ and $B$ if and only if $x \in A$ and $x \notin B$. This tells us that

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




A-B: Remove B from A

***Remark:*** The difference of sets *A* and *B* is sometimes denoted by $A \setminus B$.

**Example:** The difference of $\{1, 3, 5\}$ and $\{1, 2, 3\}$ is the set $\{5\}$; that is, $\{1, 3, 5\} - \{1, 2, 3\} = \{5\}$. This is different from the difference of $\{1, 2, 3\}$ and $\{1, 3, 5\}$, which is the set $\{2\}$.

Complement of a set: Let *U* be the universal set. The *complement* of the set *A,* denoted by $\bar{A}$, is the complement of *A* with respect to *U*. Therefore, the complement of the set *A* is $U - A$. An element belongs to $\bar{A}$ if and only if $x \notin A$. This tells us that

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

**Example:** Let $A$ = {a, e, i, o, u} (where the universal set is the set of letters of the English alphabet). Then $\bar{A}$ = {b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z}. U = {a, b, c, d, e, ..., x, y, z}; 21 ← cardinality

**Example:** Let *A* be the set of positive integers greater than 10 (with universal set the set of all positive integers). Then $\bar{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. A = {11, 12, 13, 14, 15, .....}; U = {1, 2, 3, 4, ..., 10, 11, ....}

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

A universal set is a set which contains all the elements or objects of other sets, including its own elements. It is usually denoted by the symbol 'U'.



Suppose Set A consists of all even numbers such that, A = {2, 4, 6, 8, 10, ...} and set B consists of all odd numbers, such that, B = {1, 3, 5, 7, 9, ...}. The universal set U consists of all natural numbers, such that, U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10,....}.

**Solution:** We will prove that the two sets $\overline{A \cap B}$ and $\overline{A} \cup \overline{B}$ are equal by showing that each set is a subset of the other. First, we will show that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. We do this by showing that if *x* is in $\overline{A \cap B}$, then it must also be in $\overline{A} \cup \overline{B}$. Now suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, we see that the proposition $\neg((x \in A) \wedge (x \in B))$ is true. By applying De Morgan's law for propositions, we see that $\neg(x \in A)$ or $\neg(x \in B)$. Using the definition of negation of propositions, we have $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, we see that this implies that $x \in \overline{A}$ or $x \in \overline{B}$. Consequently, by the definition of union, we see that $x \in \overline{A} \cup \overline{B}$. We have now shown that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. Next, we will show that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. We do this by showing that if *x* is in $\overline{A} \cup \overline{B}$, then it must also be in $\overline{A \cap B}$. Now suppose that $x \in \overline{A} \cup \overline{B}$. By the definition of union, we know that $x \in \overline{A}$ or $x \in \overline{B}$. Using the definition of complement, we see that $x \notin A$ or $x \notin B$. Consequently, the proposition $\neg(x \in A) \vee \neg(x \in B)$ is true. By De Morgan's law for propositions, we conclude that $\neg((x \in A) \wedge (x \in B))$ is true. By the definition of intersection, it follows that $\neg(x \in A \cap B)$. We now use the definition of complement to conclude that $x \in \overline{A \cap B}$. This shows that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. Because we have shown that each set is a subset of the other, the two sets are equal, and the identity is proved.

Principle of inclusion–exclusion.

The subtraction rule: Suppose that a task can be done in one of two ways, but some of the ways to do it are common to both ways. In this situation, we cannot use the sum rule to count the number of ways to do the task. If we add the number of ways to do the tasks in these two ways, we get an overcount of the total number of ways to do it, because the ways to do the task that are common to the two ways are counted twice. To correctly count the number of ways to do the two tasks, we must subtract the number of ways that are counted twice. This leads us to an important counting rule.

"If a task can be done in either $n_1$ ways or $n_2$ ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways."

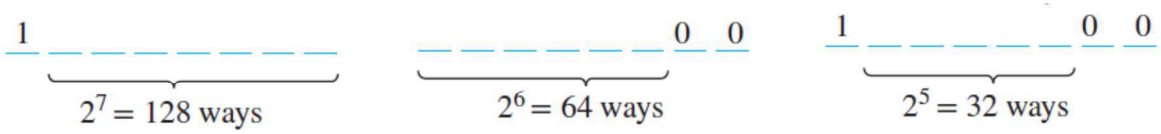
The subtraction rule is also known as the **principle of inclusion–exclusion**, especially when it is used to count the number of elements in the union of two sets. Suppose that $A_1$ and $A_2$ are sets.

Then, there are $|A_1|$ ways to select an element from $A_1$ and $|A_2|$ ways to select an element from $A_2$. The number of ways to select an element from $A_1$ or from $A_2$, that is, the number of ways to select an element from their union, is the sum of the number of ways to select an element from $A_1$ and the number of ways to select an element from $A_2$, minus the number of ways to select an element that is in both $A_1$ and $A_2$. Because there are $|A_1 \cup A_2|$ ways to select an element in either $A_1$ or in $A_2$, and $|A_1 \cap A_2|$ ways to select an element common to both sets, we have

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

**Example:** How many bit strings of length eight start with a 1 bit or end with the two bits 00?

*Solution:* we need three counting problems to solve before we can apply the principle of inclusion–exclusion. We can construct a bit string of length eight that starts with a 1 bit or ends with the two bits 00, by constructing a bit string of length eight beginning with a 1 bit or by constructing a bit string of length eight that ends with the two bits 00.




We can construct a bit string of length eight that begins with a 1 in $2^7 = 128$ ways. This follows by the product rule, because the first bit can be chosen in only one way and each of the other seven bits can be chosen in two ways. Similarly, we can construct a bit string of length eight ending with the two bits 00, in $2^6 = 64$ ways. This follows by the product rule, because each of the first six bits can be chosen in two ways and the last two bits can be chosen in only one way. Some of the ways to construct a bit string of length eight starting with a 1 are the same as the ways to construct a bit string of length eight that ends with the two bits 00. There are $2^5 = 32$ ways to construct such a string. This follows by the product rule, because the first bit can be chosen in only one way, each of the second through the sixth bits can be chosen in two ways, and the last two bits can be chosen in one way. Consequently, the number of bit strings of length eight that begin with a 1 or end with a 00, which equals the number of ways to construct a bit string of length eight that begins with a 1 or that ends with 00, equals 128 + 64 − 32 = 160.

**Example:** How many positive integers not exceeding 100 are divisible either by 4 or by 6?

Solution: Let $A$ be the set of positive integers not exceeding 100 that are divisible by 4 and $B$ be the set of positive integers not exceeding 100 that are divisible by 6. Then $A \cap B$ is the set of positive integers not exceeding 100 that are divisible by 4 and 6. That is, $A \cap B$ is the set of positive integers not exceeding 100 that are divisible by 12. Also $A \cup B$ is the set of positive integers not exceeding 100 are divisible either by 4 or by 6. Then $|A| = [100/4] = 25$, $|B| = [100/6] = 16$, $|A \cap B| = [100/12] = 8$. Thus,

$$|A \cup B| = |A| + |B| - |A \cap B| = 25 + 16 - 8 = 33.$$

Therefore, there are 33 positive integers not exceeding 100 are divisible either by 4 or by 6.

More generally if $A_1, A_2, \ldots A_m$ are finite sets, then

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{i=1}^{m} |A_i| - \sum_{1 \le i < j \le m} |A_i \cap A_j| + \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k| - \ldots$$

$$+(-1)^{m-1} |A_1 \cap A_2 \cap \cdots \cap A_m|.$$

**Example:** How many positive integers not exceeding 100 are divisible by 4,or by 5, or by 6?

Solution: Let $A$ be the set of positive integers not exceeding 100 that are divisible by 4,

$B$ be the set of positive integers not exceeding 100 that are divisible by 5 and

$C$ be the set of positive integers not exceeding 100 that are divisible by 6. Then

$A \cap B$ is the set of positive integers not exceeding 100 that are divisible by 4 and 5,

$A \cap C$ is the set of positive integers not exceeding 100 that are divisible by 4 and 6 ,

$B \cap C$ is the set of positive integers not exceeding 100 that are divisible by 5 and 6 and

$A \cap B \cap C$ is the set of positive integers not exceeding 100 that are divisible by 4 and 5 and 6.

Then

$$|A| = \left[\frac{100}{4}\right] = 25, |B| = \left[\frac{100}{5}\right] = 20, |C| = \left[\frac{100}{6}\right] = 16,$$

$$|A \cap B| = \left[\frac{100}{20}\right] = 5. |A \cap C| = \left[\frac{100}{12}\right] = 8, |B \cap C| = \left[\frac{100}{30}\right] = 3, |A \cap B \cap C| = \left[\frac{100}{60}\right] = 1.$$

Thus,

$$|A \cup B \cup c| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap BC|$$
$$= 25 + 20 + 16 - 5 - 8 - 3 + 1 = 46.$$

Therefore, there are 46 positive integers not exceeding 100 are divisible by 4,or by 5, or by 6.

## Cartesian Products

The order of elements in a collection is often important. Because sets are unordered, a different structure is needed to represent ordered collections. This is provided by ordered *n*-tuples. The *ordered n-tuple* $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has $a_1$ as its first element, $a_2$ as its second element, . . . , and $a_n$ as its $n$th element. We say that two ordered *n*-tuples are equal if and only if each corresponding pair of their elements are equal. In other words, $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ if and only if $a_i = b_i$ , for $i = 1, 2, \ldots, n$. In particular, ordered 2-tuples are called **ordered pairs**. The ordered pairs $(a, b)$ and $(c, d)$ are equal if and only if $a = c$ and $b = d$. Note that $(a, b)$ and $(b, a)$ are not equal unless $a = b$.

Let *A* and *B* be nonempty sets. The *Cartesian product* of *A* and *B*, denoted by $A \times B$, is the set of all ordered pairs $(a, b)$, where $a \in A$ and $b \in B$. Hence,

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

**Example:** What is the Cartesian product of $A = \{1, 2\}$ and $B = \{a, b, c\}$?

**Solution:** The Cartesian product $A \times B$ is

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

Note that the Cartesian products $A \times B$ and $B \times A$ are not equal, unless $A = B$.

**Definition:** The *Cartesian product* of the sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered *n*-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i$ belongs to $A_i$ for $i = 1, 2, \ldots, n$. In other words,

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

We use the notation $A^2$ to denote $A \times A$, the Cartesian product of the set *A* with itself. Similarly, $A^3 = A \times A \times A$, $A^4 = A \times A \times A \times A$, and so on. More generally,

$$A^n = \{(a_1, a_2, \ldots, a_n) | a_i \in A \text{ for } i = 1, 2, \ldots, n\}.$$

**Example:** Suppose that $A = \{1, 2\}$. It follows that $A^2 = \{(1,1), (1,2), (2,1), (2,2)\}$ and $A^3 = \{(1,1,1), (1,1,2), (1,2,1), (1,2,2), (2,1,1), (2,1,2), (2,2,1), (2,2,2)\}$.

## Relations

The most direct way to express a relationship between elements of two sets is to use ordered pairs made up of two related elements. For this reason, sets of ordered pairs are called binary relations.

Binary relation: Let *A* and *B* be sets. A binary relation *from A to B* is a subset of $A \times B$.

In other words, a binary relation from *A* to *B* is a set *R* of ordered pairs where the first element of each ordered pair comes from *A* and the second element comes from *B*. We use the notation $a\ R\ b$ to denote that $(a, b) \in R$. Moreover, when $(a, b)$ belongs to *R*, $a$ is said to be related to $b$ by *R*. Binary relations represent relationships between the elements of two sets.

**Example:** Let $A = \{0, 1, 2\}$ and $B = \{a, b\}$. Then $\{(0, a), (0, b), (1, a), (2, b)\}$ is a relation from *A* to *B*.

**Note:** A *relation on a set A* is a relation from $A$ to $A$. In other words, a relation on a set $A$ is a subset of $A \times A$.

**Example:** Let *A* be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) \mid a \text{ divides } b\}$?

**Solution:** Because $(a, b)$ is in $R$ if and only if *a* and *b* are positive integers not exceeding 4 such that $a$ divides $b$, we see that

$$R = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}.$$

**Example:** How many relations are there on a set with *n* elements?

**Solution:** A relation on a set *A* is a subset of $A \times A$. Because $A \times A$ has $n^2$ elements when $A$ has $n$ elements, and a set with *m* elements has $2^m$ subsets, there are $2^{n^2}$ subsets of $A \times A$. Thus, there are $2^{n^2}$ relations on a set with $n$ elements. For example, there are $2^{3^2} = 2^9 = 512$ relations on the set {*a, b, c*}.

Properties of Relations: Let $R$ be a relation on a set $A$. The relation $R$ is called *reflexive* if $(a, a) \in R$ for every element $a \in A$. The relation $R$ is called *symmetric* if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$. In the relation $R$, if $(a, b) \in R$ and $(b, a) \in R$, imply $a = b$ then $R$ is called *antisymmetric*. The relation $R$ *is* called *transitive* if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

**Example:** Consider the following relations on $\{1, 2, 3, 4\}$:

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$,

$R_2 = \{(1,1), (1,2), (2,1)\}$,

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$,

$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$,

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$,

$R_6 = \{(3,4)\}$.

Which of these relations are reflexive, symmetric, antisymmetric and transitive?

**Solution:** The relations $R_3$ and $R_5$ are reflexive because they both contain all pairs of the form $(a, a)$, namely, $(1, 1), (2, 2), (3, 3)$, and $(4, 4)$. The other relations are not reflexive because they do not contain all of these ordered pairs. In particular, $R_1, R_2, R_4$, and $R_6$ are not reflexive because $(3, 3)$ is not in any of these relations.

The relations $R_2$ and $R_3$ are symmetric, because in each case $(b, a)$ belongs to the relation whenever $(a, b)$ does. For $R_2$, the only thing to check is that both $(2, 1)$ and $(1, 2)$ are in the relation. For $R_3$, it is necessary to check that both $(1, 2)$ and $(2, 1)$ belong to the relation, and $(1, 4)$ and $(4, 1)$ belong to the relation. None of the other relations is symmetric. This is done by finding a pair $(a, b)$ such that it is in the relation but $(b, a)$ is not.

The relations $R_4, R_5$, and $R_6$ are all antisymmetric. For each of these relations there is no pair of elements $a$ and $b$ with $a \neq b$ such that both $(a, b)$ and $(b, a)$ belong to the relation. None of the other relations is antisymmetric. This is done by finding a pair $(a, b)$ with $a \neq b$ such that $(a, b)$ and $(b, a)$ are both in the relation.

The relations $R_4, R_5$, and $R_6$ are transitive. For each of these relations, we can show that it is transitive by verifying that if $(a, b)$ and $(b, c)$ belong to this relation, then $(a, c)$also does. For instance, $R_4$ is transitive, because $(3, 2)$ and $(2, 1)$, $(4, 2)$ and $(2, 1)$, $(4, 3)$ and $(3, 1)$, and $(4, 3)$ and $(3, 2)$ are the only such sets of pairs, and $(3, 1), (4, 1)$, and $(4, 2)$ belong to $R_4$. $R_1$ is not transitive because $(3, 4)$ and $(4, 1)$ belong to $R_1$, but $(3, 1)$ does not. $R_2$ is not transitive because $(2, 1)$ and $(1, 2)$ belong to $R_2$, but $(2, 2)$ does not. $R_3$ is not transitive because $(4, 1)$ and $(1, 2)$ belong to $R_3$, but $(4, 2)$ does not.

**Example:** Is the "divides" relation on the set of positive integers reflexive, symmetric, antisymmetric and transitive?

**Solution***:* Because $a \mid a$ whenever $a$ is a positive integer, the "divides" relation is reflexive. (Note that if we replace the set of positive integers with the set of all integers the relation is not reflexive because by definition $0$ does not divide $0$.) This relation is not symmetric because $1|2$, but $2 \nmid 1$. It is antisymmetric, for if $a$ and $b$ are positive integers with $a \mid b$ and $b \mid a$, then $a = b$. Suppose that $a$ divides $b$ and $b$ divides $c$. Then there are positive integers $k$ and $l$ such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so $a$ divides $c$. It follows that this relation is transitive.

**Example:** How many reflexive relations are there on a set with $n$ elements?

**Solution:** A relation $R$ on a set $A$ is a subset of $A \times A$. Consequently, a relation is determined by specifying whether each of the $n^2$ ordered pairs in $A \times A$ is in $R$. However, if $R$ is reflexive, each of the $n$ ordered pairs $(a, a)$ must be in *R* for $a \in A$. Each of the other $n^2 - n$ ordered pairs of the form $(a, b)$, where $a \neq b$, may or may not be in $R$. Hence, by the product rule for counting, there are $2^{n(n-1)}$ reflexive relations [this is the number of ways to choose whether each element $(a, b)$, with $a \neq b$, belongs to $R$].

**Example:** How many symmetric relations are there on a set with $n$ elements?

**Example:** How many reflexive and symmetric relations are there on a set with $n$ elements?

**Example:** The relation $\Delta = \{(a, a) \mid a \in A\}$ is called the **diagonal relation** on *A*.

## Combining Relations

**Example:** Let $A = \{1,2,3\}$ and $B = \{1,2,3,4\}$. The relations $R_1 = \{(1,1),(2,2),(3,3)\}$ and $R_2 = \{(1,1),(1,2),(1,3),(1,4)\}$ can be combined to obtain $R_1 \cup R_2 = \{(1,1),(1,2),((1,3),(1,4),(2,2),(3,3)\}$, $R_1 \cap R_2 = \{(1,1)\}$, $R_1 - R_2 = \{(2,2),(3,3)\}$ and $R_2 - R_1 = \{(1,2),(1,3),(1,4)\}$.

**Example:** Let *A* and *B* be the set of all students and the set of all courses at a school, respectively. Suppose that $R_1$ consists of all ordered pairs $(a,b)$, where $a$ is a student who has taken course $b$, and $R_2$ consists of all ordered pairs $(a,b)$, where $a$ is a student who requires course $b$ to graduate. What are the relations $R_1 \cup R_2, R_1 \cap R_2, R_1 \oplus R_2, R_1 - R_2$, and $R_2 - R_1$?

**Solution:** The relation $R_1 \cup R_2$ consists of all ordered pairs $(a,b)$, where $a$ is a student who either has taken course $b$ or needs course $b$ to graduate, and $R_1 \cap R_2$ is the set of all ordered pairs $(a,b)$, where $a$ is a student who has taken course $b$ and needs this course to graduate. Also, $R_1 \oplus R_2$ consists of all ordered pairs $(a,b)$, where student $a$ has taken course $b$ but does not need it to graduate or needs course $b$ to graduate but has not taken it. $R_1 - R_2$is the set of ordered pairs $(a,b)$, where $a$ has taken course $b$ but does not need it to graduate; that is, $b$ is an elective course that $a$ has taken. $R_2 - R_1$is the set of all ordered pairs $(a,b)$, where $b$ is a course that $a$ needs to graduate but has not taken by $a$.

**Example:** Let $R_1$ be the "less than" relation on the set of real numbers and let $R_2$ be the "greater than" relation on the set of real numbers, that is, $R_1 = \{(x,y) \mid x < y\}$ and $R_2 = \{(x,y) \mid x > y\}$. What are $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$, and $R_1 \oplus R_2$?

**Solution:** We note that $(x,y) \in R_1 \cup R_2$ if and only if $(x,y) \in R_1$ *or* $(x,y) \in R_2$. Hence, $(x,y) \in R_1 \cup R_2$ if and only if $x < y$ or $x > y$. Because the condition $x < y$ or $x > y$ is the same as the condition $x \neq y$, it follows that $R_1 \cup R_2 = \{(x,y) \mid x \neq y\}$. In other words, the union of the "less than" relation and the "greater than" relation is the "not equals" relation. It is impossible for a pair $(x,y)$ to belong to both $R_1$ and $R_2$ because it is impossible that $x < y$ and $x > y$. It follows that $R_1 \cap R_2 = \emptyset$. We also see that $R_1 - R_2 = R_1$ , $R_2 - R_1 = R_2$, and $R_1 \oplus R_2 = (R_1 \cup R_2) - (R_1 \cap R_2) = \{(x,y) \mid x \neq y\}$.

Composition of relations: Let $R$ be a relation from a set $A$ to a set $B$ and $S$ a relation from $B$ to a set $C$. The *composite* of $R$ and $S$ is the relation consisting of ordered pairs $(a,c)$, where $a \in$

$A, c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. We denote the composite of $R$ and $S$ by $S \circ R$.

**Example:** What is the composite of the relations $R$ and $S$, where $R$ is the relation from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$ with $R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$ and $S$ is the relation from $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$ with $S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$?

*Solution:* $S \circ R$ is constructed using all ordered pairs in $R$ and ordered pairs in $S$, where the second element of the ordered pair in $R$ agrees with the first element of the ordered pair in $S$. For example, the ordered pairs $(2, 3) \in R$ and $(3, 1) \in S$ produce the ordered pair $(2, 1) \in S \circ R$. Computing all the ordered pairs in the composite, we find $S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}$.

**Example: Composing the Parent Relation with Itself.** Let $R$ be the relation on the set of all people such that $(a, b) \in R$ if person $a$ is a parent of person $b$. Then $(a, c) \in R \circ R$ if and only if there is a person $b$ such that $(a, b) \in R$ and $(b, c) \in R$, that is, if and only if there is a person $b$ such that $a$ is a parent of $b$ and $b$ is a parent of $c$. In other words, $(a, c) \in R \circ R$ if and only if $a$ is a grandparent of $c$.

The powers of a relation $R$ can be recursively defined from the definition of a composite of two relations. Let $R$ be a relation on the set $A$. The powers $R^n, n = 1, 2, 3, \ldots$, are defined recursively by $R^1 = R$ and $R^{n+1} = R^n \circ R$.

The definition shows that $R^2 = R \circ R$, $R^3 = R^2 \circ R = (R \circ R) \circ R$, and so on.

**Example:** Let $R = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$. Find the powers $Rn, n = 2, 3, 4, \ldots$.

**Solution:** Because $R^2 = R \circ R$, we find that $R^2 = \{(1, 1), (2, 1), (3, 1), (4, 2)\}$. Furthermore, because $R^3 = R^2 \circ R = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$. Additional computation shows that $R^4$ is the same as $R^3$, so $R^4 = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$. It also follows that $R^n = R^3$ for $n = 5, 6, 7, \ldots$.

**Theorem:** The relation $R$ on a set $A$ is transitive if and only if $R^n \subseteq R$ for $n = 1, 2, 3, \ldots$.

***Proof:*** We first prove the "if" part of the theorem. We suppose that $R^n \subseteq R$ for $n = 1, 2, 3, \ldots$. In particular, $R^2 \subseteq R$. To see that this implies *R* is transitive, note that if $(a, b) \in R$ and $(b, c) \in R$, then by the definition of composition, $(a, c) \in R^2$. Because $R^2 \subseteq R$, this means that $(a, c) \in R$. Hence, $R$ is transitive. We will use mathematical induction to prove the only if part of the theorem. Note that this part of the theorem is trivially true for $n = 1$. Assume that $R^n \subseteq R$, where $n$ is a positive integer. This is the inductive hypothesis. To complete the inductive step, we must show that this implies that $R^{n+1}$ is also a subset of $R$. To show this, assume that $(a, b) \in R^{n+1}$. Then, because $R^{n+1} = R^n \circ R$, there is an element $x$ with $x \in A$ such that $(a, x) \in R$ and $(x, b) \in R^n$. The inductive hypothesis, namely, that $R^n \subseteq R$, implies that $(x, b) \in R$. Furthermore, because *R* is transitive, and $(a, x) \in R$ and $(x, b) \in R$, it follows that $(a, b) \in R$. This shows that $R^{n+1} \subseteq R$, completing the proof.

Inverse relation: Let $R$ be a relation from a set $A$ to a set $B$. The inverse relation of $R$ is a relation from $B$ to $A$, denoted by $R^{-1}$, given by the set $\{(b, a) \mid (a, b) \in R\}$. The complementary relation $\bar{R}$ is the set of ordered pairs $\{(a, b) \mid (a, b) \notin R\}$.

**Example:** Let $R = \{(a, b) \mid a < b\}$ be the relation on the set of integers. Then the inverse relation of

$$R^{-1} = \{(b, a) | (a, b) \in R\} = \{(b, a) | a < b\} = \{(b, a) | b > a\}.$$

And the complementary relation of $R$

$$\bar{R} = \{(a, b) | (a, b) \notin R\} = \{(a, b) | a \not< b\} = \{(a, b) | a \geq b\}.$$

**Example**: Let $R = \{(a, b) \mid a \text{ divides } b\}$ be the relation on the set of positive integers. Then

$$R^{-1} = \{(b, a) | (a, b) \in R\} = \{(b, a) | a \text{ divides } b\} = \{(b, a) |\ b \text{ is divisible } by\ a\}.$$

And

$$\bar{R} = \{(a, b) | (a, b) \notin R\} = \{(a, b) |\ a \text{ does not divides } b\}.$$

**Example:** Let $R$ *and* $S$ be the relations with $R \subseteq S$, then $R^{-1} \subseteq S^{-1}$.

**Example**: Let $R$ *and* $S$ be two relations, then $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$, $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$ and $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

**Example:** On a set of $n$ elements the number of reflexive relations is $2^{n(n-1)}$, number of symmetric relation is $2^{\frac{n(n+1)}{2}}$ and the number of reflexive and symmetric relations is $2^{\frac{n(n-1)}{2}}$.

## Representing Relations Using Matrices

A relation between finite sets can be represented using a zero–one matrix. Suppose that $R$ is a relation from $A = \{a_1, a_2, \ldots, a_m\}$ to $B = \{b_1, b_2, \ldots, b_n\}$. The relation *R* can be represented by the matrix $\boldsymbol{M}_R = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

In other words, the zero–one matrix representing $R$ has a 1 as its $(i, j)$ entry when $a_i$ is related to $b_j$, and a 0 in this position if $a_i$ is not related to $b_j$. (Such a representation depends on the orderings used for *A* and *B*.)

**Example:** Suppose that $A = \{1, 2, 3\}$ and $B = \{1, 2\}$. Let $R$ be the relation from $A$ to $B$ containing $(a, b)$ if $a > b$. What is the matrix representing $R$ ?

*Solution:* Because $R = \{(2, 1), (3, 1), (3, 2)\}$, the matrix for *R* is

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

**Example:** Let $A = \{a_1, a_2, a_3\}$ *and* $B = \{b_1, b_2, b_3, b_4, b_5\}$. Which ordered pairs are in the relation *R* represented by the matrix

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}?$$

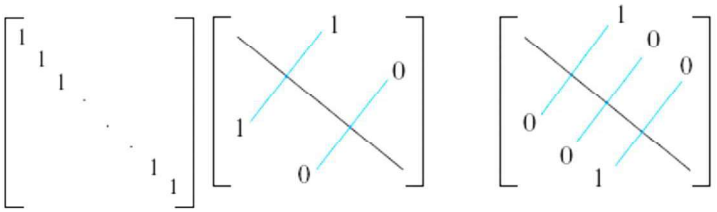
*Solution:* Because $R$ consists of those ordered pairs $(a_i, b_j)$ with $m_{ij} = 1$, it follows that $R = \{(a_1, b_2), (a_2, b_1), (a2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}$.

The matrix of a relation on a set, which is a square matrix, can be used to determine whether the relation has certain properties. Recall that a relation $R$ on $A$ is reflexive if $(a, a) \in R$ whenever $a \in A$. Thus, $R$ is reflexive if and only if $(a_i, a_i) \in R$ for $i = 1, 2, \ldots, n$. Hence, $R$ is reflexive if and only if $m_{ii} = 1$, for $i = 1, 2, \ldots, n$. In other words, $R$ is reflexive if all the elements

on the main diagonal of $M_R$ are equal to 1. Note that the elements off the main diagonal can be either 0 or 1.

The relation $R$ is symmetric if $(a, b) \in R$ implies that $(b, a) \in R$. Consequently, the relation $R$ on the set $A = \{a_1, a_2, \ldots, a_n\}$ is symmetric if and only if $(a_j, a_i) \in R$ whenever $(a_i, a_j) \in R$. In terms of the entries of $M_R$, $R$ is symmetric if and only if $m_{ji} = 1$ whenever $m_{ij} = 1$. This also means $m_{ji} = 0$ whenever $m_{ij} = 0$. Consequently, $R$ is symmetric if and only if $m_{ij} = m_{ji}$, for all pairs of integers $i$ and $j$ with $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n$. Recalling the definition of the transpose of a matrix, we see that $R$ is symmetric if and only if $M_R = M_R^T$ that is, if $M_R$ is a symmetric matrix.

The relation $R$ is antisymmetric if and only if $(a, b) \in R$ and $(b, a) \in R$ imply that $a = b$. Consequently, the matrix of an antisymmetric relation has the property that if $m_{ij} = 1$ with $i \neq j$, then $m_{ji} = 0$. Also, it may be both $m_{ij} = 0$ and $m_{ji} = 0$. In other words, $m_{ij} = 0$ or $m_{ji} = 0$ when $i \neq j$.



**Example:** Suppose that the relation $R$ on a set is represented by the matrix $M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. Is $R$ reflexive, symmetric, and/or antisymmetric?

*Solution:* Because all the diagonal elements of this matrix are equal to 1, $R$ is reflexive. Moreover, because $M_R$ is symmetric, it follows that *R* is symmetric. It is also easy to see that *R* is not antisymmetric as $m_{12} = 1 = m_{21}$.

A matrix all of whose entries are either 0 or 1 is called a **zero–one matrix**. Zero–one matrices are often used to represent discrete structures. Algorithms using these structures are based on Boolean arithmetic with zero–one matrices. This arithmetic is based on the Boolean operations $\wedge$ and $\vee$, which operate on pairs of bits, defined by

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

and

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

**Definition:** Let $A = [a_{ij}]$ and $B = [b_{ij}]$ are two $m \times n$ zero–one matrices. Then the *join* of $A$ and $B$ is the zero–one matrix with $(i,j)$th entry $a_{ij} \vee b_{ij}$. The join of $A$ and $B$ is denoted by $A \vee B$. The *meet* of $A$ and $B$ is the zero–one matrix with $(i,j)$th entry $a_{ij} \wedge b_{ij}$. The meet of $A$ and $B$ is denoted by $A \wedge B$.

**Example:** Find the join and meet of the zero–one matrices

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \text{ and } A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

*Solution:* We find that the join of $A$ and $B$ is

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

and the meet of $A$ and $B$ is

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

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

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

**Example:** Find the Boolean product of $A$ and $B$, where

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

*Solution:* The Boolean product $A \odot B$ is given by

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

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

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

Hence

$$A^{[r]} = A \odot A \odot A \odot \cdot \cdot \cdot \odot A \text{ , } r \text{ times}$$

(This is well defined because the Boolean product of matrices is associative.) We also define $A^{[0]}$ to be the identity matrix $I_n$.

The Boolean operations join and meet can be used to find the matrices representing the union and the intersection of two relations. Suppose that $R_1$ and $R_2$ are relations on a set $A$ represented by the matrices $M_{R_1}$ and $M_{R_2}$ , respectively. The matrix representing the inverse, union and intersection of these relations are

$$M_{R_1^{-1}} = \left(M_{R_1}\right)^T, \; M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} \text{ and } M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}.$$

We now turn our attention to determining the matrix for the composite of relations. This matrix can be found using the Boolean product of the matrices for these relations. In particular, suppose that $R$ is a relation from $A$ to $B$ and $S$ is a relation from $B$ to $C$. Suppose that $A, B$, and $C$ have $m, n$, and $p$ elements, respectively. Let the zero–one matrices for $S \circ R$, $R$, and $S$ be $M_{S \circ R} = [t_{ij}]$, $M_R = [r_{ij}]$, and $M_S = [s_{ij}]$, respectively (these matrices have sizes $m \times p$, $m \times n$, and $n \times p$, respectively). The ordered pair $(a_i, c_j)$ belongs to $S \circ R$ if and only if there is an element $b_k$ such that $(a_i, b_k)$ belongs to *R* and $(b_k, c_j)$ belongs to *S*. It follows that $t_{ij} = 1$ if and only if $r_{ik} = s_{kj} = 1$ for some $k$. From the definition of the Boolean product, this means that

$$M_{S \circ R} = M_R \odot M_S.$$

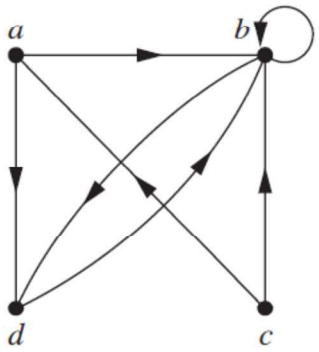
**Note:** We have $M_{R^n} = M_R \odot M_R \odot \cdots \odot M_R = M_R^{[n]}$.

## Representing Relations Using Digraphs

**Definition:** A *directed graph*, or *digraph*, consists of a set $V$ of *vertices* (or *nodes*) together with a set $E$ of ordered pairs of elements of $V$ called *edges* (or *arcs*). The vertex $a$ is called the *initial*

*vertex* of the edge $(a, b)$, and the vertex $b$ is called the *terminal vertex* of this edge. An edge of the form $(a, a)$ is represented using an arc from the vertex $a$ back to itself. Such an edge is called a **loop**.

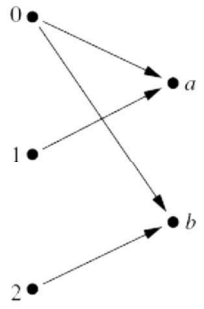
**Example:** The directed graph with vertices $\{a, b, c, d\}$, and edges $\{(a, b), (a, d), (b, b), (b, d), (c, a), (c, b), (d, b)\}$ is displayed below:



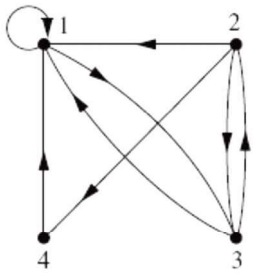

The relation $R$ on a set $A$ is represented by the directed graph that has the elements of $A$ as its vertices and the ordered pairs $(a, b)$, where $(a, b) \in R$, as edges. This assignment sets up a one-to-one correspondence between the relations on a set $A$ and the directed graphs with $A$ as their set of vertices. Thus, every statement about relations corresponds to a statement about directed graphs, and vice versa. Directed graphs give a visual display of information about relations. As such, they are often used to study relations and their properties.

Note that relations from a set $A$ to a set $B$ can be represented by a directed graph where there is a vertex for each element of $A$ and a vertex for each element of $B$. However, when *A* = *B*, such representation provides much less insight than the digraph representations described here.

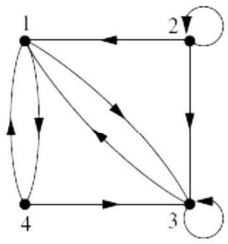
**Example:** Let $A = \{0, 1, 2\}$ and $B = \{a, b\}$. $R = \{(0, a), (0, b), (1, a), (2, b)\}$ is a relation from $A$ to $B$. This Relation can be represented graphically,



**Example:** The directed graph of the relation $R = \{(1,1),(1,3),(2,1),(2,3),(2,4),(3,1),(3,2),(4,1)\}$ on the set $\{1,2,3,4\}$ is shown bellow:

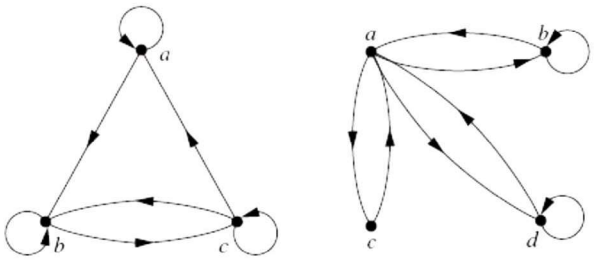



**Example:** What are the ordered pairs in the relation $R$ represented by the directed graph shown in the bellow figure?




*Solution:* The ordered pairs $(x,y)$ in the relation are $R = \{(1,3),(1,4),(2,1),(2,2),(2,3),(3,1),(3,3),(4,1),(4,3)\}$. Each of these pairs corresponds to an edge of the directed graph, with $(2,2)$ and $(3,3)$ corresponding to loops.

**Example:** Determine whether the relations for the directed graphs shown in bellow Figure are reflexive, symmetric, antisymmetric, and/or transitive.



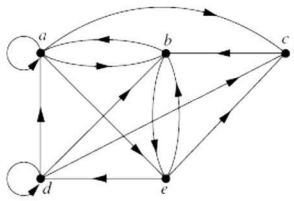

(a) Directed graph of $R$ (b) Directed graph of $S$

*Solution:* Because there are loops at every vertex of the directed graph of $R$, it is reflexive. $R$ is neither symmetric nor antisymmetric because there is an edge from $a$ to $b$ but not one from $b$ to $a$, but there are edges in both directions connecting $b$ and $c$. Finally, $R$ is not transitive because there is an edge from $a$ to $b$ and an edge from $b$ to $c$, but no edge from $a$ to $c$.

Because loops are not present at all the vertices of the directed graph of $S$, this relation is not reflexive. It is symmetric but not antisymmetric, because every edge between distinct vertices is accompanied by an edge in the opposite direction. It is also not hard to see from the directed graph that $S$ is not transitive, because $(c, a)$ and $(a, b)$ belong to $S$, but $(c, b)$ does not belong to $S$.

Paths in Directed Graphs: A *path* from $a$ to $b$ in the directed graph $G$ is a sequence of edges $(x_0, x_1), (x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n)$ in *G*, where $n$ is a nonnegative integer, and $x_0 = a$ and $x_n = b$, that is, a sequence of edges where the terminal vertex of an edge is the same as the initial vertex in the next edge in the path. This path is denoted by $x_0, x_1, x_2, \ldots, x_{n-1}, x_n$ and has *length* $n$. We view the empty set of edges as a path of length zero from $a$ to $a$. A path of length $n \geq 1$ that begins and ends at the same vertex is called a *circuit* or *cycle*.

**Example:** Which of the following are paths in the directed graph shown in the bellow figure: (i) $a, b, e, d$; (ii) $a, e, c, d, b$; (iii) $b, a, c, b, a, a, b$; (iv) $d, c$; (v) $c, b, a$; (vi) $e, b, a, b, a, b, e$? What are the lengths of those that are paths? Which of the paths in this list are circuits?




*Solution:* (i) Because each of $(a, b)$, $(b, e)$, and $(e, d)$ is an edge, $a, b, e, d$ is a path of length three. (ii) Because $(c, d)$ is not an edge, $a, e, c, d, b$ is not a path. (iii) Also, $b, a, c, b, a, a, b$ is a path of length six because $(b, a)$, $(a, c)$, $(c, b)$, $(b, a)$, $(a, a)$, and $(a, b)$ are all edges. (iv) We see that $d, c$ is a path of length one, because $(d, c)$ is an edge. (v) Also $c, b, a$ is a path of length two, because $(c, b)$ and $(b, a)$ are edges. (vi) All of $(e, b)$, $(b, a)$, $(a, b)$, $(b, a)$, $(a, b)$, and $(b, e)$ are edges, so $e, b, a, b, a, b, e$ is a path of length six. The two paths $b, a, c, b, a, a, b$ and $e, b, a, b, a, b, e$ are circuits because they begin and end at the same vertex. The paths $a, b, e, d$; $c, b, a$; and $d, c$ are not circuits.

**Theorem:** Let $R$ be a relation on a set $A$. Then $(a, b) \in R^n$ if and only if there is a path of length $n$ from $a$ to $b$, where $n$ is a positive integer.

***Proof:*** We will use mathematical induction. By definition, there is a path from $a$ to $b$ of length one if and only if $(a, b) \in R$, so the theorem is true when $n = 1$. Assume that the theorem is true for the positive integer $n$. This is the inductive hypothesis. There is a path of length $n + 1$ from $a$ to $b$ if and only if there is an element $c \in A$ such that there is a path of length one from $a$ to $c$, so $(a, c) \in R$, and a path of length $n$ from $c$ to $b$, that is, $(c, b) \in R^n$. Consequently, by the inductive hypothesis, there is a path of length $n + 1$ from $a$ to $b$ if and only if there is an element $c$ with $(a, c) \in R$ and $(c, b) \in R^n$. But there is such an element if and only if $(a, b) \in R^{n+1}$. Therefore, there is a path of length $n + 1$ from $a$ to $b$ if and only if $(a, b) \in R^{n+1}$. This completes the proof.

## Closures of Relations

A computer network has data centers in Boston, Chicago, Denver, Detroit, New York, and San Diego. There are direct, one-way telephone lines from Boston to Chicago, from Boston to Detroit, from Chicago to Detroit, from Detroit to Denver, and from New York to San Diego. Let $R$ be the relation containing $(a, b)$ if there is a telephone line from the data center in $a$ *to* that in $b$. How can we determine if there is some (possibly indirect) link composed of one or more telephone lines from one center to another? Because not all links are direct, such as the link from Boston to Denver that goes through Detroit, $R$ cannot be used directly to answer this. In the language of relations, $R$ is not transitive, so it does not contain all the pairs that can be linked. As we will show, we can find all pairs of data centers that have a link by constructing a transitive relation $S$ containing $R$ such that $S$ is a subset of every transitive relation containing $R$. Here, $S$ is the smallest transitive relation that contains $R$. This relation is called the transitive closure of $R$. In general, let $R$ be a relation on a set $A$ and $R$ may or may not have some property $\boldsymbol{P}$, such as reflexivity, symmetry, or transitivity. If there is a relation $S$ with property $\boldsymbol{P}$ containing $R$ such that $S$ is a subset of every relation with property $\boldsymbol{P}$ containing $R$, then $S$ is called the **closure** of $R$ with respect to $\boldsymbol{P}$. (Note that the closure of a relation with respect to a property may not exist.) We will show how reflexive, symmetric, and transitive closures of relations can be found.

The relation $R = \{(1,1),(1,2),(2,1),(3,2)\}$ on the set $A = \{1,2,3\}$ is not reflexive. How can we produce a reflexive relation containing $R$ that is as small as possible? This can be done by adding $(2,2)$ and $(3,3)$ to $R$, because these are the only pairs of the form $(a,a)$ that are not in $R$. Clearly, this new relation contains $R$. Furthermore, *any* reflexive relation that contains $R$ must also contain $(2,2)$ and $(3,3)$. Because this relation contains $R$, is reflexive, and is contained within every reflexive relation that contains $R$, it is called the **reflexive closure** of $R$.

Reflexive closure: Let $R$ be a relation on a set $A$ and $S$ is reflexive closure of $R$. Then $S$ is a reflexive relation containing $R$ and if $T$ is a reflexive relation containing $R$ then, $S \subseteq T$. The reflexive closure of $R$ can be formed by adding all pairs of the form $(a,a)$ with $a \in A$ to $R$. The addition of these pairs produces a new relation that is reflexive, contains $R$, and is contained within any reflexive relation containing $R$. We see that the reflexive closure of $R$ equals $R \cup \Delta$, where $\Delta = \{(a,a) \mid a \in A\}$ the diagonal relation on $A$.

**Example:** What is the reflexive closure of the relation $R = \{(a,b) \mid a < b\}$ on the set of integers?

*Solution:* The reflexive closure of *R* is

$$R \cup \Delta = \{(a,b) \mid a < b\} \cup \{(a,a) \mid a \in \boldsymbol{Z}\} = \{(a,b) \mid a \leq b\}.$$

The relation $\{(1,1),(1,2),(2,2),(2,3),(3,1),(3,2)\}$ on $\{1,2,3\}$ is not symmetric. How can we produce a symmetric relation that is as small as possible and contains $R$ ? To do this, we need only add $(2,1)$ and $(1,3)$, because these are the only pairs of the form $(b,a)$ with $(a,b) \in R$ that are not in $R$. This new relation is symmetric and contains $R$. Furthermore, *any* symmetric relation that contains $R$ must contain this new relation, because a symmetric relation that contains $R$ must contain $(2,1)$ and $(1,3)$. Consequently, this new relation is called the **symmetric closure** of $R$.

Symmetric closure: Let $R$ be a relation on a set $A$ and $S$ is symmetric closure of $R$. Then $S$ is a symmetric relation containing $R$ and if $T$ is a symmetric relation containing $R$ then, $S \subseteq T$. The symmetric closure of a relation $R$ can be constructed by adding all ordered pairs of the form $(b,a)$, where $(a,b)$ is in the relation, that are not already present in $R$. Adding these pairs produces a relation that is symmetric, that contains $R$, and that is contained in any symmetric

relation that contains $R$. The symmetric closure of a relation can be constructed by taking the union of a relation with its inverse that is, $R \cup R^{-1}$ is the symmetric closure of $R$, where $R^{-1} = \{(b,a) \mid (a,b) \in R\}$.

**Example:** What is the symmetric closure of the relation $R = \{(a,b) \mid a > b\}$ on the set of positive integers?

*Solution:* The symmetric closure of *R* is the relation

$$R \cup R^{-1} = \{(a,b) \mid a > b\} \cup \{(b,a) \mid a > b\} = \{(a,b) \mid a \neq b\}.$$

This last equality follows because *R* contains all ordered pairs of positive integers where the first element is greater than the second element and *R*−1 contains all ordered pairs of positive integers where the first element is less than the second.

Transitive closures: Suppose that a relation $R$ is not transitive. How can we produce a transitive relation that contains *R* such that this new relation is contained within any transitive relation that contains *R*? Can the transitive closure of a relation $R$ be produced by adding all the pairs of the form $(a,c)$, where $(a,b)$ and $(b,c)$ are already in the relation?

Consider the relation $R = \{(1,3),(1,4),(2,1),(3,2)\}$ on the set $\{1,2,3,4\}$. This relation is not transitive because it does not contain $(3,1)$ where $(3,2)$ and $(2,1)$ are in $R$. The pairs of this form not in $R$ are $(1,2)$, $(2,3)$, $(2,4)$, and $(3,1)$. Adding these pairs does *not* produce a transitive relation, because the resulting relation contains $(3,1)$ and $(1,4)$ but does not contain $(3,4)$. This shows that constructing the transitive closure of a relation is more complicated than constructing either the reflexive or symmetric closure.

**Definition:** Let $R$ be a relation on a set $A$. The *connectivity relation* $R^*$ consists of the pairs $(a,b)$ such that there is a path of length at least one from $a$ to $b$ in $R$.

Because $R^n$ consists of the pairs $(a,b)$ such that there is a path of length $n$ from $a$ to $b$, it follows that $R^*$ is the union of all the sets $R^n$. In other words,

$$R^* = \bigcup_{n=1}^{\infty} R^n.$$

**Theorem:** The transitive closure of a relation *R* equals the connectivity relation $R^*$.

Now that we know that the transitive closure equals the connectivity relation, we turn our attention to the problem of computing this relation. We do not need to examine arbitrarily long paths to determine whether there is a path between two vertices in a finite directed graph. As the following theorem shows, it is sufficient to examine paths containing no more than $n$ edges, where $n$ is the number of elements in the set.

**Theorem:** Let $R$ be a relation on a set $A$ with $n$ elements. If there is a path of length at least one in $R$ from $a$ to $b$, then there is such a path with length not exceeding $n$. Moreover, when $a \neq b$, if there is a path of length at least one in $R$ from $a$ to $b$, then there is such a path with length not exceeding $n - 1$.

From above theorem, we see that the transitive closure of $R$ is the union of $R, R^2, R^3, \ldots$, and $R^n$. This follows because there is a path in $R^*$ between two vertices if and only if there is a path between these vertices in $R^i$, for some positive integer $i$ with $i \leq n$. Because

$$R^* = R \cup R^2 \cup R^3 \cup \cdots \cup R^n$$

and the zero–one matrix representing a union of relations is the join of the zero–one matrices of these relations, the zero–one matrix for the transitive closure is the join of the zero–one matrices of the first $n$ powers of the zero–one matrix of $R$.

**Theorem:** Let $M_R$ be the zero–one matrix of the relation $R$ on a set with *n* elements. Then the zero–one matrix of the transitive closure $R^*$ is

$$M_{R^*} = M_R \vee M_{R^2} \vee M_{R^3} \vee \cdots \vee M_{R^n} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \cdots \vee M_R^{[n]}.$$

**Example:** Find the zero–one matrix of the transitive closure of the relation $R$ where

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

*Solution:* The zero–one matrix of the transitive closure $R^*$ is

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]}.$$

Because $M_R^{[2]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ and $M_R^{[3]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$, it follows that

$$M_{R^*} = \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 1 & 0\end{bmatrix} \vee \begin{bmatrix}1 & 1 & 1\\ 0 & 1 & 0\\ 1 & 1 & 1\end{bmatrix} \vee \begin{bmatrix}1 & 1 & 1\\ 0 & 1 & 0\\ 1 & 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 0 & 1 & 0\\ 1 & 1 & 1\end{bmatrix}.$$

Warshall's Algorithm: Warshall's algorithm, named after Stephen Warshall, who described it in 1960, is an efficient method for computing the transitive closure of a relation.

**Lemma:** Let $W_k = [w_{ij}^{[k]}]$ be the zero–one matrix that has a 1 in its $(i, j)$th position if and only if there is a path from $v_i$ to $v_j$ with interior vertices from the set $\{v_1, v_2, \ldots, v_k\}$. Then

$$w_{ij}^{[k]} = w_{ij}^{[k-1]} \vee (w_{ik}^{[k-1]} \wedge w_{kj}^{[k-1]}),$$

whenever $i, j$ , and $k$ are positive integers not exceeding *n*.

Warshall's algorithm computes $M_{R^*}$ by efficiently computing $W_0 = M_R, W_1, W_2, \ldots, W_n = M_{R^*}$.

**Example:** Let $A = \{a_1, a_2\ a_3, a_4, a_5\}$ and $R$ be a relation on $A$ given by $R = \{(a_1, a_1), (a_1, a_2), (a_1, a_4), (a_2, a_3), (a_3, a_3), (a_3, a_5), (a_4, a_4), (a_5, a_2)\}$. Find the transitive closure of R using Warshall's algorithm.

*Solution:* The matrix of the relation $R$ $$M_R = \begin{bmatrix}1 & 1 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 0\end{bmatrix}.$$

**Step 1**. We set $W_0 = M_R$ , i.e.,

$$W_0 = \begin{bmatrix}1 & 1 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 0\end{bmatrix}.$$

**Step 2.** Construct $W_1$. First transfer all 1's of $W_0$to $W_1$

$$W_1 = \begin{bmatrix} 1 & 1 & & 1 & \\ & & 1 & & \\ & & 1 & & 1 \\ & & & 1 & \\ & 1 & & & \end{bmatrix}.$$

In column 1 of $W_0$: Nonzero entry at position 1. In row 1 of $W_0$: Nonzero entry at positions 1,2 and 4. Thus, at the position $(1,1)$, $(1,2)$, and $(1,4)$ of $W_1$make the entries 1. Therefore

$$W_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

**Step 3.** Construct $W_2$. First transfer all 1's of $W_1$to $W_2$

$$W_2 = \begin{bmatrix} 1 & 1 & & 1 & \\ & & 1 & & \\ & & 1 & & 1 \\ & & & 1 & \\ & 1 & & & \end{bmatrix}.$$

In column 2 of $W_1$: Nonzero entry at positions 1 and 5. In row 2 of $W_1$: Nonzero entry at position 3. Thus at the position (1, 3), and (5, 3) of $W_2$ make the entries 1. Therefore

$$W_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

**Step 4.** Construct $W_3$.

$$W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Step 5. Construct $W_4$.

$$W_4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Step 6. Construct $W_5$.

$$W_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

From $W_5$, we can conclude that the transitive closure of R is:

$$R^* = \{(a_1, a_1), (a_1, a_2), (a_1, a_3), (a_1, a_4), (a_1, a_5), (a_2, a_2), (a_2, a_3), (a_2, a_5),$$
$$(a_3, a_2)(a_3, a_3), (a_3, a_5), (a_4, a_4), (a_5, a_2), (a_5, a_3), (a_5, a_5)\}.$$

**Example:** Let $R = \{(a, c), (b, d), (c, a), (d, b), (e, d)\}$ be a relation on the set $A = \{a, b, c, d, e, f\}$. Check whether $R$ is reflexive, symmetric, antisymmetric or transitive. Find reflexive, symmetric and Transitive closure of $R$. Use Warshall's algorithm to find the transitive closuer.

**Solution:** Given that $A = \{a, b, c, d, e, f\}$ and $R = \{(a, c), (b, d), (c, a), (d, b), (e, d)\}$ is a relation on $A$.

(i) $R$ is not reflexive as $(a, a) \notin R$.

(ii) $R$ is not symmetric as $(e, d) \in R$, but $(d, e) \notin R$.

(iii) $R$ is not antisymmetric as $(a, c) \in R$ and $(c, a) \in R$ but $a \neq c$.

(iv) $R$ is not transitive as $(a, c) \in R$ and $(c, a) \in R$ but $(a, a) \notin R$.

(v) Reflexive closure of $R$ is $R \cup \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f)\}$
= $\{(a, c), (b, d), (c, a), (d, b), (e, d), (a, a), (b, b), (c, c), (d, d), (e, e), (f, f)\}$.

(vi) Symmetric closure of $R$ is $R \cup R^{-1} = \{(a, c), (b, d), (c, a), (d, b), (e, d), (d, e)\}$

For Transitive closure we use Warshall's algorithm.

The matrix of the relation $R$ $$M_R = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Step 1. We set $W_0 = M_R$ , i.e. ,

$$W_0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Step 2. Construct $W_1$. First transfer all 1's of $W_0$to $W_1$

$$W_1 = \begin{bmatrix} & & 1 & & \\ & & & 1 & \\ 1 & & & & \\ & 1 & & & \\ & & & 1 & \end{bmatrix}.$$

In column 1 of $W_0$: Nonzero entry at position 3.

In row 1 of $W_0$: Nonzero entry at position 3.

So, at the position (3, 3) of $W_1$make the entries 1. Rest are zero. Therefore

$$W_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Step 3. Construct $W_2$. First transfer all 1's of $W_1$to $W_2$

In column 2 of $W_1$: Nonzero entry at position 4.

In row 2 of $W_1$: Nonzero entry at position 4

So, at the position $(4,4)$ of $W_2$ make the entries 1. Rest are zero. Therefore

$$W_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Similarly

Step 4. Construct $W_3$.

$$W_3 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Step 5. Construct $W_4$.

$$W_4 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Step 6. Construct $W_5$.

$$W_5 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

From $W_5$, we can conclude that the transitive closure of R is:

$$\{(a,a),(a,c),(b,b),(b,d),(c,a),(c,c),(d,b),(d,d),(e,b),(e,d)\}.$$

## Equivalence Relations

**Definition:** A relation on a set $A$ is called an *equivalence relation* if it is reflexive, symmetric, and transitive. Two elements $a$ and $b$ that are related by an equivalence relation are called *equivalent*. The notation $a \sim b$ is often used to denote that $a$ and $b$ are equivalent elements with respect to a particular equivalence relation.

**Example:** Let $R$ be the relation on the set of integers such that $(a,b) \in R$ if and only if $a = b$ or $a = -b$. Then $R$ is reflexive, symmetric, and transitive. It follows that $R$ is an equivalence relation.

**Example:** Let $R$ be the relation on the set of real numbers such that $(a,b) \in R$ if and only if $a - b$ is an integer. Is $R$ an equivalence relation?

Solution: Because $a - a = 0$ is an integer for all real numbers $a$, $(a,a) \in R$ for all real numbers $a$. Hence, $R$ is reflexive. Now suppose that $(a,b) \in R$ . Then $a - b$ is an integer, so $b - a$ is also an integer. Hence, $(b,a) \in R$. It follows that $R$ is symmetric. If $(a,b) \in R$ and $(b,a) \in R$ , then $a - b$ and $b - c$ are integers. Therefore, $a - c = (a - b) + (b - c)$ is also an integer. Hence, $(a,c) \in R$. Thus, $R$ is transitive. Consequently, *R* is an equivalence relation.

**Example: Congruence Modulo $m$.** Let $m$ be an integer with $m > 1$. Show that the relation $R = \{(a,b) \mid a \equiv b \pmod{m}\}$ is an equivalence relation on the set of integers.

*Solution:* We know that $a \equiv b \pmod{m}$ if and only if $m$ divides $a - b$. Note that $a - a = 0$ is divisible by $m$, because $0 = 0 \cdot m$. Hence, $a \equiv a \pmod{m}$, i.e. $(a, a) \in R$. So, congruence modulo $m$ is reflexive. Let $(a, b) \in R$. So, $a \equiv b \pmod{m}$. Then $a - b$ is divisible by $m$, so $a - b = km$, where $k$ is an integer. It follows that $b - a = (-k)m$, so $b \equiv a \pmod{m}$. Thus, $(b, a) \in R$, hence, congruence modulo $m$ is symmetric. Next, suppose $(a, b), (b, c) \in R$. That is $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then $m$ divides both $a - b$ and $b - c$. Therefore, there are integers $k$ and $l$ with $a - b = km$ and $b - c = lm$. Adding these two equations shows that $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Thus, $a \equiv c \pmod{m}$. Thus, $(a, c) \in R$. Therefore, congruence modulo $m$ is transitive. It follows that congruence modulo $m$ is an equivalence relation.

**Example:** Show that the "divides" relation on the set of positive integers is not an equivalence relation.

**Example:** Let $R$ be the relation on the set of real numbers such that $(x, y) \in R$ if and only if $x$ and $y$ are real numbers that differ by less than 1, that is $|x - y| < 1$. Showthat $R$ is not an equivalence relation.

**Example:** Let $R$ be a reflexive relation on a set $A$ such that

$$(a, b) \in R, (a, c) \in R \Longrightarrow (b, c) \in R.$$

Show that $R$ is an equivalence relation.

## Equivalence Classes and Partitions

Equivalence Classes: Let $R$ be an equivalence relation on a set $A$. The set of all elements that are related to an element $a$ of $A$ is called the *equivalence class* of $a$. The equivalence class of $a$ with respect to $R$ is denoted by $[a]_R$. When only one relation is under consideration, we may not use the subscript $R$ and write $[a]$ for this equivalence class. In other words, if $R$ is an equivalence relation on a set $A$, the equivalence class of the element $a$ is $[a]_R = \{x \in A \mid (a, x) \in R\}$. If $b \in [a]_R$, then $b$ is called a **representative** of this equivalence class. Any element of a class can be used as a representative of this class. That is, there is nothing special about the particular element chosen as the representative of the class.

**Example:** What are the equivalence classes of $0$ and $1$ for congruence modulo $4$?

*Solution:* The equivalence class of $0$ contains all integers $a$ such that $a \equiv 0 \pmod 4$. The integers in this class are those divisible by $4$. Hence, the equivalence class of $0$ for this relation is

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}.$$

The equivalence class of 1 contains all the integers $a$ such that $a \equiv 1 \pmod 4$. The integers in this class are those that have a remainder of 1 when divided by 4. Hence, the equivalence class of 1 for this relation is

$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}.$$

**Example:** Suppose that $R$ is the relation on the set of strings of English letters such that $a\ R\ b$ if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string $x$. Is $R$ an equivalence relation?

**Example:** Let $n$ be a positive integer and $S$ a set of strings. Suppose that $R_n$ is the relation on $S$ such that $s\ R_n\ t$ if and only if $s = t$, or both $s$ and $t$ have at least $n$ characters and the first $n$ characters of $s$ and $t$ are the same. That is, a string of fewer than $n + 1$ characters is related only to itself; a string $s$ with at least $n + 1$ characters is related to a string $t$ if and only if $t$ has at least $n$ characters and $t$ begins with the $n$ characters at the start of $s$. For example, let $n = 3$ and let $S$ be the set of all bit strings. Then $s\ R_3\ t$ either when $s = t$ or both $s$ and $t$ are bit strings of length $3$ or more that begin with the same three bits. For instance, $01\ R_3\ 01$ and $00111\ R_3\ 00101$, but not $01\ R_3\ 010$, and $01011\ R_3\ 01110$. Then for every set of strings $S$ and every positive integer $n$, $R_n$ is an equivalence relation on *S*.

**Example:** What is the equivalence class of the string $0111$ with respect to the equivalence relation $R_3$ on the set of all bit strings?

*Solution:* The bit strings equivalent to $0111$ are the bit strings with at least three bits that begin with $011$. These are the bit strings $011, 0110, 0111, 01100, 01101, 01110, 01111$, and so on. Consequently,

$$[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \ldots\}.$$

Let $A$ be the set of students at your school who are majoring in exactly one subject, and let $R$ be the relation on $A$ consisting of pairs $(x, y)$, where $x$ and $y$ are students with the same major.

Then $R$ is an equivalence relation, as the reader should verify. We can see that $R$ splits all students in $A$ into a collection of disjoint subsets, where each subset contains students with a specified major. For instance, one subset contains all students majoring (just) in computer science and a second subset contains all students majoring in history. Furthermore, these subsets are equivalence classes of $R$. This example illustrates how the equivalence classes of an equivalence relation partition a set into disjoint, nonempty subsets. We will make these notions more precise in the following discussion.

Let $R$ be a relation on the set $A$. The following theorem shows that the equivalence classes of two elements of $A$ are either identical or disjoint.

**Theorem:** Let $R$ be an equivalence relation on a set $A$. These statements for elements $a$ and $b$ of $A$ are equivalent:

(i) $(a, b) \in R$ (ii) $[a] = [b]$ (iii) $[a] \cap [b] \neq \emptyset$.

***Proof:*** We first show that (i) implies (ii). Assume that $(a, b) \in R$. We will prove that $[a] = [b]$ by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a]$. Then $(a, c) \in R$. Because $(a, b) \in R$ and $R$ is symmetric, $(b, a) \in R$. Furthermore, because *R* is transitive and $(b, a) \in R$ and $(a, c) \in R$, it follows that $(b, c) \in R$. Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar.

Second, we will show that (ii) implies (iii). Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (because $a \in [a]$ because $_R$ is reflexive).

Next, we will show that (iii) implies (i). Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element $c$ with $c \in [a]$ and $c \in [b]$. In other words, $(a, c) \in R$ and $(b, c) \in R$. By the symmetric property, $(c, b) \in R$. Then by transitivity, because $(a, c) \in R$ and $(c, b) \in R$, we have $(a, b) \in R$. Because (i) implies (ii), (ii) implies (iii), and (iii) implies (i), the three statements, (i), (ii), and (iii) are equivalent.

Partition of a set: A partition of a set $S$ is a collection of disjoint nonempty subsets of $S$ that have $S$ as their union.

**Example:** Suppose that $S = \{1, 2, 3, 4, 5, 6\}$. The collection of sets $A_1 = \{1, 2, 3\}, A_2 = \{4, 5\}$, and $A_3 = \{6\}$ forms a partition of *S*, because these sets are disjoint and their union is *S*.

We are now in a position to show how an equivalence relation gives a partition of a set. Let $R$ be an equivalence relation on a set $A$. The union of the equivalence classes of $R$ is all of $A$, because an element $a$ of $A$ is in its own equivalence class, namely, $[a]_R$. In other words,

$$\bigcup_{a \in A} [a]_R = A.$$

In addition, these equivalence classes are either equal or disjoint, so $[a]_R \cap [b]_R = \emptyset$, when $[a]_R \neq [b]_R$. These two observations show that the equivalence classes form a partition of $A$, because they split $A$ into disjoint subsets.

**Theorem:** Let $R$ be an equivalence relation on a set $S$. Then the equivalence classes of $R$ form a partition of $S$. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set $S$, there is an equivalence relation $R$ that has the sets $A_i, i \in I$, as its equivalence classes.

**Example:** List the ordered pairs in the equivalence relation $R$ produced by the partition $A_1 = \{1, 2, 3\}, A_2 = \{4, 5\}$, and $A_3 = \{6\}$ of $S = \{1, 2, 3, 4, 5, 6\}$.

*Solution:* The subsets in the partition are the equivalence classes of $R$. The pair $(a, b) \in R$ if and only if $a$ and $b$ are in the same subset of the partition. The pairs $(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2)$, and $(3, 3)$ belong to $R$ because $A_1 = \{1, 2, 3\}$ is an equivalence class; the pairs $(4, 4), (4, 5), (5, 4)$, and $(5, 5)$ belong to $R$ because $A_2 = \{4, 5\}$ is an equivalence class; and finally the pair $(6, 6)$ belongs to $R$ because $\{6\}$ is an equivalence class. No pair other than those listed belongs to *R* and hence

$$R = \{(1, 1),(1, 2),(1, 3),(2, 1),(2, 2),(2, 3),(3, 1),(3, 2),(3, 3),(4, 4),(4, 5),(5, 4),(5, 5),(6, 6)\}.$$

**Example:** What are the sets in the partition of the integers arising from congruence modulo $4$?

*Solution:* There are four congruence classes, corresponding to $[0]_4, [1]_4, [2]_4$, and $[3]_4$. They are the sets

$$[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\},$$

$$[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\},$$
$$[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

These congruence classes are disjoint, and every integer is in exactly one of them. In other words, these congruence classes form a partition of set of integers.

**Example:** What are the sets in the partition of the set of all bit strings arising from the relation $R_3$ on the set of all bit strings? (Recall that $s\ R_3\ t$ , where $s$ and $t$ are bit strings, if $s = t$ or $s$ and $t$ are bit strings with at least three bits that agree in their first three bits.)

*Solution:* Note that every bit string of length less than three is equivalent only to itself. Hence $[\lambda]_{R_3} = \{\lambda\}$, $[0]_{R_3} = \{0\}$, $[1]_{R_3} = \{1\}$, $[00]_{R_3} = \{00\}$, $[01]_{R_3} = \{01\}$, $[10]_{R_3} = \{10\}$, and $[11]_{R_3} = \{11\}$. Note that every bit string of length three or more is equivalent to one of the eight bit strings $000, 001, 010, 011, 100, 101, 110$, and $111$.We have

$$[000]_{R_3} = \{000, 0000, 0001, 00000, 00001, 00010, 00011, \ldots\},$$
$$[001]_{R_3} = \{001, 0010, 0011, 00100, 00101, 00110, 00111, \ldots\},$$
$$[010]_{R_3} = \{010, 0100, 0101, 01000, 01001, 01010, 01011, \ldots\},$$
$$[[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \ldots\},$$
$$[100]_{R_3} = \{100, 1000, 1001, 10000, 10001, 10010, 10011, \ldots\},$$
$$[101]_{R_3} = \{101, 1010, 1011, 10100, 10101, 10110, 10111, \ldots\},$$
$$[110]_{R_3} = \{110, 1100, 1101, 11000, 11001, 11010, 11011, \ldots\},$$
$$[111]_{R_3} = \{111, 1110, 1111, 11100, 11101, 11110, 11111, \ldots\}.$$

These 8 equivalence classes are disjoint and every bit string is in exactly one of them. So, these equivalence classes partition the set of all bit strings.

## Partial Ordering Relations

We often use relations to order some or all of the elements of sets. For instance, we order words using the relation containing pairs of words $(x, y)$, where $x$ comes before $y$ in the dictionary. We schedule projects using the relation consisting of pairs $(x, y)$, where $x$ and $y$ are tasks in a project such that $x$ must be completed before $y$ begins. We order the set of integers using the relation containing the pairs $(x, y)$, where $x$ is less than $y$. When we add all of the pairs of the form $(x, x)$ to these relations, we obtain a relation that is reflexive, antisymmetric, and transitive. These are properties that characterize relations used to order the elements of sets.

**Definition:** A relation $R$ on a set $A$ is called a *partial ordering* or *partial order* if it is reflexive, antisymmetric, and transitive. A set $A$ together with a partial ordering $R$ is called a *partially ordered set*, or *poset*, and is denoted by $(A, R)$. Members of $A$ are called *elements* of the poset.

**Example:** Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

**Example:** Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set $A$.

**Example:** The divisibility relation is a partial ordering on the set of positive integers.

Customarily, the notation $a \preccurlyeq b$ is used to denote that $(a, b) \in R$ in an arbitrary poset $(A, R)$. This notation is used because the "less than or equal to" relation on the set of real numbers is the most familiar example of a partial ordering and the symbol $\preccurlyeq$ is similar to the $\leq$ symbol. (Note that the symbol $\preccurlyeq$ is used to denote the relation in *any* poset, not just the "less than or equals" relation.) The notation $a \prec b$ denotes that $a \preccurlyeq b$, but $a \neq b$. Also, we say "*a* is less than *b*" or "*b* is greater than *a*" if $a \prec b$.

**Definition:** The elements $a$ and $b$ of a poset $(A, \preccurlyeq)$ are called *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$. When $a$ and $b$ are elements of $A$ such that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, $a$ and $b$ are called *incomparable*. If every two elements of $A$ are comparable, $A$ is called a *totally ordered* or *linearly ordered set*, and $\preccurlyeq$ is called a *total order* or a *linear order.* A totally ordered set is also called a *chain*.

**Example:** The poset $(\mathbb{Z}, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever $a$ and $b$ are integers.

**Example:** In the poset $(\mathbb{Z}^+, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?

*Solution:* The integers 3 and 9 are comparable, because $3 \mid 9$. The integers 5 and 7 are incomparable, because $5 \nmid 7$ and $7 \nmid 5$.

Product Partial order relation: Let $(A_1, \preccurlyeq_1)$ and $(A_2, \preccurlyeq_2)$ be two posets. Define a relation $\preccurlyeq$ on the set $A_1 \times A_2$ by $(a, b) \preccurlyeq (c, d)$ iff $a \preccurlyeq_1 c$ and $b \preccurlyeq_2 d$. Then $\preccurlyeq$ is partial order relation and is called Product Partial order relation.

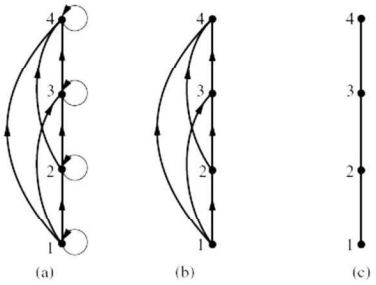
## Lexicographic Order

The words in a dictionary are listed in alphabetic, or lexicographic order, which is based on the ordering of the letters in the alphabet. This is a special case of an ordering of strings on a set constructed from a partial ordering on the set. We will show how this construction works in any poset. First, we will show how to construct a partial ordering on the Cartesian product of two posets, $(A_1, \preccurlyeq_1)$ and $(A_2, \preccurlyeq_2)$. The **lexicographic ordering** $\preccurlyeq$ on $A_1 \times A_2$ is defined by specifying that one pair is less than a second pair if the first entry of the first pair is less than ($\preccurlyeq_1$) the first entry of the second pair, or if the first entries are equal, but the second entry of this pair is less than ($\preccurlyeq_2$) the second entry of the second pair. In other words,

$$(a_1, a_2) \preccurlyeq (b_1, b_2), \text{ if either } a_1 \prec_1 b_1 \text{ or } a_1 = b_1 \text{ and } a_2 \preccurlyeq_2 b_2.$$

## Hasse Diagrams

Many edges in the directed graph for a finite poset do not have to be shown because they must be present. For instance, consider the directed graph for the partial ordering $\{(a, b) \mid a \leq b\}$ on the set {1, 2, 3, 4}, shown in bellow Figure (a).



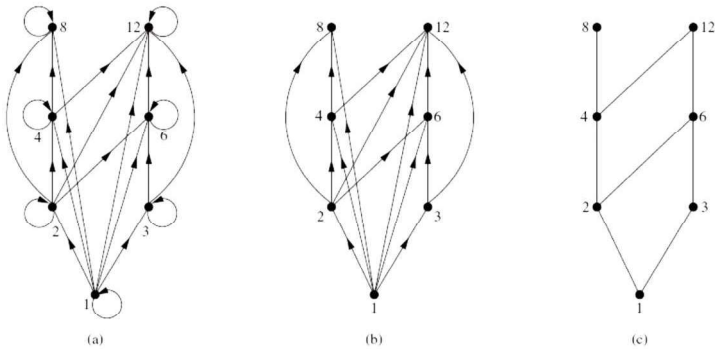

Because this relation is a partial ordering, it is reflexive, and its directed graph has loops at all vertices. Consequently, we do not have to show these loops because they must be present; in Figure (b) loops are not shown. Because a partial ordering is transitive, we do not have to show those edges that must be present because of transitivity. For example, in Figure (c) the edges $(1, 3)$, $(1, 4)$, and $(2, 4)$ are not shown because they must be present. If we assume that all edges are pointed "upward" (as they are drawn in the figure), we do not have to show the directions of

the edges; Figure (c) does not show directions. In general, we can represent a finite poset $(S, \preccurlyeq)$ using this procedure: Start with the directed graph for this relation. Because a partial ordering is reflexive, a loop $(a, a)$ is present at every vertex $a$. Remove these loops. Next, remove all edges that must be in the partial ordering because of the presence of other edges and transitivity. That is, remove all edges $(x, y)$ for which there is an element $z \in S$ such that $x \preccurlyeq z$ and $z \preccurlyeq y$. Finally, arrange each edge so that its initial vertex is below its terminal vertex. Remove all the arrows on the directed edges, because all edges point "upward" toward their terminal vertex. These steps are well defined, and only a finite number of steps need to be carried out for a finite poset. When all the steps have been taken, the resulting diagram contains sufficient information to find the partial ordering. The resulting diagram is called the **Hasse diagram** of $(S, \preccurlyeq)$, named after the twentieth-century German mathematician Helmut Hasse who made extensive use of them.

Let $(S, \preccurlyeq)$ be a poset. We say that an element $y \in S$ **covers** an element $x \in S$ if $x \prec y$ and there is no element $z \in S$ such that $x \prec z \prec y$**.** The set of pairs $(x, y)$ such that $y$ covers $x$ is called the **covering relation** of $(S, \preccurlyeq)$. From the description of the Hasse diagram of a poset, we see that the edges in the Hasse diagram of$(S, \preccurlyeq)$ are upwardly pointing edges corresponding to the pairs in the covering relation of $(S, \preccurlyeq)$. Furthermore, we can recover a poset from its covering relation, because it is the reflexive transitive closure of its covering relation. This tells us that we can construct a partial ordering from its Hasse diagram.

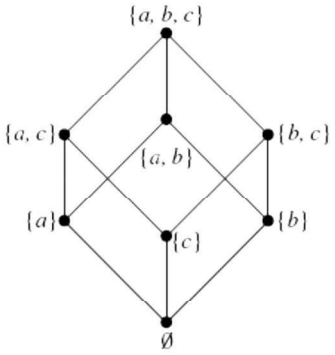
**Example:** Draw the Hasse diagram representing the partial ordering $\{(a, b) \mid a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$.

*Solution:* Begin with the digraph for this partial order, as shown in Figure (a). Remove all loops, as shown in Figure (b). Then delete all the edges implied by the transitive property. These are $(1, 4), (1, 6), (1, 8), (1, 12), (2, 8), (2, 12)$, and $(3, 12)$. Arrange all edges to point upward, and delete all arrows to obtain the Hasse diagram. The resulting Hasse diagram is shown below.



**Example:** Draw the Hasse diagram for the partial ordering $\{(A, B) \mid A \subseteq B\}$ on the power set $P(S)$ where $S = \{a, b, c\}$.

*Solution:* The Hasse diagram for this partial ordering is obtained from the associated digraph by deleting all the loops and all the edges that occur from transitivity, namely $(\emptyset, \{a, b\}), (\emptyset, \{a, c\}), (\emptyset, \{b, c\}), (\emptyset, \{a, b, c\}), (\{a\}, \{a, b, c\}), (\{b\}, \{a, b, c\})$, and $(\{c\}, \{a, b, c\})$. Finally all edges point upward, and arrows are deleted. The resulting Hasse diagram is illustrated in below Figure.

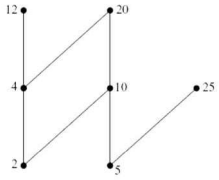



## Maximal and Minimal Elements

Elements of a poset that have certain extremal properties are important for many applications. An element of a poset is called maximal if it is not less than any element of the poset. That is, $a$ is **maximal** in the poset $(S, \preccurlyeq)$ if there is no $b \in S$ such that $a \prec b$. Similarly, an element of a poset is called minimal if it is not greater than any element of the poset. That is, $a$ is **minimal** if there is no element $b \in S$ such that $b \prec a$. Maximal and minimal elements are easy to spot using a Hasse diagram. They are the "top" and "bottom" elements in the diagram.

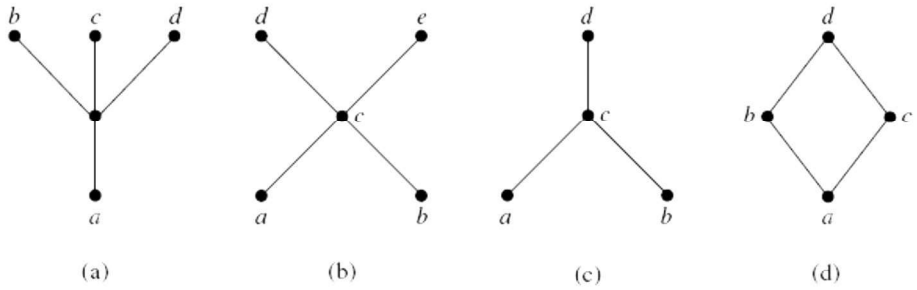
**Example:** Which elements of the poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$ are maximal, and which are minimal?

*Solution:* The Hasse diagram in bellow Figure for this poset shows that the maximal elements are 12, 20, and 25, and the minimal elements are 2 and 5. As this example shows, a poset can have more than one maximal element and more than one minimal element.



Sometimes there is an element in a poset that is greater than every other element. Such an element is called the greatest element. That is, $a$ is the **greatest element** of the poset $(S, \preccurlyeq)$ if $b \preccurlyeq a$ for all $b \in S$. The greatest element is unique when it exists. Likewise, an element is called the least element if it is less than all the other elements in the poset. That is, $a$ is the **least element** of $(S, \preccurlyeq)$ if $a \preccurlyeq b$ for all $b \in S$. The least element is unique when it exists.

**Example:** Determine whether the posets represented by each of the Hasse diagrams in bellow figure have a greatest element and a least element.




*Solution:* The least element of the poset with Hasse diagram (a) is $a$. This poset has no greatest element. The poset with Hasse diagram (b) has neither a least nor a greatest element. The poset with Hasse diagram (c) has no least element. Its greatest element is $d$. The poset with Hasse diagram (d) has least element $a$ and greatest element $d$.

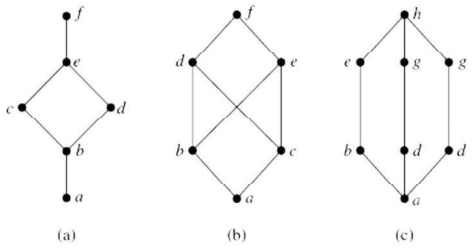
Sometimes it is possible to find an element that is greater than or equal to all the elements in a subset $A$ of a poset $(S, \preccurlyeq)$. If $u$ is an element of $S$ such that $a \preccurlyeq u$ for all elements $a \in A$, then $u$ is called an **upper bound** of $A$. Likewise, there may be an element less than or equal to all the elements in $A$. If $l$ is an element of $S$ such that $l \preccurlyeq a$ for all elements $a \in A$, then $l$ is called a **lower bound** of $A$.

The element $x$ is called the **least upper bound** of the subset $A$ if $x$ is an upper bound that is less than every other upper bound of $A$. Because there is only one such element, if it exists, it makes sense to call this element *the* least upper bound. That is, $x$ is the least upper bound of $A$ if $a \preccurlyeq x$ whenever $a \in A$, and $x \preccurlyeq z$ whenever $z$ is an upper bound of $A$. Similarly, the element $y$ is called the **greatest lower bound** of $A$ if $y$ is a lower bound of $A$ and $z \preccurlyeq y$ whenever $z$ is a lower bound of $A$. The greatest lower bound of $A$ is unique if it exists. The greatest lower bound and least upper bound of a subset $A$ are denoted by $\text{glb}(A)$ and $\text{lub}(A)$, respectively.

## Lattices

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a **lattice**. Lattices have many special properties. Furthermore, lattices are used in many different applications such as models of information flow and play an important role in Boolean algebra.

**Example:** Determine whether the posets represented by each of the Hasse diagrams in bellow figure are lattices.




*Solution:* Posets represented by the Hasse diagrams in (a) and (c) are both lattices because in each poset every pair of elements has both a least upper bound and a greatest lower bound, as the reader should verify. On the other hand, the poset with the Hasse diagram shown in (b) is not a lattice, because the elements $b$ and $c$ have no least upper bound. To see this, note that each of the elements $d$, $e$, and $f$ is an upper bound, but none of these three elements precedes the other two with respect to the ordering of this poset.

**Example:** Is the poset $(\mathbb{Z}^+, |)$ a lattice?

*Solution:* Let $a$ and $b$ be two positive integers. The least upper bound and greatest lower bound of these two integers are the least common multiple and the greatest common divisor of these integers, respectively, as the reader should verify. It follows that this poset is a lattice.

**Example:** Determine whether the posets $(\{1, 2, 3, 4, 5\}, |)$ and $(\{1, 2, 4, 8, 16\}, |)$ are lattices.

*Solution:* Because 2 and 3 have no upper bounds in $(\{1, 2, 3, 4, 5\}, |)$, they certainly do not have a least upper bound. Hence, the first poset is not a lattice. Every two elements of the second poset have both a least upper bound and a greatest lower bound. The least upper bound of two

elements in this poset is the larger of the elements and the greatest lower bound of two elements is the smaller of the elements, as the reader should verify. Hence, this second poset is a lattice.

**Example:** Determine whether $(P\ (S), \subseteq)$ is a lattice where *S* is a set.

*Solution:* Let *A* and *B* be two subsets of *S*. The least upper bound and the greatest lower bound of *A* and *B* are $A\ \cup\ B$ and $A\ \cap\ B$, respectively. Hence, $(P\ (S), \subseteq)$ is a lattice.

## Functions

Let $A$ and $B$ be nonempty sets. A function $f$ from $A$ to $B$ is a relation from $A$ to $B$ which relates exactly one element of $B$ to each element of $A$. We write $f(a) = b$ if $b$ is the unique element of $B$ assigned by the function $f$ to the element $a$ of $A$. If $f$ is a function from $A$ to $B$, we write $f: A \to B$. Functions are sometimes also called **mappings** or **transformations.** If $f$ is a function from $A$ to $B$, we say that $A$ is the domain of $f$ and $B$ is the codomain of $f$. If $f\ (a) = b$, we say that $b$ is the image of $a$ and $a$ is a preimage of $b$. The range, or image of $f$ is the set of all images of elements of $A$. Also, if $f$ is a function from $A$ to $B$, we say that $f$ maps $A$ to $B$.

**Example:** Let $A = \{-1,2,-3,4,-5\}$ and $B = \{1,2,\cdots,30\}$. The relation $f = \{(-1,2),\ (2,5),\ (-3,10),\ (4,17),\ (-5,26)\}$ is a function from $A$ to $B$. We can write this function as

$$f(-1) = 2, f(2) = 5, f(-3) = 10, f(4) = 17, f(-5) = 26.$$

A function is called **real-valued** if its codomain is the set of real numbers, and it is called **integer-valued** if its codomain is the set of integers. Two real-valued functions or two integer-valued functions with the same domain can be added, as well as multiplied. Let, $f$ and $g$ be functions from a ser $A$ to real numbers $\mathbb{R}$. Then $f + g$ and $fg$ are also functions from $A$ to $\mathbb{R}$ defined for all $x\ \in\ A$ by

$$(f + g)(x)\ =\ f(x)\ +\ g(x) \text{ and } \quad (fg)(x)\ =\ f(x)g(x).$$

**Example:** Let $f$ and $g$ be functions from $\mathbb{R}$ to $\mathbb{R}$ such that $f(x)\ =\ x^2$ and $g(x)\ =\ x\ -\ x^2$. What are the functions $f + g$ and $fg$?

*Solution:* From the definition of the sum and product of functions, it follows that

$$(f + g)(x) = f(x) + g(x) = x^2 + (x - x^2) = x.$$

And

$$(fg)(x) = f(x)g(x) = x^2(x - x^2) = x^3 - x^4.$$

One-to-One Functions: A function $f$ is said to be one-to-one, or an injection, if and only if $f(a) = f(b)$ implies that $a = b$ for all $a$ and $b$ in the domain of $f$. A function is said to be injective if it is one-to-one. Note that a function $f$ is one-to-one if and only if $f(a) \neq f(b)$ whenever $a \neq b$. This way of expressing that $f$ is one-to-one is obtained by taking the contrapositive of the implication in the definition.

**Example:** The function $f$ from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$ with $f(a) = 4, f(b) = 5, f(c) = 1$, and $f(d) = 3$ is one-to-one.

**Example:** the function $f(x) = x^2$ from the set of integers to the set of integers is not one-to-one because, for instance, $f(1) = f(-1) = 1$, but $1 \neq -1$.

**Example:** Determine whether the function $f(x) = x + 1$ from the set of real numbers to itself is one-to-one.

*Solution:* Suppose that $x$ and $y$ are real numbers with $f(x) = f(y)$, so that $x + 1 = y + 1$. This means that $x = y$. Hence, $f(x) = x + 1$ is a one-to-one function from $\mathbb{R}$ to $\mathbb{R}$.

Onto Functions: A function $f$ from $A$ to $B$ is called *onto,* or a *surjection,* if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A function $f$ is called *surjective* if it is onto.

**Example:** The function $f$ from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, \}$ with $f(a) = 4, f(b) = 2, f(c) = 1$, and $f(d) = 3$ is onto.

**Example:** Is the function $f(x) = x^2$ from the set of integers to the set of integers onto?

*Solution:* The function $f$ is not onto because there is no integer $x$ with $x^2 = -1$, for instance.

Bijection: The function $f$ is a **bijection,** if it is both one-to-one and onto. We also say that such a function is bijective.

**Example:** The function $f$ from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, \}$ with $f(a) = 4, f(b) = 2, f(c) = 1$, and $f(d) = 3$ is bijective.

Now consider a one-to-one correspondence $f$ from the set $A$ to the set $B$. Because $f$ is an onto function, every element of $B$ is the image of some element in $A$. Furthermore, because $f$ is also a one-to-one function, every element of $B$ is the image of a *unique* element of $A$. Consequently, we can define a new function from $B$ to $A$ that reverses the correspondence given by $f$.

Inverse Function: Let $f$ be a one-to-one correspondence from the set $A$ to the set $B$. The *inverse function* of $f$ is the function that assigns to an element $b$ belonging to $B$ the unique element $a$ in $A$ such that $f(a) = b$. The inverse function of $f$ is denoted by $f^{-1}$. Hence, $f^{-1}(b) = a$ when $f(a) = b$.

A one-to-one correspondence is called **invertible** because we can define an inverse of this function. A function is **not invertible** if it is not a one-to-one correspondence, because the inverse of such a function does not exist.

**Example:** Let $f$ be the function from $\{a, b, c\}$ to $\{1, 2, 3\}$ such that $f(a) = 2, f(b) = 3$, and $f(c) = 1$. Is $f$ invertible, and if it is, what is its inverse?

*Solution:* The function $f$ is invertible because it is a one-to-one correspondence. The inverse function $f^{-1}$ reverses the correspondence given by $f$, so $f^{-1}(1) = c, f^{-1}(2) = a$, and $f^{-1}(3) = b$.

**Example:** Let $f : \mathbb{Z} \to \mathbb{Z}$ be such that $f(x) = x + 1$. Is $f$ invertible, and if it is, what is its inverse?

*Solution:* The function $f$ has an inverse because it is a one-to-one correspondence. To reverse the correspondence, suppose that $y$ is the image of $x$, so that $y = x + 1$. Then $x = y - 1$. This means that $y - 1$ is the unique element of $\mathbb{Z}$ that is sent to $y$ by $f$. Consequently, $f^{-1}(y) = y - 1$.

**Example**: Let $f$ be the function from $\mathbb{R}$ to $\mathbb{R}$with $f(x) = x^2$. Is $f$ invertible?

*Solution:* Because $f(-2) = f(2) = 4$, $f$ is not one-to-one. If an inverse function were defined, it would have to assign two elements to 4. Hence, $f$ is not invertible

Compositions of Functions: Let $g$ be a function from the set $A$ to the set $B$ and let $f$ be a function from the set $B$ to the set $C$. The *composition* of the functions $f$ and $g$, denoted for all $a \in A$ by $f \circ g$, is the function from $A$ to $C$ defined by

$$(f \circ g)(a) = f(g(a)).$$

**Example:** Let $g$ be the function from the set $\{a, b, c\}$ to itself such that $g(a) = b, g(b) = c$, $g(c) = a$. Let $f$ be the function from the set $\{a, b, c\}$ to the set $\{1, 2, 3\}$ such that $f(a) = 3, f(b) = 2, f(c) = 1$. What is the composition of $f$ and $g$, and what is the composition of $g$ and $f$ ?

*Solution:* The composition $f \circ g$ is defined by $(f \circ g)(a) = f\big(g(a)\big) = f(b) = 2, (f \circ g)(b) = f(g(b)) = f(c) = 1, (f \circ g)(c) = f(g(c)) = f(a) = 3$. Note that $g \circ f$ is not defined, because the range of $f$ is not a subset of the domain of $g$.

**Example:** Let $f$ and $g$ be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of $f$ and $g$? What is the composition of $g$ and $f$ ?

*Solution:* Both the compositions $f \circ g$ and $g \circ f$ are defined. Moreover,

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

and

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11.$$

Note that even though $f \circ g$ and $g \circ f$ are defined for some functions $f$ and $g$, they are not equal. In otherwords, the commutative law does not hold for the composition of functions.

Some Important Functions

The **floor function** assigns to the real number $x$ the largest integer that is less than or equal to $x$. The value of the floor function at $x$ is denoted by $\lfloor x \rfloor$. The **ceiling function** assigns to the real number $x$ the smallest integer that is greater than or equal to $x$. The value of the ceiling function at $x$ is denoted by $\lceil x \rceil$. The floor function is often also called the ***greatest integer function***. It is often denoted by [$x$]. These are some values of the floor and ceiling functions:

$$\left\lfloor \frac{1}{2} \right\rfloor = 0,\ \left\lceil \frac{1}{2} \right\rceil = 1,\ \left\lfloor -\frac{1}{2} \right\rfloor = -1,\ \left\lceil -\frac{1}{2} \right\rceil = 0,\ \lfloor 3.1 \rfloor = 3,\ \lceil 3.1 \rceil = 4,\ \lfloor 7 \rfloor = 7, \lceil 7 \rceil = 7.$$

**Example:** Data stored on a computer disk or transmitted over a data network are usually represented as a string of bytes. Each byte is made up of 8 bits. How many bytes are required to encode 100 bits of data?

*Solution:* To determine the number of bytes needed, we determine the smallest integer that is at least as large as the quotient when 100 is divided by 8, the number of bits in a byte. Consequently, $\left\lceil \frac{100}{8} \right\rceil = \lceil 12.5 \rceil = 13$ bytes are required.

The **factorial function** $f: \mathbb{N} \to \mathbb{N}$, denoted by $f(n) = n!$. The value of $f(n) = n!$ is the product of the first $n$ positive integers, so $f(n) = 1 \cdot 2 \cdots (n-1) \cdot n$ and $f(0) = 0! = 1$. We have $f(1) = 1! = 1, f(2) = 2! = 1 \cdot 2 = 2, f(6) = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$.

A **permutation** is a bijective function on a finite set. There are $n!$ permutations on a set of $n$ elements.

**Example:** Let $A = \{1, 2, 3\}$ and $f$ is function on $A$ given by $f(1) = 2, f(2) = 1, f(3) = 3$. The function $f$ is one to one and onto function and hence is a permutation on the set $A$. The function $f$ can also be written as $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. The other permutations are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

A **sequence** is a function from a subset of the set of integers to a set S. We use the notation $a_n$ to denote the image of the integer $n$. We call $a_n$ a term of the sequence. We use the notation $\{a_n\}$ to describe the sequence.

**Example:** Consider the sequence $\{a_n\}$, where $a_n = \frac{1}{n};\ n \geq 1$. The function is given by $f(n) = \frac{1}{n}$. The list of the terms of this sequence are $a_1 = f(1), a_2 = f(2), a_3 = f(3), \ldots$. Therefore $a_1 = 1, a_2 = \frac{1}{2}, a_3 = \frac{1}{3}, a_4 = \frac{1}{4}, \ldots$.