# Predicates and Quantifiers

Propositional logic cannot adequately express the meaning of all statements in mathematics and in natural language. For example, suppose that we know that

**"Every computer connected to the university network is functioning properly."**

No rules of propositional logic allow us to conclude the truth of the statement

**"MATH3 is functioning properly,"**

Where **MATH3** is one of the computers connected to the university network. Likewise, we cannot use the rules of propositional logic to conclude from the statement

**"CS2 is under attack by an intruder,"**

where CS2 is a computer on the university network, to conclude the truth of

**"There is a computer on the university network that is under attack by an intruder."**

In this section we will introduce a more powerful type of logic called **predicate logic**. We will see how predicate logic can be used to express the meaning of a wide range of statements in mathematics and computer science in ways that permit us to reason and explore relationships between objects. To understand predicate logic, we first need to introduce the concept of a predicate. Afterward, we will introduce the notion of quantifiers, which enable us to reason with statements that assert that a certain property holds for all objects of a certain type and with statements that assert the existence of an object with a particular property.

# Predicates

Statements involving variables, such as

**"$x > 3$," "$x = y + 3$," "$x + y = z$,"**

and

**"computer *x* is under attack by an intruder,"**

and

**"computer *x* is functioning properly,"**

are often found in mathematical assertions, in computer programs, and in system specifications.

These statements are neither true nor false when the values of the variables are not specified. <u>In this section, we will discuss the ways that propositions can be produced from such statements.</u>

The statement "$x$ is greater than 3" has two parts. The first part, the variable $x$, is the subject of the statement. The second part—the **predicate**, "is greater than 3"—refers to a property that the subject of the statement can have. We can denote the statement "$x$ is greater than 3" by $P(x)$, where $P$ denotes the predicate "is greater than 3" and $x$ is the variable. The statement $P(x)$ is also said to be the value of the **propositional function** $P$ at $x$. Once a value has been assigned to the variable $x$, the statement $P(x)$ becomes a proposition and has a truth value. Consider Examples 1 and 2.

**EXAMPLE 1** Let $P(x)$ denote the statement "$x > 3$." What are the truth values of $P(4)$ and $P(2)$?

***Solution:*** We obtain the statement $P(4)$ by setting $x = 4$ in the statement "$x > 3$." Hence, $P(4)$, which is the statement "$4 > 3$," is true. However, $P(2)$, which is the statement "$2 > 3$," is false.

**EXAMPLE 2** Let $A(x)$ denote the statement "Computer $x$ is under attack by an intruder." Suppose that of the computers on campus, only CS2 and MATH1 are currently under attack by intruders. What are truth values of *A*(CS1), *A*(CS2), and *A*(MATH1)?

**Solution**: We obtain the statement *A*(CS1) by setting $x$ = CS1 in the statement "Computer $x$ is under attack by an intruder." Because CS1 is not on the list of computers currently under attack, we conclude that *A*(CS1) is false. Similarly, because CS2 and MATH1 are on the list of computers under attack, we know that *A*(CS2) and *A*(MATH1) are true.

We can also have statements that involve more than one variable. For instance, consider the statement "$x = y + 3$." We can denote this statement by $Q(x, y)$, where $x$ and $y$ are variables and $Q$ is the predicate. When values are assigned to the variables $x$ and $y$, the statement $Q(x, y)$ has a truth value.

**EXAMPLE 3** Let $Q(x, y)$ denote the statement "$x = y + 3$." What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

**Solution**: To obtain $Q(1, 2)$, set $x = 1$ and $y = 2$ in the statement $Q(x, y)$. Hence, $Q(1, 2)$ is the statement "1 = 2 + 3," which is false. The statement $Q(3, 0)$ is the proposition "3 = 0 + 3," which is true.

**EXAMPLE 4** Let $A(c, n)$ denote the statement "Computer $c$ is connected to network $n$," where $c$ is a variable representing a computer and $n$ is a variable representing a network. Suppose that the computer MATH1 is connected to network CAMPUS2, but not to network CAMPUS1. What are the values of *A*(MATH1, CAMPUS1) and *A*(MATH1, CAMPUS2)?

**Solution**: Because MATH1 is not connected to the CAMPUS1 network, we see that *A*(MATH1,CAMPUS1) is false. However, because MATH1 is connected to the CAMPUS2 network, we see that *A*(MATH1, CAMPUS2) is true.

Similarly, we can let $R(x, y, z)$ denote the statement`‘ $x + y = z$.” When values are assigned to the variables $x$, $y$, and $z$, this statement has a truth value.

**EXAMPLE 5** What are the truth values of the propositions $R(1, 2, 3)$ and $R(0, 0, 1)$?

**Solution**: The proposition $R(1, 2, 3)$ is obtained by setting $x = 1$, $y = 2$, and $z = 3$ in the statement $R(x, y, z)$. We see that $R(1, 2, 3)$ is the statement “$1 + 2 = 3$,” which is true. Also note that $R(0, 0, 1)$, which is the statement “$0 + 0 = 1$,” is false.

In general, a statement involving the $n$ variables $x_1, x_2, \ldots, x_n$ can be denoted by $P(x_1, x_2, \ldots, x_n)$.

A statement of the form $P(x_1, x_2, \ldots, x_n)$ is the value of the propositional function $P$ at the $n$-tuple $(x_1, x_2, \ldots, x_n)$, and $P$ is also called an $n$-place predicate or a $n$-ary predicate.

Propositional functions occur in computer programs, as Example 6 demonstrates.

**EXAMPLE 6** Consider the statement if $x > 0$ then $x := x + 1$.

When this statement is encountered in a program, the value of the variable $x$ at that point in the execution of the program is inserted into $P(x)$, which is “$x > 0$.” If $P(x)$ is true for this value of $x$, the assignment statement $x := x + 1$ is executed, so the value of $x$ is increased by 1. If $P(x)$ is false for this value of $x$, the assignment statement is not executed, so the value of $x$ is not changed.

**PRECONDITIONS AND POSTCONDITIONS** Predicates are also used to establish the correctness of computer programs, that is, to show that computer programs always produce the desired output when given valid input. The statements that describe valid input are known as **preconditions** and the conditions that the output should satisfy when the program has run are known as **postconditions**. As Example 7 illustrates, we use predicates to describe both preconditions and postconditions.

**EXAMPLE 7** Consider the following program, designed to interchange the values of two variables $x$ and $y$.

*temp* := $x$

$x := y$

$y :=$ *temp*

Find predicates that we can use as the precondition and the postcondition to verify the correctness of this program. Then explain how to use them to verify that for all valid input the program does what is intended.

**Solution**: For the precondition, we need to express that $x$ and $y$ have particular values before we run the program. So, for this precondition we can use the predicate $P(x, y)$, where $P(x, y)$ is the statement "$x = a$ and $y = b$," where $a$ and $b$ are the values of x and y before we run the program. Because we want to verify that the program swaps the values of $x$ and $y$ for all input values, for the postcondition we can use $Q(x, y)$, where $Q(x, y)$ is the statement "$x = b$ and $y = a$."

To verify that the program always does what it is supposed to do, suppose that the precondition $P(x, y)$ holds. That is, we suppose that the statement "$x = a$ and $y = b$" is true. This means that $x = a$ and $y = b$. The first step of the program, *temp* := $x$, assigns the value of $x$ to the variable temp, so after this step we know that $x = a$, *temp* $= a$, and $y = b$. After the second step of the program, $x := y$, we know that $x = b$, *temp* $= a$, and $y = b$. Finally, after the third step, we know that $x = b$, *temp* $= a$, and $y = a$. Consequently, after this program is run, the postcondition $Q(x, y)$ holds, that is, the statement "$x = b$ and $y = a$" is true.

## Quantifiers

When the variables in a propositional function are assigned values, the resulting statement becomes a proposition with a certain truth value. However, there is another important way, called **quantification**, to create a proposition from a propositional function. Quantification expresses the extent to which a predicate is true over a range of elements. In English, the words *all, some, many, none,* and *few* are used in quantifications. We will focus on two types of quantification here: universal quantification, which tells us that a predicate is true for every element under consideration, and existential quantification, which tells us that there is one or more element under consideration for which the predicate is true. The area of logic that deals with predicates and quantifiers is called the *predicate calculus*.

**THE UNIVERSAL QUANTIFIER** Many mathematical statements assert that a property is true for all values of a variable in a particular domain, called the **domain of discourse** (or the **universe of discourse**), often just referred to as the **domain**. Such a statement is expressed using universal quantification. The universal quantification of $P(x)$ for a particular domain is the proposition that asserts that $P(x)$ is true for all values of $x$ in this domain. Note that the domain specifies the possible values of the variable $x$. The meaning of the universal quantification of $P(x)$ changes when we change the domain. The domain must always be specified when a universal quantifier is used; without it, the universal quantification of a statement is not defined.

**DEFINITION 1** The *universal quantification* of $P(x)$ is the statement

"$P(x)$ for all values of $x$ in the domain."

The notation $\forall x P(x)$ denotes the universal quantification of $P(x)$. Here $\forall$ is called the **universal quantifier.** We read $\forall x P(x)$ as "for all $x P(x)$" or "for every $x P(x)$." An element for which $P(x)$ is false is called a **counterexample** of $\forall x P(x)$.

The meaning of the universal quantifier is summarized in the first row of Table 1.

**TABLE 1 Quantifiers.**

| *Statement* | *When True?* | *When False?* |
|---|---|---|
| $\forall x P(x)$ | $P(x)$ is true for every $x$. | There is an $x$ for which $P(x)$ is false. |
| $\exists x P(x)$ | There is an $x$ for which $P(x)$ is true. | $P(x)$ is false for every $x$. |

**EXAMPLE 8** Let *P(x)* be the statement "$x + 1 > x$." What is the truth value of the quantification $\forall x P(x)$, where the domain consists of all real numbers?

**Solution**: Because *P(x)* is true for all real numbers *x*, the quantification $\forall x P(x)$ is true.

Besides "*for all*" and "*for every*," universal quantification can be expressed in many other ways, including "*all of*," "*for each*," "*given any*," "*for arbitrary*," "*for each*," and "*for any*."

***Remark***: It is best to avoid using "for any *x*" because it is often ambiguous as to whether "any" means "every" or "some." In some cases, "any" is unambiguous, such as when it is used in negatives, for example, "there is not any reason to avoid studying."

A statement $\forall x P(x)$ is false, where *P(x)* is a propositional function, if and only if *P(x)* is not always true when *x* is in the domain. One way to show that *P(x)* is not always true when *x* is in the domain is to find a counterexample to the statement $\forall x P(x)$. Note that a single counterexample is all we need to establish that $\forall x P(x)$ is false. Example 9 illustrates how counterexamples are used.

**EXAMPLE 9** Let $Q(x)$ be the statement "$x < 2$." What is the truth value of the quantification $\forall x\, Q(x)$, where the domain consists of all real numbers?

**Solution**: $Q(x)$ is not true for every real number $x$, because, for instance, $Q(3)$ is false. That is, $x = 3$ is a counterexample for the statement $\forall x\, Q(x)$. Thus $\forall x\, Q(x)$ is false.

**EXAMPLE 10** Suppose that $P(x)$ is "$x^2 > 0$." To show that the statement $\forall x\, P(x)$ is false where the universe of discourse consists of all integers, we give a counterexample. We see that $x = 0$ is a counterexample because $x^2 = 0$ when $x = 0$, so that $x^2$ is not greater than 0 when $x = 0$.

Looking for counterexamples to universally quantified statements is an important activity in the study of mathematics.

When all the elements in the domain can be listed - say, $x_1, x_2, \ldots, x_n$ - it follows that the universal quantification $\forall x\, P(x)$ is the same as the conjunction

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n),$$

because this conjunction is true if and only if $P(x_1), P(x_2), \ldots, P(x_n)$ are all true.

**EXAMPLE 11** What is the truth value of $\forall x\, P(x)$, where $P(x)$ is the statement "$x^2 < 10$" and the domain consists of the positive integers not exceeding 4?

**Solution**: The statement $\forall x\, P(x)$ is the same as the conjunction

$$P(1) \wedge P(2) \wedge P(3) \wedge P(4),$$

because the domain consists of the integers 1, 2, 3, and 4. Because $P(4)$, which is the statement "$4^2 < 10$," is false, it follows that $\forall x\, P(x)$ is false.

**EXAMPLE 12** What does the statement $\forall x\, N(x)$ mean if $N(x)$ is "Computer $x$ is connected to the network" and the domain consists of all computers on campus?

**Solution**: The statement $\forall x\, N(x)$ means that for every computer $x$ on campus, that computer $x$ is connected to the network. This statement can be expressed in English as *"Every computer on campus is connected to the network."*

As we have pointed out, specifying the domain is mandatory when quantifiers are used. The truth value of a quantified statement often depends on which elements are in this domain, as Example 13 shows.

**EXAMPLE 13** What is the truth value of $\forall x\ (x^2 \geq x)$ if the domain consists of all real numbers? What is the truth value of this statement if the domain consists of all integers?

**Solution**: The universal quantification $\forall x\ (x^2 \geq x)$, where the domain consists of all real numbers, is false. For example, $(1/2)^2 < 1/2$. Note that $x^2 \geq x$ if and only if $x^2 - x = x(x - 1) \geq 0$. Consequently, $x^2 \geq x$ if and only if $x \leq 0$ or $x \geq 1$. It follows that $\forall x\ (x^2 \geq x)$ is false if the domain consists of all real numbers (because the inequality is false for all real numbers $x$ with $0 < x < 1$). However, if the domain consists of the integers, $\forall x\ (x^2 \geq x)$ is true, because there are no integers $x$ with $0 < x < 1$.

**THE EXISTENTIAL QUANTIFIER** Many mathematical statements assert that there is an element with a certain property. Such statements are expressed using existential quantification. With existential quantification, we form a proposition that is true if and only if $P(x)$ is true for at least one value of $x$ in the domain.

**DEFINITION 2** The *existential quantification* of $P(x)$ is the proposition

"There exists an element $x$ in the domain such that $P(x)$."

We use the notation $\exists x P(x)$ for the existential quantification of $P(x)$. Here $\exists$ is called the *existential quantifier*.

A domain must always be specified when a statement $\exists x\ P(x)$ is used. Furthermore, the meaning of $\exists x\ P(x)$ changes when the domain changes. Without specifying the domain, the statement $\exists x\ P(x)$ has no meaning.

Besides the phrase "*there exists*," we can also express existential quantification in many other ways, such as by using the words "*for some*," "*for at least one*," or "*there is*." The existential quantification $\exists x\, P(x)$ is read as

*"There is an x such that P(x)," "There is at least one x such that P(x),"* or *"For some x P(x)."*

The meaning of the existential quantifier is summarized in the second row of Table 1.

We illustrate the use of the existential quantifier in Examples 14–16.

**EXAMPLE 14** Let $P(x)$ denote the statement "$x > 3$." What is the truth value of the quantification $\exists x\, P(x)$, where the domain consists of all real numbers?

**Solution**: Because "$x > 3$" is sometimes true - for instance, when $x = 4$ - the existential quantification of $P(x)$, which is $\exists x\, P(x)$, is true.

Observe that the statement $\exists x\, P(x)$ is false if and only if there is no element $x$ in the domain for which $P(x)$ is true. That is, $\exists x\, P(x)$ is false if and only if $P(x)$ is false for every element of the domain. We illustrate this observation in Example 15.

**EXAMPLE 15** Let $Q(x)$ denote the statement "$x = x + 1$." What is the truth value of the quantification $\exists x\, Q(x)$, where the domain consists of all real numbers?

**Solution**: Because $Q(x)$ is false for every real number $x$, the existential quantification of $Q(x)$, which is $\exists x\, Q(x)$, is false.

***Remark***: Generally, an implicit assumption is made that all domains of discourse for quantifiers are nonempty. If the domain is empty, then $\exists x\, Q(x)$ is false whenever $Q(x)$ is a propositional function because when the domain is empty, there can be no element $x$ in the domain for which $Q(x)$ is true.

When all elements in the domain can be listed - say, $x_1, x_2, \ldots, x_n$ - the existential quantification $\exists x\, P(x)$ is the same as the disjunction

$$P(x1) \vee P(x2) \vee \cdots \vee P(xn),$$

because this disjunction is true if and only if at least one of $P(x_1), P(x_2), \ldots, P(x_n)$ is true.

**EXAMPLE 16** What is the truth value of $\exists x\, P(x)$, where $P(x)$ is the statement "$x^2 > 10$" and the universe of discourse consists of the positive integers not exceeding 4?

**Solution**: Because the domain is {1, 2, 3, 4}, the proposition $\exists x\, P(x)$ is the same as the disjunction

$$P(1) \vee P(2) \vee P(3) \vee P(4).$$

Because $P(4)$, which is the statement "$4^2 > 10$," is true, it follows that $\exists x\, P(x)$ is true.

It is sometimes helpful to think in terms of looping and searching when determining the truth value of a quantification. Suppose that there are $n$ objects in the domain for the variable $x$. To determine whether $\forall x\, P(x)$ is true, we can loop through all $n$ values of $x$ to see whether $P(x)$ is always true. If we encounter a value $x$ for which $P(x)$ is false, then we have shown that $\forall x\, P(x)$ is false. Otherwise, $\forall x\, P(x)$ is true. To see whether $\exists x\, P(x)$ is true, we loop through the $n$ values of $x$ searching for a value for which $P(x)$ is true. If we find one, then $\exists x\, P(x)$ is true. If we never find such an $x$, then we have determined that $\exists x\, P(x)$ is false. (Note that this searching procedure does not apply if there are infinitely many values in the domain. However, it is still a useful way of thinking about the truth values of quantifications.)

**Quantifiers with Restricted Domains**

An abbreviated notation is often used to restrict the domain of a quantifier. In this notation, a condition a variable must satisfy is included after the quantifier. This is illustrated in Example 17.

**EXAMPLE 17** What do the statements $\forall x < 0\ (x^2 > 0)$, $\forall y \neq 0\ (y^3 \neq 0)$, and $\exists z > 0\ (z^2 = 2)$ mean, where the domain in each case consists of the real numbers?

**Solution**: The statement $\forall x < 0\ (x^2 > 0)$ states that for every real number $x$ with $x < 0$, $x^2 > 0$. That is, it states "The square of a negative real number is positive." This statement is the same as $\forall x(x < 0 \rightarrow x^2 > 0)$.

The statement $\forall y \neq 0\ (y^3 \neq 0)$ states that for every real number y with $y \neq 0$, we have $y^3 \neq 0$. That is, it states "The cube of every nonzero real number is nonzero." Note that this statement is equivalent to $\forall y\ (y \neq 0 \rightarrow y^3 \neq 0)$.

Finally, the statement $\exists z > 0\ (z^2 = 2)$ states that there exists a real number $z$ with $z > 0$ such that $z^2 = 2$. That is, it states "There is a positive square root of 2." This statement is equivalent to $\exists z\ (z > 0 \wedge z^2 = 2)$.

Note that the restriction of a universal quantification is the same as the universal quantification of a conditional statement. For instance, $\forall x < 0\ (x^2 > 0)$ is another way of expressing $\forall x\ (x < 0 \rightarrow x^2 > 0)$. On the other hand, the restriction of an existential quantification is the same as the existential quantification of a conjunction. For instance, $\exists z > 0\ (z^2 = 2)$ is another way of expressing $\exists z\ (z > 0 \wedge z^2 = 2)$.

**Precedence of Quantifiers**

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus. For example, $\forall x\ P(x) \vee Q(x)$ is the disjunction of $\forall x\ P(x)$ and $Q(x)$. In other words, it means $(\forall x\ P(x)) \vee Q(x)$ rather than $\forall x\ (P(x) \vee Q(x))$.

**Negating Quantified Expressions**

We will often want to consider the negation of a quantified expression. For instance, consider the negation of the statement

*"Every student in your class has taken a course in calculus."*

This statement is a universal quantification, namely, $\forall x\ P(x)$, where $P(x)$ is the statement "*x has taken a course in calculus*" and the domain consists of the students in your class. The negation of this statement is "*It is not the case that every student in your class has taken a course in calculus*." This is equivalent to "*There is a student in your class who has not taken a course in calculus*." And this is simply the existential quantification of the negation of the original propositional function, namely, $\exists x\ \neg P(x)$.

This example illustrates the following logical equivalence:

$$\neg\forall x\ P(x) \equiv \exists x\ \neg P(x).$$

Suppose we wish to negate an existential quantification. For instance, consider the proposition "There is a student in this class who has taken a course in calculus." This is the existential quantification $\exists x\ Q(x)$, where $Q(x)$ is the statement "*x has taken a course in calculus*." The negation of this statement is the proposition "*It is not the case that there is a student in this class who has taken a course in calculus."* This is equivalent to "*Every student in this class has not taken calculus*," which is just the universal quantification of the negation of the original propositional function, or, phrased in the language of quantifiers, $\forall x\ \neg Q(x)$. This example illustrates the equivalence:

$$\neg\exists x\ Q(x) \equiv \forall x\ \neg Q(x).$$

**EXAMPLE 18** What are the negations of the statements $\forall x\ (x^2 > x)$ and $\exists x\ (x^2 = 2)$?

**Solution**: The negation of $\forall x\ (x^2 > x)$ is the statement $\neg\forall x\ (x^2 > x)$, which is equivalent to $\exists x\ \neg(x^2 > x)$. This can be rewritten as $\exists x\ (x^2 \le x)$. The negation of $\exists x\ (x^2 = 2)$ is the statement $\neg\exists x\ (x^2 = 2)$, which is equivalent to $\forall x\ \neg(x^2 = 2)$. This can be rewritten as $\forall x\ (x^2 \neq 2)$. The truth values of these statements depend on the domain.

**Using Quantifiers in System Specifications**

**EXAMPLE 19** Use predicates and quantifiers to express the system specifications "Every mail message larger than one megabyte will be compressed" and "If a user is active, at least one network link will be available."

**Solution**: Let $S(m, y)$ be "*Mail message m is larger than y megabytes*," where the variable $x$ has the domain of all mail messages and the variable $y$ is a positive real number, and let $C(m)$ denote "*Mail message m will be compressed*." Then the specification "*Every mail message larger than one megabyte will be compressed*" can be represented as $\forall m\ (S(m, 1) \rightarrow C(m))$.

Let $A(u)$ represent "*User u is active*," where the variable $u$ has the domain of all users, let $S(n, x)$ denote "*Network link n is in state x*," where $n$ has the domain of all network links and $x$ has the domain of all possible states for a network link. Then the specification "*If a user is active, at least one network link will be available*" can be represented by:

$$\exists u\ A(u) \rightarrow \exists n\ S(n, available).$$

**Nested Quantifiers**

Nested quantifiers commonly occur in mathematics and computer science, where one quantifier is within the scope of another, such as $\forall x \exists y\ (x + y = 0)$.

To understand statements involving nested quantifiers, we need to unravel what the quantifiers and predicates that appear mean.

**EXAMPLE 20** Assume that the domain for the variables $x$ and $y$ consists of all real numbers. The statement $\forall x \forall y\ (x + y = y + x)$ says that $x + y = y + x$ for all real numbers $x$ and $y$. This is the commutative law for addition of real numbers. Likewise, the statement $\forall x \exists y\ (x + y = 0)$ says that for every real number $x$ there is a real number $y$ such that $x + y = 0$. This states that every real number has an additive inverse. Similarly, the statement $\forall x \forall y \forall z\ (x + (y + z) = (x + y) + z)$ is the associative law for addition of real numbers.

**EXAMPLE 21** Translate into English the statement $\forall x \forall y\ ((x > 0) \wedge (y < 0) \rightarrow (xy < 0))$, where the domain for both variables consists of all real numbers.

**Solution**: This statement says that for every real number $x$ and for every real number $y$, if $x > 0$ and $y < 0$, then $xy < 0$. That is, this statement says that for real numbers $x$ and $y$, if $x$ is positive and $y$ is negative, then $xy$ is negative. This can be stated more succinctly as "*The product of a positive real number and a negative real number is always a negative real number*."

**EXAMPLE 22** Let $Q(x, y)$ denote "$x + y = 0$." What are the truth values of the quantifications $\exists y \forall x\ Q(x, y)$ and $\forall x \exists y\ Q(x, y)$, where the domain for all variables consists of all real numbers?

**Solution**: The quantification $\exists y \forall x\ Q(x, y)$ denotes the proposition "*There is a real number y such that for every real number x, Q(x, y).*"

No matter what value of $y$ is chosen, there is only one value of $x$ for which $x + y = 0$. Because there is no real number $y$ such that $x + y = 0$ for all real numbers $x$, the statement $\exists y \forall x\ Q(x, y)$ is **false**.

The quantification $\forall x \exists y\ Q(x, y)$ denotes the proposition "*For every real number x there is a real number y such that Q(x, y).*"

Given a real number $x$, there is a real number $y$ such that $x + y = 0$; namely, $y = -x$. Hence, the statement $\forall x \exists y\ Q(x, y)$ is **true**.

Example 22 illustrates that the order in which quantifiers appear makes a difference.

# Integer Representations

Integers can be expressed using any integer greater than one as a **base**. Although we commonly use decimal (base 10), representations, binary (base 2), octal (base 8), and hexadecimal (base 16) representations are often used, especially in computer science.
In everyday life we use decimal notation to express integers. For example, 965 is used to denote $(9 \cdot 10^2 + 6 \cdot 10 + 5)$. However, it is often convenient to use bases other than 10. In particular, computers usually use binary notation (with 2 as the base) when carrying out arithmetic, and octal (base 8) or hexadecimal (base 16) notation when expressing characters, such as letters or digits. In fact, we can use any integer greater than 1 as the base when expressing integers. This is stated in Theorem 1

**THEOREM**

Let $b$ be an integer greater than 1. Then if $n$ is a positive integer, it can be expressed uniquely in the form

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

where $k$ is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than $b$, and $a_k \neq 0$.

The representation of n given in Theorem 1 is called the base b expansion of n. The base b expansion of n is denoted by $(a^k a^{k-1} \ldots a^1 a^0)_b$. For instance, $(245)_8$ represents $2 \cdot 82 + 4 \cdot 8 + 5 = 165$. Typically, the subscript 10 is omitted for base 10 expansions of integers because base 10, or decimal expansions, are commonly used to represent integers.

## Primes and Greatest Common Divisors

### Primes

Every integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself. Positive integers that have exactly two different positive integer factors are called **primes**.

**DEFINITION** An integer $p$ greater than 1 is called *prime* if the only positive factors of $p$ are 1 and $p$. A positive integer that is greater than 1 and is not prime is called *composite*.

**Remark**: The integer n is composite if and only if there exists an integer a such that **a | n** and **1 < a < n.**

**THEOREM** **THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

**EXAMPLE** The prime factorizations of 100, 641, 999, and 1024 are given by

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,

$641 = 641$,

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$,

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$.

**Trial Division**

It is often important to show that a given integer is prime. For instance, in cryptology, large primes are used in some methods for making messages secret. One procedure for showing that an integer is prime is based on the following observation.

**THEOREM** If $n$ is a composite integer, then $n$ has a prime divisor less than or equal to $\sqrt{n}$.

From Theorem above, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root. This leads to the brute-force algorithm known as trial division. To use trial division we divide n by all primes not exceeding $\sqrt{n}$ and conclude that n is prime if it is not divisible by any of these primes. In Example 3 we use trial division to show that 101is prime.

**EXAMPLE** Show that 101 is prime.

**Solution**: The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

**EXAMPLE** Find the prime factorization of 7007.

***Solution***: To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with 7007/7 = 1001. Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because 1001/7 = 143. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and 143/11 = 13. Because 13 is prime, the procedure is completed. It follows that $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Consequently, the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

## Greatest Common Divisor and Least Common Multiple

### 1- Greatest Common Divisor

The largest integer that divides both of two integers is called the **greatest common divisor** of these integers.

**DEFINITION** Let $a$ and $b$ be integers, not both zero. The largest integer $d$ such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of $a$ and $b$. The greatest common divisor of $a$ and $b$ is denoted by $\gcd(a, b)$.

The greatest common divisor of two integers, not both zero, exists because the set of common divisors of these integers is nonempty and finite. One way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor.

**EXAMPLE** What is the greatest common divisor of 24 and 36?

*Solution:* The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, gcd(24, 36) = 12.

- **Relatively Prime**

The integers a and b are relatively prime if their greatest common divisor is 1.

**EXAMPLE** What is the greatest common divisor of 17 and 22?

Solution: The integers 17 and 22 have no positive common divisors other than 1, so that gcd(17, 22) = 1. So, 17 and 22 are relatively prime numbers.

**Finding the Greatest Common Divisor using Prime Factorization**

Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both, with zero exponents if necessary. Then:

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

**EXAMPLE** Because the prime factorizations of 120 and 500 are

$120 = 2^3 \cdot 3 \cdot 5,$ and

$500 = 2^2 \cdot 5^3,$

The greatest common divisor is:

$$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20.$$

### 2- Least Common Multiple

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by lcm(a; b).

**Finding the Least Common Multiple Using Prime Factorizations**
Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both, with zero exponents if necessary. Then:

$$\mathrm{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

**EXAMPLE** What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?
*Solution:* We have

$$\mathrm{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,\,4)} 3^{\max(5,\,3)} 7^{\max(2,\,0)} = 2^4 3^5 7^2$$

**THEOREM** Let $a$ and $b$ be positive integers. Then

$$ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b).$$

## The Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient. The reason is that it is time-consuming to find prime factorizations.

We will give a more efficient method of finding the greatest common divisor, called the

*Euclidean algorithm*. This algorithm has been known since ancient times. It is named after the ancient Greek mathematician Euclid, who included a description of this algorithm in his book *The Elements*.

We will show how Euclidean algorithm is used to find gcd(91, 287).

First, divide 287, the larger of the two integers, by 91, the smaller, to obtain

$287 = 91 \cdot 3 + 14.$

Any divisor of 91 and 287 must also be a divisor of $287 - 91 \cdot 3 = 14$. Also, any divisor of 91 and 14 must also be a divisor of $287 = 91 \cdot 3 + 14$. Hence, the greatest common divisor of 9 and 287 is the same as the greatest common divisor of 91 and 14. This means that the problem of finding gcd(91, 287) has been reduced to the problem of finding gcd(91, 14).

Next, divide 91 by 14 to obtain $91 = 14 \cdot 6 + 7$.

Because any common divisor of 91 and 14 also divides $91 - 14 \cdot 6 = 7$ and any common divisor of 14 and 7 divides 91, it follows that gcd(91, 14) = gcd(14, 7).

Continue by dividing 14 by 7, to obtain $14 = 7 \cdot 2$.

Because 7 divides 14, it follows that gcd(14, 7) = 7. Furthermore, because gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7, the original problem has been solved.

Generally, *Euclidean algorithm* state that:

Let $a = bq + r$ where $a; b; q$, and $r$ are integers. Then:

$$\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b}) = \mathbf{gcd}(\boldsymbol{b}, \boldsymbol{r})$$

Also written as:

$$\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b}) = \mathbf{gcd}((\boldsymbol{b}, (\boldsymbol{a} \textbf{\textit{ mod }} \boldsymbol{b}))$$

**EXAMPLE** Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

**Solution**: Successive uses of the division algorithm give:

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

$82 = 2 \cdot 41.$

Hence, gcd(414, 662) = 2, because 2 is the last nonzero remainder.

# Sequences and Summations

Sequences are ordered lists of elements, used in discrete mathematics in many ways. For example, they can be used to represent solutions to certain counting problems. They are also an important data structure in computer science. We will often need to work with sums of terms of sequences in our study of discrete mathematics. This section reviews the use of summation notation, basic properties of summations, and formulas for the sums of terms of some particular types of sequences.

## 1- Sequences

A sequence is a discrete structure used to represent an ordered list. For example, 1, 2, 3, 5, 8 is a sequence with five terms and 1, 3, 9, 27, 81 , . . . , $3^n$, . . . is an infinite sequence.

**DEFINITION** A *sequence* is a function from a subset of the set of integers (usually either the set $\{0, 1, 2, \ldots\}$ or the set $\{1, 2, 3, \ldots\}$) 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. We describe sequences by listing the terms of the sequence in order of increasing subscripts.

**EXAMPLE** Consider the sequence $\{a_n\}$, where $a_n = \frac{1}{n}$

The list of the terms of this sequence, beginning with $a1$, namely,

$a_1, a_2, a_3, a_4, \ldots,$

starts with

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots.$$

**DEFINITION** A *geometric progression* is a sequence of the form

$$a, ar, ar^2, \ldots, ar^n, \ldots$$

where the *initial term a* and the *common ratio r* are real numbers.

***Remark:*** A geometric progression is a discrete analogue of the exponential function $f(x) = ar^x$.

**EXAMPLE** The sequences $\{b_n\}$ with $b_n = (-1)^n$, $\{c_n\}$ with $c_n = 2 \cdot 5^n$, and $\{d_n\}$ with $d_n = 6 \cdot (1/3)^n$ are geometric progressions with initial term and common ratio equal to 1 and −1; 2 and 5; and 6 and 1/3, respectively, if we start at $n = 0$. The list of terms $b_0, b_1, b_2, b_3, b_4, \ldots$ begins with

$1, -1, 1, -1, 1, \ldots;$

the list of terms $c_0, c_1, c_2, c_3, c_4, \ldots$ begins with

$2, 10, 50, 250, 1250, \ldots;$

and the list of terms $d_0, d_1, d_2, d_3, d_4, \ldots$ begins with

$$6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \ldots.$$

**DEFINITION** An *arithmetic progression* is a sequence of the form

$$a, a+d, a+2d, \ldots, a+nd, \ldots$$

where the *initial term a* and the *common difference d* are real numbers.

***Remark:*** An arithmetic progression is a discrete analogue of the linear function $f(x) = dx + a$.

**EXAMPLE 3** The sequences $\{s_n\}$ with $s_n = -1 + 4n$ and $\{t_n\}$ with $t_n = 7 - 3n$ are both arithmetic progressions with initial terms and common differences equal to −1 and 4, and 7 and −3, respectively, if we start at $n = 0$. The list of terms $s_0, s_1, s_2, s_3, \ldots$ begins with −1, 3, 7, 11, . . . , and the list of terms $t_0, t_1, t_2, t_3, \ldots$ begins with 7, 4, 1,−2, . . . .

Sequences of the form $a_1, a_2, \ldots, a_n$ are often used in computer science. These finite sequences are also called **strings**. This string is also denoted by $a_1a_2 \ldots a_n$. The **length** of a string is the number of terms in this string. The **empty string**, denoted by $\lambda$, is the string that has no terms. The empty string has length zero.

**EXAMPLE** The string *abcd* is a string of length four.

- **Recurrence Relations**

In examples above we specified sequences by providing explicit formulas for their terms. There are many other ways to specify a sequence. For example, another way to specify a sequence is to *provide one or more initial terms together with a rule for determining subsequent terms from those that precede them.*

**DEFINITION** A *recurrence relation* for the sequence $\{a_n\}$ is an equation that expresses $a_n$ in terms of one or more of the previous terms of the sequence, namely, $a_0, a_1, \ldots, a_{n-1}$, for all integers $n$ with $n \geq n_0$, where $n_0$ is a nonnegative integer. A sequence is called a *solution* of a recurrence relation if its terms satisfy the recurrence relation. (A recurrence relation is said to *recursively define* a sequence. We will explain this alternative terminology in Chapter 5.)

**EXAMPLE** Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \ldots$, and suppose that $a_0 = 2$. What are $a_1$, $a_2$, and $a_3$?

**Solution**: We see from the recurrence relation that $a_1 = a_0 + 3 = 2 + 3 = 5$. It then follows that $a_2 = 5 + 3 = 8$ and $a_3 = 8 + 3 = 11$.

**EXAMPLE** Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$ , and suppose that $a_0 = 3$ and $a_1 = 5$. What are $a_2$ and $a_3$?

**Solution**: We see from the recurrence relation that $a_2 = a_1 - a_0 = 5 - 3 = 2$ and $a_3 = a_2 - a_1 = 2 - 5 = -3$.We can find $a_4$, $a_5$, and each successive term in a similar way.

**DEFINITION** The *Fibonacci sequence*, $f_0, f_1, f_2, \ldots$, is defined by the initial conditions $f_0 = 0$, $f_1 = 1$, and the recurrence relation

$$f_n = f_{n-1} + f_{n-2}$$

for $n = 2, 3, 4, \ldots$.

**EXAMPLE** Find the Fibonacci numbers $f_2$, $f_3$, $f_4$, $f_5$, and $f_6$.

**Solution**: The recurrence relation for the Fibonacci sequence tells us that we find successive terms by adding the previous two terms. Because the initial conditions tell us that $f_0 = 0$ and $f_1 = 1$, using the recurrence relation in the definition we find that

$f_2 = f_1 + f_0 = 1 + 0 = 1,$

$f_3 = f_2 + f_1 = 1 + 1 = 2,$

$f_4 = f_3 + f_2 = 2 + 1 = 3,$

$f_5 = f_4 + f_3 = 3 + 2 = 5,$

$f_6 = f_5 + f_4 = 5 + 3 = 8.$

**EXAMPLE** Suppose that $\{a_n\}$ is the sequence of integers defined by $a_n = n!$, the value of the factorial function at the integer $n$, where $n = 1, 2, 3, \ldots$. Because $n! = n((n-1)(n-2) \ldots 2 \cdot 1) = n(n-1)! = na_{n-1}$, we see that the sequence of factorials satisfies the recurrence relation $a_n = na_{n-1}$, together with the initial condition $a1 = 1$.

***NOTE****: We say that we have solved the recurrence relation together with the initial conditions when we find an explicit formula, called a* ***closed formula****, for the terms of the sequence.*

**EXAMPLE** Determine whether the sequence $\{a_n\}$, where $a_n = 3n$ for every nonnegative integer $n$, is a solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$ . Answer the same question where $a_n = 2^n$ and where $a_n = 5$.

***Solution***: Suppose that $a_n = 3n$ for every nonnegative integer $n$. Then, for $n \geq 2$, we see that $2a_{n-1} - a_{n-2} = 2(3(n-1)) - 3(n-2) = 3n = a_n$. Therefore, $\{a_n\}$, where $a_n = 3n$, is a solution of the recurrence relation.

Suppose that $a_n = 2^n$ for every nonnegative integer $n$. Note that $a_0 = 1$, $a_1 = 2$, and $a_2 = 4$. Because $2a_1 - a_0 = 2 \cdot 2 - 1 = 3 \neq a_2$, we see that $\{a_n\}$, where $a_n = 2^n$, is not a solution of the recurrence relation.

Suppose that $a_n = 5$ for every nonnegative integer $n$. Then for $n \geq 2$, we see that $a_n = 2a_{n-1} - a_{n-2} = 2 \cdot 5 - 5 = 5 = a_n$. Therefore, $\{a_n\}$, where $a_n = 5$, is a solution of the recurrence relation.

**EXAMPLE Compound Interest** Suppose that a person deposits $10,000 in a savings account at a bank yielding 11% per year with interest compounded annually. How much will be in the account after 30 years?

***Solution***: To solve this problem, let $P_n$ denote the amount in the account after $n$ years. Because the amount in the account after $n$ years equals the amount in the account after $n-1$ years plus interest for the $n$th year, we see that the sequence $\{P_n\}$ satisfies the recurrence relation $P_n = P_{n-1} + 0.11P_{n-1} = (1.11)P_{n-1}$.

The initial condition is $P_0 = 10{,}000$. We can use an iterative approach to find a formula for $P_n$. Note that

$P_1 = (1.11)P_0$

$P_2 = (1.11)P_1 = (1.11)^2P_0$

$P_3 = (1.11)P_2 = (1.11)^3P_0$

...

$P_n = (1.11)P_{n-1} = (1.11)^n P_0$.

When we insert the initial condition $P_0 = 10{,}000$, the formula $P_n = (1.11)^n 10{,}000$ is obtained.

Inserting $n = 30$ into the formula $P_n = (1.11)^n 10{,}000$ shows that after 30 years the account contains

$P_{30} = (1.11)^{30} 10{,}000 = \$228{,}922.97$.

**EXAMPLE** How can we produce the terms of a sequence if the first 10 terms are 5, 11, 17, 23, 29, 35, 41, 47, 53, 59?

***Solution**:* Note that each of the first 10 terms of this sequence after the first is obtained by adding 6 to the previous term. (We could see this by noticing that the difference between consecutive terms is 6.) Consequently, the $n$th term could be produced by starting with 5 and adding 6 a total of $n - 1$ times; that is, a reasonable guess is that the $n$th term is $5 + 6(n - 1) = 6n - 1$.

(This is an arithmetic progression with $a = 5$ and $d = 6$.)

**EXAMPLE** Conjecture a simple formula for $a_n$ if the first 10 terms of the sequence $\{a_n\}$ are 1, 7, 25, 79, 241, 727, 2185, 6559, 19681, 59047.

***Solution**:* To attack this problem, we begin by looking at the difference of consecutive terms, but we do not see a pattern. When we form the ratio of consecutive terms to see whether each term is a multiple of the previous term, we find that this ratio, although not a constant, is close to 3. So it is reasonable to suspect that the terms of this sequence are generated by a formula involving $3^n$. Comparing these terms with the corresponding terms of the sequence $\{3^n\}$, i.e. (3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, . . .), we notice that the $n$th term is 2 less than the corresponding power of 3. We see that $a_n = 3^n - 2$ for $1 \le n \le 10$ and conjecture that this formula holds for all $n$.

## 2- Summations

Next, we consider the addition of the terms of a sequence. For this we introduce **summation notation**. We begin by describing the notation used to express the sum of the terms

$a_m, a_{m+1}, \ldots, a_n$

from the sequence $\{an\}$.We use the notation

$$\sum_{j=m}^{n} a_j, \qquad \sum\nolimits_{j=m}^{n} a_j, \qquad \text{or} \qquad \sum\nolimits_{m \le j \le n} a_j$$

(read as the sum from $j = m$ to $j = n$ of $aj$ ) to represent

$am + am+1 + \cdot \cdot \cdot +an.$

Here, the variable $j$ is called the **index of summation**, and the choice of the letter $j$ as the variable is arbitrary; that is, we could have used any other letter, such as $i$ or $k$. Or, in notation,

$$\sum_{j=m}^{n} a_j = \sum_{i=m}^{n} a_i = \sum_{k=m}^{n} a_k.$$

Here, the index of summation runs through all integers starting with its **lower limit** $m$ and ending with its **upper limit** $n$. A large uppercase Greek letter sigma, $\sum$ , is used to denote summation.

The usual laws for arithmetic apply to summations. For example, when $a$ and $b$ are real numbers, we have

$$\sum\nolimits_{j=1}^{n}(ax_j + by_j) = a\sum\nolimits_{j=1}^{n} x_j + b\sum\nolimits_{j=1}^{n} y_j$$

where $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are real numbers.

**EXAMPLE** Use summation notation to express the sum of the first 100 terms of the sequence $\{a_j\}$, where $a_j = 1/j$ for $j = 1, 2, 3, \ldots$ .

***Solution***: The lower limit for the index of summation is 1, and the upper limit is 100. We write this sum as

$$\sum_{j=1}^{100} \frac{1}{j}.$$

**EXAMPLE** What is the value of $\sum_{j=1}^{5} j^2$?

***Solution:*** We have

$$\begin{aligned}\sum_{j=1}^{5} j^2 &= 1^2 + 2^2 + 3^2 + 4^2 + 5^2 \\ &= 1 + 4 + 9 + 16 + 25 \\ &= 55.\end{aligned}$$

**EXAMPLE** What is the value of $\sum_{k=4}^{8} (-1)^k$?

***Solution:*** We have

$$\begin{aligned}\sum_{k=4}^{8} (-1)^k &= (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8 \\ &= 1 + (-1) + 1 + (-1) + 1 \\ &= 1\end{aligned}$$

**EXAMPLE** Double summations arise in many contexts (as in the analysis of nested loops in computer programs). An example of a double summation is

$$\sum_{i=1}^{4} \sum_{j=1}^{3} ij.$$

To evaluate the double sum, first expand the inner summation and then continue by computing the outer summation:

$$\begin{aligned}\sum_{i=1}^{4} \sum_{j=1}^{3} ij &= \sum_{i=1}^{4} (i + 2i + 3i) \\ &= \sum_{i=1}^{4} 6i \\ &= 6 + 12 + 18 + 24 = 60.\end{aligned}$$

We can also use summation notation to add all values of a function, or terms of an indexed set, where the index of summation runs over all values in a set. That is, we write

$$\sum_{s \in S} f(s)$$

to represent the sum of the values *f (s)*, for all members *s* of *S*.

**EXAMPLE** What is the value of $\sum_{s \in \{0,2,4\}} s$?

***Solution**:* Because_*s* ∈ {0,2,4} *s* represents the sum of the values of *s* for all the members of the set {0, 2, 4}, it follows that

$$\sum_{s \in \{0,2,4\}} s = 0 + 2 + 4 = 6.$$

Certain sums arise repeatedly throughout discrete mathematics. Having a collection of formulae for such sums can be useful; Table 1 provides a small table of formulae for commonly occurring sums.

**EXAMPLE** Find $\sum_{k=50}^{100} k^2$.

***Solution**:* First note that because $\sum_{k=1}^{100} k^2 = \sum_{k=1}^{49} k^2 + \sum_{k=50}^{100} k^2$, we have

$$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2.$$

Using the formula $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$ from Table 1 we see that

$$\sum_{k=50}^{100} k^2 = \frac{100 \cdot 101 \cdot 201}{6} - \frac{49 \cdot 50 \cdot 99}{6} = 338{,}350 - 40{,}425 = 297{,}925.$$

**TABLE 1 Some Useful Summation Formulae.**

| *Sum* | *Closed Form* |
|---|---|
| $\sum_{k=0}^{n} ar^k \ (r \neq 0)$ | $\frac{ar^{n+1}-a}{r-1}, r \neq 1$ |
| $\sum_{k=1}^{n} k$ | $\frac{n(n+1)}{2}$ |
| $\sum_{k=1}^{n} k^2$ | $\frac{n(n+1)(2n+1)}{6}$ |
| $\sum_{k=1}^{n} k^3$ | $\frac{n^2(n+1)^2}{4}$ |
| $\sum_{k=0}^{\infty} x^k, \lvert x\rvert < 1$ | $\frac{1}{1-x}$ |
| $\sum_{k=1}^{\infty} kx^{k-1}, \lvert x\rvert < 1$ | $\frac{1}{(1-x)^2}$ |

# Counting

Suppose that a password on a computer system consists of six, seven, or eight characters. Each of these characters must be a digit or a letter of the alphabet. Each password must contain at least one digit. How many such passwords are there? The techniques needed to answer this question and a wide variety of other counting problems will be introduced in this section. Counting problems arise throughout mathematics and computer science. For example, we must count the successful outcomes of experiments and all the possible outcomes of these experiments to determine probabilities of discrete events. We need to count the number of operations used by an algorithm to study its time complexity. We will introduce the basic techniques of counting in this section. These methods serve as the foundation for almost all counting techniques.

## Basic Counting Principles

We first present two basic counting principles, the ***product rule*** and the ***sum rule***. Then we will show how they can be used to solve many different counting problems.

**1- THE PRODUCT RULE** Suppose that a procedure can be broken down into a sequence of two tasks. If there are $n_1$ ways to do the first task and for each of these ways of doing the first task, there are $n_2$ ways to do the second task, then there are $n_1n_2$ ways to do the procedure.

**EXAMPLE 1** A new company with just two employees, Sanchez and Patel, rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?

**Solution**: The procedure of assigning offices to these two employees consists of assigning an office to Sanchez, which can be done in 12 ways, then assigning an office to Patel different from the office assigned to Sanchez, which can be done in 11 ways. By the product rule, there are $12 \cdot 11 = 132$ ways to assign offices to these two employees.

**EXAMPLE 2** The chairs of an auditorium are to be labeled with an uppercase English letter followed by a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently?

**Solution**: The procedure of labeling a chair consists of two tasks, namely, assigning to the seat one of the 26 uppercase English letters, and then assigning to it one of the 100 possible integers.

The product rule shows that there are $26 \cdot 100 = 2600$ different ways that a chair can be labeled. Therefore, the largest number of chairs that can be labeled differently is 2600.

**EXAMPLE 3** There are 32 microcomputers in a computer center. Each microcomputer has 24 ports. How many different ports to a microcomputer in the center are there?

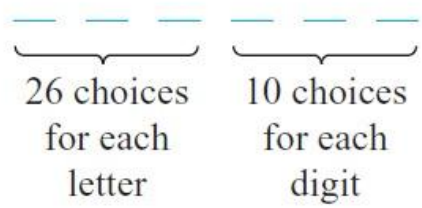
**Solution**: The procedure of choosing a port consists of two tasks, first picking a microcomputer and then picking a port on this microcomputer. Because there are 32 ways to choose the microcomputer and 24 ways to choose the port no matter which microcomputer has been selected, the product rule shows that there are $32 \cdot 24 = 768$ ports.

- An extended version of the product rule is often useful. Suppose that a procedure is carried out by performing the tasks $T_1, T_2, \ldots, T_m$ in sequence. If each task $T_i$, $i = 1, 2, \ldots, n$, can be done in $n_i$ ways, regardless of how the previous tasks were done, then there are $n_1 \cdot n_2 \cdot \cdots \cdot n_m$ ways to carry out the procedure.

**EXAMPLE 4** How many different bit strings of length seven are there?

**Solution**: Each of the seven bits can be chosen in two ways, because each bit is either 0 or 1. Therefore, the product rule shows there are a total of 27 = 128 different bit strings of length seven.

**EXAMPLE 5** How many different license plates can be made if each plate contains a sequence of three uppercase English letters followed by three digits (and no sequences of letters are prohibited, even if they are obscene)?




**Solution**: There are 26 choices for each of the three uppercase English letters and ten choices for each of the three digits. Hence, by the product rule there are a total of $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 17{,}576{,}000$ possible license plates.

**EXAMPLE 6 *Counting Functions*:** How many functions are there from a set with $m$ elements to a set with $n$ elements?

**Solution**: A function corresponds to a choice of one of the $n$ elements in the codomain for each of the $m$ elements in the domain. Hence, by the product rule there are $n \cdot n \cdot \cdots \cdot n = nm$ functions from a set with $m$ elements to one with $n$ elements. For example, there are $5^3 = 125$ different functions from a set with three elements to a set with five elements.

**EXAMPLE 7 *Counting One-to-One***: Functions How many one-to-one functions are there from a set with $m$ elements to one with $n$ elements?

**Solution**: First note that when $m > n$ there are no one-to-one functions from a set with $m$ elements to a set with $n$ elements.

Now let $m \leq n$. Suppose the elements in the domain are $a_1, a_2, \ldots, a_m$. There are $n$ ways to choose the value of the function at $a_1$. Because the function is one-to-one, the value of the function at $a_2$ can be picked in $n - 1$ ways (because the value used for $a_1$ cannot be used again).

In general, the value of the function at $a_k$ can be chosen in $n - k + 1$ ways. By the product rule, there are $n(n - 1)(n - 2) \cdots (n - m + 1)$ one-to-one functions from a set with $m$ elements to one with $n$ elements.

For example, there are $5 \cdot 4 \cdot 3 = 60$ one-to-one functions from a set with three elements to a set with five elements.

**EXAMPLE 8** ***The Telephone Numbering Plan***: The North American numbering plan (*NANP*) specifies the format of telephone numbers in the U.S., Canada, and many other parts of North America. A telephone number in this plan consists of 10 digits, which are split into a three-digit area code, a three-digit office code, and a four-digit station code. To specify the allowable format, let X denote a digit that can take any of the values 0 through 9, let N denote a digit that can take any of the values 2 through 9, and let Y denote a digit that must be a 0 or a 1. Two numbering plans, which will be called the old plan, and the new plan, will be discussed. In the old plan, the formats of the area code, office code, and station code are NYX, NNX, and XXXX, respectively, so that telephone numbers had the form NYX-NNX-XXXX. In the new plan, the formats of these codes are NXX, NXX, and XXXX, respectively, so that telephone numbers have the form NXX-NXX-XXXX.

How many different North American telephone numbers are possible under the old plan and under the new plan?

**Solution**: By the product rule, there are $8 \cdot 2 \cdot 10 = 160$ area codes with format NYX and $8 \cdot 10 \cdot 10 = 800$ area codes with format NXX. Similarly, by the product rule, there are $8 \cdot 8 \cdot 10 = 640$ office codes with format NNX. The product rule also shows that there are:
$10 \cdot 10 \cdot 10 \cdot 10 = 10{,}000$ station codes with format XXXX.

Consequently, applying the product rule again, it follows that under the old plan there are $160 \cdot 640 \cdot 10{,}000 =$ **1,024,000,000** different numbers available in North America.

Under the new plan, there are $800 \cdot 800 \cdot 10{,}000 =$ **6,400,000,000** different numbers available.

**2- THE SUM RULE** If a task can be done either in one of $n_1$ ways or in one of $n_2$ ways, where none of the set of $n_1$ ways is the same as any of the set of $n_2$ ways, then there are $n_1 + n_2$ ways to do the task.

**EXAMPLE 9** Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee. How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student?

**Solution**: There are 37 ways to choose a member of the mathematics faculty and there are 83 ways to choose a student who is a mathematics major. Choosing a member of the mathematics faculty is never the same as choosing a student who is a mathematics major because no one is both a faculty member and a student. By the sum rule it follows that there are $37 + 83 = 120$ possible ways to pick this representative.

- We can extend the sum rule to more than two tasks. Suppose that a task can be done in one of $n_1$ ways, in one of $n_2$ ways, . . . , or in one of $n_m$ ways, where none of the set of $n_i$ ways of doing the task is the same as any of the set of $n_j$ ways, for all pairs $i$ and $j$ with $1 \leq i < j \leq m$. Then the number of ways to do the task is $n_1 + n_2 + \cdots + n_m$.

**EXAMPLE 10** A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

**Solution**: The student can choose a project by selecting a project from the first list, the second list, or the third list. Because no project is on more than one list, by the sum rule there are 23 + 15 + 19 = 57 ways to choose a project.

**More Complex Counting Problems**

Many counting problems cannot be solved using just the sum rule or just the product rule. However, many complicated counting problems can be solved using both of these rules in combination.

**EXAMPLE 11** In a version of the computer language BASIC, the name of a variable is a string of one or two alphanumeric characters, where uppercase and lowercase letters are not distinguished. (An alphanumeric character is either one of the 26 English letters or one of the 10 digits.) Moreover, a variable name must begin with a letter and must be different from the five strings of two characters that are reserved for programming use. How many different variable names are there in this version of BASIC?

**Solution**: Let $V$ equal the number of different variable names in this version of BASIC. Let $V_1$ be the number of these that are one character long and $V_2$ be the number of these that are two characters long. Then by the sum rule, $V = V_1 + V_2$. Note that $V_1 = 26$, because a one-character variable name must be a letter. Furthermore, by the product rule there are $26 \cdot 36$ strings of length two that begin with a letter and end with an alphanumeric character. However, five of these are excluded, so $V_2 = 26 \cdot 36 - 5 = 931$. Hence, there are $V = V_1 + V_2 = 26 + 931 = 957$ different names for variables in this version of BASIC.

**EXAMPLE 12** Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there?

**Solution**: Let $P$ be the total number of possible passwords, and let $P_6$, $P_7$, and $P_8$ denote the number of possible passwords of length $6$, $7$, and $8$, respectively. By the sum rule, $P = P_6 + P_7 + P_8$.We will now find $P_6$, $P_7$, and $P_8$. Finding $P_6$ directly is difficult. To find $P_6$ it is easier to find the number of strings of uppercase letters and digits that are six characters long, including those with no digits, and subtract from this the number of strings with no digits. By the product rule, the number of strings of six characters is $36^6$, and the number of strings with no digits is $26^6$. Hence,

$P_6 = 36^6 - 26^6 = 2{,}176{,}782{,}336 - 308{,}915{,}776 = 1{,}867{,}866{,}560.$

Similarly, we have

$P_7 = 36^7 - 26^7 = 78{,}364{,}164{,}096 - 8{,}031{,}810{,}176 = 70{,}332{,}353{,}920$

and

$P_8 = 36^8 - 26^8 = 2{,}821{,}109{,}907{,}456 - 208{,}827{,}064{,}576 = 2{,}612{,}282{,}842{,}880.$

Consequently,

$P = P_6 + P_7 + P_8 = 2{,}684{,}483{,}063{,}360.$

### 3- The Subtraction Rule

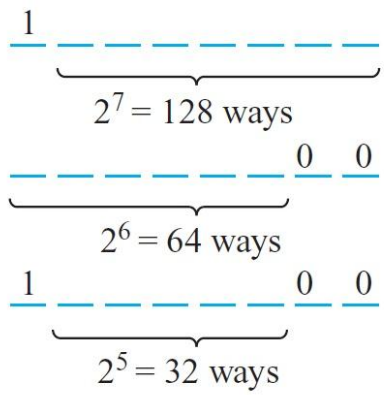
Suppose that a task can be done in one of two ways, but some of the ways to do it are common to both ways. In this situation, we cannot use the sum rule to count the number of ways to do the task. If we add the number of ways to do the tasks in these two ways, we get an overcount of the total number 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.

THE SUBTRACTION 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 *A1* 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 13** How many bit strings of length eight either start with a 1 bit or end with the two bits 00?




***Solution****:* We can construct a bit string of length eight that either 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 14** A computer Company receives 350 applications from computer graduates for a job planning a line of new Web servers. Suppose that 220 of these applicants majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business?

***Solution**:* To find the number of these applicants who majored neither in computer science nor in business, we can subtract the number of students who majored either in computer science or in business (or both) from the total number of applicants. Let $A_1$ be the set of students who majored in computer science and $A_2$ the set of students who majored in business. Then $A_1 \cup A_2$ is the set of students who majored in computer science or business (or both), and $A_1 \cap A_2$ is the set of students who majored both in computer science and in business. By the subtraction rule the number of students who majored either in computer science or in business (or both) equals

$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 220 + 147 - 51 = 316.$

We conclude that $350 - 316 = 34$ of the applicants majored neither in computer science nor in business.

- The subtraction rule, or the principle of inclusion–exclusion, can be generalized to find the number of ways to do one of $n$ different tasks or, equivalently, to find the number of elements in the union of $n$ sets, whenever $n$ is a positive integer.

### 4- The Division Rule

We have introduced the product, sum, and subtraction rules for counting. You may wonder whether there is also a division rule for counting. In fact, there is such a rule, which can be useful when solving certain types of enumeration problems.

> THE DIVISION RULE There are $n/d$ ways to do a task if it can be done using a procedure that can be carried out in $n$ ways, and for every way $w$, exactly $d$ of the $n$ ways correspond to way $w$.

We can restate the division rule in terms of sets: "If the finite set $A$ is the union of $n$ pairwise disjoint subsets each with $d$ elements, then $n = |A|/d$." We can also formulate the division rule in terms of functions: "If $f$ is a function from $A$ to $B$ where $A$ and $B$ are finite sets, and that for every value $y \in B$ there are exactly $d$ values $x \in A$ such that $f(x) = y$ (in which case, we say that $f$ is $d$-to-one), then $|B| = |A|/d$."

**EXAMPLE 15** How many different ways are there to seat four people around a circular table, where two seatings are considered the same when each person has the same left neighbor and the same right neighbor?

***Solution***: We arbitrarily select a seat at the table and label it seat 1. We number the rest of the seats in numerical order, proceeding clockwise around the table. Note that are four ways to select the person for seat 1, three ways to select the person for seat 2, two ways to select the person for seat 3, and one way to select the person for seat 4. Thus, there are $4! = 24$ ways to order the given four people for these seats. However, each of the four choices for seat 1 leads to the same arrangement, as we distinguish two arrangements only when one of the people has a different immediate left or immediate right neighbor. Because there are four ways to choose the person for seat 1, by the division rule there are $24/4 = 6$ different seating arrangements of four people around the circular table.

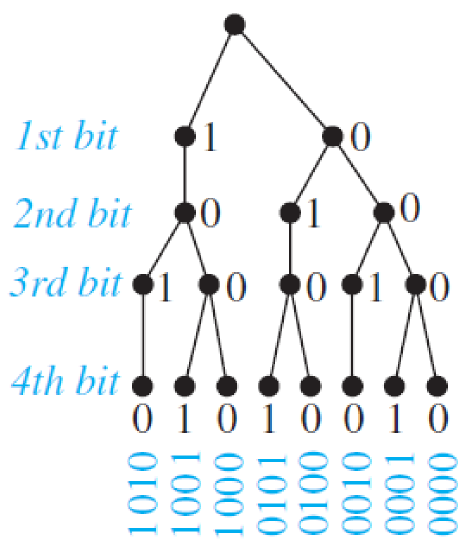
## 5- Tree Diagrams

Counting problems can be solved using **tree diagrams**. A tree consists of a root, a number of branches leaving the root, and possible additional branches leaving the endpoints of other branches. To use trees in counting, we use a branch to represent each possible choice. We represent the possible outcomes by the leaves, which are the endpoints of branches not having other branches starting at them.

Note that when a tree diagram is used to solve a counting problem, the number of choices of which branch to follow to reach a leaf can vary.

**EXAMPLE 16** How many bit strings of length four do not have two consecutive 1s?

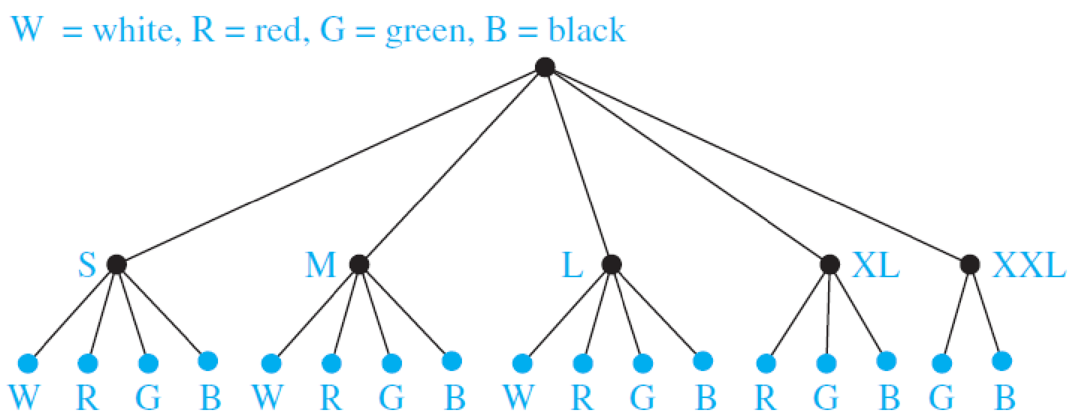
***Solution:*** The tree diagram in Figure 2 displays all bit strings of length four without two consecutive 1s. We see that there are eight bit strings of length four without two consecutive 1s.




**EXAMPLE 17** Suppose that “I Love New Jersey” T-shirts come in five different sizes: S, M, L, XL, and XXL. Further suppose that each size comes in four colors, white, red, green, and black, except for XL, which comes only in red, green, and black, and XXL,

which comes only in green and black. How many different shirts does a souvenir shop have to stock to have at least one of each available size and color of the T-shirt?

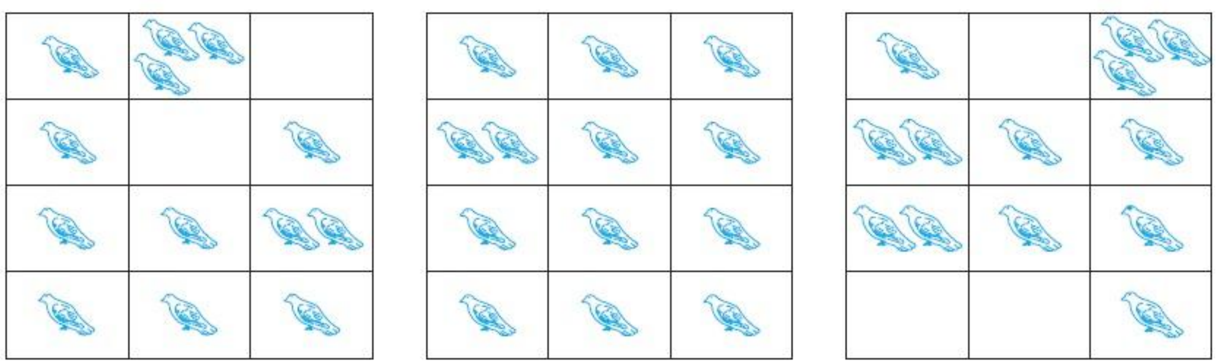
***Solution:*** The tree diagram in Figure 4 displays all possible size and color pairs. It follows that the souvenir shop owner needs to stock 17 different T-shirts.



# The Pigeonhole Principle

Suppose that a flock of 20 pigeons flies into a set of 19 pigeonholes to roost. Because there are 20 pigeons but only 19 pigeonholes, a least one of these 19 pigeonholes must have at least two pigeons in it. To see why this is true, note that if each pigeonhole had at most one pigeon in it, at most 19 pigeons, one per hole, could be accommodated. This illustrates a general principle called the **pigeonhole principle**, which states that if there are more pigeons than pigeonholes, then there must be at least one pigeonhole with at least two pigeons in it (see Figure 1). Of course, this principle applies to other objects besides pigeons and pigeonholes.

**THEOREM** **THE PIGEONHOLE PRINCIPLE** If $k$ is a positive integer and $k + 1$ or more objects are placed into $k$ boxes, then there is at least one box containing two or more of the objects.



(a) (b) (c)

**FIGURE 1** **There Are More Pigeons Than Pigeonholes.**

We will illustrate the usefulness of the pigeonhole principle. We first show that it can be used to prove a useful corollary about functions.

**COROLLARY 1** A function $f$ from a set with $k + 1$ or more elements to a set with $k$ elements is not one-to-one.

***Proof:*** Suppose that for each element *y* in the codomain of *f* we have a box that contains all elements *x* of the domain of *f* such that $f(x) = y$. Because the domain contains $k + 1$ or more elements and the codomain contains only *k* elements, the pigeonhole principle tells us that one of these boxes contains two or more elements *x* of the domain. This means that *f* cannot be one-to-one.

**EXAMPLE 1** Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.

**EXAMPLE 2** In any group of 27 English words, there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.

**EXAMPLE 3** How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points?

***Solution:*** There are 101 possible scores on the final. The pigeonhole principle shows that among any 102 students there must be at least 2 students with the same score.

**THE GENERALIZED PIGEONHOLE PRINCIPLE** If *N* objects are placed into *k* boxes, then there is at least one box containing at least $\lceil N/K \rceil$ objects.

**EXAMPLE 4** Among 100 people there are at least $\lceil 100/12 \rceil$= 9 who were born in the same month.

**EXAMPLE 5** What is the minimum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D, and F?

***Solution****:* The minimum number of students needed to ensure that at least six students receive the same grade is the smallest integer $N$ such that $\lceil N/5 \rceil = 6$. The smallest such integer is $N = 5 \cdot 5 + 1 = 26$. If you have only 25 students, it is possible for there to be five who have received each grade so that no six students have received the same grade. Thus, 26 is the minimum number of students needed to ensure that at least six students will receive the same grade.

**EXAMPLE 6** How many cards must be selected from a standard deck of 52 cards to guarantee that at least three cards of the same suit are chosen?

***Solution****:* Suppose there are four boxes, one for each suit, and as cards are selected they are placed in the box reserved for cards of that suit. Using the generalized pigeonhole principle, we see that if $N$ cards are selected, there is at least one box containing at least $\lceil N/4 \rceil$ cards. Consequently, we know that at least three cards of one suit are selected if $\lceil N/4 \rceil \geq 3$. The smallest integer $N$ such that $\lceil N/4 \rceil \geq 3$ is $N = 2 \cdot 4 + 1 = 9$, so nine cards suffice. Note that if eight cards are selected, it is possible to have two cards of each suit, so more than eight cards are needed. Consequently, nine cards must be selected to guarantee that at least three cards of one suit are chosen. One good way to think about this is to note that after the eighth card is chosen, there is no way to avoid having a third card of some suit.

**EXAMPLE 7** What is the least number of area codes needed to guarantee that the 25 million phones in a state can be assigned distinct 10-digit telephone numbers? (Assume that telephone numbers are of the form *NXX*-*NXX*-*XXXX*, where the first three digits form the area code, $N$ represents a digit from 2 to 9 inclusive, and $X$ represents any digit.)

***Solution**:* There are eight million different phone numbers of the form *NXX-XXXX*. Hence, by the generalized pigeonhole principle, among 25 million telephones, at least $\lceil 25{,}000{,}000/8{,}000{,}000 \rceil$= 4 of them must have identical phone numbers. Hence, at least four area codes are required to ensure that all 10-digit numbers are different.

# Permutations and Combinations

## Introduction

Many counting problems can be solved by finding the number of ways to arrange a specified number of distinct elements of a set of a particular size, where the order of these elements matters. Many other counting problems can be solved by finding the number of ways to select a particular number of elements from a set of a particular size, where the order of the elements selected does not matter. For example, in how many ways can we select three students from a group of five students to stand in line for a picture? How many different committees of three students can be formed from a group of four students? In this section we will develop methods to answer questions such as these.

### 1- Permutations

We begin by solving the first question posed in the introduction to this section, as well as related questions.

**EXAMPLE 1** In how many ways can we select three students from a group of five students to stand in line for a picture? In how many ways can we arrange all five of these students in a line for a picture?

***Solution***: First, note that the order in which we select the students matters. There are five ways to select the first student to stand at the start of the line. Once this student has been selected, there are four ways to select the second student in the line. After the first and second students have been selected, there are three ways to select the third student in the line. By the product rule, there are $5 \cdot 4 \cdot 3 = 60$ ways to select three students from a group of five students to stand in line for a picture.

To arrange all five students in a line for a picture, we select the first student in five ways, the second in four ways, the third in three ways, the fourth in two ways, and the fifth in one way. Consequently, there are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ ways to arrange all five students in a line for a picture.

Example 1 illustrates how ordered arrangements of distinct objects can be counted. This leads to some terminology.
A **permutation** of a set of distinct objects is an ordered arrangement of these objects.
We also are interested in ordered arrangements of some of the elements of a set. An ordered arrangement of *r* elements of a set is called an ***r*-permutation**.
**EXAMPLE 2** Let S = {1, 2, 3}.The ordered arrangement 3, 1, 2 is a permutation of S. The ordered arrangement 3, 2 is a 2-permutation of S.

The number of r-permutations of a set with n elements is denoted by $P(n, r)$. We can find $P(n, r)$ using the product rule.

**EXAMPLE 3** Let S = {a, b, c}. The 2-permutations of S are the ordered arrangements a, b; a, c; b, a; b, c; c, a; and c, b. Consequently, there are six 2-permutations of this set with three elements. There are always six 2-permutations of a set with three elements. There are three ways to choose the first element of the arrangement. There are two ways to choose the second element of the arrangement, because it must be different from the first element. Hence, by the product rule, we see that $P(3, 2) = 3 \cdot 2 = 6$. the first element. By the product rule, it follows that $P(3, 2) = 3 \cdot 2 = 6$.
We now use the product rule to find a formula for $P(n, r)$ whenever n and r are positive integers with $1 \leq r \leq n$.

**THEOREM 1** If $n$ is a positive integer and $r$ is an integer with $1 \leq r \leq n$, then there are

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

$r$-permutations of a set with $n$ distinct elements.

**COROLLARY 1** If $n$ and $r$ are integers with $0 \leq r \leq n$, then $P(n, r) = \dfrac{n!}{(n-r)!}$.

**EXAMPLE 4** How many ways are there to select a first-prize winner, a second-prize winner, and a third-prize winner from 100 different people who have entered a contest?

***Solution**:* Because it matters which person wins which prize, the number of ways to pick the three prize winners is the number of ordered selections of three elements from a set of 100 elements, that is, the number of 3-permutations of a set of 100 elements. Consequently, the answer is

$P(100, 3) = 100 \cdot 99 \cdot 98 = 970{,}200.$

**EXAMPLE 5** Suppose that a saleswoman has to visit eight different cities. She must begin her trip in a specified city, but she can visit the other seven cities in any order she wishes. How many possible orders can the saleswoman use when visiting these cities?

*Solution:* The number of possible paths between the cities is the number of permutations of seven elements, because the first city is determined, but the remaining seven can be ordered arbitrarily. Consequently, there are $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$ ways for the saleswoman to choose her tour. If, for instance, the saleswoman wishes to find the path between the cities with minimum distance, and she computes the total distance for each possible path, she must consider a total of 5040 paths!

**EXAMPLE 6** How many permutations of the letters *ABCDEFGH* contain the string *ABC* ?

***Solution:*** Because the letters *ABC* must occur as a block, we can find the answer by finding the number of permutations of six objects, namely, the block *ABC* and the individual letters *D*, *E*, *F*, *G*, and *H*. Because these six objects can occur in any order, there are $6! = 720$ permutations of the letters *ABCDEFGH* in which *ABC* occurs as a block.

## 2- Combinations

We now turn our attention to counting unordered selections of objects. We begin by solving a question posed in the introduction to this section.

**EXAMPLE 7** How many different committees of three students can be formed from a group of four students?

***Solution:*** To answer this question, we need only find the number of subsets with three elements from the set containing the four students. We see that there are four such subsets, one for each of the four students, because choosing three students is the same as choosing one of the four students to leave out of the group. This means that there are four ways to choose the three students for the committee, where the order in which these students are chosen does not matter.

Example 8 illustrates that many counting problems can be solved by finding the number of subsets of a particular size of a set with *n* elements, where *n* is a positive integer.

An ***r*-combination** of elements of a set is an unordered selection of *r* elements from the set.

Thus, an *r*-combination is simply a subset of the set with *r* elements.

**EXAMPLE 8** Let *S* be the set {1, 2, 3, 4}. Then {1, 3, 4} is a 3-combination from *S*. (Note that {4, 1, 3} is the same 3-combination as {1, 3, 4}, because the order in which the elements of a set are listed does not matter.)

The number of *r*-combinations of a set with *n* distinct elements is denoted by $C(n, r)$.

**EXAMPLE 9** We see that $C(4, 2) = 6$, because the 2-combinations of {a, b, c, d} are the six subsets {a, b}, {a, c}, {a, d}, {b, c}, {b, d}, and {c, d}.

We can determine the number of *r*-combinations of a set with *n* elements using the formula for the number of *r*-permutations of a set. To do this, note that the *r*-permutations of a set can be obtained by first forming *r*-combinations and then ordering the elements in these combinations.

**THEOREM 2** The number of $r$-combinations of a set with $n$ elements, where $n$ is a nonnegative integer and $r$ is an integer with $0 \leq r \leq n$, equals

$$C(n, r) = \frac{n!}{r!\,(n-r)!}.$$

**EXAMPLE 10** How many ways are there to select five players from a 10-member tennis team to make a trip to a match at another school?

***Solution***: The answer is given by the number of 5-combinations of a set with 10 elements. By Theorem 2, the number of such combinations is

$$C(10, 5) = \frac{10!}{5!\,5!} = 252.$$

**EXAMPLE 11** How many bit strings of length *n* contain exactly *r* 1s?

***Solution:*** The positions of *r* 1s in a bit string of length *n* form an *r*-combination of the set $\{1, 2, 3, \ldots, n\}$. Hence, there are $C(n, r)$ bit strings of length *n* that contain exactly *r* 1s.

**EXAMPLE 12** Suppose that there are 9 faculty members in the mathematics department and 11 in the computer science department. How many ways are there to select a committee to develop a discrete mathematics course at a school if the committee is to consist of three faculty members from the mathematics department and four from the computer science department?

***Solution****:* By the product rule, the answer is the product of the number of 3-combinations of a set with nine elements and the number of 4-combinations of a set with 11 elements. By Theorem 2, the number of ways to select the committee is

$C(9, 3) \cdot C(11, 4) = \frac{9!}{3!\,6!} \cdot \frac{11!}{4!\,7!} = 84 \cdot 330 = 27{,}720.$

# Binomial Coefficients and Identities

The number of *r*-combinations from a set with *n* elements is also denoted by $\binom{n}{r}$ in addition to $C(n, r)$. This number is also called a **binomial coefficient** because these numbers occur as coefficients in the expansion of powers of binomial expressions such as $(a + b)^n$.

**The Binomial Theorem**

The binomial theorem gives the coefficients of the expansion of powers of binomial expressions.

A **binomial** expression is simply the sum of two terms, such as $x + y$.

Example 1 illustrates how the coefficients in a typical expansion can be found and prepares us for the statement of the binomial theorem.

**EXAMPLE 1** The expansion of $(x + y)^3$ can be found using combinatorial reasoning instead of multiplying the three terms out. When $(x + y)^3 = (x + y)(x + y)(x + y)$ is expanded, all products of a term in the first sum, a term in the second sum, and a term in the third sum are added. Terms of the form $x^3$, $x^2y$, $xy^2$, and $y^3$ arise. To obtain a term of the form $x^3$, an $x$ must be chosen in each of the sums, and this can be done in only one way. Thus, the $x^3$ term in the product has a coefficient of 1. To obtain a term of the form $x^2y$, an $x$ must be chosen in two of the three sums (and consequently a $y$ in the other sum). Hence, the number of such terms is the number of 2-combinations of three objects, namely, $\binom{3}{2}$. Similarly, the number of terms of the form $xy^2$ is the number of ways to pick one of the three sums to obtain an $x$ (and consequently take a $y$ from each of the other two sums). This can be done in $\binom{3}{1}$ways. Finally, the only way to obtain a $y^3$ term is to choose the $y$ for each of the three sums in the product, and this can be done in exactly one way. Consequently, it follows that

$(x + y)^3 = (x + y)(x + y)(x + y) = (xx + xy + yx + yy)(x + y)$

$= xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$

$= x^3 + 3x^2y + 3xy^2 + y^3.$

**THEOREM 1** **THE BINOMIAL THEOREM** Let $x$ and $y$ be variables, and let $n$ be a nonnegative integer. Then

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

**EXAMPLE 2** What is the expansion of $(x + y)^4$?

***Solution:*** From the binomial theorem it follows that

$$\begin{aligned}(x+y)^4 &= \sum_{j=0}^{4} \binom{4}{j} x^{4-j} y^j \\ &= \binom{4}{0} x^4 + \binom{4}{1} x^3 y + \binom{4}{2} x^2 y^2 + \binom{4}{3} x y^3 + \binom{4}{4} y^4 \\ &= x^4 + 4x^3 y + 6x^2 y^2 + 4xy^3 + y^4.\end{aligned}$$

**EXAMPLE 3** What is the coefficient of $x^{12}y^{13}$ in the expansion of $(x + y)^{25}$?

*Solution:* From the binomial theorem it follows that this coefficient is

$$\binom{25}{13} = \frac{25!}{13!\,12!} = 5{,}200{,}300.$$

**EXAMPLE 4** What is the coefficient of $x^{12}y^{13}$ in the expansion of $(2x - 3y)^{25}$?

*Solution:* First, note that this expression equals $(2x + (-3y))^{25}$. By the binomial theorem, we have

$$(2x + (-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j} (-3y)^j.$$

Consequently, the coefficient of $x^{12}y^{13}$ in the expansion is obtained when $j = 13$, namely,

$$\binom{25}{13}2^{12}(-3)^{13} = -\frac{25!}{13!\,12!}2^{12}3^{13}.$$

We can prove some useful identities using the binomial theorem, as Corollaries 1, 2, and 3 demonstrate.

**COROLLARY 1** Let $n$ be a nonnegative integer. Then

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n.$$

*Proof:* Using the binomial theorem with $x = 1$ and $y = 1$, we see that

$$2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}1^k 1^{n-k} = \sum_{k=0}^{n}\binom{n}{k}.$$

This is the desired result.

**COROLLARY 2** Let $n$ be a positive integer. Then

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0.$$

*Proof:* When we use the binomial theorem with $x = -1$ and $y = 1$, we see that

$$0 = 0^n = ((-1) + 1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k.$$

This proves the corollary.

***Remark:*** Corollary 2 implies that

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots .$$

**COROLLARY 3** Let $n$ be a nonnegative integer. Then

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n.$$

*Proof:* We recognize that the left-hand side of this formula is the expansion of $(1 + 2)^n$ provided by the binomial theorem. Therefore, by the binomial theorem, we see that

$$(1 + 2)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 2^k = \sum_{k=0}^{n} \binom{n}{k} 2^k.$$

Hence

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n.$$

## Pascal's Identity and Triangle

The binomial coefficients satisfy many different identities. We introduce one of the most important of these now.

**THEOREM 2** **PASCAL'S IDENTITY** Let $n$ and $k$ be positive integers with $n \geq k$. Then

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

Pascal's identity is the basis for a geometric arrangement of the binomial coefficients in a triangle, as shown in Figure 1.

The *n*th row in the triangle consists of the binomial coefficients

$$\binom{n}{k}, \; k = 0, 1, \ldots, n.$$

This triangle is known as **Pascal's triangle**. Pascal's identity shows that when two adjacent binomial coefficients in this triangle are added, the binomial coefficient in the next row between these two coefficients is produced.

$$
\begin{array}{c}
\binom{0}{0} \\
\binom{1}{0}\ \binom{1}{1} \\
\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \\
\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} \\
\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4} \\
\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5} \\
\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6} \\
\binom{7}{0}\ \binom{7}{1}\ \binom{7}{2}\ \binom{7}{3}\ \binom{7}{4}\ \binom{7}{5}\ \binom{7}{6}\ \binom{7}{7} \\
\binom{8}{0}\ \binom{8}{1}\ \binom{8}{2}\ \binom{8}{3}\ \binom{8}{4}\ \binom{8}{5}\ \binom{8}{6}\ \binom{8}{7}\ \binom{8}{8} \\
\cdots
\end{array}
$$

(a)

By Pascal's identity:

$$\binom{6}{4} + \binom{6}{5} = \binom{7}{5}$$

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1 \\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1 \\
\cdots
\end{array}
$$

(b)

**FIGURE 1 Pascal's Triangle.**

## Permutations with Repetition

Counting permutations when repetition of elements is allowed can easily be done using the product rule, as Example 1 shows.

**EXAMPLE 1** How many strings of length $r$ can be formed from the uppercase letters of the English alphabet?

***Solution:*** By the product rule, because there are 26 uppercase English letters, and because each letter can be used repeatedly, we see that there are $26^r$ strings of uppercase English letters of length $r$.

**THEOREM** The number of $r$-permutations of a set of $n$ objects with repetition allowed is $n^r$.

*Proof:* There are $n$ ways to select an element of the set for each of the r positions in the $r$-permutation when repetition is allowed, because for each choice all $n$ objects are available. Hence, by the product rule there are $n^r$ $r$-permutations when repetition is allowed.

## Combinations with Repetition

Consider these examples of combinations with repetition of elements allowed.

**EXAMPLE 2** How many ways are there to select four pieces of fruit from a bowl containing apples, oranges, and pears if the order in which the pieces are selected does not matter, only the type of fruit and not the individual piece matters, and there are at least four pieces of each type of fruit in the bowl?

*Solution:* To solve this problem we list all the ways possible to select the fruit. There are 15 ways:

| | | |
|---|---|---|
| 4 apples | 4 oranges | 4 pears |
| 3 apples, 1 orange | 3 apples, 1 pear | 3 oranges, 1 apple |
| 3 oranges, 1 pear | 3 pears, 1 apple | 3 pears, 1 orange |
| 2 apples, 2 oranges | 2 apples, 2 pears | 2 oranges, 2 pears |
| 2 apples, 1 orange, 1 pear | 2 oranges, 1 apple, 1 pear | 2 pears, 1 apple, 1 orange |

The solution is the number of 4-combinations with repetition allowed from a three-element set, {*apple*, *orange*, *pear*}.

To solve more complex counting problems of this type, we need a general method for counting the r-combinations of an n-element set. In Example 3 we will illustrate such a method.

**EXAMPLE 3** How many ways are there to select five bills from a cash box containing \$1 bills, \$2 bills, \$5 bills, \$10 bills, \$20 bills, \$50 bills, and \$100 bills? Assume that the order in which the bills are chosen does not matter, that the bills of each denomination are indistinguishable, and that there are at least five bills of each type.

***Solution***: Because the order in which the bills are selected does not matter and seven different types of bills can be selected as many as five times, this problem involves counting 5-combinations with repetition allowed from a set with seven elements. Listing all possibilities would be tedious, because there are a large number of solutions. Instead, we will illustrate the use of a technique for counting combinations with repetition allowed.

Suppose that a cash box has seven compartments, one to hold each type of bill, as illustrated in Figure 1. These compartments are separated by six dividers, as shown in the picture. The choice of five bills corresponds to placing five markers in the compartments holding different types of bills. Figure 2 illustrates this correspondence for three different ways to select five bills, where the six dividers are represented by bars and the five bills by stars.

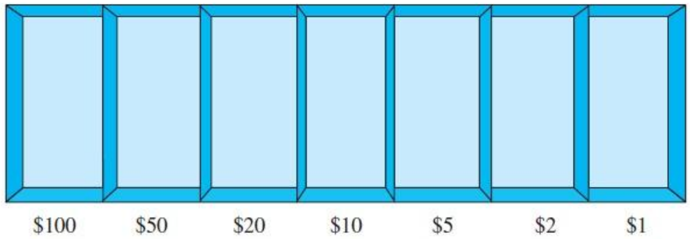



**FIGURE 1** **Cash Box with Seven Types of Bills.**

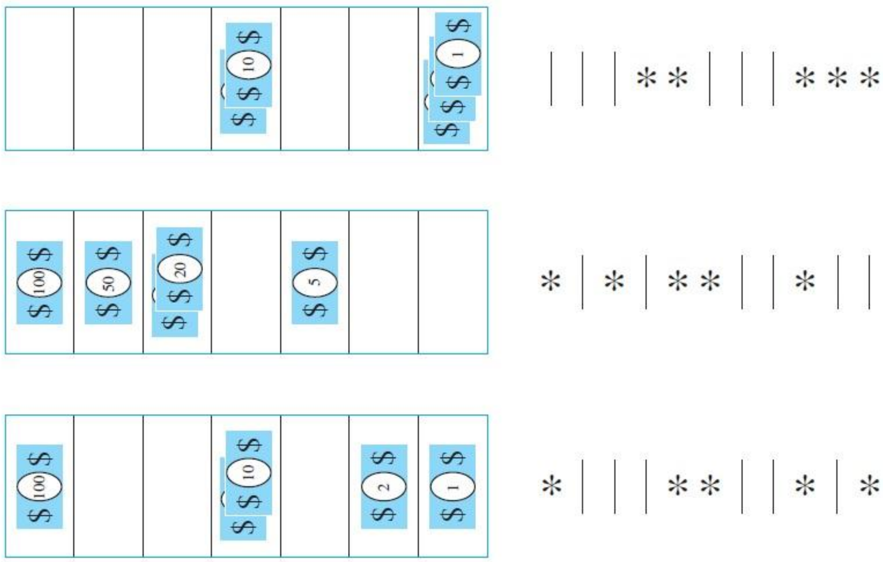


**FIGURE 2** **Examples of Ways to Select Five Bills.**

The number of ways to select five bills corresponds to the number of ways to arrange six bars and five stars in a row with a total of 11 positions. Consequently, the number of ways to select the five bills is the number of ways to select the positions of the five stars from the 11 positions. This corresponds to the number of unordered selections of 5 objects from a set of 11 objects, which can be done in $C(11, 5)$ ways. Consequently, there are

$$C(11, 5) = \frac{11!}{5!\,6!} = 462$$

ways to choose five bills from the cash box with seven types of bills.

**THEOREM** There are $C(n + r - 1, r) = C(n + r - 1, n - 1)$ $r$-combinations from a set with $n$ elements when repetition of elements is allowed.

**EXAMPLE 4** Suppose that a cookie shop has four different kinds of cookies. How many different ways can six cookies be chosen? Assume that only the type of cookie, and not the individual cookies or the order in which they are chosen, matters.

***Solution**:* The number of ways to choose six cookies is the number of 6-combinations of a set with four elements. From Theorem 2 this equals $C(4 + 6 - 1, 6) = C(9, 6)$. Because

$$C(9, 6) = C(9, 3) = \frac{9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3} = 84,$$

there are 84 different ways to choose the six cookies.

Table 1 lists the permutation and combination formulas with and without repetition.

**TABLE 1 Combinations and Permutations With and Without Repetition.**

| *Type* | *Repetition Allowed?* | *Formula* |
|---|---|---|
| $r$-permutations | No | $\frac{n!}{(n-r)!}$ |
| $r$-combinations | No | $\frac{n!}{r!\,(n-r)!}$ |
| $r$-permutations | Yes | $n^r$ |
| $r$-combinations | Yes | $\frac{(n+r-1)!}{r!\,(n-1)!}$ |