3.6 Propositions over a Universe

Example 3.6.1. Consider the sentence "He was a member of the Boston Red Sox." There is no way that we can assign a truth value to this sentence unless "he" is specified. For that reason, we would not consider it a proposition. However, "he" can be considered a variable that holds a place for any name. We might want to restrict the value of "he" to all names in the major-league baseball record books. If that is the case, we say that the sentence is a proposition over the set of major-league baseball players, past and present.

Definition: Proposition over a Universe. Let \( U \) be a nonempty set. A proposition over \( U \) is a sentence that contains a variable that can take on any value in \( U \) and that has a definite truth value as a result of any such substitution.

Example 3.6.2.

(a) A few propositions over the integers are \( 4x^2 - 3x = 0, \ 0 \leq n \leq 5, \) and "\( k \) is a multiple of 3."

(b) A few propositions over the rational numbers are \( 4x^2 - 3x = 0, \ y^2 = 2, \) and \( (s - 1)(s + 1) = s^2 - 1. \)

(c) A few propositions over the subsets of \( \mathbb{P} \) are \( (A = \emptyset), \ (A = \mathbb{P}), \ 3 \in A, \) and \( A \cap \{1, 2, 3\} \neq \emptyset. \)

All of the laws of logic that we listed in Section 3.4 are valid for propositions over a universe. For example, if \( p \) and \( q \) are propositions over the integers, we can be certain that \( p \land q \Rightarrow p, \) because \( (p \land q) \Rightarrow p \) is a tautology and is true no matter what values the variables in \( p \) and \( q \) are given. If we specify \( p \) and \( q \) to be \( p(n) : n < 4 \) and \( q(n) : n < 8, \) we can also say that \( p \) implies \( p \land q. \) This is not a usual implication, but for the propositions under discussion, it is true. One way of describing this situation in general is with truth sets.

**TRUTH SETS**

**Definition:** Truth Set. If \( p \) is a proposition over \( U, \) the truth set of \( p \) is \( T_p = \{ a \in U \mid p(a) \text{ is true} \}. \)

Example 3.6.3. The truth set of the proposition \( \{1, 2\} \cap A = \emptyset \) taken as a proposition over the power set of \( \{1, 2, 3, 4\} \) is \( \{\emptyset, \{3\}, \{4\}, \{3, 4\}\}. \)

Example 3.6.4. In the universe \( \mathbb{Z} \) (the integers), the truth set of \( 4x^2 - 3x = 0 \) is \( \{0\}. \) If the universe is expanded to the rational numbers, the truth set becomes \( \{0, 3/4\}. \) The term solution set is often used for the truth set of an equation such as the one in this example.

**Definition:** Tautology and Contradiction. A proposition over \( U \) is a tautology if its truth set is \( U. \) It is a contradiction if its truth set is empty.

Example 3.6.5. \( (s - 1)(s + 1) = s^2 - 1 \) is a tautology over the rational numbers. \( x^2 - 2 = 0 \) is a contradiction over the rationals.

The truth sets of compound propositions can be expressed in terms of the truth sets of simple propositions. For example, if \( a \in T_{p \lor q}, \) then \( a \) makes \( p \land q \text{ true}. \) Therefore, \( a \) makes both \( p \) and \( q \text{ true}, \) which means that \( a \in T_p \cap T_q. \) This explains why the truth set of the conjunction of two propositions equals the intersection of the truth sets of the two propositions. The following list summarizes the connection between compound and simple truth sets:

\[
\begin{align*}
T_{p \land q} & = T_p \cap T_q \\
T_{p \lor q} & = T_p \cup T_q \\
T_{\neg p} & = T_p^c \\
T_{p \Rightarrow q} & = \left(T_p \cap T_q\right) \cup \left(T_p^c \cap T_q^c\right) \\
T_{p \Leftarrow q} & = T_p^c \cup T_q
\end{align*}
\]

**Definition:** Equivalence. Two propositions are equivalent if \( p \iff q \text{ is a tautology. In terms of truth sets, this means that } p \text{ and } q \text{ are equivalent if } T_p = T_q. \)

Example 3.6.6.

(a) \( n + 4 = 9 \text{ and } n = 5 \text{ are equivalent propositions over the integers.} \)

(b) \( A \cap \{4\} \neq \emptyset \text{ and } 4 \in A \text{ are equivalent propositions over the power set of the natural numbers.} \)

**Definition:** Implication. If \( p \text{ and } q \text{ are propositions over } U, p \text{ implies } q \text{ if } p \Rightarrow q \text{ is a tautology.} \)

Since the truth set of \( p \Rightarrow q \text{ is } T_p^c \cup T_q, \) the Venn diagram for \( T_{p \Rightarrow q} \) in Figure 3.6.1 shows that \( p \Rightarrow q \text{ when } T_p \subseteq T_q. \)
Example 3.6.7.
(a) Over the natural numbers: \( n < 4 \Rightarrow n < 8 \) since \( \{0, 1, 2, 3, 4\} \subseteq \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \).
(b) Over the power set of the integers: \( |A^c| = 1 \) implies \( A \cap \{0, 1\} \neq \emptyset \).
(c) \( A \subseteq \) even integers \( \Rightarrow A \cap \) odd integers = \( \emptyset \).

EXERCISES FOR SECTION 3.6
A Exercises
1. If \( U = \mathcal{P}(\{1, 2, 3, 4\}) \), what are the truth sets of the following propositions?
   (a) \( A \cap \{2, 4\} = \emptyset \).
   (b) \( 3 \in A \) and \( 1 \notin A \).
   (c) \( A \cup \{1\} = A \).
   (d) \( A \) is a proper subset of \( \{2, 3, 4\} \).
   (e) \( |A| = |A^c| \).

2. Over the universe of positive integers, define
   \( p(n) : n \) is prime and \( n < 32 \).
   \( q(n) : n \) is a power of 3.
   \( r(n) : n \) is a divisor of 27.
   (a) What are the truth sets of these propositions?
   (b) Which of the three propositions implies one of the others?

3. If \( U = \{0, 1, 2\} \), how many propositions over \( U \) could you list without listing two that are equivalent?

4. Given the propositions over the natural numbers:
   \( p : n < A \)
   \( q : 2n > 17 \)
   \( r : n \) is a divisor of 18
   what are the truth sets of:
   (a) \( q \)
   (b) \( p \land q \)
   (c) \( r \)
   (d) \( q \Rightarrow r \)

5. Suppose that \( s \) is a proposition over \( \{1, \ldots, 8\} \). If \( T_s = \{1, 3, 5, 7\} \), give two examples of propositions that are equivalent to \( s \).

6. (a) Determine the truth sets of the following propositions over the positive integers:
   \( p(n) : n \) is a perfect square and \( n < 100 \).
\( q(n) : n = |P(A)| \) for some set \( A \)

(b) Determine \( T_{p/q} \) for \( p \) and \( q \) above.

7. Let the universe be \( \mathbb{Z} \), the set of integers. Which of the following propositions are equivalent over \( \mathbb{Z} \)?

a: \( 0 < n^2 < 9 \).

b: \( 0 < n^3 < 27 \).

c: \( 0 < n < 3 \).
### 3.7 Mathematical Induction

In this section, we will examine mathematical induction, a technique for proving propositions over the positive integers. Mathematical (or finite) induction reduces the proof that all of the positive integers belong to a truth set to a finite number of steps.

Mathematical Induction is sometimes called finite induction.

**Example 3.7.1.** Consider the following proposition over the positive integers, which we will label \( p(n) \): The sum of the positive integers from 1 to \( n \) is \( \frac{n(n+1)}{2} \). This is a well-known formula that is quite simple to verify for a given value of \( n \). For example, \( p(5) \) is: The sum of the positive integers from 1 to 5 is \( \frac{5(5+1)}{2} \). Indeed, \( 1 + 2 + 3 + 4 + 5 = 15 = \frac{5(5+1)}{2} \). Unfortunately, this doesn’t serve as a proof that \( p(n) \) is a tautology. All that we’ve established is that \( 5 \) is in the truth set of \( p \). Since the positive integers are infinite, we certainly can’t use this approach to prove the formula.

**An Analogy:** Mathematical induction is often useful in overcoming a problem such as this one. A proof by mathematical induction is similar to knocking over a row of closely spaced dominos that are standing on end. To knock over the five dominos in Figure 3.7.1, all you need to do is push Domino 1 to the right. To be assured that they all will be knocked over, some work must be done ahead of time. The dominos must be positioned so that if any domino is pushed to the right, it will push the next domino in the line.

![Figure 3.7.1 Illustration of example 3.7.1](image)

Now imagine the propositions \( p(1) \), \( p(2) \), \( p(3) \), … to be an infinite line of dominos. Let’s see if these propositions are in the same formation as the dominos were. First, we will focus on one specific point of the line: \( p(99) \) and \( p(100) \). We are not going to prove that either of these propositions is true, just that the truth of \( p(99) \) implies the truth of \( p(100) \). In terms of our analogy, if \( p(99) \) is knocked over, it will knock over \( p(100) \).

In proving \( p(99) \) \( \Rightarrow \) \( p(100) \), we will use \( p(99) \) as our premise. We must prove: The sum of the positive integers from 1 to 100 is \( \frac{100(100+1)}{2} \). We start by observing that the sum of the positive integers from 1 to 100 is \( (1 + 2 + \cdots + 99) + 100 \). That is, the sum of the positive integers from 1 to 100 equals the sum of the first ninety-nine plus the final number, 100. We can now apply our premise, \( p(99) \), to the sum \( 1 + 2 + \cdots + 99 \). After rearranging our numbers, we obtain the desired expression for \( 1 + 2 + \cdots + 100 \):

\[
1 + 2 + \cdots + 99 + 100 = (1 + 2 + \cdots + 99) + 100 \\
= \frac{99(99+1)}{2} + 100 \\
= \frac{99 \times 100}{2} + \frac{2 \times 100}{2} \\
= \frac{99 \times 100}{2} + \frac{200}{2} \\
= \frac{99 \times 100 + 200}{2}
\]

What we’ve just done is analogous to checking two dominos in a line and finding that they are properly positioned. Since we are dealing with an infinite line, we must check all pairs at once. This is accomplished by proving that \( p(n) \) \( \Rightarrow \) \( p(n + 1) \) for all \( n \geq 1 \):

\[
1 + 2 + \cdots + n + (n + 1) = (1 + 2 + \cdots + n) + (n + 1) \\
= \frac{n(n+1)}{2} + (n + 1) \quad \text{by } p(n) \\
= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
= \frac{n(n+1) + 2(n+1)}{2} \\
= \frac{(n+1)(n+2)}{2}
\]

They are all lined up! Now look at \( p(1) \): The sum of the positive integers from 1 to 1 is \( \frac{1+1}{2} \). Clearly, \( p(1) \) is true. This sets off a chain reaction. Since \( p(1) \) \( \Rightarrow \) \( p(2) \) and \( p(2) \) is true. Since \( p(2) \) \( \Rightarrow \) \( p(3) \), \( p(3) \) is true; and so on. ■

**The Principle of Mathematical Induction.** Let \( p(n) \) be a proposition over the positive integers, then \( p(n) \) is a tautology if

1. \( p(1) \) is true, and
2. for all \( n \geq 1 \), \( p(n) \) \( \Rightarrow \) \( p(n + 1) \).

Note: The truth of \( p(1) \) is called the basis for the induction proof. The premise that \( p(n) \) is true in Statement (b) is called the induction hypothesis. The proof that \( p(n) \) implies \( p(n + 1) \) is called the induction step of the proof. Despite our analogy, the basis is usually done first in an induction proof. The order doesn’t really matter.
Example 3.7.3. For all $n \geq 1, n^3 + 2n$ is a multiple of 3. An inductive proof follows:

Basis: $1^3 + 2(1) = 3$ is a multiple of 3.

The basis is almost always this easy!

Induction: Assume that $n \geq 1$ and $n^3 + 2n$ is a multiple of 3. Consider $(n + 1)^3 + 2(n + 1)$. Is it a multiple of 3?

\[
(n + 1)^3 + 2(n + 1) = (n^3 + 3n^2 + 3n + 1) + (2n + 2)
\]

\[
= n^3 + 2n + 3n^2 + 3n + 3 \quad \text{Rearrange the terms}
\]

\[
= (n^3 + 2n) + 3(n^2 + n + 1)
\]

Yes, $(n + 1)^3 + 2(n + 1)$ is the sum of two multiples of 3; therefore, it is also a multiple of 3. ■

Variations of Induction

Now we will discuss some of the variations of the principle of mathematical induction. The first simply allows for universes that are similar to $P$, like $\{-2, -1, 0, 1, \ldots\}$ or $\{5, 6, 7, 8, \ldots\}$.

Principle of Mathematical Induction (Generalized). If $p(n)$ is a proposition over $\{k_0, k_0 + 1, k_0 + 2, \ldots\}$, where $k_0$ is any integer, then $p(n)$ is a tautology if

1. $p(k_0)$ is true, and
2. for all $n \geq k_0$, $p(n) \Rightarrow p(n + 1)$.

Example 3.7.4. In Chapter 2, we stated that the number of different permutations of $k$ elements taken from an $n$ element set, $P(n; k)$, can be computed with the formula $\frac{n!}{(n-k)!}$. We can prove this statement by induction on $n$. For $n \geq 0$, let $q(n)$ be the proposition

\[ P(n; k) = \frac{n!}{(n-k)!} \quad \text{for all } k \text{ from } 0 \text{ to } n. \]

Basis: $q(0)$ states that

\[ P(0; 0) = \text{the number of ways that 0 elements can be selected from the empty set and arranged in order} = 0! / 0! = 1. \]

This is true — a general law in combinatorics is that there is exactly one way of doing nothing.

Induction: Assume that $q(n)$ is true for some natural number $n$. It is left for us to prove that this assumption implies that $q(n + 1)$ is true. Suppose that we have a set of cardinality $n + 1$ and want to select and arrange $k$ of its elements. There are two cases to consider, the first of which is easy. If $k = 0$, then there is one way of selecting zero elements from the set; hence

\[ P(n + 1; 0) = 1 = \frac{(n+1)!}{(n+1+0)!}. \]

and the formula works in this case.

The more challenging case is to verify the formula when $k$ is positive and less than or equal to $n + 1$. Here we count the value of $P(n + 1; k)$ by counting the number of ways that the first element in the arrangement can be filled and then counting the number of ways that the
remaining \( k - 1 \) elements can be filled in using the induction hypothesis.

There are \( n + 1 \) possible choices for the first element. Since that leaves \( n \) elements to fill in the remaining \( k - 1 \) positions, there are \( P(n; \ k - 1) \) ways of completing the arrangement. By the rule of products,

\[
P(n + 1; k) = (n + 1) P(n; k - 1)
\]

\[
= (n + 1) \frac{n!}{(n-k+1)!}
\]

\[
= \frac{(n+1)!}{(n-k)!}
\]

A second variation allows for the expansion of the induction hypothesis. The course-of-values principle includes the previous generalization. It is also sometimes called strong induction.

**The Course-of-Values Principle of Mathematical Induction.** If \( p(n) \) is a proposition over \( \{k_0, k_0 + 1, k_0 + 2, \ldots\} \), where \( k_0 \) is any integer, then \( p(n) \) is a tautology if

1. \( p(k_0) \) is true, and
2. for all \( n \geq k_0, \ p(k_0), \ p(k_0 + 1), \ldots, \ p(n) \Rightarrow p(n + 1) \).

**Example 3.7.5.** A prime number is defined as a positive integer that has exactly two positive divisors, 1 and itself. There are an infinite number of primes. The list of primes starts with 2, 3, 5, 7, 11, ... . The proposition over \( \{2, 3, 4, \ldots\} \) that we will prove here is \( p(n) : n \) can be written as the product of one or more primes. In most texts, the assertion that \( p(n) \) is a tautology would appear as:

**Theorem.** Every positive integer greater than or equal to 2 has a prime decomposition.

If you were to encounter this theorem outside the context of a discussion of mathematical induction, it might not be obvious that the proof can be done by induction. Recognizing when an induction proof is appropriate is mostly a matter of experience. Now on to the proof!

**Basis:** Since 2 is a prime, it is already decomposed into primes (one of them).

**Induction:** Suppose that for some \( k \geq 2 \) all of the integers 2, 3, ..., \( k \) have a prime decomposition. Notice the course-of-value hypothesis. Consider \( k + 1 \). Either \( k + 1 \) is prime or it isn't. If \( k + 1 \) is prime, it is already decomposed into primes. If not, then \( k + 1 \) has a divisor, \( d \), other than 1 and \( k + 1 \). Hence, \( k + 1 = c d \) where both \( c \) and \( d \) are between 2 and \( k \). By the induction hypothesis, \( c \) and \( d \) have prime decompositions, \( c_1 c_2 \cdots c_m \) and \( d_1 d_2 \cdots d_n \), respectively. Therefore, \( k + 1 \) has the prime decomposition \( c_1 c_2 \cdots c_m d_1 d_2 \cdots d_n \).

**HISTORICAL NOTE**

Mathematical induction originated in the late nineteenth century. Two mathematicians who were prominent in its development were Richard Dedekind and Giuseppe Peano. Dedekind developed a set of axioms that describe the positive integers. Peano refined these axioms and gave a logical interpretation to them. The axioms are usually called the Peano Postulates.

**Peano’s Postulates.** The system of positive integers consists of a nonempty set, \( P \); a least element of \( P \), denoted 1; and a "successor function," \( s \), with the properties

1. If \( k \in P \), then there is an element of \( P \) called the successor of \( k \), denoted \( s(k) \).
2. No two elements of \( P \) have the same successor.
3. No element of \( P \) has 1 as its successor.
4. If \( S \subseteq P, \ 1 \in S, \) and \( k \in S \Rightarrow s(k) \in S \), then \( S = P \).

Notes:

(a) You might recognize \( s(k) \) as simply being \( k + 1 \).
(b) Axiom 4, mentioned above, is the one that makes mathematical induction possible. In an induction proof, we simply apply that axiom to the truth set of a proposition.
Exercises for Section 3.7

A Exercises
1. Prove that the sum of the first \( n \) odd integers equals \( n^2 \).
2. Prove that if \( n \geq 1 \), then \( 1(1!) + 2(2!) + \cdots + n(n!) = (n + 1)! - 1 \).
3. Prove that for \( n \geq 1 \):
   \[
   \sum_{k=1}^{n} k^2 = \frac{1}{6} n(n + 1)(2n + 1).
   \]
4. Prove that for \( n \geq 1 \):
   \[
   \sum_{k=0}^{n} 2^k = 2^{n+1} - 1.
   \]
5. Use mathematical induction to show that for \( n \geq 1 \),
   \[
   \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.
   \]
6. Prove that if \( n \geq 2 \), the generalized DeMorgan’s Law is true:
   \[
   \neg (p_1 \land p_2 \land \cdots \land p_n) \Leftrightarrow (\neg p_1) \lor (\neg p_2) \lor \cdots \lor (\neg p_n).
   \]

B Exercises
7. The number of strings of \( n \) zeros and ones that contain an even number of ones is \( 2^{n-1} \). Prove this fact by induction for \( n \geq 1 \).
8. Let \( p(n) \) be \( 8^n - 3^n \) a multiple of 5. Prove that \( p(n) \) is a tautology over \( \mathbb{N} \).
9. Suppose that there are \( n \) people in a room, \( n \geq 1 \), and that they all shake hands with one another. Prove that \( \frac{n(n-1)}{2} \) handshakes will have occurred.
10. Prove that it is possible to make up any postage of eight cents or more using only three- and five-cent stamps.

C Exercises
11. Generalized associativity. It is well known that if \( a_1, a_2, \) and \( a_3 \) are numbers, then no matter what order the sums in the expression \( a_1 + a_2 + a_3 \) are taken in, the result is always the same. Call this fact \( p(3) \) and assume it is true. Prove using course-of-values induction that if \( a_1, a_2, \ldots, a_n \) are numbers, then no matter what order the sums in the expression \( a_1 + a_2 + \cdots + a_n \) are taken in, the result is always the same.
12. Let \( S \) be the set of all numbers that can be produced by applying any of the rules below in any order a finite number of times.
   
   Rule 1: \( \frac{1}{2} \in S \)
   
   Rule 2: \( 1 \in S \)
   
   Rule 3: If \( a \) and \( b \) have been produced by the rules, then \( a \cdot b \in S \).
   
   Rule 4: If \( a \) and \( b \) have been produced by the rules, then \( \frac{a+b}{2} \in S \).
   
   Prove by course-of-values induction that \( a \in S \Rightarrow 0 < a \leq 1 \). Hint: The number of times the rules are applied should be the integer that you do the induction on.
13. A recursive definition is similar to an inductive proof. It consists of a basis, usually the simple part of the definition, and the recursion, which defines complex objects in terms of simpler ones. For example, if \( x \) is a real number and \( n \) is a positive integer, we can define \( x^n \) as follows:
   
   Basis: \( x^1 = x \).
   
   Recursion: if \( n \geq 2 \), \( x^n = x^{n-1} \cdot x \).
   
   For example, \( x^3 = x \cdot x \cdot x \cdot (x \cdot x) \cdot x = (x \cdot x) \cdot x \cdot x \). Proofs involving objects that are defined recursively are often inductive. Prove that if \( n, m \in \mathbb{P} \), \( x^{mn} = x^m \cdot x^n \). Hint: Let \( p(m) \) be the proposition that \( x^{mn} = x^m \cdot x^n \) for all \( n \geq 1 \). There is much more on recursion in Chapter 8.
14. Let \( S \) be a finite set and let \( P_n \) be defined recursively by \( P_1 = S \) and \( P_{n+1} = S \times P_n \) for \( n \geq 2 \).
   
   (a) List the elements of \( P_3 \) for the case \( S = \{a, b\} \).
   
   (b) Determine the formula for \( |P_n| \), given that \( |S| = k \), and prove your formula by induction.
3.8 Quantifiers

As we saw in Section 3.6, if \( p(n) \) is a proposition over a universe \( U \), its truth set \( T_p \) is equal to a subset of \( U \). In many cases, such as when \( p(n) \) is an equation, we are most concerned with whether \( T_p \) is empty or not. In other cases, we might be interested in whether \( T_p = U \); that is, whether \( p(n) \) is a tautology. Since the conditions \( T_p \neq \emptyset \) and \( T_p = U \) are so often an issue, we have a special system of notation for them.

THE EXISTENTIAL QUANTIFIER

If \( p(n) \) is a proposition over \( U \) with \( T_p \neq \emptyset \), we commonly say "There exists an \( n \) in \( U \) such that \( p(n) \) (is true)." We abbreviate this with the symbols \( (\exists n)_{U} (p(n)) \). The symbol \( \exists \) is called the existential quantifier. If the context is clear, the mention of \( U \) is dropped: \( (\exists n) (p(n)) \).

Example 3.8.1.

(a) \( (\exists k)_{\mathbb{Z}} (k^2 - k - 12 = 0) \) is another way of saying that there is an integer that solves the equation \( k^2 - k - 12 = 0 \). The fact that two such integers exist doesn't affect the truth of this proposition in any way.

(b) \( (\exists k)_{\mathbb{Z}} (3k = 102) \) simply states that 102 is a multiple of 3, which is true. On the other hand, \( (\exists k)_{\mathbb{Z}} (3k = 100) \) states that 100 is a multiple of 3, which is false.

(c) \( (\exists x)_{\mathbb{R}} (x^2 + 1 = 0) \) is false since the solution set of the equation \( x^2 + 1 = 0 \) in the real numbers is empty. It is common to write \( (\exists x)_{\mathbb{R}} (x^2 + 1 = 0) \) in this case.

There are a wide variety of ways that you can write a proposition with an existential quantifier. Table 3.8.1 contains a list of different variations that could be used for both the existential and universal quantifiers.

THE UNIVERSAL QUANTIFIER

If \( p(n) \) is a proposition over \( U \) with \( T_p = U \), we commonly say "For all \( n \) in \( U \), \( p(n) \) (is true)." We abbreviate this with the symbols \( (\forall n)_{U} (p(n)) \). The symbol \( \forall \) is called the universal quantifier. If the context is clear, the mention of \( U \) is dropped: \( (\forall n) (p(n)) \).

Example 3.8.2.

(a) We can say that the square of every real number is non-negative symbolically with a universal quantifier: \( (\forall x)_{\mathbb{R}} (x^2 \geq 0) \).

(b) \( (\forall n)_{\mathbb{Z}} (n + 0 = 0 + n = n) \) says that the sum of zero and any integer \( n \) is \( n \). This fact is called the identity property of zero for addition.

<table>
<thead>
<tr>
<th>Table 3.8.1 Notational Variations for Existential and Universal Quantifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Quantifier</td>
</tr>
<tr>
<td>((\forall n)_{U} (p(n)))</td>
</tr>
<tr>
<td>((\forall n \in U) (p(n)))</td>
</tr>
<tr>
<td>(\forall n \in U, \ p(n))</td>
</tr>
<tr>
<td>(p(n), \ \forall n \in U)</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

THE NEGATION OF QUANTIFIED PROPOSITIONS

When you negate a quantified proposition, the existential and universal quantifiers complement one another.

Example 3.8.3. Over the universe of animals, define \( F(x) : x \) is a fish and \( W(x) : x \) lives in the water. We know that the proposition \( W(x) \rightarrow F(x) \) is not always true. In other words, \( (\forall x) (W(x) \rightarrow F(x)) \) is false. Another way of stating this fact is that there exists an animal that lives in the water and is not a fish; that is,

\[ \neg (\forall x) (W(x) \rightarrow F(x)) \iff (\exists x) (\neg (W(x) \rightarrow F(x))) \]

\[ \iff (\exists x) (W(x) \land \neg F(x)) \]

Note that the negation of a universally quantified proposition is an existentially quantified proposition. In addition, when you negate an existentially quantified proposition, you obtain a universally quantified proposition. Symbolically,

\[ \neg (\forall n) (p(n)) \iff (\exists n) \neg (p(n)) \]
\[ \neg (\exists n) (p(n)) \iff (\forall n) \neg (p(n)) \]

Example 3.8.4.
(a) The ancient Greeks first discovered that \( \sqrt{2} \) is an irrational number; that is, \( \sqrt{2} \) is not a rational number. \( \neg((\exists r)_R (r^2 = 2)) \) and \( (\forall r)_R (r^2 \neq 2) \) both state this fact symbolically.

(b) \( \neg((\forall n)_R (n^2 - n + 41 \text{ is prime})) \) is equivalent to \( (\exists n)_R (n^2 - n + 41 \text{ is composite}) \). They are both either true or false.

**MULTIPLE QUANTIFIERS**

If a proposition has more than one variable, then you can quantify it more than once. For example, if \( p(x, y) : x^2 - y^2 = (x + y)(x - y) \) is a tautology over the set of all pairs of real numbers because it is true for each pair \((x, y)\) in \( \mathbb{R} \times \mathbb{R} \). Another way to look at this proposition as a proposition with two variables. The assertion that \( p(x, y) \) is a tautology could be quantified as \( (\forall x)_R ((\forall y)_R (p(x, y))) \) or \( (\forall y)_R ((\forall x)_R (p(x, y))) \).

In general, multiple universal quantifiers can be arranged in any order without logically changing the meaning of the resulting proposition. The same is true for multiple existential quantifiers. For example, \( p(x, y) : x + y = 4 \) and \( x - y = 2 \) is a proposition over \( \mathbb{R} \times \mathbb{R} \). \( (\exists x)_R ((\exists y)_R ((x + y = 4) \land (x - y = 2))) \) and \( (\exists y)_R ((\exists x)_R ((x + y = 4) \land (x - y = 2))) \) are equivalent. A proposition with multiple existential quantifiers such as this one says that there are simultaneous values for the quantified variables that make the proposition true. A similar example is \( q(x, y) : 2x - y < 2 \) and \( 4x - 2y = 5 \) which is always false; and the following are all equivalent

\[
(\neg((\exists x)_R ((\exists y)_R (q(x, y)))))
\]

A proposition with multiple quantifiers is true for each assignment of values to the variables for which it is true. However, for a proposition with multiple quantifiers, it is a tautology over \( \mathbb{R} \) and we are justified in saying that \( x \) is true. The key to understanding propositions like \( x \) on your own is to experiment with actual values for the outermost variables as we did above.

**TIPS ON READING MULTIPLY QUANTIFIED PROPOSITIONS**

It is understandable that you would find propositions such as \( x \) difficult to read. The trick to deciphering these expressions is to "peel" one quantifier off the proposition just as you would peel off the layers of an onion (but quantifiers shouldn't make you cry). Since the outermost quantifier in \( x \) is universal, \( x \) says that \( z(a) : (\exists b)_R (a = b) \) is true for each value that a can take on. Now take the time to select a value for \( a \), like 6. For the value that we selected, we get \( z(6) : (\exists b)_R (6 = b) = 1 \), which is obviously true since \( 6b = 1 \) has a solution in the positive real numbers.

Another way of convincing yourself that \( y \) is false is to convince yourself that \( \neg y \) is true:

\[
(\neg((\exists b)_R ((\forall a)_R (a = b))))
\]

In words, for each value of \( a \), a value for \( b \) that makes \( a \neq b \). One such value is \( \frac{1}{b} + 1 \). Therefore, \( \neg y \) is true.

**EXERCISES FOR SECTION 3.8**

**A Exercises**

1. Let \( C(x) \) be "\( x \) is cold-blooded," let \( F(x) \) be "\( x \) is a fish," and let \( S(x) \) be "\( x \) lives in the sea."

(a) Translate into a formula: Every fish is cold-blooded.

(b) Translate into English: \((\exists x)(S(x) \land \neg F(x))\)

2. Let \( M(x) \) be "\( x \) is a mammal," let \( A(x) \) be "\( x \) is an animal," and let \( W(x) \) be "\( x \) is warm-blooded."

(a) Translate into a formula: Every mammal is warm-blooded.

(b) Translate into English: \((\exists x)(A(x) \land (\neg M(x)))\).

3. Over the universe of books, define the propositions \( B(x) \) : \( x \) has a blue cover, \( M(x) \) : \( x \) is a mathematics book, \( C(x) \) : \( x \) is published in the United States, and \( R(x, y) \) : The bibliography of \( x \) includes \( y \). Translate into words:

(a) \((\forall x)(\neg B(x))\).
(b) \((\forall x) (M(x) \land U(x) \rightarrow B(x))\).
(c) \((\exists x) (M(x) \land \neg B(x))\).
(d) \((\exists y) ((\forall x) (M(x) \rightarrow R(x, y)))\).

Express using quantifiers:

(e) Every book with a blue cover is a mathematics book.

(f) There are mathematics books that are published outside the United States.

(g) Not all books have bibliographies.

4. Let the universe of discourse, \(U\), be the set of all people, and let \(M(x, y)\) be "\(x\) is the mother of \(y\)."

(a) Which of the following is a true statement? Translate it into English.

(i) \((\exists x_U) ((\forall y_U) (M(x, y)))\)

(ii) \((\forall y_U) ((\exists x_U) (M(x, y)))\)

(b) Translate the following statement into logical notation using quantifiers and the proposition \(M(x, y)\) over \(U\): "Everyone has a grandmother."

5. Translate into your own words and indicate whether it is true or false that \((\exists u) \{4u^2 - 9 = 0\}\).

6. Use quantifiers to say that \(\sqrt{3}\) is an irrational number.

7. What do the following propositions say, where \(U\) is the power set of \([1, 2, \ldots, 9]\)? Which of these propositions are true?

(a) \((\forall A_U) (|A| \neq |A^c|)\).

(b) \((\exists A_U) (\exists B_U) (|A| = 5, |B| = 5, \text{ and } A \cap B = \emptyset)\)

(c) \((\forall A_U) (\forall B_U) (A - B = B - A^c)\)

8. Use quantifiers to state that for every positive integer, there is a larger positive integer.

9. Use quantifiers to state that the sum of any two rational numbers is rational.

10. Over the universe of real numbers, use quantifiers to say that the equation \(a + x = b\) has a solution for all values of \(a\) and \(b\). Hint: You will need three quantifiers.

11. Let \(n\) be a positive integer. Describe using quantifiers:

(a) \(x \in \bigcup_{k=1}^{n} A_k\)

(b) \(x \in \bigcap_{k=1}^{n} A_k\)

12. Prove that \((\exists x) (\forall y) (p(x, y)) \Rightarrow (\forall y) (\exists x) (p(x, y))\), but the converse is not true.
3.9 A Review of Methods of Proof

One of the major goals of this chapter is to acquaint the reader with the key concepts in the nature of proof in logic, which of course carries over into all areas of mathematics and its applications. In this section we will stop, reflect, and "smell the roses," so that these key ideas are not lost in the many concepts covered in logic. In Chapter 4 we will use set theory as a vehicle for further practice and insights into methods of proof.

KEY CONCEPTS IN PROOF

1. All theorems in mathematics can be expressed in "If P then C" (P ⇒ C) format, or in "C if and only if C₂" (P ⇔ C) format. The latter is equivalent to "If C₁ then C₂, and if C₂ then C₁." Alternate ways of expressing conditional propositions are found in Section 3.1.
2. In "If P then C," P is the premise (or hypothesis) and C is the conclusion. It is important to realize that a theorem makes a statement that is dependent on the premise being true.
3. There are two basic methods for proving P ⇒ C:
   (a) Direct: Assume P is true and prove C is true; and
   (b) Indirect (proof by contradiction): Assume P is true and C is false and prove that this leads to a contradiction of some premise, theorem, or basic concept.

4. The method of proof for "If and only if" (iff) theorems is found in the law (P ⇔ C) ⇔ ((P → C) ∧ (C → P)). Hence to prove an "If and only if" statement one must prove an "if . . . then . . ." statement and its converse.

The initial response of most people when confronted with the task of being told they must be able to read and do proofs is:
(1) the actual meaning of the theorems, and
(2) the basic definitions and concepts of the topic discussed.

For example, when we discuss rational numbers and refer to a number x as being rational, this means we can substitute a fraction \( \frac{p}{q} \) in place of \( x \), with the understanding that \( p \) and \( q \) are integers and \( q \neq 0 \). Therefore, to prove a theorem about rational numbers it is absolutely necessary that you know what a rational number "looks like."

It's easy to comment on the response, "I cannot do proofs." Have you tried? As elementary school students we were in awe of anyone who could handle algebraic expressions, especially complicated ones. We learned by trying and applying ourselves. Maybe we cannot solve all problems in algebra or calculus, but we are comfortable enough with these subjects to know that we can solve many and can express ourselves intelligently in these areas. The same remarks hold true for proofs.

THE ART OF PROVING P ⇒ C

First one must completely realize what is given, the hypothesis. The importance of this is usually overlooked by beginners. It makes sense, whenever you begin any task, to spend considerable time thinking about the tools at your disposal. Write down the premise in precise language. Similarly, you have to know when the task is finished. Write down the conclusion in precise language. Then you usually start with \( P \) and attempt to show that \( C \) follows logically. How do you begin? Basically you attack the proof the same way you solve a complicated equation in elementary algebra. You may not know exactly what each and every step is but you must try something. If we are lucky, \( C \) follows naturally; if it doesn't, try something else. Often what is helpful is to work backward from \( C \). Finally, we have all learned, possibly the hard way, that mathematics is a participating sport, not a spectator sport. One learns proofs by doing them, not by watching others do them. We give several illustrations of how to set up the proofs of several examples. Our aim here is not to prove the statements given, but to concentrate on the logical procedure.

Example 3.9.1. We will outline a proof that the sum of any two odd integers is even. Our first step will be to write the theorem in the familiar conditional form: If \( j \) and \( k \) are odd integers, then \( j + k \) is even. The premise and conclusion of this theorem should be clear now. Notice that if \( j \) and \( k \) are not both odd, then the conclusion may or may not be true. Our only objective is to show that the truth of the premise forces the conclusion to be true. Therefore, we can express the integers \( j \) and \( k \) in the form that all integers take; that is:

\[ n \in \mathbb{Z} \text{ is odd implies } (\exists m \in \mathbb{Z}) (n = 2m + 1). \]

This observation allows us to examine the sum \( y + k \) and to verify that it must be even.

Example 3.9.2. Let \( n \in \mathbb{Z} \). We will outline a proof that \( n^2 \) is even if and only if \( n \) is even.
Outline of a proof: Since this is an "If and only if theorem we must prove two facts (see key concept number 4 above):

I. (⇒) If \( n^2 \) is even, then \( n \) is even. To do this directly, assume that \( n^2 \) is even and prove that \( n \) is even. To do this indirectly, assume \( n^2 \) is even and that \( n \) is odd, and reach a contradiction. It turns out that the latter of the two approaches is easiest here.

II. (⇐) If \( n \) is even, then \( n^2 \) is even. To do this directly, assume that \( n \) is even and prove that \( n^2 \) is even.

Now that we have broken the theorem down into two parts and know what to prove, we proceed to prove the two implications. The final ingredient that we need is a convenient way of describing even integers. When we refer to an integer \( n \) (or \( m \), or \( k \), . . .) as even, we can always replace it with a product of the form \( 2q \), where \( q \) is an integer (more precisely, \( (\exists q) \exists (n = 2q) \)). In other words, for an integer to be even it must have a factor of two in its prime decomposition.

Example 3.9.3. Our final example will be an outline of the proof that the square root of 2 is irrational (not an element of \( \mathbb{Q} \)). This is an example of the theorem that does not appear to be in the standard \( P \Rightarrow C \) form. One way to rephrase the theorem is: If \( x \) is a rational number, then \( x^2 \neq 2 \). A direct proof of this theorem would require that we verify that the square of every rational number is not equal to 2. There is no convenient way of doing this, so we must turn to the indirect method of proof. In such a proof, we assume that \( x \) is a rational number and that \( x^2 = 2 \) (i.e., \( \sqrt{2} \) is a rational number). This will lead to a contradiction. In order to reach this contradiction, we need to use the following facts:

(a) A rational number is a quotient of two integers.
(b) Every fraction can be reduced to lowest terms, so that the numerator and denominator have no common factor greater than 1.
(c) If \( n \) is an integer, \( n^2 \) is even if and only if \( n \) is even.

EXERCISES FOR SECTION 3.9

B Exercises

1. Prove that the sum of two odd positive integers is even.
2. Write out a complete proof that if \( n \) is an integer, \( n^2 \) is even if and only if \( n \) is even.
3. Write out a complete proof that \( \sqrt{2} \) is irrational.
4. Prove that \( \sqrt{2} \) is an irrational number.
5. Prove that if \( x \) and \( y \) are real numbers such that \( x + y \leq 1 \), then either \( x \leq \frac{1}{2} \) or \( y \leq \frac{1}{2} \).
6. Use the following definition of absolute value to prove the given statements: If \( x \) is a real number, then the absolute value of \( x \), \( |x| \), is defined by:

\[
|x| = \begin{cases} 
  x & \text{if } x \geq 0 \\
  -x & \text{if } x < 0
\end{cases}
\]

(a) For any real number \( x \), \( |x| \geq 0 \). Moreover, \( |x| = 0 \) implies \( x = 0 \).
(b) For any two real numbers \( x \) and \( y \), \( |x| \cdot |y| = |xy| \).
(c) For any two real numbers \( x \) and \( y \), \( |x + y| \leq |x| + |y| \).