## 3.2 Variables and Quantifiers

### Variables and universes

Statements we use in computer languages to control loops or conditionals are statements about variables. When we declare these variables, we give the computer information about their possible values. For example, in some programming languages we may declare a variable to be a "boolean" or an "integer" or a "real."[4] In English and in mathematics, we also make statements about variables, but it is not always clear which words are being used as variables and what values these variables may take on. We use the phrase *varies over* to describe the set of values a variable may take on. For example, in English, we might say "If someone's umbrella is up, then it must be raining." In this case, the word "someone" is a variable, and presumably it *varies over* the people who happen to be in a given place at a given time. In mathematics, we might say "For every pair of positive integers $m$ and $n$, there are nonnegative integers $q$ and $r$ with $0 \leq r < n$ such that $m = nq + r$." In this case $m$, $n$, $q$, and $r$ are clearly our variables; our statement itself suggests that two of our variables range over the positive integers and two range over the nonnegative integers. We call the set of possible values for a variable the *universe* of that variable.

In the statement "$m$ is an even integer," it is clear that $m$ is a variable, but the universe is not given. It might be the integers, just the even integers, or the rational numbers, or one of many other sets. The choice of the universe is crucial for determining the truth or falsity of a statement. If we choose the set of integers as the universe for $m$, then the statement is true for some integers and false for others. On the other hand, if we choose integer multiples of 10 as our universe, then the statement is always true. In the same way, when we control a while loop with a statement such as "$i < j$" there are some values of $i$ and $j$ for which the statement is true and some for which it is false. In statements like "$m$ is an even integer" and "$i < j$" our variables are not constrained and so are called *free variables.* For each possible value of a free variable, we have a new statement, which might be either true or false, determined by substituting the possible value for the variable. The truth value of the statement is determined only after such a substitution.

**Exercise 3.2-1** For what values of $m$ is the statement $m^2 > m$ a true statement and for what values is it a false statement? Since we have not specified a universe, your answer will depend on what universe you choose to use.

If you used the universe of positive integers, the statement is true for every value of $m$ but 1; if you used the real numbers, the statement is true for every value of $m$ except for those in the closed interval $[0, 1]$. There are really two points to make here. First, a statement about a variable can often be interpreted as a statement about more than one universe, and so to make it unambiguous, the universe must be clearly stated. Second, a statement about a variable can be true for some values of a variable and false for others.

[4]Note that to declare a variable $x$ as an integer in, say, a C program does not mean that same thing as saying that $x$ is an integer. In a C program, an integer may really be a 32-bit integer, and so it is limited to values between $2^{31} - 1$ and $-2^{31}$. Similarly a real has some fixed precision, and hence a real variable $y$ may not be able to take on a value of, say, $10^{-985}$.

### Quantifiers

In contrast, the statement

$$\text{For every integer } m,\ m^2 > m. \tag{3.1}$$

is false; we do not need to qualify our answer by saying that it is true some of the time and false at other times. To determine whether Statement 3.1 is true or false, we could substitute various values for $m$ into the simpler statement $m^2 > m$, and decide, for each of these values, whether the statement $m^2 > m$ is true or false. Doing so, we see that the statement $m^2 > m$ is true for values such as $m = -3$ or $m = 9$, but false for $m = 0$ or $m = 1$. Thus it is not the case that for every integer $m$, $m^2 > m$, so Statement 3.1 is false. It is false as a statement because it is an assertion that the simpler statement $m^2 > m$ holds for each integer value of $m$ we substitute in. A phrase like "for every integer $m$" that converts a symbolic statement about potentially any member of our universe into a statement about the universe instead is called a *quantifier.* A quantifier that asserts a statement about a variable is true for every value of the variable in its universe is called a *universal quantifier.*

The previous example illustrates a very important point.

> If a statement asserts something for every value of a variable, then to show the statement is false, we need only give one value of the variable for which the assertion is untrue.

Another example of a quantifier is the phrase "There is an integer $m$" in the sentence

> There is an integer $m$ such that $m^2 > m$.

This statement is also about the universe of integers, and as such it is true—there are plenty of integers $m$ we can substitute into the symbolic statement $m^2 > m$ to make it true. This is an example of an "existential quantifier." An *existential quantifier* asserts that a certain element of our universe exists. A second important point similar to the one we made above is:

> To show that a statement with an existential quantifier is *true*, we need only exhibit one value of the variable being quantified that makes the statement true.

As the more complex statement

> For every pair of positive integers $m$ and $n$, there are nonnegative integers $q$ and $r$ with $0 \leq r < n$ such that $m = qn + r$,

shows, statements of mathematical interest abound with quantifiers. Recall the following definition of the "big-O" notation you have probably used in earlier computer science courses:

**Definition 3.2** *We say that $f(x) = O(g(x))$ if there are positive numbers $c$ and $n_0$ such that $f(x) \leq cg(x)$ for every $x > n_0$.*

**Exercise 3.2-2** Quantification is present in our everyday language as well. The sentences "Every child wants a pony" and "No child wants a toothache" are two different examples of quantified sentences. Give ten examples of everyday sentences that use quantifiers, but use different words to indicate the quantification.

**Exercise 3.2-3** Convert the sentence "No child wants a toothache" into a sentence of the form "It is not the case that..." Find an existential quantifier in your sentence.

**Exercise 3.2-4** What would you have to do to show that a statement about one variable with an existential quantifier is *false*? Correspondingly, what would you have to do to show that a statement about one variable with a universal quantifier is *true*?

As Exercise 3.2-2 points out, English has many different ways to express quantifiers. For example, the sentences, "All hammers are tools", "Each sandwich is delicious", "No one in their right mind would do that", "Somebody loves me", and "Yes Virginia, there is a Santa Claus" all contain quantifiers. For Exercise 3.2-3, we can say "It is not the case that there is a child who wants a toothache." Our quantifier is the phrase "there is."

To show that a statement about one variable with an existential quantifier is false, we have to show that every element of the universe makes the statement (such as $m^2 > m$) false. Thus to show that the statement "There is an $x$ in $[0, 1]$ with $x^2 > x$" is false, we have to show that every $x$ in the interval makes the statement $x^2 > x$ false. Similarly, to show that a statement with a universal quantifier is true, we have to show that the statement being quantified is true for every member of our universe. We will give more details about how to show a statement about a variable is true or false for every member of our universe later in this section.

Mathematical statements of theorems, lemmas, and corollaries often have quantifiers. For example in Lemma 2.5 the phrase "for any" is a quantifier, and in Corollary 2.6 the phrase "there is" is a quantifier.

### Standard notation for quantification

Each of the many variants of language that describe quantification describe one of two situations:

A quantified statement about a variable $x$ asserts either

- that the statement is true for all $x$ in the universe, or
- that there exists an $x$ in the universe that makes the statement true.

All quantified statements have one of these two forms. We use the standard shorthand of $\forall$ for the phrase "for all" and the standard shorthand of $\exists$ for the phrase "there exists." We also adopt the convention that we parenthesize the expression that is subject to the quantification. For example, using $Z$ to stand for the universe of all integers, we write

$$\forall n \in Z\ (n^2 \geq n)$$

as a shorthand for the statement "For all integers $n$, $n^2 \geq n$." It is perhaps more natural to read the notation as "For all $n$ in $Z$, $n^2 \geq n$," which is how we recommend reading the symbolism. We similarly use

$$\exists n \in Z(n^2 \not> n)$$

to stand for "There exists an $n$ in $Z$ such that $n^2 \not> n$." Notice that in order to cast our symbolic form of an existence statement into grammatical English we have included the supplementary word "an" and the supplementary phrase "such that." People often leave out the "an" as they read an existence statement, but rarely leave out the "such that." Such supplementary language is not needed with $\forall$.

As another example, we rewrite the definition of the "Big Oh" notation with these symbols. We use the letter $R$ to stand for the universe of real numbers, and the symbol $R^+$ to stand for the universe of positive real numbers.

$$f = O(g) \text{ means that } \exists c \in R^+(\exists n_0 \in R^+(\forall x \in R(x > n_0 \Rightarrow f(x) \leq cg(x))))$$

We would read this literally as

> $f$ is big Oh of $g$ means that there exists a $c$ in $R^+$ such that there exists an $n_0$ in $R^+$ such that for all $x$ in $R$, if $x > n_0$, then $f(x) \leq cg(x)$.

Clearly this has the same meaning (when we translate it into more idiomatic English) as

> $f$ is big Oh of $g$ means that there exist a $c$ in $R^+$ and an $n_0$ in $R^+$ such that for all real numbers $x > n_0$, $f(x) \leq cg(x)$.

This statement is identical to the definition of "big Oh" that we gave earlier in Definition 3.2, except for more precision as to what $c$ and $n_0$ actually are.

**Exercise 3.2-5** How would you rewrite Euclid's division theorem, Theorem 2.12 using the shorthand notation we have introduced for quantifiers? Use $Z^+$ to to stand for the positive integers and $N$ to stand for the nonnegative integers.

We can rewrite Euclid's division theorem as

$$\forall m \in N(\forall n \in Z^+(\exists q \in N(\exists r \in N((r < n) \wedge (m = qn + r))))).$$

### Statements about variables

To talk about statements about variables, we need a notation to use for such statements. For example, we can use $p(n)$ to stand for the statement $n^2 > n$. Now, we can say that $p(4)$ and $p(-3)$ are true, while $p(1)$ and $p(.5)$ are false. In effect we are introducing variables that stand for statements about (other) variables! We typically use symbols like $p(n)$, $q(x)$, etc. to stand for statements about a variable $n$ or $x$. Then the statement "For all $x$ in $U$ $p(x)$" can be written as $\forall x \in U(p(x))$ and the statement "There exists an $n$ in $U$ such that $q(n)$" can be written as $\exists n \in U(q(n))$. Sometimes we have statements about more than one variable; for example, our definition of "big Oh" notation had the form $\exists c(\exists n_0(\forall x(p(c, n_0, x))))$, where $p(c, n_0, x)$ is $(x > n_0 \Rightarrow f(x) \leq cg(x))$. (We have left out mention of the universes for our variables here to emphasize the form of the statement.)

**Exercise 3.2-6** Rewrite Euclid's division theorem, using the notation above for statements about variables. Leave out the references to universes so that you can see clearly the order in which the quantifiers occur.

The form of Euclid's division theorem is $\forall m(\forall n(\exists q(\exists r(p(m, n, q, r)))))$.

### Rewriting statements to encompass larger universes

It is sometimes useful to rewrite a quantified statement so that the universe is larger, and the statement itself serves to limit the scope of the universe.

**Exercise 3.2-7** Let $R$ to stand for the real numbers and $R^+$ to stand for the positive real numbers. Consider the following two statements:

a) $\forall x \in R^+(x > 1)$

b) $\exists x \in R^+(x > 1)$

Rewrite these statements so that the universe is all the real numbers, but the statements say the same thing in everyday English that they did before.

For Exercise 3.2-7, there are potentially many ways to rewrite the statements. Two particularly simple ways are $\forall x \in R(x > 0 \Rightarrow x > 1)$ and $\exists x \in R(x > 0 \wedge x > 1)$. Notice that we translated one of these statements with "implies" and one with "and." We can state this rule as a general theorem:

**Theorem 3.2** *Let $U_1$ be a universe, and let $U_2$ be another universe with $U_1 \subseteq U_2$. Suppose that $q(x)$ is a statement such that*

$$U_1 = \{x|\ q(x) \text{ is true}\}. \tag{3.2}$$

*Then if $p(x)$ is a statement about $U_2$, it may also be interpreted as a statement about $U_1$, and*

(a) *$\forall x \in U_1(p(x))$ is equivalent to $\forall x \in U_2(q(x) \Rightarrow p(x))$.*

(b) *$\exists x \in U_1(p(x))$ is equivalent to $\exists x \in U_2(q(x) \wedge p(x))$.*

**Proof:** By Equation 5 the statement $q(x)$ must be true for all $x \in U_1$ and false for all $x$ in $U_2$ but not $U_1$. To prove part (a) we must show that $\forall x \in U_1(p(x))$ is true in exactly the same cases as the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$. For this purpose, suppose first that $\forall x \in U_1(p(x))$ is true. Then $p(x)$ is true for all $x$ in $U_1$. Therefore, by the truth table for "implies" and our remark about Equation 5, the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$ is true. Now suppose $\forall x \in U_1(p(x))$ is false. Then there exists an $x$ in $U_1$ such that $p(x)$ is false. Then by the truth table for "implies," the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$ is false. Thus the statement $\forall x \in U_1(p(x))$ is true if and only if the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$ is true. Therefore the two statements are true in exactly the same cases. Part (a) of the theorem follows.

Similarly, for Part (b), we observe that if $\exists x \in U_1(p(x))$ is true, then for some $x' \in U_1$, $p(x')$ is true. For that $x'$, $q(x')$ is also true, and hence $p(x') \wedge q(x')$ is true, so that $\exists x \in U_2(q(x) \wedge p(x))$ is true as well. On the other hand, if $\exists x \in U_1(p(x))$ is false, then no $x \in U_1$ has $p(x)$ true. Therefore by the truth table for "and" $q(x) \wedge p(x)$ won't be true either. Thus the two statements in Part (b) are true in exactly the same cases and so are equivalent. ■

### Proving quantified statements true or false

**Exercise 3.2-8** Let $R$ stand for the real numbers and $R^+$ stand for the positive real numbers. For each of the following statements, say whether it is true or false and why.

a) $\forall x \in R^+(x > 1)$

b) $\exists x \in R^+(x > 1)$

c) $\forall x \in R(\exists y \in R(y > x))$

d) $\forall x \in R(\forall y \in R(y > x))$

e) $\exists x \in R(x \geq 0 \land \forall y \in R^+(y > x))$

In Exercise 3.2-8, since .5 is not greater than 1, statement (a) is false. However since $2 > 1$, statement (b) is true. Statement (c) says that for each real number $x$ there is a real number $y$ bigger than $x$, which we know is true. Statement (d) says that every $y$ in $R$ is larger than every $x$ in $R$, and so it is false. Statement (e) says that there is a nonnegative number $x$ such that every positive $y$ is larger than $x$, which is true because $x = 0$ fills the bill.

We can summarize what we know about the meaning of quantified statements as follows.

**Principle 3.2 (The meaning of quantified statements)**

- *The statement $\exists x \in U(p(x))$ is true if there is at least one value of $x$ in $U$ for which the statement $p(x)$ is true.*
- *The statement $\exists x \in U(p(x))$ is false if there is no $x \in U$ for which $p(x)$ is true.*
- *The statement $\forall x \in U(p(x))$ is true if $p(x)$ is true for each value of $x$ in $U$.*
- *The statement $\forall x \in U(p(x))$ is false if $p(x)$ is false for at least one value of $x$ in $U$.*

### Negation of quantified statements

An interesting connection between $\forall$ and $\exists$ arises from the negation of statements.

**Exercise 3.2-9** What does the statement "It is not the case that for all integers $n$, $n^2 > 0$" mean?

From our knowledge of English we see that since the statement $\neg\forall n \in Z(n^2 > 0)$ asserts that it is not the case that, for all integers $n$, we have $n^2 > 0$, there must be some integer $n$ such that $n^2 \not> 0$. In other words, it says there is some integer $n$ such that $n^2 \leq 0$. Thus the negation of our "for all" statement is a "there exists" statement. We can make this idea more precise by recalling the notion of equivalence of statements. We have said that two symbolic statements are *equivalent* if they are true in exactly the same cases. By considering the case when $p(x)$ is true for all $x \in U$, (we call this case "always true") and the case when $p(x)$ is false for at least one $x \in U$ (we call this case "not always true") we can analyze the equivalence. The theorem that follows, which formalizes the example above in which $p(x)$ was the statement $x^2 > 0$, is proved by dividing these cases into two possibilities.

**Theorem 3.3** *The statements* $\neg\forall x \in U(p(x))$ *and* $\exists x \in U(\neg p(x))$ *are equivalent.*

**Proof:** Consider the following table which we have set up much like a truth table, except that the relevant cases are not determined by whether $p(x)$ is true or false, but by whether $p(x)$ is true for all $x$ in the universe $U$ or not.

| $p(x)$ | $\neg p(x)$ | $\forall x \in U(p(x))$ | $\neg\forall x \in U(p(x))$ | $\exists x \in U(\neg p(x))$ |
|---|---|---|---|---|
| always true | always false | true | false | false |
| not always true | not always false | false | true | true |

Since the last two columns are identical, the theorem holds. ■

**Corollary 3.4** *The statements* $\neg\exists x \in U(q(x))$ *and* $\forall x \in U(\neg q(x))$ *are equivalent.*

**Proof:** Since the two statements in Theorem 3.3 are equivalent, their negations are also equivalent. We then substitute $\neg q(x)$ for $p(x)$ to prove the corollary. ■

Put another way, to negate a quantified statement, you switch the quantifier and "push" the negation inside.

To deal with the negation of more complicated statements, we simply take them one quantifier at a time. Recall Definition 3.2, the definition of big Oh notation,

$$f(x) = O(g(x)) \text{ if } \exists c \in R^+(\exists n_0 \in R^+(\forall x \in R(x > n_0 \Rightarrow f(x) \leq cg(x)))).$$

What does it mean to say that $f(x)$ is *not* $O(g(x))$? First we can write

$$f(x) \neq O(g(x)) \text{ if } \neg\exists c \in R^+(\exists n_0 \in R^+(\forall x \in R(x > n_0 \Rightarrow f(x) \leq cg(x)))).$$

After one application of Corollary 3.4 we get

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+(\neg\exists n_0 \in R^+(\forall x \in R(x > n_0 \Rightarrow f(x) \leq cg(x)))).$$

After another application of Corollary 3.4 we obtain

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+(\forall n_0 \in R^+(\neg\forall x \in R(x > n_0 \Rightarrow f(x) \leq cg(x)))).$$

Now we apply Theorem 3.3 and obtain

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+(\forall n_0 \in R^+(\exists x \in R(\neg(x > n_0 \Rightarrow f(x) \leq cg(x))))).$$

Now $\neg(p \Rightarrow q)$ is equivalent to $p \wedge \neg q$, so we can write

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+(\forall n_0 \in R^+(\exists x \in R((x > n_0) \wedge (f(x) \not\leq cg(x))))).$$

Thus $f(x)$ is *not* $O(g(x))$ if for every $c$ in $R+$ and every $n_0$ in $R^+$, there is an $x$ such that $x > n_0$ and $f(x) \not\leq cg(x)$.

In our next exercise, we use the "Big Theta" notation defined as follows:

**Definition 3.3** *$f(x) = \Theta(g(x))$ means that $f(x) = O(g(x))$* **and** *$g(x) = O(f(x))$.*

**Exercise 3.2-10** Express $\neg(f(x) = \Theta(g(x)))$ in terms similar to those we used to describe $f(x) \neq O(g(x))$.

**Exercise 3.2-11** Suppose the universe for a statement $p(x)$ is the integers from 1 to 10. Express the statement $\forall x(p(x))$ without any quantifiers. Express the negation in terms of $\neg p$ without any quantifiers. Discuss how negation of "for all" and "there exists" statements corresponds to DeMorgan's Law.

By DeMorgan's law, $\neg(f = \Theta(g))$ means $\neg(f = O(g)) \vee \neg(g = O(f))$. Thus $\neg(f = \Theta(g))$ means that either for every $c$ and $n_0$ in $R^+$ there is an $x$ in $R$ with $x > n_0$ and $f(x) \not< cg(x)$ or for every $c$ and $n_0$ in $R^+$ there is an $x$ in $R$ with $x > n_0$ and $g(x) < cf(x)$ (or both).

For Exercise 3.2-11 we see that $\forall x(p(x))$ is simply

$$p(1) \wedge p(2) \wedge p(3) \wedge p(4) \wedge p(5) \wedge p(6) \wedge p(7) \wedge p(8) \wedge p(9) \wedge p(10).$$

By DeMorgan's law the negation of this statement is

$$\neg p(1) \vee \neg p(2) \vee \neg p(3) \vee \neg p(4) \vee \neg p(5) \vee \neg p(6) \vee \neg p(7) \vee \neg p(8) \vee \neg p(9) \vee \neg p(10).$$

Thus the relationship that negation gives between "for all" and "there exists" statements is the extension of DeMorgan's law from a finite number of statements to potentially infinitely many statements about a potentially infinite universe.

### Implicit quantification

**Exercise 3.2-12** Are there any quantifiers in the statement "The sum of even integers is even?"

It is an elementary fact about numbers that the sum of even integers is even. Another way to say this is that if $m$ and $n$ are even, then $m + n$ is even. If $p(n)$ stands for the statement "$n$ is even," then this last sentence translates to $p(m) \wedge p(n) \Rightarrow p(m + n)$. From the logical form of the statement, we see that our variables are free, so we could substitute various integers in for $m$ and $n$ to see whether the statement is true. But in Exercise 3.2-12, we said we were stating a more general fact about the integers. What we meant to say is that for *every pair of integers $m$* and $n$, if $m$ and $n$ are even, then $m + n$ is even. In symbols, using $p(k)$ for "$k$ is even," we have

$$\forall m \in Z(\forall n \in Z(p(m) \wedge p(n) \Rightarrow p(m + n))).$$

This way of representing the statement captures the meaning we originally intended. This is one of the reasons that mathematical statements and their proofs sometimes seem confusing—just as in English, sentences in mathematics have to be interpreted in context. Since mathematics has to be written in some natural language, and since context is used to remove ambiguity in natural language, so must context be used to remove ambiguity from mathematical statements made in natural language. In fact, we frequently rely on context in writing mathematical statements with implicit quantifiers because, in context, it makes the statements easier to read. For example, in Lemma 2.8 we said

> The equation
> $$a \cdot_n x = 1$$
> has a solution in $Z_n$ if and only if there exist integers $x$ and $y$ such that
> $$ax + ny = 1.$$

In context it was clear that the $a$ we were talking about was an arbitrary member of $Z_n$. It would simply have made the statement read more clumsily if we had said

> For every $a \in Z_n$, the equation
> $$a \cdot_n x = 1$$
> has a solution in $Z_n$ if and only if there exist integers $x$ and $y$ such that
> $$ax + ny = 1.$$

On the other hand, we were making a transition from talking about $Z_n$ to talking about the integers, so it was important for us to include the quantified statement "there exist integers $x$ and $y$ such that $ax+ny = 1$." More recently in Theorem 3.3, we also did not feel it was necessary to say "For all universes $U$ and for all statements $p$ about $U$," at the beginning of the theorem. We felt the theorem would be easier to read if we kept those quantifiers implicit and let the reader (not necessarily consciously) infer them from context.

### Proof of quantifiedstatements

We said that "the sum of even integers is even" is an elementary fact about numbers. How do we know it is a fact? One answer is that we know it because our teachers told us so. (And presumably they knew it because their teachers told them so.) But someone had to figure it out in the first place, and so we ask how we would prove this statement? A mathematician asked to give a proof that the sum of even numbers is even might write

> If $m$ and $n$ are even, then $m = 2i$ and $n = 2j$ so that
> $$m + n = 2i + 2j = 2(i + j)$$
> and thus $m + n$ is even.

Because mathematicians think and write in natural language, they will often rely on context to remove ambiguities. For example, there are no quantifiers in the proof above. However the sentence, while technically incomplete as a proof, captures the essence of why the sum of two even numbers is even. A typical complete (but more formal and wordy than usual) proof might go like this.

> Let $m$ and $n$ be integers. Suppose $m$ and $n$ are even. If $m$ and $n$ are even, then by definition there are integers $i$ and $j$ such that $m = 2i$ and $n = 2j$. Thus there are integers $i$ and $j$ such that $m = 2i$ and $n = 2j$. Then
> $$m + n = 2i + 2j = 2(i + j),$$
> so by definition $m + n$ is an even integer. We have shown that if $m$ and $n$ are even, then $m + n$ is even. Therefore for every $m$ and $n$, if $m$ and $n$ are even integers, then so is $m + n$.

We began our proof by assuming that $m$ and $n$ are integers. This gives us symbolic notation for talking about two integers. We then appealed to the definition of an even integer, namely that an integer $h$ is even if there is another integer $k$ so that $h = 2k$. (Note the use of a quantifier in the definition.) Then we used algebra to show that $m+n$ is also two times another number. Since this is the definition of $m+n$ being even, we concluded that $m+n$ is even. This allowed us to say that if $m$ and $n$ are even, the $m+n$ is even. Then we asserted that for every pair of integers $m$ and $n$, if $m$ and $n$ are even, then $m+n$ is even.

There are a number of principles of proof illustrated here. The next section will be devoted to a discussion of principles we use in constructing proofs. For now, let us conclude with a remark about the limitations of logic. How did we know that we wanted to write the symbolic equation

$$m + n = 2i + 2j = 2(i + j)?$$

It was not logic that told us to do this, but intuition and experience.

**Important Concepts, Formulas, and Theorems**

1. *Varies over.* We use the phrase *varies over* to describe the set of values a variable may take on.

2. *Universe.* We call the set of possible values for a variable the *universe* of that variable.

3. *Free variables.* Variables that are not constrained in any way whatever are called *free variables.*

4. *Quantifier.* A phrase that converts a symbolic statement about potentially any member of our universe into a statement about the universe instead is called a *quantifier*. There are two types of quantifiers:

   - *Universal quantifier.* A quantifier that asserts a statement about a variable is true for every value of the variable in its universe is called a *universal quantifier.*
   - *Existential quantifier.* A quantifier that asserts a statement about a variable is true for at least one value of the variable in its universe is called an *existential quantifier.*

5. *Larger universes.* Let $U_1$ be a universe, and let $U_2$ be another universe with $U_1 \subseteq U_2$. Suppose that $q(x)$ is a statement such that

$$U_1 = \{x|\ q(x) \text{ is true}\}.$$

   Then if $p(x)$ is a statement about $U_2$, it may also be interpreted as a statement about $U_1$, and

   (a) $\forall x \in U_1(p(x))$ is equivalent to $\forall x \in U_2(q(x) \Rightarrow p(x))$.

   (b) $\exists x \in U_1(p(x))$ is equivalent to $\exists x \in U_2(q(x) \wedge p(x))$.

6. *Proving quantified statements true or false.*

   - The statement $\exists x \in U(p(x))$ is true if there is at least one value of $x$ in $U$ for which the statement $p(x)$ is true.

- The statement $\exists x \in U(p(x))$ is false if there is no $x \in U$ for which $p(x)$ is true.
- The statement $\forall x \in U(p(x))$ is true if $p(x)$ is true for each value of $x$ in $U$.
- The statement $\forall x \in U(p(x))$ is false if $p(x)$ is false for at least one value of $x$ in $U$.

7. *Negation of quantified statements.* To negate a quantified statement, you switch the quantifier and push the negation inside.
   - The statements $\neg\forall x \in$U$(p(x))$ and $\exists x \in U(\neg p(x))$ are equivalent.
   - The statements $\neg\exists x \in$U$(p(x))$ and $\forall x \in U(\neg p(x))$ are equivalent.
8. *Big-Oh* We say that $f(x) = O(g(x))$ if there are positive numbers $c$ and $n_0$ such that $f(x) \le cg(x)$ for every $x > n_0$.
9. *Big-Theta.* $f(x) = \Theta(g(x))$ means that $f = O(g(x))$ **and** $g = O(f(x))$.
10. *Some notation for sets of numbers.* We use $R$ to stand for the real numbers, $R^+$ to stand for the positive real numbers, $Z$ to stand for the integers (positive, negative, and zero), $Z^+$ to stand for the positive integers, and $N$ to stand for the nonnegative integers.

## Problems

1. For what positive integers $x$ is the statement $(x-2)^2 + 1 \le 2$ true? For what integers is it true? For what real numbers is it true? If we expand the universe for which we are considering a statement about a variable, does this always increase the size of the statement's truth set?
2. Is the statement "There is an integer greater than 2 such that $(x-2)^2 + 1 \le 2$" true or false? How do you know?
3. Write the statement that the square of every real number is greater than or equal to zero as a quantified statement about the universe of real numbers. You may use $R$ to stand for the universe of real numbers.
4. The definition of a prime number is that it is an integer greater than 1 whose only positive integer factors are itself and 1. Find two ways to write this definition so that all quantifiers are explicit. (It may be convenient to introduce a variable to stand for the number and perhaps a variable or some variables for its factors.)
5. Write down the definition of a greatest common divisor of $m$ and $n$ in such a way that all quantifiers are explicit and expressed explicitly as "for all" or "there exists." Write down Euclid's extended greatest common divisor theorem that relates the greatest common divisor of $m$ and $n$ algebraically to $m$ and $n$. Again make sure all quantifiers are explicit and expressed explicitly as "for all" or "there exists."
6. What is the form of the definition of a greatest common divisor, using $s(x, y, z)$ to be the statement $x = yz$ and $t(x, y)$ to be the statement $x < y$? (You need not include references to the universes for the variables.)
7. Which of the following statements (in which $Z^+$ stands for the positive integers and $Z$ stands for all integers) is true and which is false, and why?

(a) $\forall z \in Z^+(z^2 + 6z + 10 > 20)$.

(b) $\forall z \in Z(z^2 - z \geq 0)$.

(c) $\exists z \in Z^+(z - z^2 > 0)$.

(d) $\exists z \in Z(z^2 - z = 6)$.

8. Are there any (implicit) quantifiers in the statement "The product of odd integers is odd?" If so, what are they?

9. Rewrite the statement "The product of odd integers is odd," with all quantifiers (including any in the definition of odd integers) explicitly stated as "for all" or "there exist."

10. Rewrite the following statement without any negations. It is not the case that there exists an integer $n$ such that $n > 0$ and for all integers $m > n$, for every polynomial equation $p(x) = 0$ of degree $m$ there are no real numbers for solutions.

11. Consider the following slight modification of Theorem 3.2. For each part below, either prove that it is true or give a counterexample.

    Let $U_1$ be a universe, and let $U_2$ be another universe with $U_1 \subseteq U_2$. Suppose that $q(x)$ is a statement such that $U_1 = \{x|\ q(x) \text{ is true}\}$.

    (a) $\forall x \in U_1(p(x))$ is not equivalent to $\forall x \in U_2(q(x) \wedge p(x))$.

    (b) $\exists x \in U_1(p(x))$ is equivalent to $\exists x \in U_2(q(x) \Rightarrow p(x))$.

12. Let $p(x)$ stand for "$x$ is a prime," $q(x)$ for "$x$ is even," and $r(x, y)$ stand for "$x = y$." Write down the statement "There is one and only one even prime," using these three symbolic statements and appropriate logical notation. (Use the set of integers for your universe.)

13. Each expression below represents a statement about the integers. Using $p(x)$ for "$x$ is prime," $q(x, y)$ for "$x = y^2$," $r(x, y)$ for "$x \leq y$," $s(x, y, z)$ for "$z = xy$," and $t(x, y)$ for "$x = y$," determine which expressions represent true statements and which represent false statements.

    (a) $\forall x \in Z(\exists y \in Z(q(x, y) \vee p(x)))$

    (b) $\forall x \in Z(\forall y \in Z(s(x, x, y) \Leftrightarrow q(x, y)))$

    (c) $\forall y \in Z(\exists x \in Z(q(y, x)))$

    (d) $\exists z \in Z(\exists x \in Z(\exists y \in Z(p(x) \wedge p(y) \wedge \neg t(x, y)))$

14. Find a reason why $(\exists x \in U(p(x))) \wedge (\exists y \in U(q(y)))$ is not equivalent to $\exists z \in U(p(z) \vee q(z))$. Are the statements $(\exists x \in U(p(x))) \vee (\exists y \in U(q(y)))$ and $\exists z \in U(p(z) \vee q(z))$ equivalent?

15. Give an example (in English) of a statement that has the form $\forall x \in U(\exists y \in V(p(x, y)))$. (The statement can be a mathematical statement or a statement about "everyday life," or whatever you prefer.) Now write in English the statement using the same $p(x, y)$ but of the form $\exists y \in V(\forall x \in U(p(x, y)))$. Comment on whether "for all" and "there exist" commute.