Unit Lo

Logic

Logic is the tool for reasoning about the truth and falsity of statements. There are two main directions in which logic develops.

- The first is the depth to which we explore the structure of statements. The study of the basic level of structure is called propositional logic. First order predicate logic, which is often called just predicate logic, studies structure on a deeper level.
- The second direction is the nature of truth. For example, one may talk about statements that are usually true or true at certain times. We study only the simplest situation: a statement is either always true or it is considered false.

"True" and "false" could be replaced by 1 and 0 (or any other two symbols) in our discussions. Using 1 and 0 relates logic to Boolean functions. In fact, *propositional logic* is the study of Boolean functions, where 1 plays the role of "true" and 0 the role of "false." As we saw in Unit BF, Boolean functions can be thought of as computer circuits. Thus, propositional logic, Boolean functions, and computer circuits are different ways of interpreting the same thing.

Propositional logic is not sufficient for all our logic needs. Mathematics requires predicate logic. This and other logics are employed in the design of expert systems, robots and artificial intelligence.

Section 1: Propositional Logic

If it is not fresh in your mind, you should review the material in the first section of Unit BF (Boolean Functions). In that section we were wearing our "arithmetic hat." Now we are wearing our "logic hat" and so refer to things differently:

Arithmetic Hat	Logic Hat
0 and 1, respectively	false and true, respectively
Boolean variable	statement variable
form of function	statement form
value of function	truth value of statement (form)
equality of function (forms)	equivalence of statement forms

We should explain some of these terms a bit more.

- In English, statement variables have structure — verbs, subjects, prepositional phrases, and so on. In propositional logic, we don't see the structure. You're used to that because variables in high school algebra don't have any structure; they just stand for (unknown) numbers.

- A function can be written in many ways. For example, $xy + x$, $x + yx$, $x(y + 1)$ and $(x + z)y + x - yz$ are all ways of writing the same function. Logicians refer to the particular way a function is written as a *statement form.*

You may wonder why we're concerned with statement *forms* since we're not concerned with function forms in other areas of mathematics but just their values. That is a misconception. We **are concerned** with function forms in algebra. It's just that you're so used to the equality of different forms that you've forgotten that. Knowing that certain forms represent the same function allow us to manipulate formulas. For example, the commutative ($ab = ba$ and $a + b = b + a$) and distributive ($a(b + c) = ab + ac$) laws allow us to manipulate the function forms $xy + x$, $x + yx$ and $x(y + 1)$ to show that they all have the same value; that is, they all represent the same function. As soon as the equality of the function forms is less familiar, you're aware of their importance. For example $(a^u)^v = a^{uv}$, $\sin(2x) = 2\sin x \cos x$ and $\mathrm{d}(e^x)/\mathrm{d}x = e^x$.

Since some of you may still be confused, let's restate this. For our purposes, we shall say that two statement forms are *different as statement forms*, or simply *different* if they "look different." They are the same if they "look the same." This is not very precise, but is good enough. Thus, for example, $p \vee q$ and $q \vee p$ look different and so are different statement forms. We say that two statement forms are *logically equivalent* (or simply *equivalent*) if they have the same truth table. The statement forms $p \vee q$ and $q \vee p$ are equivalent (have same truth table). Likewise, $(p \wedge q) \vee r$ and $(p \vee r) \wedge (q \vee r)$ are different statement forms that are equivalent, as may be seen by doing a truth table for each form and comparing them. We are familiar with these ideas from high school algebra. For example, $x(y + z)$ and $xy + xz$ look different but are equivalent functions.

Sometimes we'll let our logic hat slip and use Boolean function terminology. In particular, we'll often use 0 instead of "false" and 1 instead of "true."

The constant functions are particularly important and are given special names.

Definition 1 (Tautology, contradiction) *A statement form that represents the constant 1 function is called a tautology. In other words, the statement form is true for all truth values of the statement variables. A statement form that represents the constant 0 function is called a contradiction. In other words, the statement form is false for all truth values of the statement variables.*

Recall the some of the basic functions studied in Unit BF: **not**, **and** and **or**, denoted by $\sim$, $\wedge$ and $\vee$, respectively. We defined these three functions by giving their values in tabular form, which is called a *truth table* just as it is for Boolean functions in Unit BF. In that unit, definitions were as follows, where we have replaced 0 and 1 by F and T to emphasize "false" and "true;" however, we'll usually use 0 and 1.

p	$\sim p$
F	T
T	F

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

p	q	p "equals" q
F	F	T
F	T	F
T	F	F
T	T	T

We said there were three functions, but there is a fourth table. Besides, p "equals" q isn't a function—is it? What happened? The statement p "equals" q is either true of false. Thus, we can think of "equals" as a function with domain $\{F,T\}^2$ and range $\{F,T\}$. In symbols, "equals" : $\{F,T\}^2 \to \{F,T\}$. In what follows, we'll replace "equals" with the symbol "$\Leftrightarrow$" (equivalence) which is usually used in logic. We use the more familiar "=" for assigning meaning and values. Thus

- $q =$ "the sky is blue" assigns an English meaning to q.
- $q = p \vee r$ says that q "means" $p \vee r$; that is, we should replace q by the statement form $p \vee r$.
- $p = 1$ means we are assigning the value 1 (true) to p.

Since propositional logic can be viewed as the study of Boolean functions, the techniques we developed for proving results about Boolean functions (Venn diagrams, truth tables and algebraic) can also be used in propositional logic. For convenience, we recall the theorem for manipulating Boolean statements:

Theorem 1 (Algebraic rules for statement forms) *Each rule states that two different statement forms are equivalent. That is, they look different but have the same truth table.*

Associative Rules:	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
Distributive Rules:	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
Idempotent Rules:	$p \wedge p \Leftrightarrow p$	$p \vee p \Leftrightarrow p$
Double Negation:	$\sim\sim p \Leftrightarrow p$	
DeMorgan's Rules:	$\sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q$	$\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$
Commutative Rules:	$p \wedge q \Leftrightarrow q \wedge p$	$p \vee q \Leftrightarrow q \vee p$
Absorption Rules:	$p \vee (p \wedge q) \Leftrightarrow p$	$p \wedge (p \vee q) \Leftrightarrow p$
Bound Rules:	$p \wedge 0 \Leftrightarrow 0 \qquad p \wedge 1 \Leftrightarrow p$	$p \vee 1 \Leftrightarrow 1 \qquad p \vee 0 \Leftrightarrow p$
Negation Rules:	$p \wedge (\sim p) \Leftrightarrow 0$	$p \vee (\sim p) \Leftrightarrow 1$

Truth tables and algebraic rules are practically the same as the tabular method and algebraic rules for sets discussed in Section 1 of Unit SF. The next example explains why this is so. You may want to read the first four pages of Unit SF now.

Example 1 (Logic and Sets) We've already pointed out that propositional logic and Boolean arithmetic can be viewed as different aspects of the same thing. In this example, we show that basic manipulation of sets are also related.

Suppose we are studying some sets, say P, Q and R. Let the corresponding lower case letters p, q and r stand for the statement that x belongs to the set. For example p is the statement "$x \in P$".

Consider the distributive rule for sets:

$$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R).$$

It is equivalent to saying that

$$x \in P \cap (Q \cup R) \qquad \text{if and only if} \qquad x \in (P \cap Q) \cup (P \cap R)$$

for all x in the universal set. What does $x \in P \cap (Q \cup R)$ mean? It means $x \in P$ and $x \in (Q \cup R)$. What does $x \in (Q \cup R)$ mean? It means $x \in Q$ or $x \in R$. Putting this all together and using our logic notation, $x \in P \cap (Q \cup R)$ means $p \wedge (q \vee r)$. Similarly $x \in (P \cap Q) \cup (P \cap R)$ means $(p \wedge q) \vee (p \wedge r)$. Thus the set form of the distributive rule is the same as

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r),$$

the distributive rule for logic.

It should be obvious how things are translated between set notation and logic notation and why we get the same algebraic rules. A practical consequence of this is that we can use Venn diagrams to prove logic statements just as we used them in Unit SF.

Why is the tabular method for proving set identities like a truth table? The answer is simple, consider P, Q and R again. There are exactly eight possibilities for the location of x, corresponding to the eight regions of the Venn diagram. For example, if $x \in P$, $x \notin Q$ and $x \in R$, then the corresponding row in the tabular method for sets begins "Yes No Yes" and the truth table for p, q and r begins $T\ F\ T$. Thus the way to translate between the two methods is Yes$\leftrightarrow T$ and No$\leftrightarrow F$. $\square$

Implication

"If it is raining, then the sidewalk is wet." This is a simple example of an *implication* statement. Some other forms are "The sidewalk is wet whenever it is raining" and "If the sidewalk isn't wet, then it isn't raining." We want to include implication in propositional logic since statements of the form "If X, then Y" play an important part in logical reasoning. To do so, we must face two problems:

- It is not clear how we should view "If X, then Y" when X is false. For example, what should we think if it isn't raining?
- Due to the variety and ambiguity of English, translation into Boolean statements may not be clear.

In the remainder of this section, we investigate carefully the relationship between English language assertions and Boolean functions (Boolean statement forms) associated with implication.

Let $r =$ "it is raining" and let $w =$ "the sidewalk is wet." In symbolic notation, we use $r \Rightarrow w$ to stand for the statement "If it is raining, then the sidewalk is wet." Usually, when such a statement is made we are primarily concerned with the situation when r is true. For the study of logic, we must be concerned with all situations, so we need to know how to think about $r \Rightarrow w$ when r is false. If it is not raining, the sidewalk may be wet (it rained earlier, the sprinklers are on, etc.) or the sidewalk may not be wet. Thus when r is false, we have no reason to disbelieve the statement $r \Rightarrow w$. Of course, we have no reason to believe it either, so we are free to choose whatever we want for the truth value in this case. We take the generous approach and call $r \Rightarrow w$ true when r is false. (Actually we're not being generous—this is the standard interpretation.)

Let's put all this into a definition.

Definition 2 (Implication) *We define $p \Rightarrow q$ to be the Boolean function, called implication or p implies q or the "conditional of q by p." As a Boolean function, $p \Rightarrow q$ has the following truth table:*

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

The expression $p \Rightarrow q$ is a Boolean statement form. It is equivalent to the statement form $\sim p \vee q$, as can be seen by comparing truth tables:

p	q	$\sim p \vee q$
0	0	1
0	1	1
1	0	0
1	1	1

Note that the Boolean function $f(p,q)$ defined by $p \Rightarrow q$ has value 1 when $p = 0$, independent of the value of q.

We've been a bit sloppy: we've said $r =$ "It is raining" and also, by the definition, $r = 1$. Clearly "It is raining" is not the same as "1." What's going on? Since we are studying the truth values of statements, we should have said

$$r = \text{the truth value of "It is raining."}$$

We'll continue with the common practice of abusing the terminology by omitting the words "the truth value of."

Example 2 (Implication, rain and Venn diagrams) Let R be the set of all times when it is raining and let W be the set of all times when the sidewalk is wet. What does our earlier example $r \Rightarrow w$ say about the sets R and W? Suppose t is a time; that is, an element of our universal set of all times.

- If $t \in R$, then it is raining at time t and so, by $r \Rightarrow w$, $t \in W$. Thus $R \subseteq W$.
- If $t \notin R$, then it is not raining at time t. In this case, $r \Rightarrow w$ gives us no information about whether or not t is in W. Why is that? When r is false, $r \Rightarrow w$ is true regardless of whether or not w is true; that is, whether or not t is in W.

What happened to the 0 case of $r \Rightarrow w$ in the definition of implication? That is the case $t \in R$ (because r is true) and $t \notin W$ (because w is false). Since the definition of implication says this is false, it says that this cannot happen. This is a consequence of $R \subseteq W$.

This is the way we represent $p \Rightarrow q$ with Venn diagrams: There is a set P where p is true and another set Q where q is true and we insist that $P \subseteq Q$.

How can we show that $p \Rightarrow q$ is not true for specific p and q? (For example, "If it is raining, then my car won't start.") We must find an instance where p is true and q is false because this is the only time $p \Rightarrow q$ is false. (It's raining, but my car starts.) You'll see more of this later. □

Example 3 (Statement forms associated with implication) Here is a table that defines the basic statement forms associated with the conversational use of implication.

p	q	$p \Rightarrow q$	$\sim q \Rightarrow \sim p$	$q \Rightarrow p$	$\sim p \Rightarrow \sim q$	$p \Leftrightarrow q$
0	0	1	1	1	1	1
0	1	1	1	0	0	0
1	0	0	0	1	1	0
1	1	1	1	1	1	1

Starting with the statement form $p \Rightarrow q$, the statement form $\sim q \Rightarrow \sim p$ is called the *contrapositive* of $p \Rightarrow q$, the statement form $q \Rightarrow p$ is called the *converse* of $p \Rightarrow q$, and the statement form $\sim p \Rightarrow \sim q$ is called the *inverse* of $p \Rightarrow q$. Note that, although the statement and its contrapositive are different statement forms (they look different) they are equivalent (i.e., the same as Boolean functions). Likewise, the converse and the inverse are equivalent. But, and this is important, the statement and its converse are **not** equivalent. The final statement form $p \Leftrightarrow q$ is called *double implication* or "biconditional" and is equivalent to $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

Here, in tabular form, are some additional facts related to implication.

p	q	$p \Rightarrow q$	$\sim p \vee q$	$\sim(p \Rightarrow q)$	$p \wedge \sim q$
0	0	1	1	0	0
0	1	1	1	0	0
1	0	0	0	1	1
1	1	1	1	0	0

The statement forms $p \Rightarrow q$ and $\sim p \vee q$ are equivalent as are $\sim(p \Rightarrow q)$ and $p \wedge \sim q$. □

Example 4 (Right triangles and the Pythagorean theorem) Throughout this example, suppose $0 < a \le b \le c$ are some fixed numbers. Take $R =$ "The triangle with side lengths a, b, c is a right triangle" and $P =$ "$a^2 + b^2 = c^2$." We know from high school that "If R then P." As a Boolean statement form we may write $R \Rightarrow P$. If you proved this fact by starting with a right triangle and using a geometric argument to show that $a^2 + b^2 = c^2$, then the statement form $R \Rightarrow P$ represented the state of your knowledge at that point in time. You then probably went on to learn the law of cosines: $a^2 + b^2 - 2\,ab\,\cos(\theta) = c^2$. Using that, you can easily see that the converse $P \Rightarrow R$ is true. Now you can represent the state of your knowledge by $R \Leftrightarrow P$.

The statement form $R \Rightarrow P$ is equivalent to $\sim R \vee P$. Either a triangle is not a right triangle or it satisfies $a^2 + b^2 = c^2$.

Start with the statement, "If the triangle with side lengths a, b, c is a right triangle, then $a^2 + b^2 = c^2$."

- The contrapositive of that statement is "If $a^2 + b^2 \neq c^2$, then the triangle with side lengths a, b, c is not a right triangle."
- The converse is, if $a^2 + b^2 = c^2$, then the triangle with side lengths a, b, c is a right triangle."
- The inverse is, "If the triangle with side lengths a, b, c is a not right triangle, then $a^2 + b^2 \neq c^2$." $\square$

Example 5 (The many English forms for $p \Rightarrow q$) In this example we'll discuss most of the ways implication is written in English. Pay careful attention to when we use the phrase "statement form" and when we use the phrase "Boolean function." Be sure to read the last part of the example where we discuss the distinction between statement form and Boolean function further.

- *if … then*: The basic English form, "If p then q," is understood to stand for the statement form $p \Rightarrow q$. Note that the "if" is associated with p. Alternatively to this, one sees "q if p." Again, the "if" is associated with p, so this stands for the statement form $p \Rightarrow q$. Thus, "If it's raining, then it's cloudy" is interpreted as the same statement form as "It's cloudy if it's raining." Both stand for the statement form "raining" $\Rightarrow$ "cloudy."
- *only if*: Sometimes we say "p only if q," as in "I'll go to the party only if I finish studying." Some people would paraphrase this as, "If I don't finish studying, then I won't go to the party." In other words "p only if q" is translated into the statement form $\sim q \Rightarrow \sim p$. This statement form is equivalent, as a Boolean function, to the statement form $p \Rightarrow q$, because an implication form is equivalent to its contrapositive form. In other words, "p only if q", however it is interpreted as a statement form, is equivalent as a Boolean function to "If I go to the party, then I finished studying." Thus the phrase "p only if q" can be translated *as a Boolean function* into either one of the equivalent statement forms $\sim q \Rightarrow \sim p$ or $p \Rightarrow q$, whichever is most convenient for the discussion at hand.
- *if and only if*: The biconditional, $p \Leftrightarrow q$ is sometimes stated as "p if and only if q" and written "p iff q".
- *sufficient*: The expression, "p is sufficient for q"(or "p is a sufficient condition for q") is usually translated into the statement form $p \Rightarrow q$. Some students find it helpful to (silently to themselves) expand this phrase to "p is sufficient *to force q to happen*." Then it is easier to remember that this means $p \Rightarrow q$. Instead of saying "p is sufficient for q", one sometimes says "a sufficient condition for q is p."
- *necessary*: The statement "p is necessary for q" usually stands for the statement form $\sim p \Rightarrow \sim q$. Some students (again silently to themselves) expand this to "p is a necessary consequence of q." They find this easier to associate with the equivalent (as a Boolean function) form $q \Rightarrow p$. Instead of saying "q is necessary for p", one says "a necessary condition for p is q."
- *necessary and sufficient*: Combining the two previous bulleted items, we see that "p is necessary and sufficient for q" is equivalent to $p \Leftrightarrow q$, the biconditional. Notice that we simply combined "necessary" and "sufficient", just as we combined "if" and "only if" earlier to get the biconditional.

- *unless*: Another possible source of confusion is the term "unless." To say "p unless q" is, formally, to specify the statement form $\sim q \Rightarrow p$. The most common usage of "unless" in English is something like, "The building is safe, unless the fire alarm is ringing." Formally, this means, "If the fire alarm is not ringing, then the building is safe." Think of a night watchman sitting in his office with the fire alarm on the wall. Since the alarm isn't ringing he relaxes, maybe even takes a nap. His assumption is that "If the fire alarm is not ringing then all is well, the building is safe, I can relax." If you asked him, "Why are you sleeping?" he might reply, "The building is safe unless the fire alarm is ringing."

  An equivalent Boolean function is $\sim p \Rightarrow q$, the contrapositive of $\sim q \Rightarrow p$. Thus we have "If the building is not safe, then the fire alarm is ringing." Note the symmetry in translating "p unless q" into either of the equivalent forms $\sim p \Rightarrow q$ or $\sim q \Rightarrow p$. In translating "p unless q" into a Boolean function, simply apply "$\sim$" to one of p or q and have that imply the other without applying "$\sim$".

Let's review the role of the concepts of a "statement form" and a "Boolean function" in the above discussion.

(a) Generally, when we are translating an English description of an implication into symbolic form, we are concerned most of all with obtaining the correct Boolean function. With a little practice you will find this easy to do.

(b) In the rare case when we are being pedantic and want to know if some statement form is the contrapositive, converse, or inverse, of an implication described in English, then we need to associate a precise *statement form* with the English sentence. Our policy will be to always give you that statement form when you need to know it for the discussion or question. The one exception to this policy is the case of "if p then q" (or "q if p") which we always associate with the statement form $p \Rightarrow q$.

Thus, in most cases, as with other English usages, all you will need to be able to do is translate "if p then q" into an equivalent form as a Boolean function: $p \Rightarrow q$, $\sim q \Rightarrow \sim p$, $\sim p \vee q$, etc. $\square$

Example 6 (A way of translating English implications) Of course, you can memorize the rules from the previous example (and that may be a good idea), but what if you forget or if you run into something new? Suppose we see a sentence that relates two phrases A and B; for example, "If A then B" or "A requires B." Suppose we also realize that an implication is involved. How can we determine whether to write $A \Rightarrow B$ or $B \Rightarrow A$ or some other implication?

Here's a trick: The truth table for $p \Rightarrow q$ has only one row which is false and that occurs when p is true and q is false. Take your sentence and figure out how to make it false and set things up so that it corresponds to (True)$\Rightarrow$(False).

Let's do some examples.

What about "A requires B?" Consider "Fishes require water." This is false if something is a fish and does not require water. In general "A requires B" is false when A is true and B is false. Thus, we have $A \Rightarrow B$.

What about "A is necessary for B?" Consider "Enrollment is necessary for credit." This is false if I receive credit even though I am not enrolled. In other words "A is necessary for B" is false when B is true and A is false. Thus we can write it as $B \Rightarrow A$.

What about "A unless B?" Consider "I will flunk unless I study." This is false when I don't flunk and I don't study. Thus, it is false when A and B are both false. Since we need (True)$\Rightarrow$(False), we need to negate something. One possibility is $\sim A \Rightarrow B$ and another is $\sim B \Rightarrow A$. Which is correct? They both are — one is the contrapositive of the other. However, they sound different in English. Compare "If I passed, then I studied" and "If I don't study, then I won't pass." The first is celebration after the fact and the second is a warning about what I should do.

What about "A or B?" Wait! There's no implication here. In logic all that matters is the truth table. Any statement form involving two variables that is false in only one of the four cases can be written as an implication. "A or B" is false only when both A and B are false. Thus $\sim A \Rightarrow B$. You've actually seen this before: we learned that $p \Rightarrow q$ and $\sim p \vee q$ are equivalent, so set $p = \sim A$ and $q = B$. $\square$

Exercises for Section 1

1.1. In Example 1 we noted that algebraic operations in propositional logic, set theory and Boolean functions can be viewed as different aspects of the same thing. What logic and set operations correspond to the exclusive or operation for Boolean functions?

1.2. Let $h =$ "he is happily married," and $w =$ "he is wealthy," and $s =$ "he is smart." Write the following statements in symbolic form:

(a) He is happily married and wealthy but not smart.

(b) He is not wealthy, but he is happily married and smart.

(c) He is neither happily married, nor wealthy, nor smart.

1.3. Let $n =$ "Nancy will major in computer science" and $k =$ "Karen will major in computer science." Write the following statement in symbolic form: Either Nancy will major in computer science or Karen will major in computer science, but not both.

1.4. Let $p =$ "computer is out of memory flag, COM, is zero (i.e., off)," and $q =$ "disk error has occurred flag, DEO, is zero," and $r =$ "ZIP disk hasn't enough memory left flag, ZIP, is zero." Write the following statements in symbolic form:

(a) COM is off and DEO is off and ZIP is off.

(b) COM is off but DEO is on.

(c) There is enough memory in the computer; however, either a disk error has occurred or the ZIP disk is out of memory.

(d) The computer is out of memory and no disk error has occurred, but the ZIP disk is out of memory.

(e) Either the computer is out of memory or both COM == 0 and DEO == 0.

1.5. Is the statement form $(p \wedge q) \vee \big(\sim p \vee (p \wedge \sim q)\big) \vee r$ a tautology, contradiction, or neither?

1.6. Is the statement form $(p \wedge \sim q) \wedge (\sim p \vee q) \wedge r$ a tautology, contradiction, or neither?

1.7. Is the statement form $\big((\sim p \wedge q) \wedge (q \vee r)\big) \wedge \sim q \wedge r$ a tautology, contradiction, or neither?

1.8. Construct a truth table for $p \vee (\sim p \wedge q) \Rightarrow q$.

1.9. Construct a truth table for $p \vee (\sim p \wedge q) \Rightarrow \sim q$.

1.10. Construct a truth table for $(p \Rightarrow q) \Rightarrow (q \Rightarrow p)$.

1.11. Write negations of the following statements in English that is as easily understood as possible.

(a) If P is a pentagon then P is a polygon.

(b) If Tom is Ann's father, then Jim is Ann's uncle and Sue is her aunt and Mary is her cousin.

1.12. Write the converses and inverses for the statements in the previous exercise.

1.13. Why is the assertion, "There is some statement $p \Rightarrow q$ that is not equivalent to its contrapositive," equivalent to the statement, "There is some statement $p \Rightarrow q$ whose converse is not equivalent to its inverse?" (Note: both statements are false.)

1.14. Write the contrapositives for the statements in Exercise 1.11.

1.15. Write the contrapositive of the statement "Dennis won't enter the America's Cup unless he is sure of victory." Use the interpretation of "p unless q" as the statement form $\sim p \Rightarrow q$.

1.16. You were told by your high school principal that you will "graduate with honor" (call that H) only if you either "make the honor roll each semester" (M) or "complete all language requirements" (C), and if, in addition, you "get straight A's in biology" (B) and "letter in at least one athletic activity" (A). You lettered in track, got straight A's in all your science classes (including biology), and completed all language requirements, but at graduation you were not given any honors. Did your high school principal lie to you?

1.17. Write two different statement forms using "if" and "then" that are equivalent to the following: "Learning to program in C is a necessary condition for learning to program in C++. "

1.18. Given $(\sim p \vee q) \Rightarrow (r \vee \sim q)$, rewrite it as a statement form using only $\sim$ and $\wedge$.

1.19. Given $\Big((p \Rightarrow (q \Rightarrow r)) \Leftrightarrow ((p \wedge q) \Rightarrow r)\Big) \wedge \sim p \wedge \sim q \wedge \sim r$, rewrite it using only $\sim$ and $\vee$.

1.20. Start with the statement form "Getting up when the alarm rings is a sufficient condition for me to get to work on time." Rewrite it in an equivalent if- then form.

1.21. Start with the statement form, "Having sides of length 3, 4, and 5 is a sufficient condition for this triangle to be a right triangle." Rewrite it in an equivalent if-then form.

1.22. Start with the statement form, "Doing all of the programming assignments is a necessary condition for Jane to pass her Java course." Rewrite this statement in an equivalent if-then form.

1.23. "If the program is running then there is at least 250K of RAM." Which of the following are equivalent to this statement?

(a) If there is at least 250K of RAM then the program is running.

(b) If there is less than 250K of RAM then the program is not running.

(c) The program will run only if there is at least 250K of RAM.

(d) If the program is not running then there is less than 250K of RAM.

(e) A necessary condition for the program to run is that there are at least 250K of RAM.

(f) A sufficient condition for the program to run is that there is at least 250K of RAM.

Section 2: Predicate Logic

We have been studying statements that are either true or false. But, consider the statement "$x^2 > 1$." In order to decide if this statement is true of false, we need to know the numerical value of x. If $x = 1.1$, then "$x^2 > 1$" is true. If $x = 0.9$, then "$x^2 > 1$" is false. The best way to think of this is to regard the statement "$x^2 > 1$" as a function $S(x) =$ "$x^2 > 1$." If we take this point of view, we need to specify the domain of S. First suppose the domain of S is $\mathbb{R}$, the set of all real numbers. The codomain (or range) of S, by our description just given, is a set of statements that are either true or false (e.g., $S(0.9) =$ "$0.9^2 > 1$", $S(2.3) =$ "$2.3^2 > 1$"). The function S is an example of a *predicate.*

Definition 3 (Predicate and truth set) *A predicate is any function whose codomain is statements that are either true or false. There are two things to be careful about:*

- *The codomain is statements* **not** *the truth value of the statements.*
- *The domain is arbitrary — different predicates can have different domains.*

The truth set of a predicate S with domain D is the set of those $x \in D$ for which $S(x)$ is true. It is written

$$\{x \in D \mid S(x) \text{ is true}\} \quad \text{or simply} \quad \{x \mid S(x)\}.$$

Note that $S(0.9) =$ "$0.9^2 > 1$" is a correct statement consistent with the way we commonly use functional notation. But $S(0.9) = \text{FALSE}$ or $S(0.9) = 0$ is not a correct statement even though "$0.9^2 > 1$" is false. This is because the codomain of S is a set of statements, not the set $\{0, 1\}$. Instead of "$S(0.9) = 0$" we should say "$S(0.9)$ is false." Likewise, we say "$S(1.1)$ is true." These are sometimes shortened to "$\sim S(0.9)$" and "$S(1.1)$."

The expression $\{x \mid S(x)\}$ may look strange, but it is consistent with the usual use of the notation. If the domain is known, there is no need to mention it and $\{x \mid \ldots\}$ means the set of those x for which $\ldots$ is true. The truth set of the predicate $S(x) =$ "$x^2 > 1$" with domain $\mathbb{R}$ is the set $\{x \mid x > 1\} \cup \{x \mid x < -1\}$.

With some domains, it is more natural to think of a predicate as a function of more than one variable. For example, the domain may be $\mathbb{R} \times \mathbb{R}$ and the predicate may be "$P(x, y) = \Big((x > y > 0) \Rightarrow (x^2 > y^2)\Big)$." Notice that $P(x, y)$ is true for all $x, y \in \mathbb{R}$. In other words "For all $x, y \in \mathbb{R}, S(x, y)$" is true. This sort of statement is the essence of predicate logic, so we introduce some terminology.

Definition 4 (Quantifiers) *The phrase "for all" is called a universal quantifier and is written $\forall$ ("A" rotated 180°). If $S(x)$ is a predicate and the set D is contained in the domain of x, the statement "$\forall x \in D,\ S(x)$" is read "for all $x \in D$, $S(x)$ is true," or just "for all $x \in D$, $S(x)$." The statement "$\forall x \in D,\ S(x)$" is true if and only if $S(x)$ is true for every $x \in D$; otherwise the statement "$\forall x \in D,\ S(x)$" is false. If the value of D is clear, we may write simply $\forall x\ S(x)$.*

The phrase "for some" is called an existential quantifier and is written $\exists$ ("E" rotated

180°). If $S(x)$ is a predicate and the set D is contained in the domain of x, the statement "$\exists x \in D,\ S(x)$" is read "for some $x \in D$, $S(x)$ is true," or just "for some $x \in D$, $S(x)$." It is also read "there exists $x \in D$ such that $S(x)$." The statement "$\exists x \in D,\ S(x)$" is true if and only if $S(x)$ is true for at least one $x \in D$; otherwise the statement "$\exists x \in D,\ S(x)$" is false. If the value of D is clear, we may write simply $\exists x\ S(x)$.

In terms of truth sets:

- "$\forall x \in D,\ S(x)$" is equivalent to saying that the truth set of $S(x)$ contains the set D.
- "$\exists x \in D,\ S(x)$" is equivalent to saying that the truth set of $S(x)$ contains at least one element of the set D

One can view much of mathematics as an attempt to understand the truth sets of certain predicates. For example, can you describe the truth set of the predicate $S(b,c) =$ "x^2+bx+c has no real roots"? You can answer this if you know that "the roots of x^2+bx+c are $(-b \pm \sqrt{b^2-4c})/2$" is true for all $(b,c) \in \mathbb{R} \times \mathbb{R}$ and that "$(\sqrt{d} \in \mathbb{R}) \Leftrightarrow (d \geq 0)$" is true for all $d \in \mathbb{R}$. The answer is $\{(b,c) \mid b^2 < 4c\}$.

To work with the notation and also introduce ideas we will need later, we'll look at some examples from elementary number theory. The word "elementary" here means easy to state, not, necessarily, easy to solve. To make it easier to specify domains, we need some notation.

Definition 5 (Notation for sets of numbers) *Recall that $\mathbb{R}$ denotes the real numbers, $\mathbb{Z}$ denotes the integers, and $\mathbb{Q}$ denotes the rational numbers (ratios of integers). In addition, $\mathbb{N}$ denotes the nonnegative integers (the "natural numbers"), $\mathbb{N}^+$ denotes the nonzero natural numbers (positive integers), and $\mathbb{P}$ denotes the primes. A natural number n is prime if $n \geq 2$ and the only divisors of n are n and 1. An integer $n \geq 2$ that is not prime is composite.*

The number 2 is the smallest prime and the only even prime. The other primes less than 20 are $3, 5, 7, 11, 13, 17, 19$.

Example 7 (Goldbach's conjecture) A mathematician named Christian Goldbach (1690–1764), noticed that $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 5+5$, $12 = 5+7$, $14 = 7+7$, $16 = 5+11$, etc., making him think that every even number greater than or equal to 4 can be written as the sum of two primes. We can state this in our notation:

$$\forall\, n \in \mathbb{N},\ \Big((n \geq 4) \wedge (n \text{ even})\Big) \Rightarrow \Big(\exists\, p, q \in \mathbb{P},\ n = p+q\Big).$$

Goldbach made this conjecture in 1742 in a letter to Euler (1701-1783). Of course, it can be written in various other ways; for example,

$$\forall\, n \geq 2,\ \exists\, p, q \in \mathbb{P},\ 2n = p+q,$$

where it is understood from the context that n must be an integer and not something like $\sqrt{5}$ or π.

Sadly (for mathematicians, since few others are interested) it is unknown whether or not Goldbach's conjecture is true. At least we have learned how to make the assertion, if not how to prove or disprove it. However, something is known for odd numbers: It is known that

$$\exists\, K \in \mathbb{N},\ \forall\, n \geq K,\ \Big((n \text{ odd}) \Rightarrow \exists\, p, q, r \in \mathbb{P},\ n = p + q + r\Big)$$

is true. This can be stated as "every sufficiently large odd number is the sum of three primes." (The "sufficiently large" is due to "$n \geq K$.") This was proved by Ivan Vinogradov (1891–1983) in 1937. $\square$

Example 8 (Sets and logic again) In Example 1 we saw how set identities could be thought of in terms of propositional logic. We can also phrase this in predicate logic terms.

Let U be the universal set. For every set A, B, C and so on that is being considered, introduce the predicates $A(x), B(x), C(x)$ and so on. Define $A(x)$ to be true if and only if $x \in A$ and do likewise for the other predicates.[1] A statement about sets is now equivalent to the corresponding statement about predicates with a universal quantifier. For example, $\sim\!(A \cup B) = (\sim\! A \cap \sim\! B)$ is true if and only if

$$\forall\, x \in U,\ \Big(\sim\!(A(x) \vee B(x)) \Leftrightarrow (\sim\! A(x) \wedge \sim\! B(x))\Big).$$

Why is that? The logic statement asserts that $x \in \sim\!(A \cup B)$ if and only if $x \in (\sim\! A \cap \sim\! B)$. This is essentially the element method of proof. $\square$

Example 9 (Quantifiers and negation) Let $R(x) =$ "$x + 2$ is prime" be a predicate. The statement "$\forall\, n \in \mathbb{P},\ R(n)$" is an example of the universal quantifier "for all" applied to this predicate. Another way to say the same thing is "$\forall (n \in \mathbb{P}),\ (n + 2 \in \mathbb{P})$." We have used parentheses to make it easier to see that the predicate is $n + 2 \in \mathbb{P}$ and that $n \in \mathbb{P}$ belongs with the quantifier. You should practice inserting parentheses in what follows to make it easier to read.

Using the normal English meanings of the statements, you should be able to see that the negation of these statements is "$\exists\, n \in \mathbb{P}, \sim\! R(n)$," which can be written "$\exists\, n \in \mathbb{P},\ n + 2 \notin \mathbb{P}$." Both negation statement forms mean the same thing. The symbol "$\notin$" is the negation of $\in$. Since $\in$ stands for "is in" or "is an element of," $\notin$ stands for "is not in" or "is not an element of."

In this case, "$\forall\, n \in \mathbb{P},\ R(n)$" is false and "$\exists\, n \in \mathbb{P},\ \sim\! R(n)$" is true since $7 \in \mathbb{P}$ and $9 \notin \mathbb{P}$. When $\exists$ is read "there exists," the symbol $\ni$ is sometimes used for "such that." Thus we can write either "$\exists\, n \in \mathbb{P},\ n + 2 \notin \mathbb{P}$" or "$\exists\, n \in \mathbb{P} \ni n + 2 \notin \mathbb{P}$." $\square$

The negation of a "for all" to get a "for some" in the previous example is an application of the following theorem for moving negation through quantifiers. You should be able to

[1] If you remember the definition of "characteristic function," you should be able to see that $A(x)$ is simply the characteristic function for the set A.

see that the theorem is true by translating the notation into ordinary English. We omit the formal proof

Theorem 2 (Negating quantifiers) *Let D be a set and let $P(x)$ be a predicate that is defined for $x \in D$. Then*

$$\sim\Big(\forall(x \in D),\ P(x)\Big) \ \Leftrightarrow\ \Big(\exists(x \in D),\ \sim P(x)\Big)$$

and

$$\sim\Big(\exists(x \in D),\ P(x)\Big) \ \Leftrightarrow\ \Big(\forall(x \in D),\ \sim P(x)\Big)$$

Example 10 (You can't buy it here) A grocery store chain has the disclaimer

ALL ITEMS NOT AVAILABLE AT ALL STORES.

in its weekly flyer of specials. What did they say and how could they have said what they meant?

Let I be the set of items referred to and S the set of stores. Let $A(i, s)$ be the predicate indicating that item i is available at store s. To translate the statement, we need to know how NOT should be applied. If the interpretation is

ALL ITEMS NOT (AVAILABLE AT ALL STORES),

then we can rewrite the statement as $\forall\, i \in I,\ \sim\Big(\forall\, s \in S,\ A(i, s)\Big)$, which our theorem tells us is equivalent to $\forall\, i \in I,\ \exists\, s \in S,\ \sim A(i, s)$. In English this says that, for every item in the flyer, the company has at least one store where you won't be able to get it. That's not a good way to run a business, so our choice of parentheses must be wrong.

The other possibility is

ALL ITEMS (NOT AVAILABLE) AT ALL STORES,

which translates as $\forall\, i \in I, \forall\, s \in S,\ \sim A(i, s)$. This is even worse! In English it says no matter what item you look for and no matter what store you look in, the item won't be available.

It seems fairly obvious that what they want to say is $\sim\forall\, i \in I,\ \forall\, s \in S,\ A(i, s)$. In other words, it is not the case that all items are available at all stores. This is rather awkward. Moving the negation through the quantifiers, we obtain $\exists\, i \in I,\ \exists\, s \in S,\ \sim A(i, s)$, which can be written as

SOME ITEMS ARE UNAVAILABLE AT SOME STORES.

Notice that we have written "UNAVAILABLE" instead of "NOT AVAILABLE" to avoid the problem of where to put parentheses that we considered in the two previous paragraphs. $\square$

Example 11 (Twin primes) Let $S(x) =$"x and $x+2$ are prime" be a predicate.[2] If $S(x)$ is true, we call x and $x+2$ twin primes. We could rewrite $S(x)$ as "$(x \in \mathbb{P}) \wedge (x+2 \in \mathbb{P})$."

The Twin Prime conjecture asserts that there are infinitely many twin primes. How can we express this in our notation since we do not have the phrase "infinitely many?" Here is a precise way of stating the Twin Prime conjecture:

"For all $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that $n \geq m$ and $S(n)$."

Using the symbols we've just learned, we can rewrite it as

$$\text{“}\forall\, m \in \mathbb{N} \Big(\exists\, n \in \mathbb{N} \ni \big((n \geq m) \wedge S(n)\big)\Big)\text{.”}$$

We often combine $\exists\, n \in \mathbb{N}$ and $n \geq m$ and often omit the $\ni$:

$$\text{“}\forall\, m \in \mathbb{N},\ \exists\, n \geq m,\ S(n)\text{.”}$$

If you are puzzled why this states that there are infinitely many primes n such that $n+2$ is also a prime, it helps to look at the negation. The negation of the statement is

$$\begin{aligned} \sim\Big(\forall\, m \in \mathbb{N},\ \exists\, n \geq m,\ S(n)\Big) \quad &\Leftrightarrow \quad \exists\, m \in \mathbb{N},\ \sim\Big(\exists\, n \geq m,\ S(n)\Big) \\ &\Leftrightarrow \quad \exists\, m \in \mathbb{N},\ \forall\, n \geq m,\ \sim S(n). \end{aligned}$$

Note that we applied Theorem 2 twice: the first time to move $\sim$ inside "$\forall\, m \in \mathbb{N}$" and the second time to move $\sim$ inside "$\exists\, n \geq m$."

Let's look at our negative statement $\exists\, m \in \mathbb{N},\ \forall\, n \geq m,\ \sim S(n)$. If there were only finitely many primes p such that $p+2$ is also prime, we could take m to be bigger than the largest such p, and the negative would be proved. On the other hand, if there were infinitely many twin primes, no matter how we chose m, there would be larger twin primes (i.e., larger n so that $S(n)$ is true) and so the negative would not be true. $\square$

Example 12 (Fermat numbers) A Fermat number (Pierre de Fermat, 1601–1665) is an integer of the form $F_n = 2^{2^n} + 1$ for $n \in \mathbb{N}$. The first five Fermat numbers are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, and $F_5 = 4294967297$. In 1640 Fermat conjectured that F_n is a prime for every n. Let $S(n) =$ "$F_n \in \mathbb{P}$." If we want to assert that all F_n are primes, we would say, "$\forall\, n \in \mathbb{N},\ S(n)$," or "$\forall\, n \in \mathbb{N},\ F_n \in \mathbb{P}$." The negation of this statement is, "$\exists\, n \in \mathbb{N},\ F_n \notin \mathbb{P}$." The negation is true, since $F_5 = 4294967297 = 641 \times 6700417$. F_5 is the first composite (i.e. non-prime) Fermat number. It is easy to factor F_5 with modern computers, but it was hard when people computed by hand. Thus Fermat was led to the false conjecture "$\forall n \in \mathbb{N}, S(n)$." Are there infinitely many Fermat primes (i.e., Fermat numbers that are prime)? If we thought so, we would conjecture "$\forall\, m \in \mathbb{N},\ \exists\, n \geq m,\ S(n)$." If we thought not, we would conjecture "$\exists\, m \in \mathbb{N},\ \forall\, n \geq m,\ \sim S(n)$." No one knows which assertion is correct. It is known that F_6 through F_{20} are, like F_5, composite.

[2] This is not the same as the predicate R in Example 9. Explain why. Express $S(x)$ in terms of R.

High school math students who take geometry often suffer through "straight edge and compass" constructions of various geometric figures. The ancient Greeks figured out that any regular polygon with $3 \cdot 2^k$ sides, $k \in \mathbb{N}$, or with $5 \cdot 2^k$ sides, $k \in \mathbb{N}$ could be constructed with straight edge and compass. This led them to wonder (in Greek, of course) "For which n can a regular polygon with n sides be constructed with straight edge and compass?" Let $P(n)$ be the predicate "a regular n-sided polygon can be constructed with straight edge and compass." We have just said that the Greeks proved $\forall\, k \in \mathbb{N},\ \big(P(3\cdot 2^k) \wedge P(5\cdot 2^k)\big)$ and they wondered what the truth set of $P(n)$ is. In 1796, Karl Friedrich Gauss (1777–1855), then 18 years old, proved that it is possible to construct a polygon with $m \cdot 2^k$ sides ($k \in \mathbb{N}$ and m odd) using ruler and compass if and only if m is a product of distinct Fermat primes, including $m = 1$, the empty product. (In other words, he found the truth set for $P(n)$.) Thus, such constructions are known to be possible for $m = 1$, 3, 5, 17, 257, 65535, 3×5, 5×17, and so on up to $3 \times 5 \times 17 \times 257 \times 65535 = 4294967295$. If more Fermat primes are found, we can add to this list. It should be noted that, although only 18, Gauss worked very hard at math. $\square$

Example 13 (Mersenne primes and perfect numbers) A number of the form $M_p = 2^p - 1$, where $p \in \mathbb{P}$, is called a *Mersenne number* after Marin Marsenne (1588–1648). If M_p is prime, then it is called a *Mersenne prime.* $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ and $M_7 = 127$ are Mersenne primes. But, $M_{11} = 23 \times 89$ is not a prime. The first thirty-one values of p for which M_p is prime are 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091. (The 25^{th} and 26^{th} Mersenne primes, corresponding to $p = 21701$ and $p = 23209$, were discovered in 1978 by two high school students, Laura Nickel and Curt Noll.) It is not known whether or not the statement "$\forall\, k \in \mathbb{N},\ \exists\, p \in \mathbb{P},\ \Big((p \geq k) \wedge (M_p \in \mathbb{P})\Big)$" is true or false. (What does this statement assert about the number of Mersenne primes?)

A mathematician named Leonhard Euler (1701–1783) studied numbers called *perfect numbers* and found a remarkable connection between them and Mersenne primes in 1770. A perfect number $n \in \mathbb{N}^+$ is a number that is equal to the sum of all of its factors (other than itself). The smallest perfect number is $6 = 3 + 2 + 1$. The next smallest is $28 = 14 + 7 + 4 + 2 + 1$. It is known that

$$\forall\, n \in \mathbb{N}^+,\ \Big(\exists\, p \in \mathbb{P},\ \big((n = 2^{p-1}M_p) \wedge (M_p \in \mathbb{P})\big) \ \Leftrightarrow\ \big(n \text{ is even and perfect}\big)\Big).$$

Euclid knew the "if-then" part (the left side implies the right). Euler proved the reverse implication — a gap of about two millennia! Thus $2^{2-1}M_2 = 6$, $2^{3-1}M_3 = 28$, $2^{5-1}M_5 = 496$ and $2^{7-1}M_7 = 8128$ are the first four even perfect numbers.

One could make the statement, "$\forall\, k \in \mathbb{N},\ \exists\, n > k,\ (n$ is even and perfect)." Is that statement known to be true or false? What do you think and why?

One could also make the statement, "$\exists\, n \in \mathbb{N}^+,\ (n$ is odd and perfect)." No one knows whether this statement is true or false. It is known that there are no odd perfect numbers less than 10^{160}, in other words "$\sim\exists\, n < 10^{160},\ (n$ is odd and perfect)" is true. $\square$

Example 14 (Fermat's Last Theorem) In 1637, Pierre de Fermat wrote, in French, "I have discovered a truly remarkable proof which this margin is too small to contain." Proof of what? He wrote it in his private shorthand notation which we have learned to decode. In our notation his claim was

$$\forall\, n \in \mathbb{N}^+ \Big\{ \Big(\exists\,(x,y,z) \in \mathbb{N}^+ \times \mathbb{N}^+ \times \mathbb{N}^+,\ (x^n + y^n = z^n) \Big) \ \Leftrightarrow\ (n \le 2) \Big\}.$$

This is known as *Fermat's Last Theorem.* If you have been watching TV in the last few years you will know that this "marginal statement" has finally been proven true by Andrew Wiles, after more than 350 years of attempts by many mathematicians.

You may wonder why Fermat never wrote up his proof and why it took so long to rediscover his proof. Fermat claimed to have proved many things without writing down the proofs. (Don't try this on a test!) He also made many conjectures. All his claims, except the "last theorem" were proven some time ago. All his conjectures are false. What was Fermat's proof of his "last theorem?" Most mathematicians believe that his proof was incorrect. One of the techniques that Fermat used is known as "infinite descent." It can be used for the cases $n = 3$ and $n = 4$, but cannot be used in general. Some people believe Fermat assumed it would work in general because it worked in these two cases. $\square$

This concludes our "number theory" examples. They were chosen to show you how to work with the notation of predicate logic. They were also chosen to introduce you to some famous problems in number theory. There are important applications of number theory to computer science, but not, so far as we know, applications of these particular examples. They are just hard problems and, as such, intellectual challenges.

At this moment the two Voyager spacecraft (Voyager I and Voyager II) are speeding away from the solar system at the rate of a million miles per day. They were launched in 1977. About 2010 they will arrive at the heliopause and enter interstellar space. Aboard each is a recording containing greetings in 59 languages, a whale noise, 12 minutes of sound — including the smack of a kiss, a baby's cry, an EEG of a young women in love, 116 pictures of this and that, 90 minutes of music including a Navajo chant, a Japanese *shakuhachi* piece, a Pygmy girl's initiation song, a Peruvian wedding song, Bach, Beethoven, Mozart, Stravinsky, Louis Armstrong, Blind Willie Johnson, and, last but not least, Chuck Berry singing "Johnny B. Goode." If any aliens find that stuff, they may think we are nuts sending such material and keep right on going. Much better would have been short crisp questions, easily translated,[3] asking questions such as, "Are there any odd perfect numbers?" "Is Goldbach's conjecture true?" The ability to answer such questions should be a matter of intellectual pride to any culture. At the time Voyager was launched, Fermat's Last Theorem was the "obvious" candidate question. Ironically, we now know the answer without any help from aliens.

[3] Questions in physics would also be of interest, but more background concepts may be needed than are needed for simple number theory problems.

Example 15 (Algebraic rules for predicate logic) In propositional logic we have Theorem 1 to help us manipulate statement forms. What about analogous rules for predicate logic?

As long as we are not trying to pull things through quantifiers, the same rules apply. For example

$$P(x) \vee (Q(y) \wedge R(x,y)) \quad \Leftrightarrow \quad (P(x) \vee Q(y)) \wedge (P(x) \vee R(x,y)).$$

Why is this? For each particular choice of x and y, the predicates become statement variables and so we are back in propositional logic.

What happens when quantifiers are involved? Theorem 2 tells us how to move $\sim$ through quantifiers. Sometimes we can move quantifiers through $\vee$ and $\wedge$, and sometimes not:

$$\begin{array}{lrcl}
\text{True:} & \forall\, x \in D,\ (P(x) \wedge Q(x)) & \Leftrightarrow & (\forall\, x \in D,\ P(x)) \wedge (\forall\, x \in D,\ Q(x)) \\
\text{False:} & \exists\, x \in D,\ (P(x) \wedge Q(x)) & \Leftrightarrow & (\exists\, x \in D,\ P(x)) \wedge (\exists\, x \in D,\ Q(x)) \\
\text{False:} & \forall\, x \in D,\ (P(x) \vee Q(x)) & \Leftrightarrow & (\forall\, x \in D,\ P(x)) \vee (\forall\, x \in D,\ Q(x)) \\
\text{True:} & \exists\, x \in D,\ (P(x) \vee Q(x)) & \Leftrightarrow & (\exists\, x \in D,\ P(x)) \vee (\exists\, x \in D,\ Q(x))
\end{array}$$

In the exercises, you will be asked to explain this.

It should be clear from this that manipulating quantifiers is trickier than the manipulations of propositional logic. Given the problems with algebraic manipulation, how does one go about proving statements in predicate logic? Since the variables often have infinite domains (as in our number theory examples), we can't construct truth tables because the would have to have an infinite number of rows. Proving things in predicate logic can be difficult.

Now you know why this section has less manipulation and proofs than the section on Boolean functions in Unit BF. $\square$

Exercises for Section 2

The following exercises will give you basic practice in predicate logic.

2.1. Each statement below should be rewritten in the form "$\forall \cdots x, \cdots .$"

(a) Every real number is negative, zero, or positive.

(b) No computer scientists are unemployed.

2.2. Start with the statement, "$\forall n \in \mathbb{N}$, if n^2 is even then n is even." Which of the following statements say the same thing? Which are true and which are false?

(a) Every integer has an even square and is even.

(b) If a given integer has an even square then that integer is even.

(c) For all integers, some will have an even square.

(d) Any integer that has an even square will be even.

(e) If the square of some integer is even then it is even.

(f) All integers that are even have an even square.

2.3. For each of the following statements, construct a statement of the form, "$\forall$ $\cdots$, if $\cdots$ then $\cdots$." that says the same thing.

(a) Any correct algorithm, correctly coded, runs correctly.

(b) Given any two odd integers, their product is odd.

(c) Given any two integers whose product is odd, the integers themselves are odd.

2.4. Consider the statement, "Every computer science student needs to take Java Programming." Rewrite this in two ways, corresponding to the statement forms

(a) "$\forall x$, if $\cdots$ then $\cdots$."

(b) "$\forall x$, $\cdots$."

2.5. Consider the statement, "Some questions are easy." Rewrite this statement in two ways, corresponding to the statement forms

(a) "$\exists \cdots x$ such that $\cdots$."

(b) "$\exists x$ such that $\cdots$ and $\cdots$."

2.6. An number in $\mathbb{R} - \mathbb{Q}$ is called *irrational*. Consider the statement, "The product of any irrational number and any rational number is irrational." Is the following proposed negation of this statement the correct negation? If not, what is the correct negation? "There exists an irrational number x and an irrational number y such that the product xy is rational." Which is true, the original statement or its negation?

2.7. Consider the statement, "For all computer programs P, if P is correctly programmed then P compiles without warning messages." What is the negation of this statement? Which is true, the original statement or its negation?

2.8. Consider the statement, "For all real numbers x and y, if $x^2 = y^2$ then $x = y$." Is the following proposed negation of this statement the correct negation? If not, what is the correct negation? "If $x \neq y$ then $x^2 \neq y^2$." Which is true, the original statement or its negation?

2.9. Consider the statement,"For all primes $p \in \mathbb{P}$, either p is odd or p is 2." What is the negation of this statement? Which is true, the original statement or its negation?

2.10. Consider the statement, "For all animals x, if x is a tiger then x has stripes and x has claws." What is the negation of this statement? Which is true, the original statement or its negation?

2.11. Start with the statement, "$\exists\, x \in \mathbb{R}$, $\forall$ negative $y \in \mathbb{R}$, $x > y$."

(a) Form a statement by reversing the existential and universal quantifiers. Which statement is true?

(b) Form the negation of the original statement. Is it true?

2.12. Start with the statement, "For all computer programs P, if P is correct then P compiles without error messages." Form the contrapositive, converse, and inverse of this statement.

2.13. Start with the statement, "$\forall\, n \in \mathbb{N}$, if n^2 is even then n is even." Form the contrapositive, converse, and inverse of this statement. Which statements are true?

2.14. Start with the statement, "$\forall\, n \in \mathbb{N}$, if n is prime then n is odd or $n = 2$." Form the contrapositive, converse, and inverse of this statement. Which statements are true?

2.15. Consider the statement "A large income is a necessary condition for happiness."

(a) Let P be the set of people. For $x \in P$, let $L(x)$ indicate that x has a large income and $H(x)$ that x is happy. Rewrite the given statement using the notation of logic rather than the English language.

(b) Write the statement in ordinary English, without using "necessary" or "sufficient."

(c) Write the negation of the statement in logic notation. Move the negation inside the statement as far as possible.

(d) Write this negation in ordinary English, without using "necessary" or "sufficient."

2.16. Which of the following statements are true, which are false ($\exists!$ means "there exists exactly one").

(a) $\exists!\, x \in \mathbb{Z} \ni 1/x \in \mathbb{Z}$.

(b) $\forall\, x \in \mathbb{R}\ \exists!\, y \in \mathbb{R} \ni x + y = 0$.

2.17. Let S be a predicate with domain D. Write the statement, "$\exists!\ x \in D \ni S(x)$" using $\forall$ and $\exists$ instead of $\exists!$.

2.18. In each case, is the given statement true or false? Explain.

(a) $\forall\, m \in \mathbb{N}$, $\exists\, n \geq m$, n even, $\exists\, p, q \in \mathbb{P}$, $n = p + q$.

(b) $\forall\, m \in \mathbb{N},\ \exists\, n \geq m$, n odd, $\exists\, p, q \in \mathbb{P},\ n = p + q$.

2.19. Let $P(x)$ and $Q(x)$ be predicates with domain D. For each pair of statement forms, state which are equivalent and explain your answer.

(a) $\forall\, x \in D,\ (P(x) \wedge Q(x))$ compared with $(\forall\, x \in D, P(x)) \wedge (\forall\, x \in D, Q(x))$

(b) $\exists\, x \in D,\ (P(x) \wedge Q(x))$ compared with $(\exists\, x \in D, P(x)) \wedge (\exists\, x \in D, Q(x))$

(c) $\forall\, x \in D,\ (P(x) \vee Q(x))$ compared with $(\forall\, x \in D, P(x)) \vee (\forall\, x \in D, Q(x))$

(d) $\exists\, x \in D,\ (P(x) \vee Q(x))$ compared with $(\exists\, x \in D, P(x)) \vee (\exists\, x \in D, Q(x))$

2.20. Suppose $n > 1$ is an integer. Prove:

If n is composite then $2^n - 1$ is composite.

Thus, if you are going to search for primes of the form $2^n - 1$, you can limit your search to n a prime.

2.21. Suppose $2^n - 1$ is a prime number (that is, a Mersenne prime). Prove that $N = 2^{n-1}(2^n - 1)$ is an even perfect number. (The converse is true but harder to prove.)

Multiple Choice Questions for Review

In each case there is one correct answer (given at the end of the problem set). Try to work the problem first without looking at the answer. Understand both why the correct answer is correct and why the other answers are wrong.

1. Consider the statement form $p \Rightarrow q$ where $p =$"If Tom is Jane's father then Jane is Bill's niece" and $q =$"Bill is Tom's brother." Which of the following statements is equivalent to this statement?

(a) If Bill is Tom's Brother, then Tom is Jane's father and Jane is not Bill's niece.

(b) If Bill is not Tom's Brother, then Tom is Jane's father and Jane is not Bill's niece.

(c) If Bill is not Tom's Brother, then Tom is Jane's father or Jane is Bill's niece.

(d) If Bill is Tom's Brother, then Tom is Jane's father and Jane is Bill's niece.

(e) If Bill is not Tom's Brother, then Tom is not Jane's father and Jane is Bill's niece.

2. Consider the statement, "If n is divisible by 30 then n is divisible by 2 and by 3 and by 5." Which of the following statements is equivalent to this statement?

(a) If n is not divisible by 30 then n is divisible by 2 or divisible by 3 or divisible by 5.

(b) If n is not divisible by 30 then n is not divisible by 2 or not divisible by 3 or not divisible by 5.

(c) If n is divisible by 2 and divisible by 3 and divisible by 5 then n is divisible by 30.

(d) If n is not divisible by 2 or not divisible by 3 or not divisible by 5 then n is not divisible by 30.

(e) If n is divisible by 2 or divisible by 3 or divisible by 5 then n is divisible by 30.

3. Which of the following statements is the contrapositive of the statement, "You win the game if you know the rules but are not overconfident."

(a) If you lose the game then you don't know the rules or you are overconfident.

(b) A sufficient condition that you win the game is that you know the rules or you are not overconfident.

(c) If you don't know the rules or are overconfident you lose the game.

(d) If you know the rules and are overconfident then you win the game.

(e) A necessary condition that you know the rules or you are not overconfident is that you win the game.

4. The statement form $(p \Leftrightarrow r) \Rightarrow (q \Leftrightarrow r)$ is equivalent to

(a) $[(\sim p \vee r) \wedge (p \vee \sim r)] \vee \sim[(\sim q \vee r) \wedge (q \vee \sim r)]$

(b) $\sim[(\sim p \vee r) \wedge (p \vee \sim r)] \wedge [(\sim q \vee r) \wedge (q \vee \sim r)]$

(c) $[(\sim p \vee r) \wedge (p \vee \sim r)] \wedge [(\sim q \vee r) \wedge (q \vee \sim r)]$

(d) $[(\sim p \vee r) \wedge (p \vee \sim r)] \vee [(\sim q \vee r) \wedge (q \vee \sim r)]$

(e) $\sim[(\sim p \vee r) \wedge (p \vee \sim r)] \vee [(\sim q \vee r) \wedge (q \vee \sim r)]$

5. Consider the statement, "Given that people who are in need of refuge and consolation are apt to do odd things, it is clear that people who are apt to do odd things are in need of refuge and consolation." This statement, of the form $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$, is logically equivalent to

(a) People who are in need of refuge and consolation are not apt to do odd things.

(b) People are apt to do odd things if and only if they are in need of refuge and consolation.

(c) People who are apt to do odd things are in need of refuge and consolation.

(d) People who are in need of refuge and consolation are apt to do odd things.

(e) People who aren't apt to do odd things are not in need of refuge and consolation.

6. A sufficient condition that a triangle T be a right triangle is that $a^2 + b^2 = c^2$. An equivalent statement is

(a) If T is a right triangle then $a^2 + b^2 = c^2$.

(b) If $a^2 + b^2 = c^2$ then T is a right triangle.

(c) If $a^2 + b^2 \neq c^2$ then T is not a right triangle.

(d) T is a right triangle only if $a^2 + b^2 = c^2$.

(e) T is a right triangle unless $a^2 + b^2 = c^2$.

7. Which of the following statements is **NOT** equivalent to the statement, "There exists either a computer scientist or a mathematician who knows both discrete math and Java."

(a) There exists a person who is a computer scientist and who knows both discrete math and Java or there exists a person who is a mathematician and who knows both discrete math and Java.

(b) There exists a person who is a computer scientist or there exists a person who is a mathematician who knows discrete math or who knows Java.

(c) There exists a person who is a computer scientist and who knows both discrete math and Java or there exists a mathematician who knows both discrete math and Java.

(d) There exists a computer scientist who knows both discrete math and Java or there exists a person who is a mathematician who knows both discrete math and Java.

(e) There exists a person who is a computer scientist or a mathematician who knows both discrete math and Java.

8. Which of the following is the negation of the statement, "For all odd primes $p < q$ there exists positive non-primes $r < s$ such that $p^2 + q^2 = r^2 + s^2$."

(a) For all odd primes $p < q$ there exists positive non-primes $r < s$ such that $p^2 + q^2 \neq r^2 + s^2$.

(b) There exists odd primes $p < q$ such that for all positive non-primes $r < s$, $p^2 + q^2 = r^2 + s^2$.

(c) There exists odd primes $p < q$ such that for all positive non-primes $r < s$, $p^2+q^2 \neq r^2 + s^2$.

(d) For all odd primes $p < q$ and for all positive non-primes $r < s$, $p^2 + q^2 \neq r^2 + s^2$.

(e) There exists odd primes $p < q$ and there exists positive non-primes $r < s$ such that $p^2 + q^2 \neq r^2 + s^2$

9. Consider the following assertion: "The two statements
(1) $\exists x \in D, (P(x) \wedge Q(x))$ and
(2) $(\exists x \in D, P(x)) \wedge (\exists x \in D, Q(x))$ have the same
truth value." Which of the following is correct?

(a) This assertion is false. A counterexample is $D = \mathbb{N}$, $P(x) =$ "x is divisible by 6," $Q(x) =$ "x is divisible by 3."

(b) This assertion is true. The proof follows from the distributive law for $\wedge$.

(c) This assertion is false. A counterexample is $D = \mathbb{Z}$, $P(x) =$ "$x < 0$," $Q(x) =$ "$x \geq 0$."

(d) This assertion is true. To see why, let $D = \mathbb{N}$, $P(x) =$ "x is divisible by 6," $Q(x) =$ "x is divisible by 3." If $x = 6$, then x is divisible by both 3 and 6 so both statements in the assertion have the same truth value for this x.

(e) This assertion is false. A counterexample is $D = \mathbb{N}$, $P(x) =$ "x is a square," $Q(x) =$ "x is odd."

10. Which of the following is an unsolved conjecture?

(a) $\exists n \in \mathbb{N},\ 2^{2^n} + 1 \notin \mathbb{P}$

(b) $\exists\, K \in \mathbb{N},\ \forall n \geq K$, n odd, $\exists\, p, q, r \in \mathbb{P},\ \ n = p + q + r$

(c) $(\exists\, x, y, z, n \in \mathbb{N}^+,\ x^n + y^n = z^n) \;\Leftrightarrow\; (n = 1, 2)$

(d) $\forall\, m \in \mathbb{N}\,,\ \exists\, n \geq m$, n even, $\exists\, p, q \in \mathbb{P},\ n = p + q$

(e) $\forall\, m \in \mathbb{N}\,,\ \exists\, n \geq m,\ n \in \mathbb{P}$ and $n + 2 \in \mathbb{P}$

11. Which of the following is a solved conjecture?

(a) $\forall\, m \in \mathbb{N}\,,\ \exists\, n \geq m$, n odd, $\exists\, p, q \in \mathbb{P},\ n = p + q$

(b) $\forall\, m \in \mathbb{N}\,,\ \exists\, n \geq m,\ n \in \mathbb{P}$ and $n + 2 \in \mathbb{P}$

(c) $\forall\, m \in \mathbb{N}\,,\ \exists\, n \geq m,\ 2^{2^n} + 1 \in \mathbb{P}$

(d) $\forall k \in \mathbb{N}\,, \exists p \in P,\ p \geq k\,, 2^p - 1 \in \mathbb{P}$

(e) $\forall\, n \geq 4,\ n$ even$\,, \exists\, p, q \in \mathbb{P},\ n = p + q$

Answers: **1** (b), **2** (d), **3** (a), **4** (e), **5** (c), **6** (b), **7** (b), **8** (c), **9** (c), **10** (e), **11** (a).