Chapter 3

Reflections on Logic and Proof

In this chapter, we cover some basic principles of logic and describe some methods for constructing proofs. This chapter is not meant to be a complete enumeration of all possible proof techniques. The philosophy of this book is that most people learn more about proofs by reading, watching, and attempting proofs than by an extended study of the logical rules behind proofs. On the other hand, now that we have some examples of proofs, it will help you read and do proofs if we reflect on their structure and to discuss what constitutes a proof. To do so so we first develop a language that will allow us to talk about proofs, and then we use this language to describe the logical structure of a proof.

3.1 Equivalence and Implication

Equivalence of statements

Exercise 3.1-1 A group of students are working on a project that involves writing a merge sort program. Joe and Mary have each written an algorithm for a function that takes two lists, `List1` and `List2`, of lengths p and q and merges them into a third list, `List3`. Part of Joe's algorithm is the following:

```
(1)   if ((i + j ≤ p + q) && (i ≤ p) && ((j ≥ q)||(List1[i] ≤ List2[j])))
(2)            List3[k] = List1[i]
(3)            i = i + 1
(4)   else
(5)            List3[k] = List2[j]
(6)            j = j + 1

(7)   k = k + 1
(8)   Return List3
```

The corresponding part of Mary's algorithm is

```
(1)   if (((i + j ≤ p + q) && (i ≤ p) && (j ≥ q))
          || ((i + j ≤ p + q) && (i ≤ p) && (List1[i] ≤ List2[j])))
```

```
(2)                 List3[k] = List1[i]
(3)                 i = i + 1
(4)   else
(5)                 List3[k] = List2[j]
(6)                 j = j + 1

(7)   k = k + 1
(8)   Return List3
```

Do Joe and Mary's algorithms do the same thing?

Notice that Joe and Mary's algorithms are exactly the same except for the if statement in line 1. (How convenient; they even used the same local variables!) In Joe's algorithm we put entry i of List1 into position k of List3 if

$$i + j \leq p + q \text{ and } i \leq p \text{ and } (j \geq q \text{ or } \texttt{List1}[i] \leq \texttt{List2}[j]),$$

while in Mary's algorithm we put entry i of List1 into position k of List3 if

$$(i + j \leq p + q \text{ and } i \leq p \text{ and } j \geq q) \text{ or } (i + j \leq p + q \text{ and } i \leq p \text{ and } \texttt{List1}[i] \leq \texttt{List2}[j]).$$

Joe and Mary's statements are both built up from the same constituent parts (namely comparison statements), so we can name these constituent parts and rewrite the statements. We use

- s to stand for $i + j \leq p + q$,

- t to stand for $i \leq p$,

- u to stand for $j \geq q$, and

- v to stand for $\texttt{List1}[i] \leq \texttt{List2}[j]$

The condition in Mary's if statement on Line 1 of her code becomes

s and t and (u or v)

while Joe's if statement on Line 1 of his code becomes

(s and t and u) or (s and t and v).

By recasting the statements in this symbolic form, we see that s and t always appear together as "s and t." We can thus simplify their expressions by substituting w for "s and t." Mary's condition how has the form

w and (u or v)

and Joe's has the form

(w and u) or (w and v).

Although we can argue, based on our knowledge of the structure of the English language, that Joe's statement and Mary's statement are saying the same thing, it will help us understand logic if we formalize the idea of "saying the same thing." If you look closely at Joe's and Mary's statements, you can see that we are saying that, the word "and" distributes over the word "or," just as set intersection distributes over set union, and multiplication distributes over addition. In order to analyze when statements mean the same thing, and explain more precisely what we mean when we say something like "and" distributes over "or," logicians have adopted a standard notation for writing symbolic versions of compound statements. We shall use the symbol $\wedge$ to stand for "and" and $\vee$ to stand for "or." In this notation, Mary's condition becomes

$$w \wedge (u \vee v)$$

and Joe's becomes

$$(w \wedge u) \vee (w \wedge v).$$

We now have a nice notation (which makes our compound statements look a lot like the two sides of the distributive law for intersection of sets over union), but we have not yet explained why two statements with this symbolic form mean the same thing. We must therefore give a precise definition of "meaning the same thing," and develop a tool for analyzing when two statements satisfy this definition. We are going to consider symbolic compound statements that may be built up from the following notation:

- symbols (s, t, etc.) standing for statements (these will be called *variables*),

- the symbol $\wedge$, standing for "and,"

- the symbol $\vee$, standing for "or,"

- the symbol $\oplus$ standing for "exclusive or," and

- the symbol $\neg$, standing for "not."

Truth tables

We will develop a theory for deciding when a compound statement is true based on the truth or falsity of its component statements. Using this theory, we will determine, for a particular setting of variables, say s, t and u, whether a particular compound statement, say $(s \oplus t) \wedge (\neg u \vee (s \wedge t)) \wedge \neg(s \oplus (t \vee u))$, is true or false. Our technique uses truth tables, which you have probably seen before. We will see how truth tables are the proper tool to determine whether two statements are equivalent.

As with arithmetic, the order of operations in a logical statement is important. In our sample compound statement $(s \oplus t) \wedge (\neg u \vee (s \wedge t)) \wedge \neg(s \oplus (t \vee u))$ we used parentheses to make it clear which operation to do first, with one exception, namely our use of the $\neg$ symbol. The symbol $\neg$ always has the highest priority, which means that when we wrote $\neg u \vee (s \wedge t)$, we meant $(\neg u) \vee (s \wedge t)$, rather than $\neg(u \vee (s \wedge t))$. The principle we use here is simple; the symbol $\neg$

applies to the smallest number of possible following symbols needed for it to make sense. This is the same principle we use with minus signs in algebraic expressions. With this one exception, we will always use parentheses to make the order in which we are to perform operations clear; you should do the same.

The operators $\wedge$, $\vee$, $\oplus$ and $\neg$ are called *logical connectives*. The truth table for a logical connective states, in terms of the possible truth or falsity of the component parts, when the compound statement made by connecting those parts is true and when it is false. The the truth tables for the connectives we have mentioned so far are in Figure 3.1

Figure 3.1: The truth tables for the basic logical connectives.

AND				OR				XOR				NOT	
s	t	$s \wedge t$		s	t	$s \vee t$		s	t	$s \oplus t$		s	$s \oplus t$
T	T	T		T	T	T		T	T	F		T	F
T	F	F		T	F	T		T	F	T		F	T
F	T	F		F	T	T		F	T	T			
F	F	F		F	F	F		F	F	F			

These truth tables define the words "and," "or," "exclusive or" ("xor" for short), and "not" in the context of symbolic compound statements. For example, the truth table for $\vee$—or—tells us that when s and t are both true, then so is "s or t." It tells us that when s is true and t is false, or s is false and t is true, then "s or t" is true. Finally it tells us that when s and t are both false, then so is "s or t." Is this how we use the word "or" in English? The answer is sometimes! The word "or" is used ambiguously in English. When a teacher says "Each question on the test will be short answer or multiple choice," the teacher is presumably not intending that a question could be both. Thus the word "or" is being used here in the sense of "exclusive or"—the "$\oplus$" in the truth tables above. When someone says "Let's see, this afternoon I could take a walk or I could shop for some new gloves," she probably does not mean to preclude the possibility of doing both—perhaps even taking a walk downtown and then shopping for new gloves before walking back. Thus in English, we determine the way in which someone uses the word "or" from context. In mathematics and computer science we don't always have context and so we agree that we will say "exclusive or" or "xor" for short when that is what we mean, and otherwise we will mean the "or" whose truth table is given by $\vee$. In the case of "and" and "not" the truth tables are exactly what we would expect.

We have been thinking of s and t as variables that stand for statements. The purpose of a truth table is to define when a compound statement is true or false in terms of when its component statements are true and false. Since we focus on just the truth and falsity of our statements when we are giving truth tables, we can also think of s and t as variables that can take on the values "true" (T) and "false" (F). We refer to these values as the *truth values* of s and t. Then a truth table gives us the truth values of a compound statement in terms of the truth values of the component parts of the compound statement. The statements $s \wedge t$, $s \vee t$ and $s \oplus t$ each have two component parts, s and t. Because there are two values we can assign to s, and for each value we assign to s there are two values we can assign to t, by the product principle, there are $2 \cdot 2 = 4$ ways to assign truth values to s and t. Thus we have four rows in our truth table, one for each way of assigning truth values to s and t.

For a more complex compound statement, such as the one in Line 1 in Joe and Mary's programs, we still want to describe situations in which the statement is true and situations in

Table 3.1: The truth table for Joe's statement

w	u	v	$u \vee v$	$w \wedge (u \vee v)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

which the statement is false. We will do this by working out a truth table for the compound statement from the truth tables of its symbolic statements and its connectives. We use a variable to represent the truth value each symbolic statement. The truth table has one column for each of the original variables, and for each of the pieces we use to build up the compound statement. The truth table has one row for each possible way of assigning truth values to the original variables. Thus if we have two variables, we have, as above, four rows. If we have just one variable, then we have, as above, just two rows. If we have three variables then we will have $2^3 = 8$ rows, and so on.

In Table 3.1 we give the truth table for the symbolic statement that we derived from Line 1 of Joe's algorithm. The columns to the left of the double line contain the possible truth values of the variables; the columns to the right correspond to various sub-expressions whose truth values we need to compute. We give the truth table as many columns as we need in order to correctly compute the final result; as a general rule, each column should be easily computed from one or two previous columns.

In Table 3.2 we give the truth table for the statement that we derived from Line 1 of Mary's algorithm.

Table 3.2: The truth table for Mary's statement

w	u	v	$w \wedge u$	$w \wedge v$	$(w \wedge u) \vee (w \wedge v)$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	F	F	F
F	F	F	F	F	F

You will notice that the pattern of T's and F's that we used to the left of the double line in both Joe's and Mary's truth tables are the same—namely, reverse alphabetical order.[1] Thus

---

[1]Alphabetical order is sometimes called *lexicographic order*. Lexicography is the study of the principles and

row i of Table 3.1 represents exactly the same assignment of truth values to u , v, and w as row i of Table 3.2. The final columns of the two truth tables are identical, which means that Joe's symbolic statement and Mary's symbolic statement are true in exactly the same cases. Therefore, the two statements must say the same thing, and Mary and Joe's program segments return exactly the same values. We say that two symbolic compound statements are *equivalent* if they are true in exactly the same cases. Alternatively, two statements are equivalent if their truth tables have the same final column (assuming both tables assign truth values to the original symbolic statements in the same pattern).

Tables 3.1 and 3.2 actually prove a *distributive law*:

Lemma 3.1 *The statements*

$$w \wedge (u \vee v)$$

and

$$(w \wedge u) \vee (w \wedge v)$$

are equivalent.

DeMorgan's Laws

Exercise 3.1-2 *DeMorgan's Laws* say that $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$, and that $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$,. Use truth tables to demonstrate that DeMorgan's laws are correct.

Exercise 3.1-3 Show that $p \oplus q$, the exclusive or of p and q, is equivalent to $(p \vee q) \wedge \neg(p \wedge q)$. Apply one of DeMorgan's laws to $\neg(\neg(p \vee q)) \wedge \neg(p \wedge q)$ to find another symbolic statement equivalent to the exclusive or.

To verify the first DeMorgan's Law, we create a pair of truth tables that we have condensed into one "double truth table" in Table 3.3. The second double vertical line separates the computation of the truth values of $\neg(p \vee q)$ and $\neg p \wedge \neg q$ We see that the fourth and the last columns are identical,

Table 3.3: Proving the first DeMorgan Law.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

and therefore the first DeMorgan's Law is correct. We can verify the second of DeMorgan's Laws by a similar process.

To show that $p \oplus q$ is equivalent to $(p \vee q) \wedge \neg(p \wedge q)$, we use the "double truth table" in Table 3.4.

By applying DeMorgan's law to $\neg(\neg(p \vee q)) \wedge \neg(p \wedge q)$, we see that $p \oplus q$ is also equivalent to $\neg(\neg(p \vee q) \vee (p \wedge q))$. It was easier to use DeMorgan's law to show this equivalence than to use another double truth table.

practices used in making dictionaries. Thus you will also see the order we used for the T's and F's called reverse lexicographic order, or reverse lex order for short.

Table 3.4: An equivalent statement to $p \oplus q$.

p	q	$p \oplus q$	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
T	T	F	T	T	F	F
T	F	T	T	F	T	T
F	T	T	T	F	T	T
F	F	F	F	F	T	F

Implication

Another kind of compound statement occurs frequently in mathematics and computer science. Recall 2.21, Fermat's Little Theorem:

If p is a prime, then $a^{p-1} \bmod p = 1$ for each non-zero $a \in Z_p$.

Fermat's Little Theorem combines two constituent statements,

p is a prime

and

$a^{p-1} \bmod p = 1$ for each non-zero $a \in Z_p$.

We can also restate Fermat's Little Theorem (a bit clumsily) as

p is a prime only if $a^{p-1} \bmod p = 1$ for each non-zero $a \in Z_p$,

or

p is a prime implies $a^{p-1} \bmod p = 1$ for each non-zero $a \in Z_p$,

or

$a^{p-1} \bmod p = 1$ for each non-zero $a \in Z_p$ if p is prime.

Using s to stand for "p is a prime" and t to stand for "$a^{p-1} \bmod p = 1$ for every non-zero $a \in Z_p$," we symbolize any of the four statements of Fermat's Little Theorem as

$$s \Rightarrow t,$$

which most people read as "s implies t." When we translate from symbolic language to English, it is often clearer to say "If s then t."

We summarize this discussion in the following definition:

Definition 3.1 *The following four English phrases are intended to mean the same thing. In other words, they are defined by the same truth table:*

- *s implies t,*

- *if s then t,*

- *t if s, and*

- *s only if t.*

Observe that the use of "only if" may seem a little different than the normal usage in English. Also observe that there are still other ways of making an "if ... then" statement in English. In a number of our lemmas, theorems, and corollaries (for example, Corollary 2.6 and Lemma 2.5) we have had two sentences. In the first we say "Suppose ...." In the second we say "Then ...." The two sentences "Suppose s." and "Then t." are equivalent to the single sentence $s \Rightarrow t$. When we have a statement equivalent to $s \Rightarrow t$, we call the statement s the *hypothesis* of the implication and we call the statement t the *conclusion* of the implication.

If and only if

The word "if" and the phrase "only if" frequently appear together in mathematical statements. For example, in Theorem 2.9 we proved

A number a has a multiplicative inverse in Z_n if and only if there are integers x and y such that $ax + ny = 1$.

Using s to stand for the statement "a number a has a multiplicative inverse in Z_n" ant t to stand for the statement "there are integers x and y such that $ax + ny = 1$," we can write this statement symbolically as

s if and only if t.

Referring to Definition 3.1, we parse this as

s if t, and s only if t,

which again by the definition above is the same as

$s \Rightarrow t$ and $t \Rightarrow s$.

We denote the statement "s if and only if t" by $s \Leftrightarrow t$. Statements of the form $s \Rightarrow t$ and $s \Leftrightarrow t$ are called *conditional statements*, and the connectives $\Rightarrow$ and $\Leftrightarrow$ are called *conditional connectives*.

Exercise 3.1-4 Use truth tables to explain the difference between $s \Rightarrow t$ and $s \Leftrightarrow t$.

In order to be able to analyze the truth and falsity of statements involving "implies" and "if and only if," we need to understand exactly how they are different. By constructing truth tables for these statements, we see that there is only one case in which they could have different truth values. In particular if s is true and t is true, then we would say that both $s \Rightarrow t$ and $s \Leftrightarrow t$ are true. If s is true and t is false, we would say that both $s \Rightarrow t$ and $s \Leftrightarrow t$ are false. In the case

that both s and t are false we would say that $s \Leftrightarrow$ is true. What about $s \Rightarrow t$? Let us try an example. Suppose that s is the statement "it is supposed to rain" and t is the statement "I carry an umbrella." Then if, on a given day, it is not supposed to rain and I do not carry an umbrella, we would say that the statement "if it is supposed to rain then I carry an umbrella" is true on that day. This suggests that we also want to say $s \Rightarrow t$ is true if s is false and t is false.[2] Thus the truth tables are identical in rows one, two, and four. For "implies" and "if and only if" to mean different things, the truth tables must therefore be different in row three. Row three is the case where s is false and t is true. Clearly in this case we would want s if and only if t to be false, so our only choice is to say that $s \Rightarrow t$ is true in this case. This gives us the truth tables in Figure 3.2.

Figure 3.2: The truth tables for "implies" and for "if and only if."

IMPLIES				IF AND ONLY IF		
s	t	$s \Rightarrow t$		s	t	$s \Leftrightarrow t$
T	T	T		T	T	T
T	F	F		T	F	F
F	T	T		F	T	F
F	F	T		F	F	T

Here is another place where (as with the usage for "or") English usage is sometimes inconsistent. Suppose a parent says "I will take the family to McDougalls for dinner if you get an A on this test," and even though the student gets a C, the parent still takes the family to McDougalls for dinner. While this is something we didn't expect, was the parent's statement still true? Some people would say "yes"; others would say "no". Those who would say "no" mean, in effect, that in this context the parent's statement meant the same as "I will take the family to dinner at McDougalls if and only if you get an A on this test." In other words, to some people, in certain contexts, "If" and "If and only if" mean the same thing! Fortunately questions of child rearing aren't part of mathematics or computer science (at least not this kind of question!). In mathematics and computer science, we adopt the two truth tables just given as the meaning of the compound statement $s \Rightarrow t$ (or "if s then t" or "t if s") and the compound statement $s \Leftrightarrow t$ (or "s if and only if t.") In particular, the truth table marked IMPLIES is the truth table referred to in Definition 3.1. This truth table thus defines the mathematical meaning of s implies t, or any of the other three statements referred to in that definition.

Some people have difficulty using the truth table for $s \Rightarrow t$ because of this ambiguity in English. The following example can be helpful in resolving this ambiguity. Suppose that I hold an ordinary playing card (with its back to you) and say "If this card is a heart, then it is a queen." In which of the following four circumstances would you say I lied:

1. the card is a heart and a queen

2. the card is a heart and a king

---

[2]Note that we are making this conclusion on the basis of one example. Why can we do so? We are not trying to prove something, but trying to figure out what the appropriate definition is for the $\Rightarrow$ connective. Since we have said that the truth or falsity of $s \Rightarrow t$ depends only on the truth or falsity of s and t, one example serves to lead us to an appropriate definition. If a different example led us to a different definition, then we would want to define two different kinds of implications, just as we have two different kinds of "ors," $\vee$ and $\oplus$. Fortunately, the only kinds of conditional statements we need for doing mathematics and computer science are "implies" and "if and only if."

3. the card is a diamond and a queen

4. the card is a diamond and a king?

You would certainly say I lied in the case the card is the king of hearts, and you would certainly say I didn't lie if the card is the queen of hearts. Hopefully in this example, the inconsistency of English language seems out of place to you and you would not say I am a liar in either of the other cases. Now we apply the principle called the *principle of the excluded middle*

Principle 3.1 *A statement is true exactly when it is not false.*

This principle tells us that that my statement is true in the three cases where you wouldn't say I lied. We used this principle implicitly before when we introduced the principle of proof by contradiction, Principle 2.1. We were explaining the proof of Corollary 2.6, which states

Suppose there is a b in Z_n such that the equation

$$a \cdot_n x = b$$

does not have a solution. Then a does not have a multiplicative inverse in Z_n.

We had assumed that the hypothesis of the corollary was true so that $a \cdot_n x = b$ does not have a solution. Then we assumed the conclusion that a does not have a multiplicative inverse was false. We saw that these two assumptions led to a contradiction, so that it was impossible for both of them to be true. Thus we concluded whenever the first assumption was true, the second had to be false. Why could we conclude this? Because the principle of the excluded middle says that the second assumption has to be either true or false. We didn't introduce the principle of the excluded middle at this point for two reasons. First, we expected that the reader would agree with our proof even if we didn't mention the principle, and second, we didn't want to confuse the reader's understanding of proof by contradiction by talking about two principles at once!

Important Concepts, Formulas, and Theorems

1. *Logical statements.* Logical statements may be built up from the following notation:

   - symbols (s, t, etc.) standing for statements (these will be called *variables*),
   - the symbol $\wedge$, standing for "and,"
   - the symbol $\vee$, standing for "or,"
   - the symbol $\oplus$ standing for "exclusive or,"
   - the symbol $\neg$, standing for "not,"
   - the symbol $\Rightarrow$, standing for "implies," and
   - the symbol $\Leftrightarrow$, standing for "if and only if."

   The operators $\wedge$, $\vee$, $\oplus$, $\Rightarrow$, $\Leftrightarrow$, and $\neg$ are called *logical connectives*. The operators $\Rightarrow$ and $\Leftrightarrow$ are called *conditional connectives*.

2. *Truth Tables.* The following are truth tables for the basic logical connectives:

AND				OR				XOR				NOT	
s	t	$s \wedge t$		s	t	$s \vee t$		s	t	$s \oplus t$		s	$s \oplus t$
T	T	T		T	T	T		T	T	F		T	F
T	F	F		T	F	T		T	F	T		F	T
F	T	F		F	T	T		F	T	T			
F	F	F		F	F	F		F	F	F			

3. *Equivalence of logical statements.* We say that two symbolic compound statements are *equivalent* if they are true in exactly the same cases.

4. *Distributive Law.* The statements

$$w \wedge (u \vee v)$$

and

$$(w \wedge u) \vee (w \wedge v)$$

are equivalent.

5. *DeMorgan's Laws.* DeMorgan's Laws say that $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$, and that $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$.

6. *Implication.* The following four English phrases are equivalent:

   - s implies t,
   - if s then t,
   - t if s, and
   - s only if t.

7. *Truth tables for implies and if and only if.*

IMPLIES				IF AND ONLY IF		
s	t	$s \Rightarrow t$		s	t	$s \Leftrightarrow t$
T	T	T		T	T	T
T	F	F		T	F	F
F	T	T		F	T	F
F	F	T		F	F	T

8. *Principle of the Excluded Middle.* A statement is true exactly when it is not false.

Problems

1. Give truth tables for the following expressions:

   a. $(s \vee t) \wedge (\neg s \vee t) \wedge (s \vee \neg t)$

   b. $(s \Rightarrow t) \wedge (t \Rightarrow u)$

   c. $(s \vee t \vee u) \wedge (s \vee \neg t \vee u)$

2. Find at least two more examples of the use of some word or phrase equivalent to "implies" in lemmas, theorems, or corollaries in Chapters One or Two.

3. Find at least two more examples of the use of the phrase "if and only if" in lemmas, theorems, and corollaries in Chapters One or Two.

4. Show that the statements $s \Rightarrow t$ and $\neg s \vee t$ are equivalent.

5. Prove the DeMorgan law which states $\neg(p \wedge q) = \neg p \vee \neg q$.

6. Show that $p \oplus q$ is equivalent to $(p \wedge \neg q) \vee (\neg p \wedge q)$.

7. Give a simplified form of each of the following expressions (using T to stand for a statement that is always true and F to stand for a statement that is always false)[3]:

   - $s \vee s$,
   - $s \wedge s$,
   - $s \vee \neg s$,
   - $s \wedge \neg s$.

8. Use a truth table to show that $(s \vee t) \wedge (u \vee v)$ is equivalent to $(s \wedge u) \vee (s \wedge v) \vee (t \wedge u) \vee (t \wedge v)$. What algebraic rule is this similar to?

9. Use DeMorgan's Law, the distributive law, and Problems 7 and 8 to show that $\neg((s \vee t) \wedge (s \vee \neg t))$ is equivalent to $\neg s$.

10. Give an example in English where "or" seems to you to mean exclusive or (or where you think it would for many people) and an example in English where "or" seems to you to mean inclusive or (or where you think it would for many people).

11. Give an example in English where "if ... then" seems to you to mean "if and only if" (or where you think it would to many people) and an example in English where it seems to you not to mean "if and only if" (or where you think it would not to many people).

12. Find a statement involving only $\wedge$, $\vee$ and $\neg$ (and s and t) equivalent to $s \Leftrightarrow t$. Does your statement have as few symbols as possible? If you think it doesn't, try to find one with fewer symbols.

13. Suppose that for each line of a 2-variable truth table, you are told whether the final column in that line should evaluate to true or to false. (For example, you might be told that the final column should contain T, F, T, and F in that order.) Explain how to create a logical statement using the symbols s, t, $\wedge$, $\vee$, and $\neg$ that has that pattern as its final column. Can you extend this procedure to an arbitrary number of variables?

14. In Problem 13, your solution may have used $\wedge$, $\vee$ and $\neg$. Is it possible to give a solution using only one of those symbols? Is it possible to give a solution using only two of these symbols?

15. We proved that $\wedge$ distributes over $\vee$ in the sense of giving two equivalent statements that represent the two "sides" of the distributive law. For each question below, explain why your answer is true.

   a. Does $\vee$ distribute over $\wedge$?
   b. Does $\vee$ distribute over $\oplus$?
   c. Does $\wedge$ distribute over $\oplus$?

---

[3]A statement that is always true is called a *tautology*; a statement that is always false is called a *contradiction*