MATH 22

Lecture E: 9/16/2003

LOGIC

Contrariwise, if it was so, it might be;
and if it were so, it would be; but as it
isn't, it ain't. That's logic.

—Lewis Carroll, *Alice's Adventures in Wonderland,* chapter 4

And faith unfaithful kept him falsely true.

—Tennyson, *Idylls of the King,* Lancelot and Elaine

Administrivia

- http://denenberg.com/LectureE.pdf
- Homeworks & projects due today
- You must *cite sources used in homeworks;* this includes any URLs
- Questions about homework, project?
- First exam: Monday 9/29 11:50–1:20, location TBA
- Preliminary course feedback
- Add/drop rules
- Office phone number is 617-995-1234 and *nothing else*
- When to find me in my office

Today: Introduction to propositional calculus: Propositions, connectives, expressions.

Logic: Background

The study of reasoning, the attempt to separate legitimate from bogus inference, goes back to the ancient Greeks. Our more modern formulation dates from the middle of the nineteenth century.

Many kinds of logic are studied by mathematicians today. The basis of all of them is the *propositional calculus*, which is where we start in this course. Learning propositional calculus is very much like learning the basics of arithmetic: addition and multiplication. The only way to do it is by working dozens of exercise—more than we provide in this course. It's a lot of fun. Try it out.

Suggested reading: If you like this stuff and want to see a more complete presentation of propositional and predicate logic, including lots of discussion of the connections between logic and English (and also many excellent exercises), you can't do better than *Methods of Logic* by W. V. O. Quine, one of the great philosophers of the twentieth century. Many examples in this lecture are drawn from this book.

Propositions

A *proposition*, or *statement,* is an utterance that is either true or false. (Book uses statement; I use proposition.)

Here are some propositions:

six times seven is thirty-five
the Red Sox won't win the 2003 World Series
Larry is an idiot
there exists some integer n such that $n^2 = 49$
there are an infinite number of twin primes
she is a happy person

Here are some utterances that are *not* propositions:

my hat	[not a sentence]
get stuffed, bozo	[not indicative mood]
x is greater than 1	[free variable]
$n^2 = 49$	[free variable]

We'll use variables p, q, r, etc., to stand for propositions, so we'll say things like "p is true" or "q is false". It's as though these were variables that can have one of two truth values, T or F. We'll say "p has value T" to mean "p stands for a true proposition". Remember: The only thing we care about is whether a proposition is T or F!

Combining Propositions

Just as we combine numbers into new numbers with the addition and multiplication operators, there are operators, called *connectives,* that we use to combine propositions. The most important are:

AND, which takes two propositions (say p and q) and makes a new proposition "p and q" written "$p \land q$" or "pq". Proposition pq is true when *both* p and q are true; otherwise it's false. (The book never uses pq but I'll do it all the time.) This connective is called *conjunction*. We also allow $p \land q \land r \land \ldots \land s$ or $pqr\ldots s$.

OR, which takes two propositions (say p and q) and makes the new proposition "p or q" written "$p \lor q$". Proposition $p \lor q$ is T when *either* of p and q is T; otherwise it's F. ($\lor$ is always the so-called "inclusive or": $p \lor q$ is T when both p and q are T.) This connective is called *disjunction*. We also permit $p \lor q \lor r \lor \ldots \lor s$ which means the obvious thing.

NOT, which takes a single proposition (say p) and makes the new proposition "not p", written "$\neg p$". Proposition $\neg p$ is true when p is false, and is false when p is true. This connective is called *negation*.

Some Examples

Suppose that

p is the proposition "He had a cold"

q is the proposition "She went to the bank"

r is the proposition "They left town"

Then

pq is the proposition "He had a cold, and she went to the bank" which is true if both things happened and false if either one didn't happen

$p \quad q$ is the proposition "He had a cold, or she went to the bank" which is true if either or both things happened, and is false only if neither happened

□p is the proposition "He didn't have a cold"

We can also build more complex propositions:

$pq \quad r$ is "Either he had a cold and she went to the bank, or else they left town (or both)"

p □ $\neg(q \quad r)$ is "He had a cold, and it is not true either that she went to the bank or that they left town"

Notice the importance of parentheses as we build up complex propositional expressions. p □ $(q \quad r)$ is very different from $(p$ □ $q) \quad r$!

More connectives

Here are other important propositional connectives. As usual, *p* and *q* are propositions.

p □ *q*, usually read "if *p* then *q*", is true when *p* is true and *q* is true, or if *p* is false (whether or not *q* is true!). (Pause for discussion of this last point.) *The only time proposition p* □ *q is false is when p is true and q is false*. This connective is called *implication* (but we must be careful about this). It can also be read "*p* implies *q*" and in many other ways. Proposition *p* is called the *antecedent* or *hypothesis* and *q* is called the *consequent* or *conclusion* of the implication.

p ≡ *q*, read "*p* if and only if *q*", is true when *p* and *q* are both true or both false. This operator is called the *biconditional* or *equivalence* (and we have to be even more careful about this!). It means that *p* and *q* have the same truth value. The text uses a two-way pointing arrow, which I can't find in my symbol font.

p ! *q*, read "*p* exclusive or *q*" or "*p* ex or *q*", is true when *p* is true or *q* is true *but not both*. (The text has a symbol for this operator that I've never seen anywhere.)

Evaluating expressions

To *evaluate* a propositional expression is to determine whether its value is T or F for a particular assignment of truth values to its propositional variables. (Such an assignment is called an *interpretation* of the variables.)

Example: What is the value of

$$(pq \vee (\neg p)(\neg r)) \rightarrow (q \equiv r)$$

when p and q are false and r is true?

Of course we evaluate propositional expressions just like we would arithmetic expressions, namely, from the inside out. In this case we note that pq is F and so is $(\neg p)(\neg r)$ since r is T, so the entire LHS is F. Hence we know that the entire expression is true without even evaluating the right-hand side (which, by the way, is F).

I hope it's clear that the value of an expression depends on the values of its propositional variables. In the above example, if all three variables are T then the value is T. In principle, you can evaluate any expression 2^n ways, where n is the number of propositional variables it contains. (There are 2^n possible ways to assign a value T or F to each of n variables.)

Truth Tables

A *truth table* is a compact way to show the possible values of a propositional formula. Make a row for each of the 2^n truth assignments of the propositional variables in the formula. Then, in each row, we compute the value of the formula for that assignment.

Truth table for *p* *q*

p	*q*	*p* *q*
F	F	F
F	T	T
T	F	T
T	T	T

Truth table for *p* □ *q*

p	*q*	*p* □ *q*
F	F	F
F	T	F
T	F	F
T	T	T

(You could think of these particular truth tables as the *definitions* of these two truth functions.)

Not a prayer of me making a complex truth table on these slides. We'll do it on the blackboard. We'll also do a Quine *truth-value analysis*, a better way to do it altogether.

[Other connectives]

He likes her, *but* she doesn't like him.

Smith will sell *unless* he hears from you.

An animal is a mammal *only if* it has a heart.

These may seem like new connectives, but they're not. Logically, *but* is the same as AND, *unless* is another way to say OR, and *only if* is a rephrasing of IMPLIES.

The bottom line is that there are a lot of ways of expressing connectives in English, and care is needed when translating words into symbols. (cf. Quine)

Arthur was president *before* Mark Twain died.

Jones died *because* he ate fish with ice cream.

The problem here is different. With other connectives we've seen the value of the expression depends *only* on the values of the components. But the truth values of *p* and *q* don't determine the truth value of "*p* before *q*" or "*p* because *q*"; you need extra outside information.

We say that *unless* and *before* are not *truth-functional*: they are not simply functions of the things they connect. In propositional calculus we study only truth-functional connectives like □, , □, □ , ≡, etc.

(*before* and *because* are handled by other logics.)

Special expressions

Suppose we evaluate the expression

$(p{\equiv}q) \quad ((q\square\ r) \square (r \square\ \ q)) \quad pr \quad (\square p)q(\square r)$

in the case where p and r are T but q is F. We find that the result is T. Actually, we find that the result is T when we evaluate this expression for *any* values of the propositional letters. If we made a truth table, we would have eight rows all with a T in the final column.

A propositional formula that evaluates to T no matter what values are given to its propositional letters is called a *valid* formula or a *tautology*. Perhaps the simplest example of a tautology is the formula $p \quad \square p$: Either he went to the store or he didn't. Another obvious tautology is $p\square\ p$: If the Bruins win then the Bruins win.

A propositional formula that always evaluates to F is called *invalid* or a *contradiction*. $p \square \neg p$ is a simple example. Is $p\square \quad \square p$ ("if the Bruins win then the Bruins don't win") a contradiction?

A formula that evaluates to T for *at least one* assignment of values is called *consistent*. All tautologies are consistent. The book doesn't use this terminology.

Logical Equivalence

Definition: Two propositional formulas *F* and *G* are called *logically equivalent*, written *F* □ *G*, if they have the same value under *every* interpretation, i.e., every assignment of truth values to the propositional variables.

For example, *p* *q* is equivalent to (□*p*)*q* *p*, as you can see by checking 4 truth assignments. Another example: *pq*□ *r* is equivalent to *p*□ (*q*□ *r*). But *pq* □ *r* is *not* equivalent to (*p*□ *q*) □ *r* since when all three variables are F the first is true but the second is false. Another example: All tautologies are equivalent, e.g., any tautology is equivalent to *p* □*p*.

Here's a tricky theorem: Let F_1 and F_2 be any formulas. Then F_1 and F_2 are equivalent if and only if the formula $F_1 \equiv F_2$ is a tautology. That is:

F_1 □ F_2 if and only if $F_1 \equiv F_2$ is a tautology

Don't be confused: The LHS is a statement about two formula, F_1 and F_2. The RHS is a statement about a new formula $F_1 \equiv F_2$. (The connective $\equiv$ combines two formulas to form a new one.) The theorem says that two formulas being equivalent is the same thing as a certain new formula being a tautology.

Be careful: □ is *not* an operator connecting two formulas into a new one; it's shorthand for a statement *about* two formulas!

Substitution

Suppose F_1 is a formula that contains a subformula G_1, and suppose that G_2 is a formula equivalent to G_1. Then if we substitute G_2 for G_1 in F_1, we get a new formula F_2 that is equivalent to F_1.
(The text calls this the "second rule of substitution".)

For example, go back to the formula

$$(p \equiv q) \quad ((q \square\ r) \square (r \square\ q)) \quad pr \quad (\square p)q(\square r)$$

It's easy to prove that $(q \square\ r) \square (r \square\ q)$ is equivalent to the formula $r \equiv q$. So this big formula is equivalent to

$$(p \equiv q) \quad (r \equiv q) \quad pr \quad (\square p)q(\square r)$$

Note that substitution doesn't have to make a formula smaller; it can also make it bigger. Also, you don't have to substitute G_2 at *every* place G_1 appears; you can substitute at just one, or just some. For example, since formula q is equivalent to $(q \quad q)$, the last formula above is also equivalent to

$$(p \equiv (q \quad q)) \quad (r \equiv q) \quad pr \quad (\square p)(q \quad q)(\square r)$$

by substituting $(q \quad q)$ for *some* of the occurrences of q.

Laws of Logic

We now come to a bunch of equivalences known as the Laws of Logic. Each of these is proved by showing that the appropriate biconditional is a tautology.

Double negation: $\neg\neg p \equiv p$

Idempotency: $p \vee p \equiv p \wedge p \equiv p$

Commutativity: $p \vee q \equiv q \vee p$

$p \wedge q \equiv q \wedge p$

Associativity: $(p \vee q) \vee r \equiv p \vee (q \vee r)$

$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

Distributivity: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(This last is a little surprising. In arithmetic, we have $x(y+z) = xy+xz$, but we *don't* have $x+yz = (x+y)(x+z)$. In logic, each operator is distributive over the other!)

Absorption: $p \vee pq \equiv p(p \vee q) \equiv p$

The text gives others with tautologies and contradictions.

DeMorgan's Laws

These immensely useful laws are named after a mid-nineteenth century mathematician.

$$\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$$
$$\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$$

That is, to negate a disjunction (OR), you negate each piece separately *but change it to a conjunction* (AND). Similarly, to negate an AND you negate each piece and change to OR.

A bigger example: The formula

$$\neg((p\square\ (\neg s)q) \quad \neg(sq\square\ \neg p))$$

whose outer form is "$\neg(F \vee G)$", is equivalent to

$$\neg(p\square\ (\neg s)q) \wedge \neg(\neg(sq\square\ \neg p))$$

By cancelling a double negation, we get

$$\neg(p\square\ (\neg s)q) \wedge (sq\square\ \neg p)$$

Simplification

We can use the laws of logic and substitution to simplify formulas. For example, if we continue with

$$\neg(p \rightarrow (\neg s)q) \rightarrow (sq \rightarrow \neg p)$$

we can use the fact that $(p \rightarrow q)$ is equivalent to $(\neg p \vee q)$ to change the left side

$$\neg(\neg p \vee (\neg s)q) \rightarrow (sq \rightarrow \neg p)$$

Now apply DeMorgan's Law to the left-hand side:

$$(\neg(\neg p) \wedge \neg((\neg s)q)) \rightarrow (sq \rightarrow \neg p)$$

Double negation and DeMorgan:

$$(p \wedge (s \vee \neg q)) \rightarrow (sq \rightarrow \neg p)$$

Again translating an implication:

$$(p \wedge (s \vee \neg q)) \rightarrow (\neg(sq) \vee \neg p)$$

Distributivity of $\wedge$ over $\vee$:

$$((ps \vee p(\neg q)) \rightarrow (\neg(sq) \vee \neg p)$$

. . . and so forth, until we get down to:

$$p \rightarrow \neg q$$

Simplification can go a long way.

Duality

Let *F* be a formula that contains only propositional variables and the connectives □, , and □. Then the *dual* of *F*, written (in the text) F^d, is the formula we get by changing every □ to   and vice versa in *F*.

For example, the dual of *p*(*q* (□*r*)) is *p* (*q*(□*r*)). (Note that □*p* is its own dual.)

Here's something incredibly interesting: If two formulas are equivalent, then their duals are also equivalent! (Handwaving proof: In logic, T and F are absolutely symmetric. So interchange them completely in truth tables! The truth table of   goes to □ and vice versa; the truth table of □ is unchanged.)

So, for example, once we prove that □(*p* v *q*) is equivalent to (□*p*) □ (□*q*), we know immediately by duality that □(*p* □ *q*) is equivalent to (□*p*) (□*q*).

By the way, what's the dual of *p*□ *q*? We have to write it using only   and □, namely □*p* *q*. Now we can make the dual: □*p* □ *q*, which is not expressible as an implication.

Implication

Consider again the implication $p \rightarrow q$. Several variants of this implication have special names:

$(\neg p) \rightarrow (\neg q)$ is called the *inverse* of $p \rightarrow q$

$q \rightarrow p$ is called the *converse* of $p \rightarrow q$

$(\neg q) \rightarrow (\neg p)$ is called the *contrapositive* of $p \rightarrow q$

Example: Let p be "I am rich", let q be "I am happy", and consider the implication "If I am rich, then I am happy". We have the following variants:

inverse: If I am not rich, then I am not happy.

converse: If I am happy, then I am rich.

contrapositive: If I am not happy, then I am not rich.

It is easy to check that any implication and its contrapositive are equivalent, which means that you can prove an implication by proving the contrapositive! But this does not apply to the other variants: An implication is NOT equivalent to its converse, nor to its inverse. (But the inverse and the converse ARE equivalent, since the inverse is the contrapositive of the converse!)

If an implication $p \rightarrow q$ and its converse are both true, then the biconditional $p \equiv q$ is true.

[Universal Connectives]

You may have noticed that we can write any formula using only , □, and □. In fact, we can write any formula using only □ and , since we can always write p□q in the equivalent form □((□*p*) (□*q*)). Similarly, we can write any formula using only □ and □.

On the other hand, there are formulas that we can't write using just and □. For example, there's no way to write a formula equivalent to □*p* using only and □.

Interestingly, we can devise connectives that by themselves suffice to write any formula! An example is the connective *not both*, *p*|*q*, which is T when *p* and *q* are not both T and as F when *p* and *q* are both T. Using only |, we can write (□*p*) as *p*|*p*, and we can write *pq* as (*p*|*q*)|(*p*|*q*). This already proves that using just | we can write an equivalent to any formula! This can also be done with the connective *neither-nor*.

By the way, how many truth functions of two variables exist? This is equivalent to saying: How many ways are there to fill out the last column of a two-variable truth table? Each way produces a different function of two variables, and clearly there are $2^4 = 16$ ways. In general, there are 2 to the 2 to the *n* truth functions of *n* variables.

Simplification II

Given a propositional formula *F*, how can we find the simplest formula that is equivalent to *F*?

For example, consider the formula:

$$p(\square q) \quad (\square p)q \quad q(\square r) \quad (\square q)r$$

It can be simplified to:

$$p(\square q) \quad (\square p)r \quad q(\square r)$$

But how can we find this algorithmically?

The text gives some examples of why this is important, involving minimizing switching circuits. But there are zillions of other reasons that you want to be able to express complex expressions in simplest form.

The answer, first proved by Cook in 1960, is that there is no computationally efficient algorithm that takes as input a propositional formula and produces as output the simplest equivalent formula! This is true for any reasonable definitions of the words "simplest" and "efficient". We will run across this whole topic again when we study computational complexity.