MATH 22

Lecture F: 9/18/2003

INFERENCE & QUANTIFICATION

> Sixty men can do a piece of work sixty times as quickly as one man. One man can dig a post-hole in sixty seconds. Therefore, sixty men can dig a post-hole in one second.
>
> —Ambrose Bierce,
> *The Devil's Dictionary*

Administrivia

- http://denenberg.com/LectureF.pdf
- Thanks for course and lecture feedback
- Barely acceptable proofs in #1 of Project 2

Logical Implication

Suppose that F and G are propositional formulas such that any interpretation of their variables that makes F true also makes G true. Then we say that F *logically implies* G, and we write F □ G. For example, formula $p(\neg q)r$ logically implies formula p□ q, since whenever the former is true, the latter is true.

(In this case it doesn't go the other way: p□ q can be true with $p(\neg q)r$ false. This doesn't matter.)

F □ G is always true if F is any tautology, that is, any tautology implies any formula. Similarly, any formula implies any contradiction.

Theorem: F □ G if and only if F □ G is a tautology.

This is the same thing we had with logical equivalence: It expresses something *about* propositions *within the language* of propositions. It says that two propositions have a certain relationship to each other (namely, one logically implies the other, i.e. we can *infer* one from the other) exactly when a certain new proposition formed from them has a particular quality (namely, it's a tautology). We often use this theorem without thinking, blurring the distinction between □ and □ .

Inference

One thing we can do with logic is to formalize chains of mathematical reasoning. The result is a format for proofs that probably looks much like proofs you once did in elementary geometry, where each step had to be justified by a previous theorem or construction.

We are going to formalize purely logical proofs, called *arguments* in the text. (Later we'll do mathematical proofs the same way.) A *formal proof* is a sequence of steps, each of which is logically implied by preceding steps. As part of the proof, we *justify* the implications.

An argument has *premises*, that is, things we assume, and a *conclusion* that is to be proved from these premises. We write an argument like this:

P_1

P_2

P_3

— — —

C

…where the P_i are premises and C is the conclusion to be proved. (There can be any number of premises.)

Proofs

A formal proof in our style will look like this:

	Steps	**Reasons**
1)	F_1	R_1
2)	F_2	R_2
3)	F_3	R_3
	…	…
n–1)	F_{n-1}	R_{n-1}
n)	C	R_n

Each line has a formula F_i which is justified by reason R_i. Note that the conclusion also needs a reason.

And what is a valid reason?   A reason can be either

- the word “Premise”, meaning that the formula is one of the things we’re assuming, or
- the application of one or more Rules of Inference to one or more of the formulas on preceding lines.

The *Rules of Inference* are the logical rules that we live by in our proofs. The Rules of Inference as defined in the book are presented on the next slide. After we see them we can try a proof.

Rules of Inference

From p□ q and p, infer q. (Detachment)

From p□ q and q□ r, infer p□ r. (Syllogism)

From p□ q and $\neg q$, infer $\neg p$. (Modus Tollens)

From p and q, infer pq. (Conjunction)

From p q and $\neg p$, infer q. (Disjunctive Syllogism)

From $\neg p$□ (*any contradiction*), infer p. (Contradiction)

From pq, infer p. (Conjunctive Simplification)

From p, infer p q. (Disjunctive Amplification)

From pq and p□ (q□ r), infer r. (Conditional Proof)

From p□ r and q□ r, infer (p q)□ r (Proof by Cases)

From p□ q, r□ s, and p   r, infer q s.

(Constructive Dilemma)

From p□ q, r□ q, and $\neg q$ $\neg s$, infer $\neg p$ $\neg r$.

(Destructive Dilemma)

Each of these rules is proved by proving that the associated conditional is a tautology, as in the first slide of today's lecture. E.g., to prove that p□ q and p together logically imply q, you must prove that

((p□ q) □ p) □ q

is a tautology. (You can do this, e.g., with a truth table.)

Using the Rules

Suppose we know both $rs \to t$ and rs. Can we infer t?

It looks like this inference can be justified by the Detachment Rule. Is it? We want to be able to use the Rules as *patterns* where we can substitute anything we like for the variables. This is permitted by the following Theorem, which the text calls the *First Substitution Rule*:

Suppose F is a tautology and p is any letter variable in F. Then if you substitute any formula for *every* occurrence of p in F, the result is another tautology.

For example, since

$$((p \to q) \wedge p) \to q$$

is a tautology, we can substitute rs for p and t for q to get

$$((rs \to t) \wedge rs) \to t$$

which, by the Theorem, is a tautology.

This tautology proves that $rs \to t$ and rs logically imply t, which is just what we wanted!

The bottom line is that when you use a Rule of Inference you can substitute any formula you like for any of its variables. Remember that you must substitute the *same* formula at *each point* the variable occurs in the Rule!

A Sample Proof

$(\neg p \quad \neg q) \,\square\, (r \,\square\, s)$

$r \,\square\, t$

$\neg t$

$———————————$

p

Steps	Reasons
1) $r \,\square\, t$	Premise
2) $\neg t$	Premise
3) $\neg r$	Modus Tollens on 1 and 2
4) $\neg r \quad \neg s$	Disjunctive Amplification on 3
5) $\neg(r \,\square\, s)$	DeMorgan on 4
6) $(\neg p \quad \neg q) \,\square\, (r \,\square\, s)$	Premise
7) $\neg(\neg p \quad \neg q)$	Modus Tollens on 6 and 5
8) $p \,\square\, q$	DeMorgan/Double Negation on 7
9) p	Conjunctive Simplification on 8

Note that we’ve not only used the Rules of Inference (□), we’ve also substituted equivalent formulas (<=>) as needed. This is OK by the substitution theorem of last lecture.

You should definitely try a few of these yourself.

Two Other Tricks

- If the conclusion of an argument has the form p□ q, you can make p a premise and make q the conclusion.

P_1
P_2
P_3
— — —
p □ q

P_1
P_2
P_3
p
— — —
q

- You can take any conclusion whatsoever, assume its negation as a premise, and prove any contradiction:

P_1
P_2
P_3
— — —
C

P_1
P_2
P_3
$\neg C$
— — —
(*any contradiction*)

Note that these aren't "reasons", they're ways to change what you're trying to prove to make the proof easier! (That is, you do them in advance, before anything else.) Each trick is justified because the conditionals associated with the two inferences are equivalent.

Quantifiers

The following utterance is *not* a proposition:

$$x^2 = 49$$

The reason, as we recall, is that the variable x is *free*: It can stand for anything we like, and the truth value of the utterance depends on what it stands for. We call a formula with free variables an *open statement*.

Suppose we write instead

There exists some number x such that $x^2 = 49$

This utterance *is* a proposition (and in fact a true one). Variable x is no longer a free variable; it's just a placeholder, used to keep track of some unspecified value—the statement is about the *existence of that value*.

The process of making a free variable into a *bound variable*—a placeholder—is called *quantification*. There are two principle types of quantification:

Universal quantification: "for all" (symbol $\forall$)

Existential quantification: "there exists" (symbol $\exists$)

The example above is an *existential quantification*, which would be written like this:

$$(\exists x)\ x^2 = 49$$

Here is an example of *universal quantification*:

$$(\forall x)\ x^2 > 0$$

The symbols $\forall$ and $\exists$ are called *quantifiers*.

Quantifier Basics

1) The variable bound by a quantifier, being just a placeholder, can be any variable at all. For example, these two statements are exactly the same:

$$(\exists x)\ x^2 = 49$$
$$(\exists y)\ y^2 = 49$$

2) Quantified statements are propositions; they can be combined with connectives like any other statements.

$$((\forall x)(x^2 > 0) \wedge (\exists x)(x-1 = 20)) \rightarrow (\exists y)(y^2 = 49)$$

This formula has form $(p \wedge q) \rightarrow r$ where p is the statement $(\forall x)\ x^2 > 0$, and q is the statement $(\exists x)\ x-1 = 20$. These statements each stand by themselves; and in particular the x in the first has nothing to do with the x in the second! We could change the two xs in the second statement to ys and nothing is affected. We could also change the two ys in the last statement to xs or zs.

3) Terminology: In a quantified formula, the formula part is called the *scope* of the quantifier; the quantifier is said to *govern* the formula in its scope. In the above example, the x of $x-1 = 20$ has nothing to do with the x of $x^2>0$ because the xs are in the scopes of different quantifiers.

Multiple Quantifiers

A formula can have more than one free variable, in which case we can quantify all or none of them. The formula is open unless *all* its variables are bound (in which case it's a *closed statement* and is true or false).

$$(\exists x)\ \ x + y \ = \ 17 \qquad\qquad \text{[open]}$$

$$(\forall y)\ (\exists x)\ \ x + y \ = \ 17 \qquad\qquad \text{[not open]}$$

In the second example, the scope of $(\exists x)$ is $x+y = 17$. The scope of $(\forall y)$ is $(\exists x)\ x+y = 17$, that is, $(\forall y)$ governs a formula that starts with an existential quantifier.

The order of quantifiers can matter! Consider the last formula above. It says that for every y, there is some x such that $x+y=17$. Surely this is true. (If y=7 we can take x=10. If y=40 take x=–23, etc.) But consider

$$(\exists x)\ (\forall y)\ \ x + y \ = \ 17$$

This closed statement says that there is some x such that for all y we have $x+y=17$. But there is no such x, so this statement is false. The difference is that now we must pick x first, *independent* of y. In the previous example, y is specified first, so x can be picked based on y and we can choose different xs for different ys.

Quantifier Facts, cont

The order of quantifiers doesn’t always matter. Example:

(□*x*)(□*y*) *xy* = *yx*

This statement is true, and remains true if we exchange the quantifiers.   It turns out that you can swap quantifiers if they’re of the same type, and not otherwise: (□*x*)(□*y*) is the same as (□*y*)(□*x*), and (□*x*)(□*y*) is the same as (□*y*)(□*x*).   Sometimes we write (□*x*,*y*,*z*) to mean (□*x*)(□*y*)(□*z*) and similarly for (□*x*,*y*,*z*).

When we say “for all *x*”, what *x* are we talking about? In   (□*x*)(□*y*) *x*=2*y*   we’re presumably talking about numbers; this statement is false if *x* can be a bird. The set of objects over which a quantified variable ranges is called the *universe of discourse* or just the *universe*. Choice of universe matters: the statement here is true in the universe of real numbers but false in the universe of integers. *Universes are always assumed to be nonempty*.

Notation: We use expressions like p(*x*) to stand for formulas with a free variable x.   Similarly, p(*x*,*y*) is a formula with two free variables, etc.   So (□*x*)p(*x*) is read “there exists some *x* such that p(*x*)” or even, more simply, “p is true of some *x*”.   Another example: (□*x*)(□*y*)q(*x*,*y*)   means   “for all *x*, there is some *y* such that q(*x*,*y*) is true” (or “. . .such that q is true of *x* and *y*”).

Rules of Negation

Consider the statement

¬ (□*x*) p(*x*)

which says “it is not the case that there exists some *x* such that p is true of *x*”, or “there is no *x* such that p(*x*)”. Clearly this is the same as

(□*x*) ¬p(*x*)

which says “for all *x*, p(*x*) is false”. In fact, the two statements are equivalent.

And what about

¬ (□*x*) p(*x*)

which says “it is not the case that p is true of all *x*”.

This is clearly equivalent to “there is some *x* such that p(*x*) is false”, which is written

(□*x*) ¬p(*x*)

These are the rules for quantifiers and negation: When you push the negation sign across a quantifier, you flip the quantifier. (Does this remind you of DeMorgan’s Laws? It should. After all, □ is just a big □, and □ is just a big .)

Distributing Quantifiers

A couple of equivalences:

$$(\forall x)(p(x) \wedge q(x)) \quad <=> \quad (\forall x)p(x) \wedge (\forall x)q(x)$$

$$(\exists x)(p(x) \vee q(x)) \quad <=> \quad (\exists x)p(x) \vee (\exists x)q(x)$$

(Are these reasonably obvious?) Said another way, you can distribute $\forall$ over $\wedge$, and you can distribute $\exists$ over $\vee$. Remember: $\forall$ is just a big $\wedge$, and $\exists$ is just a big $\vee$!

But if we try to mix $\forall$ with $\vee$ or $\exists$ with $\wedge$ it doesn't go so smoothly. Look what happens:

$$(\forall x)p(x) \vee (\forall x)q(x)$$

$$(\forall x)(p(x) \vee q(x))$$

The first of these says that either p is true of all *x*, or q is true of all *x*. The second says that either p or q is true of every *x*. Are these the same? No! If the first is true, the second is true, but the second may be true and the first one false! (Suppose p(*x*) is "*x* is even" and q(*x*) is "*x* is odd". Then surely for all *x* one or the other is true, but it's not true that either everything is even, or everything is odd!)

So we have

$$((\forall x)p(x) \vee (\forall x)q(x)) \Rightarrow (\forall x)(p(x) \vee q(x))$$

that is, the first statement *logically implies* the second, but the statements aren't *equivalent*!

Q, continued

The same thing happens if we try to distribute ∃ over ∧:

$$(\exists x)(p(x) \wedge q(x))$$

$$(\exists x)p(x) \ \wedge \ (\exists x)q(x)$$

The first statement says "for some *x*, both p and q are true of *x*". The second says "for some *x*, p is true of *x*, and for some *x*, q is true of *x*." The trouble is obvious: In the second case, it needn't be the same *x*!

(If p(*x*) is "*x* is a Tufts math professor" and q(*x*) is "*x* is smart", one says there is a smart Tufts math professor, but the other says that there is a Tufts math professor, and someone—maybe someone else—is smart.)

Again, we have implication but *not* equivalence:

$$(\exists x)(p(x) \wedge q(x)) \quad \Rightarrow \quad (\exists x)p(x) \ \wedge \ (\exists x)q(x)$$

Another:

$$(\forall x)p(x) \quad \Rightarrow \quad (\exists x)p(x)$$

This says that if every object satisfies p(*x*), then at least one object does! It's true in every nonempty universe.

Last one:

If $p(x) \Leftrightarrow q(x)$, then both $(\forall x)p(x) \Leftrightarrow (\forall x)q(x)$ and $(\exists x)p(x) \Leftrightarrow (\exists x)q(x)$ are valid equivalences.

[Words into Symbols]

The funnest thing about quantifiers is learning to use them to express, in the language of logic, relationships normally expressed in English. Examples (from *Quine*):

"There are smiles that make you blue" $(\exists x)(p(x)q(x))$

Here p(x) is "x is a smile" and q(x) is "x makes you blue."

"A lady is present" $(\exists x)(p(x)q(x))$

i.e., the same basic form, but consider:

"A scout is reverent" $(\forall x)(p(x) \Rightarrow q(x))$

which shows how capricious English idioms can be!

Note how it's critical that F $\Rightarrow$ T evaluates to T.

"No men are perfect" $(\forall x)(p(x) \Rightarrow \neg q(x))$

Can you do these? Be sure to define p and q!

– Blessed are the meek.

– There is no god but Allah.

– All that glisters is not gold.

– The rule applies to everyone.

– We should all be as happy as kings.

– A policeman's lot is not an 'appy one.

[An Awesome Proof]

Suppose G is a game played between players White (W) and Black (B), and that G has the following properties:

- W plays first, and the players alternate moves
- G is guaranteed to end after a finite number of moves
- G has no ties; when the game ends, W wins or B wins
- both players always have all information about what's going on (e.g., there are no hidden cards)
- the game has no random elements (e.g. dice).

Theorem: If G is a game as described above, then one of the players has a *winning strategy*, that is, a way to play from the beginning that he can use to always force a win.

Proof: Denote W's first move by w_1, B's first move by b_1, etc., and let N be the maximum possible number of moves. To say "W has a winning strategy" is to say

$$(\Box w_1)(\Box b_1)(\Box w_2)(\Box b_2)\ldots(\Box w_N)(\Box b_N)\ \text{W wins}$$

Suppose W does *not* have a winning strategy. That is

$$\neg\,(\Box w_1)(\Box b_1)(\Box w_2)(\Box b_2)\ldots(\Box w_N)(\Box b_N)\ \text{W wins}$$

By the rules of quantifier negation, this means

$$(\Box w_1)(\Box b_1)(\Box w_2)(\Box b_2)\ldots(\Box w_n)(\Box b_N)\ \neg(\text{W wins})$$

Since either W or B must win, this is the same as

$$(\Box w_1)(\Box b_1)(\Box w_2)(\Box b_2)\ldots(\Box w_N)(\Box b_N)\ \text{B wins}$$

But this statement says that B has a winning strategy!