Lecture 8 - What is a Proof?

6.042 - March 4, 2003

Our main objective to this point in the course has been computing answers to concrete problems. What is the probability of flipping heads on a fair coin? What is the expected value of the sum of three dice? Throughout, we've been applying standard mathematical results to specific situations. Now we tack to a new direction: understanding the structure of mathematics itself. This structure has been built over centuries and is probably growing faster now than ever before. *Proofs* are the basic building material. In general terms, a proof is a method of ascertaining truth. There are many ways to do this, in the wider world:

Jury Trial Truth is ascertained by twelve people selected at random.

Word of God Truth is ascertained by communication with God, perhaps via a third party.

Word of Authority Truth is ascertained from someone with whom it is unwise to disagree.

Experimental Science The truth is guessed and the hypothesis is confirmed or refuted by experiments.

Sampling The truth is obtained by statistical analysis of many bits of evidence. For example, public opinion is obtained by polling only a representative sample.

Inner Conviction "*My* program is perfect. I know this to be true."

"I don't see why not..." Claim something is true and then shift the burden of proof to anyone who disagrees with you.

Mathematics has its own notion of "proof" or way of ascertaining truth.

Definition 1 *A* formal proof *of a* proposition *is a chain of* logical deductions *leading to the proposition from a base set of* axioms*.*

The three key ideas in this definition are highlighted: proposition, logical deduction, and axiom. Each of these terms is discussed below.

1 Propositions

Definition 2 *A* proposition *is a statement that is either true or false.*

This definition sounds very general, but it does exclude sentences such as, "Wherefore art thou Romeo?" and "Give me an A!" More subtly, it excludes "this statement is false" (which is neither true nor false) and "this statement is true" (which is both true and false).

On the other hand, the definition of a proposition includes statements such as, "Every even integer greater than two is the sum of two primes." This is the famous *Goldbach Conjecture*, which dates back to 1742. No one yet knows whether it is true or false, but presumably it is one or the other!

1.1 Propositional Formulas

We can build up a *propositional formula* from some basic components as follows:

Atomic Propositions In general, these are statements that are either true or false. In this course, we are concerned with atomic propositions are mathematical statements, such as "$n \geq 4$". However, the precise rules governing atomic propositions are not important for the moment, so we represent them with variables.

Compound Propositions These are formed from atomic propositions and simpler compound propositions using parentheses and logical connectives.

- The *conjunction* of propositions P and Q is denoted $(P \wedge Q)$ and read "P and Q". The conjunction of P and Q is true only when both P and Q are true.
- The *disjunction* of propositions P and Q is denoted $(P \vee Q)$ and read "P or Q". It is true when P is true or Q is true or both are true.
- The *negation* of proposition P is denoted $(\neg P)$ or $\overline{P}$ and read "not P". It true when P is false.
- The *implication* $(P \rightarrow Q)$ is read "P implies Q" or "if P, then Q". This proposition is true when either P is false or Q is true.
- The *equivalence* $(P \leftrightarrow Q)$ is read "P is equivalent to Q" or "P if and only if Q". This proposition is true when P and Q agree; that is, both are true or both are false.

Thus, beginning with atomic propositions A, B, C, and D, we could use these rules to form a compound proposition such as:

$$(((A \vee (\neg B)) \wedge ((\neg C) \rightarrow D)) \leftrightarrow (A \vee C))$$

Usually, we omit some parentheses, when the meaning remains clear. For example, the expression above might be written:

$$((A \vee \neg B) \wedge (\neg C \rightarrow D)) \leftrightarrow (A \vee C)$$

1.2 Truth Assignments

A *truth assignment* for a propositional formula is a function mapping each variable in the formula to the set $\{\mathrm{T}, \mathrm{F}\}$. Here, T stands for "true", and F stands for "false".

We can determine whether a propositional formula as a whole is true with respect to a particular truth assignment much as we can evaluate an arithmetic expression such as $a(b+c)$ when each variable is assigned a numeric value. Now, however, instead of consulting addition and multiplication tables, we must consult the truth tables for the logical connectives. These are listed below:

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$	$P \rightarrow Q$	$P \leftrightarrow Q$
F	F	F	F	T	T	T
F	T	F	T	T	T	F
T	F	F	T	F	F	F
T	T	T	T	F	T	T

The table entries for $P \rightarrow Q$ are the most confusing. This proposition is defined to be true if either P is false or Q is true. For example, consider the following proposition:

If $n > 3$, then $n^2 > 9$.

We could write this in formal notation using the → connective:

$$(n > 3) \quad \rightarrow \quad (n^2 > 9)$$

Typically, one would say that this statement as "true" for all $n \in \mathbb{R}$. But let's see if our formal defintion of implication leads to that conclusion.

- If $n = 5$, this proposition is true, because both inequalities hold, and $T \rightarrow T = T$, according to the table.
- If $n = -5$, then the left inequality is violated and the right inequality holds. Therefore, the statement as a whole is true, because $F \rightarrow T = T$.
- Finally, if $n = 2$, both the left and right inequalities are false. However, the statement as a whole is still true, because $F \rightarrow F = T$.

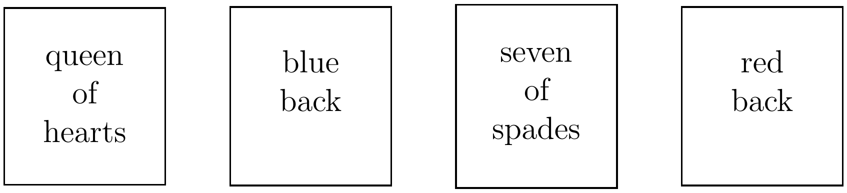
Happily, our proposition is indeed true under the formal definition of implication (at least for $n = 5$, -5, and 2). But this definition has a counterintuitive aspect: *an if-then proposition is always true if the if-part is false.* For example, the following proposition is absolutely true:

If pigs fly, then there will be no 6.042 final exam.

Rest assured that your butt *is* going to be plastered to a chair for three hours come late May; this statement is true only because pigs do not fly, and $F \to T = T$.

1.3 An Example with Cards

There are two decks of cards. All the cards in one deck have red backs, and all the cards in the other have blue backs. Now four cards are dealt from these two decks as follows:



Which of these cards must be flipped to verify that every face card has a blue back? One is tempted to say the first, second, and fourth.

Let's recast this problem in the terms of propositional logic. Let P_i be the proposition that card i is a face card, and let Q_i be the proposition that card i has a blue back. Now the assertion that we want to verify is:

$$(\underbrace{P_1}_{\text{T}} \to Q_1) \land (P_2 \to \underbrace{Q_2}_{\text{T}}) \land (\underbrace{P_3}_{\text{F}} \to Q_3) \land (P_4 \to \underbrace{Q_4}_{\text{F}})$$

At this point, we have only a partial truth assignment; known values are indicated above. Based on this limited information, the second and third clauses are guaranteed to be true, regardless of the values of P_2 and Q_3. On the other hand, the truth of the first and fourth clauses is dependent on the unknown variables Q_1 and P_4. We must flip just these two cards to verify the proposition.

1.4 Tautologies

A *tautology* is a propositional formula that is true under every truth assignment. Tautologies are useful because they allow us to rewrite propositions an equivalent way. One particularly helpful tautology is *DeMorgan's Law*:

$$(\neg P \vee \neg Q) \quad \leftrightarrow \quad \neg(P \wedge Q)$$

We can verify the correctness of this tautology by exhaustively checking that it is true under every possible truth assignment. This is done in the table below.

P	Q	$(\neg P \vee \neg Q)$	$\neg(P \wedge Q)$	$(\neg P \vee \neg Q) \leftrightarrow \neg(P \wedge Q)$
F	F	F	F	T
F	T	T	T	T
F	F	T	T	T
T	T	T	T	T

2 Proof Systems

A proof is a sequence of propositions, but not every sequence of propositions is a proof! A correct proof must start with one or more propositions that are true. Typically, we know that these starting propositions are true because they were proved previously, using proofs that, in turn, relied upon even more basic propositions. But if we work backward far enough, we eventually reach truly fundamental propositions called axioms.

Definition 3 *An* axiom *is a proposition that is assumed to be true.*

We can not prove axioms; we simply aceept them (or not). Various axiom schemata [1] have been proposed as bases for all mathematics. Probably the most famous is called ZFC, which consists of a handful of primitive, odd-looking assertions about sets. There is some philosophical debate about whether these are the "right" axioms, but ZFC is widely accepted.

In addition to axioms, we ways to logically deduce new propositions from old ones. Inference rules serve this purpose.

Definition 4 *An* inference rule *is used to combine axioms and true propositions to construct more true propositions.*

One inference rule that dates back to Aristotle is called *modus ponens.* This says that if P is true and $P \to Q$, then Q is true. This rule can be expressed in a special notation:

$$\begin{array}{l} P \\ P \to Q \\ \hline Q \end{array}$$

[1] The plural of schema.

The general is behind this notation is simple: if the stuff above the line is true, then the stuff below the line is true also. Here is another inference rule, called *modus tollens*:

$$\begin{array}{l} P \to Q \\ \neg Q \\ \hline \neg P \end{array}$$

Using this notation, we can also express the idea that a statement implies its contrapositive[2] and vice versa:

$$\begin{array}{l} P \to Q \\ \hline \neg Q \to \neg P \end{array} \qquad\qquad \begin{array}{l} \neg Q \to \neg P \\ \hline P \to Q \end{array}$$

We can also express the idea of indirect proof. In such an argument, one proves an assertion P by initially assuming the opposite ($\neg P$) and reasoning from there to a false conclusion ($\neg P \to \mathrm{F}$). According to the following inference rule, one can then conclude that the original assertion P is true:

$$\begin{array}{l} \neg P \to \mathrm{F} \\ \hline P \end{array}$$

3 Are We Done?

Unfortunately, the simple propositional logic described here is too limited to express most significant mathematical ideas. For example, propositional logic enables us to say that the squares of various integers are greater than or equal to zero:

$$(2^2 \geq 0) \wedge (35^2 \geq 0) \wedge ((-3)^2 \geq 0)$$

But there is no way in propositional logic to express the idea that the square of *every* integer is greater than or equal to zero. To do this, we must add some new logical symbols and notions. These modifications carry us beyond propositional logic to something called *first-order logic*. This more general logical system, together with the ZFC axioms, forms a basis for essentially all of standard mathematics, from $2 + 2 = 4$ to integral calculus.

This is what mathematical proofs are *in theory*. In practice, mathematicians rarely work at the level of axioms and formal inference rules. There are good reasons for this: rigidly formal proofs are long, virtually unintelligible to humans, and completely disconnected from the most important tool for finding new proofs, the mysterious thing called "intuition".

[2] The *contrapositive* of the statement "if P, then Q" is the statement "if not Q, then not P". If a statement is true, then so is its contrapositive and vice versa. You might convince yourself of this by substituting propositions about everyday life in place of P and Q.

Instead, proofs are normally written primarily in ordinary languages, such as English, with the understanding that such arguments *could* be reduced to formal proofs, if one really wanted to.

In practice, mathematical results are also usually described using a terminology that hints at their significance.

- Milestone conclusions are called *theorems.* Some particularly famous theorems are called *fundamental theorems* or even *laws.*
- Preliminary or technical results are called *lemmas* [3]. Lemmas are somewhat like subroutines in a complicated computer program; breaking a complex proof into a sequence of well-chosen lemmas can clarify the structure of the argument. Also, one can avoid walking through the same sequence of logical steps multiple times by proving an appropriate lemma and then citing it repeatedly.
- Straightforward consequences of theorems are called *corollaries.*

Precisely what constitutes a theorem, what a lemma, and what a corollary is only a matter of subjective judgement; in purely logical terms, there is no difference.

[3] Some people insist that the proper plural of "lemma" is "lemmata", much as the plural of "schema" truly is "schemata". I guess it's some Greek thing. Anyway, the author of these notes has been planning for several years to form a secretive gang dedicated to the principle that mathematicians who use the word "lemmata" need to be roughed-up until they mend their deviant ways. If you'd like to join, write to `Anti-Lemmata Society; 200 Tech Square, Room 203; Cambridge, MA 02139.`