Class Notes for Lecture 2

3 Logical Proof Systems

Recall: a logical proof system consists of:

- A **language** for stating propositions (propositional/predicate calculus)
- **Axioms:** Propositions accepted as true
- **Rules of inference:** Acceptable ways of combining propositions

  (all propositional tautologies) for example:

  $$\neg(\forall x)\neg S(x) \equiv (\exists x)S(x)$$

  (This particular one is rejected by constructivists, since it lets you prove something exists without actually saying what it is).
- **Theorems:** Propositions that can be derived by applying the inference rules to the axioms.

Note: we must always have some axioms: there are no "self evident" propositions.

3.1 Example: equality

Axioms:

- (E1) $(\forall x)(x = x)$
- (E2) For any formula F with free variable x,

  $$(\forall xyz \ldots)(x = y \Rightarrow (F \rightarrow F[x/y])$$

  where $F[x/y]$ denotes substituting y for some or all occurrences of x.

Actually (E2) is an **axiom scheme** describing an infinite number of axioms.

Inference Rules: propositional logic (e.g. modus ponens)

How can we prove $(\forall ab)(a = b \Rightarrow b = a)$?

- fix a, b
- Let F be $(x = z)$ in E2: $(\forall xyz)(x = y \Rightarrow ((x = z) \Rightarrow (y = z))$
- Thus in particular, $(a = b) \Rightarrow (a = a \Rightarrow b = a)$
- By hypothesis, $a = b$
- Modus ponens: $(a = a) \Rightarrow (b = a)$
- E1: $a = a$
- MP: $b = a$
- we proved for fixed a, b, so by universal generalization, holds for all.

This is incredibly torturous. Why do we care?

- Each step is justified by reference to previous steps.
- Justification is mechanical
- A **machine** can check the work

A true proof can be verified by purely mechanical (algorithmic) means. No creativity, common sense, or outside knowledge needed.

The mathematician Hilbert suggested that in any proof we must be able to substitute the words "points, lines, planes" with "tables, chairs, beer mugs" and arrive at the same conclusions (i.e. our method of proof should not depend on a particular representation of our mathematical objects).

3.2 Completeness/Consistency

If proofs are mechanical, where is the creativity in **finding** the proof? Well, you might have noticed that proving something is much harder than verifying it. Actually some statements are impossible to prove!

Hilbert posed (as one of his 23 famous problems) the problem of finding a rote method for proving any true theorem. One of the great accomplishments of 20th century math is the proof that no such method exists. There are actually several different kinds of obstacles.

A logical proof system is

- **consistent** if no statement and its complement can both be derived.
- **complete** if it can be used to prove or disprove every proposition.

Russell and Whitehead, in *Principia Mathematica*, tried to completely axiomatize mathematics but failed.

Gödel's Theorems:

- no axiomatization of arithmetic is complete and consistent.
- "arithmetic is consistent" is a proposition that cannot be proved in arithmetic.
- Gensen: "arithmetic is consistent" can be proved by adding some reasonable-sounding axioms, but these axioms can't be proved consistent.

There are true facts in math that cannot be proven! (Goldbach?)

We'll try to keep these off the homework.

Even if we limit ourselves to things that can be proven, computers won't be much help. Finding a proof—even, say, just a proof that a given propositional logic statement is a tautology—is **NP-complete**, meaning that it is untractable in a certain formal sense you will learn about in 6.045 or 6.046.

So we will always rely on human intuition to find the proofs, although we will be using computers more and more to check if they are right.

4 How To Prove Things

Now we discuss how proofs are actually done in practice. Sketches that it's supposed to be possible to complete. Then we'll say what we actually expect in this course, and finally we'll start going through a catalog of practical proof methods.

There are lots of ways to prove things. We now give some examples.

4.1 Direct Proof

Direct proofs are the most straightforward: we mix together previous axioms and theorems until the desired claim is inferred.

For natural numbers a and b, where $a \neq 0$, we say a *divides* b if there exists a natural number t such that $at = b$. We write $a \mid b$.

- $3 \mid 6$
- $3 \nmid 7$

Theorem 4.1 If $a \mid b$ and $a \mid c$, then $a \mid b + c$.

Proof. By definition of divisibility, $(\exists t) b = at$ and $(\exists s) c = as$.
Therefore, $b + c = at + as = a(t + s)$.
Therefore, by definition, $a \mid b + c$. ∎

Note: distributivity was assumed without mention.

4.2 Proof by Contradiction

$$\frac{p \implies FALSE}{\neg p}$$

Proofs can go "backwards":

- Begin by assuming the desired theorem is false.
- Using inference rules, conclude something known false.
- Conclude that the assumption is wrong.

Theorem 4.2 $\sqrt{2}$ is an irrational number.

Proof. (By contradiction). Assume $\sqrt{2}$ is rational.

Conclude $\sqrt{2}$ can be written as a fraction a/b in lowest terms. **big assumption!**
Then $2b^2 = a^2$.
In other words, a^2 is even (since $2b^2$ is even).
Therefore, a is even (the square of an odd number is odd) (needs proof).
Therefore, a^2 is divisible by 4.
But b is odd (since a/b is in lowest terms and a is even).
Thus $2b^2$ is not divisible by 4.
Thus 4 divides a^2, but not $2b^2 = a^2$, contradiction.

Since our assumption leads to a false conclusion, it must be false. Thus, $\sqrt{2}$ is not rational. ∎

Note: this process is based on the assumption that math is consistent, since otherwise it would be possible to prove something false.

We freely used lots of basic facts about divisibility, lowest terms for fractions, definitions of square, all without reference or proof.

Pythagoras and his followers knew this proof, but suppressed it because they axiomatically denied the existence of irrational numbers (so their system was not consistent, because they also had an axiom that every line had a numeric length).

4.3 A Nonconstructive Existence Proof

Theorem 4.3 For any number n, there is a prime number greater than n.

Proof. Fix n, and consider $n! + 1 = (1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n) + 1$. If $n! + 1$ is prime, we are done. Otherwise, $n! + 1$ has a prime factor x (relies on the prime number theorem). By definition, $n! + 1$ is divisible by x (without leaving a remainder). But if $n! + 1$ is divided by a number less than n, the remainder is 1. Therefore, $x > n$. ∎

(Note: $n! + 1$ need not be prime. $5! + 1 = 11^2$.)

We don't know what x is, only that it exists.

Constructivists would deny this is a proof.

4.4 Proof by Cases

Proof by cases:

- show $p \implies (a \vee b)$
- show $a \implies q$ and $b \implies q$
- deduce $p \implies q$

Theorem 4.4 for some irrational number α and β, α^β is rational.

Proof.

Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we are done!

If not, then it is irrational. We also know that $\sqrt{2}$ is irrational (previous proof). But then we have,

$\sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2$, which is rational!

∎

This is a wierd proof! We proved that it exists, but we didn't construct it! It's easy to follows, but hard to imagine. How did we know?

Practice. Seeing proofs develops a feeling for finding proofs.

4.5 Other Proof Methods

- Indirect proof: from $\neg q \implies \neg p$, deduce $p \implies q$ (similar to proof by contradiction).
- Vacuous proof: if p is false, then $p \implies q$ is true.
  - if x is an even prime greater than 2, then x is a perfect square.

  Boring, but often arises as one case of a proof by cases.

4.6 Fallacies

There are several ways to generate an incorrect proof.

$$
\begin{aligned}
\sqrt{-1} &= \sqrt{-1} \\
\sqrt{\frac{1}{-1}} &= \sqrt{\frac{-1}{1}} \\
\frac{\sqrt{1}}{\sqrt{-1}} &= \frac{\sqrt{-1}}{\sqrt{1}} \\
\sqrt{1}\cdot\sqrt{1} &= \sqrt{-1}\cdot\sqrt{-1} \\
1 &= -1
\end{aligned}
$$

Where's the bug?

There are several common fallacies:

Affirming the conclusion:

- If you are tired, you will fall asleep
- You fall asleep
- therefore, you are tired

The fact that the conclusion is true does not make the hypothesis true. Maybe you are just bored.

Denying the hypothesis:

- If you work hard, you will pass the course
- You don't work hard

- therefore, you will fail the course.

Even if the hypothesis is false, the conclusion can be true. Maybe you are smart enough to pass without working.

Circular reasoning: proposition: If n^2 is not divisible by 3, then n is not divisible by 3.

- If n^2 is not divisible by 3, then n^2 is not equal to $3k$ for any integer k.
- therefore, n does not equal $3l$ for any integer l.
- therefore, n is not divisible by 3.

If you assume (or prove) something FALSE, you can prove anything!