CS 121 Lecture 3

Aaron Kaufman, Shien Jin Ong, Yuanchen Zhu

September 27, 2005

Outline

This lecture will focus on writing and understanding mathematical proofs. The outline of the lecture is as follows:

Part I What is a proof? How to write a mathematical proof?

Part II Induction.

Part III Other Proof Techniques.

1 What is a proof? How to write a mathematical proof?

Before we get into the various different proof techniques, let us begin with the following theorem in mind.

Theorem 1.1 (Theorem 0.20 in Sipser). *Given two sets A and B that are subsets of a universe U, prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.*

If asked to give a proof of the above theorem, how would one approach it? The first step is to draw a diagram to help visualize the problem.

[Diagram drawn in class]

Voila, our diagram does indeed show that for the above sets A and B, $\overline{A \cup B} = \overline{A} \cap \overline{B}$! Are we done? Not quite, since we have to show that the statement is true for *all* sets A and B. Having a diagram, nevertheless, will help us structure our proof.

To show that $\overline{A \cup B} = \overline{A} \cap \overline{B}$, it can be broken up into proving two statements.

- $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$, that is every element of $\overline{A \cup B}$ is also an element of $\overline{A} \cap \overline{B}$, and

- $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$, that is every element of $\overline{A} \cap \overline{B}$ is also an element of $\overline{A \cup B}$.

In general, this technique of proving sets $X = Y$ by showing that $X \subseteq Y$ and $Y \subseteq X$ is called *mutual inclusion.*

The formal proof of Theorem 1.1 is presented in lecture.
Proof: [Done in lecture. For additional reference, refer to the proof of Theorem 0.20 of Sipser.]

Writing good proofs. A good proof is concise, states clearly what techniques are being used, and is written legibly (and of course, correctly reasoned too). Considering that not everyone of us are gifted with legible handwriting, it is encouraged that you type your solution sets (and you can certainly draw diagrams by hand). Here are a some additional tips on writing good proofs, from MIT 6.042/18.062J Fall '04 Lecture Notes by Tom Leighton and Eric Lehman.

State your game plan. A good proof begins by explaining the general line of reasoning, e.g. "We use induction" or "We argue by contradiction". This creates a rough mental picture into which the reader can fit the subsequent details.

Keep a linear flow. We sometimes see proofs that are like mathematical mosaics, with juicy tidbits of reasoning sprinkled judiciously across the page. This is not good. The steps of your argument should follow one another in a clear, sequential order.

Explain your reasoning. Many students initially write proofs the way they compute integrals. The result is a long sequence of expressions without explanation. This is bad. A good proof usually looks like an essay with some equations thrown in. Use complete sentences.

Avoid excessive symbolism. Your reader is probably good at understanding words, but much less skilled at reading arcane mathematical symbols. So use words where you reasonably can.

Introduce notation thoughtfully. Sometimes an argument can be greatly simplified by introducing a variable, devising a special notation, or defining a new term. But do this sparingly, since you're requiring the reader to remember all this new stuff. And remember to actually define the meanings of new variables, terms, or notations; don't just start using them.

Simplify. Long, complicated proofs take the reader more time and effort to understand and can more easily conceal errors. So a proof with fewer logical steps is a better proof.

Don't bully. Words such as "clearly" and "obviously" serve no logical function. Rather, they almost always signal an attempt to bully the reader into accepting something which the author is having trouble justifying rigorously. Don't use these words in your own proofs and go on the alert whenever you read one.

Finish. At some point in a proof, you'll have established all the essential facts you need. Resist the temptation to quit and leave the reader to draw the right conclusions. Instead, tie everything together yourself and explain why the original claim follows.

Detect patterns. Another important skill in solving mathematical problems, or life in general, is detecting patterns. Consider the following problem.

Problem 1.2. *How many strings are there of length n, over the alphabet $\Sigma = \{a, b\}$, such that there are no consecutive a's?*

For $n = 1$, there are two such strings, namely a and b. For $n = 2$, there are three such strings (ab, ba and bb). For $n = 3$, there are five such strings (aba, abb, bab, bba and bbb). And for $n = 4$, there are eight such strings—try to list all of them?

Notice a pattern here? Let's see $5 = 3 + 2$ and $8 = 5 + 3$—seems like we have the Fibonacci sequence! Can you find 13 strings with no consecutive a's of length five?

In the next section, we learn how to formalize our observations and prove that indeed the number of such strings indeed follow the Fibonacci sequence.

Conclusion. Let's recap what we have learnt in this section: First and foremost, understand the problem and if necessary **draw a diagram** to help you visualize it. We demonstrated a proof technique called **mutual inclusion**, particularly useful for proving that two sets X and Y are identical. Finally, we highlighted the importance of **searching for a pattern**.

2 Induction

The Ladder Analogy: Mathematical Induction can easily be thought of as a ladder with infinitely many rungs. The goal is to prove that we can climb up to any rung. In order to do that, we need to prove two things:

- Once we have already climbed to one rung, we can get to the next one. (called the *inductive step*)
- We can get started by climbing to the first rung. (called the *base case*)

Proving this is tantamount to proving that we can climb up as high as we want.

Fibonacci Revisited: The Fibonacci numbers are defined inductively as follows:
$F_0 = 0$.
$F_1 = 1$.
$F_n = F_{n-1} + F_{n-2}$ for all $n > 1$.

The first few numbers of the sequence are $0, 1, 1, 2, 3, 5, 8, 13, 21 \dots$

In the last section, we conjectured that the number of strings of length n over the alphabet $\Sigma = \{a, b\}$ with no consecutive a's fit this pattern. In this section we will prove this more formally.

Proof: Let $P[n]$ be the statement "The number of strings of length n over the alphabet $\Sigma = \{a, b\}$ with no consecutive a's is equal to F_{n+2}". We will prove by induction that $P[n]$ holds for all $n \geq 1$.

Base Cases: We will prove $P[1]$ and $P[2]$ explicitly. For $P[1]$, we note that the only strings of length 1 are a and b. Neither of them have any consecutive a's, and thus the total number of strings of length 1 with no consecutive a's is 2, which is exactly F_3. For $P[2]$, we note that the only strings of length 2 are aa, ab, ba, and bb. The string aa has 2 consecutive a's, while the other 3 don't–thus the total number of strings of length 2 with no consecutive a's is 3, which is exactly F_4.

Inductive Step: We assume $P[n]$ and $P[n-1]$ hold, and try to prove that $P[n+1]$ holds as well. Let S be the set of all strings of size $n + 1$ that have no consecutive a's. Split S into two disjoint sets as follows: Let S_a consist of all words in S that end in a and let S_b consist of all words in S that end in b.

Examine S_a first. Since all words in S_a end in a, and all such words are forbidden to have two consecutive a's, then all words in S_a must end in ba. The only constraint on the remaining $n - 1$ letters of any word in S_a is that there cannot be any consecutive a's. Since $P[n-1]$ holds, we know that the number of such $(n - 1)$-letter words is F_{n+1}. So S_a contains F_{n+1}-many words.

Examine S_b next. Since all words in S_b end in b, the only constraint is that the remaining n letters of any word in S_b cannot have any 2 consecutive a's. And since $P[n]$ holds, we know that the number of such n-letter words is F_{n+2}. So S_b contains F_{n+2}-many words.

Now, since S contains all of the words in S_a and all of the words in S_b, and since S_a and S_b have no words in common (no word can both end in a and end in b), then S must contain $F_{n+1} + F_{n+2} = F_{n+3}$ words. This proves that $P[n+1]$ holds, and completes the proof.

Questions about Base Cases: One question is "why do we need two base cases in the previous example?" Let's return to our ladder analogy. To prove that we can reach any step of the ladder, we proved (1) that we can climb to the first step, and (2) once on step n, we can get to step $n+1$. HOWEVER, in the previous example, instead of proving that once on step n we can get to step $n+1$, we needed to use the fact that we had been on both steps $n-1$ and step n in order for us to get up to step $n+1$. Thus, we needed to first prove that we can get to the first two steps. This is an important distinction; getting the wrong number of base cases can really mess things up, as we will illustrate in the following example.

Find the problem with the following proof by induction: Let $P[n]$ be the statement "$x^n = 1$". We will attempt to prove that $P[n]$ holds for all n—that is, we will prove that $x^n = 1$ for all n.

Base Case: $P[0]$ holds because x^0 is clearly equal to 1.

Inductive Step: We assume $P[n]$ and $P[n-1]$. Examine the identity:

$$x^{n+1} = \frac{x^n \cdot x^n}{x^{n-1}}$$

.

$P[n]$ tells us that $x^n = 1$ and $P[n-1]$ tells us that $x^{n-1} = 1$. Thus we have:

$$x^{n+1} = \frac{1 \cdot 1}{1} = 1$$

.

This shows that $P[n+1]$ holds, thus completing the proof.

3 Other Proof Techniques

Proof by Contradiction. Suppose we are asked to prove a statement. Often we will start with a couple of theorems and axioms related to the statement in question, and then try to use various logical reasoning methods, e.g., mathematical induction as introduced in the previous section, to arrive at the truth of the statement that we want to prove. However, sometimes it is not immediately apparent what set of theorems and axioms our starting point should be. In such cases, one approach to attack the problem is considering proof by contradiction. Here is the general work-flow of doing proofs by contradiction:

1. Assume the exact opposite of the statement that we want to prove is true.
2. Based on the assumption, try to arrive at two statements that contradict each other.

Let's do an example of proof by contradiction by proving that $\sqrt{2}$ is irrational. But first let us remind ourselves what a rational number is. A number is *rational* if it is the fraction m/n between two integers m and n ($n \neq 0$). And a number is *irrational* if it is not rational. At a first glance, it is definitely not apparent how we can approach this problem. There're potentially a large number of theorems related to integers and rational numbers. Which ones shall we use as a starting point? So let's try to prove the statement by contradiction by (1) assuming that $\sqrt{2}$ is rational, and (2) arriving at two statements that contradict each other.

Theorem 3.1 (Theorem 0.24 in Sipser). $\sqrt{2}$ *is irrational.*

Proof: [Done in lecture. For additional reference, refer to the proof of Theorem 0.24 of Sipser.]

Notice how proving Theorem 3.1 is made much more approachable by doing proof by contradiction. A proof by contradiction works backward from the statement we want to prove (actually its logical negation), and can often be used if we don't know or aren't sure which theorems or axioms our proof should use as a starting point.

Proof by Construction. A lot of the proofs that we'll be doing through out the semester are going to be constructive proofs. When we are asked to prove the existence of certain objects satisfying certain properties, we will actually come up with one such object to prove its existence. Now let's do an example by proving the following theorem.

Theorem 3.2. *There exist irrational numbers a and b satisfying that a^b is rational.*

Proof: We already know that $\sqrt{2}$ is irrational. We might as well try letting $a = b = \sqrt{2}$. Then there are two possible cases that we need to discuss.

Case I. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we are done.

Case II. If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ to get:

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2.$$

But 2 is rational, so again we are done.

Proof by Cases. Notice that in the above proof we have actually constructed two pairs of numbers. The first pair is two rational numbers that might or might not satisfy the theorem. However if the first pair does not satisfy the theorem, then the second pair definitely does satisfy the theorem. Without further work to see if $\sqrt{2}^{\sqrt{2}}$ is rational or not, we don't really know which of the two pairs is actually the construction we seek. However, the important point here is that the two cases together have already covered all the possibilities. Exactly one of the two constructions will satisfy the theorem. And that is good enough to show the existence of irrational numbers a and b satisfying that a^b is rational.