

CS121 Section 0: Proofs

September 14, 2009

Outline

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

Part 0 Basics. Notation, terminology, etc.

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

Part II Induction.

Part III Other Proof Techniques.

1 Basics

Definitions

- Sets: empty set, power set, union, intersection, cartesian product.
- Strings vs. Languages: Strings are *finite* sequences of symbols, languages are (possibly) infinite sets of strings.
- Functions map from a domain to a range and can be one-to-one (injective), onto (surjective) and bijective.
- Binary Relations relate two sets of elements, they can be reflexive, symmetric or transitive or some combination of the three properties.
- Graphs are collections of vertices and associated edges going between the vertices. A graph can be directed or undirected.

Notation in proofs

- Forall (\forall) and there exists (\exists) are symbols which occur frequently in proofs. They are mathematical shorthand.
- To prove $A \Rightarrow B$ (B if A) Assume that A is true, then using only that, prove B .
- To prove $A \iff B$ Prove $A \Rightarrow B$ and $B \Rightarrow A$. Or, prove $A \Rightarrow B$, and $\neg A \Rightarrow \neg B$

2 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.

Exercise 2.1 (Theorem 0.20 in Sipser). *Given two sets A and B that are subsets of a universe U , prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.*

1. Carefully read the statement you want to prove. Do you understand it? Do you understand all the notation?
2. Develop some intuition for the problem. Try drawing a diagram or working through a few examples. Can you begin to see why the statement is true and how to prove it?
3. When you believe you have found the proof, write it up properly. A well-written proof is a sequence of statements wherein each one follows from the previous statement by simple reasoning.

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). Note that you get a 5% bonus for typing your psets. Here are 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.

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.

Correctness Be sure that your proofs are complete and logically correct. Even seemingly small errors can lead to incorrect results. Consider the following (faulty) example.

Exercise 2.2 (Find the error). *Consider the equation $a = b$. Multiply both sides by a to obtain $a^2 = ab$. Subtract b^2 from both sides to get $a^2 - b^2 = ab - b^2$. Now factor each side, $(a + b)(a - b) = b(a - b)$ and divide each side by $(a - b)$, to get $a + b = b$. Finally, let a and b equal 1, which shows that $2 = 1$.*

3 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. Here's a simple "recipe" for writing up induction proofs:

1. Write down the variable you're doing induction on.
2. Write down the property to be proven (e.g. $P[x]$).
3. Prove your base case (e.g. prove $P[0]$)
4. Write down your inductive hypothesis that you assume to be true (e.g. $P[k]$ is true), and prove the next step (e.g. $P[k+1]$ is true).

Exercise 3.1. *Given a $2^n \times 2^n$ board with exactly one missing 1×1 square, prove that one can cover it completely with L-shaped pieces composed of 3×1 squares with no overlaps.*

Exercise 3.2 (Find the error). 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.

4 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 the problem is proof 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.

Exercise 4.1. Show that in any group of n people, at least two of them know the same number of other people within the group. (Assume that the relation knowing is symmetric and that, with all due respect to the oracle at Delphi, people can't know themselves.)

Exercise 4.2. *Show that there's a multiple of 2008 that only has 1's and 0's as digits.*

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.

Exercise 4.3. *For every even number $n \geq 4$, there exists an undirected graph in which every vertex is the endpoint of exactly three edges.*

Proof by Cases. Sometimes it is difficult to explicitly construct the necessary examples. It may be easier to split the problem into a few cases and consider each case separately.

Exercise 4.4. *There exist irrational numbers a and b such that a^b is rational.*

Exercise 4.5. *Let a_n be the number of binary strings of length n that do not contain the substring 010. Prove that $a_n = 2a_{n-1} - a_{n-2} + a_{n-3}$.*