Math 38: Graph Theory Spring 2004
Dartmouth College

On Writing Proofs

1 Introduction

What constitutes a well-written proof? A simple but rather vague answer is that a well-written proof is both clear and concise. The reader should be able to understand each step made by the author without struggling. You may assume that the audience is familiar with the relevant definitions and theorems, but has given little to no thought about the problem at hand. Lead the reader through the problem step by step. Make sure each statement follows logically from the previous statement and brings us one step closer to the goal. Once your solution is complete, the reader should have no problem reconstructing the original statement of the problem.

The following analogy may clarify what constitutes a well-written proof and how to go about writing one. Imagine that you are going to lead a group of adventurers through the jungle to the top of a mountain to view the most spectacular sunset. You can assume that your group is capable of such a trip, however none of them are familiar with the region. In order to complete this journey successfully, you must first find an appropriate route and then be able to explain to your group how to navigate every twist and turn along the way.

Before taking your group out into the jungle, your first priority should be to find at least one way to get to the mountaintop from base camp. That way you insure everyone will get to see the spectacular view. However, having found a route, you may want to reconsider whether you have chosen the best one. Is it appropriate for those traveling in your group? Did you have to backtrack at any point? Were there any shortcuts you missed? Were there any difficult climbs that can be avoided? If they can't be avoided, are you prepared to explain to everyone how to successfully navigate this portion of the journey? Once on top of the mountain, perhaps a completely different path can be seen from above that you never saw while in the jungle. You may want to investigate this new path before setting out with your group.

Once you have answered all these questions, you are ready to take your group along the most direct and enlightening route you have found. Before beginning, make sure to tell your group what lies ahead and the mode of transport you will be using (hiking, cycling, kayaking, etc.). Along the way, feel free to point out any interesting views or introduce them to an amazing creature that you have encountered, but make sure that it is relevant to the task at hand. Each step through the jungle should follow easily from the previous one. Don't make your steps too big or walk too quickly, otherwise you run the risk of losing some of your group to the jungle. And once you have completed your trek, make sure to point out what everyone has come to see. You wouldn't want anyone to miss out!

It should be clear from our analogy that finding a solution and writing up a solution are two completely different things. In the next two sections, we will further break down each task to give you a better idea of how to complete them. The final section reviews various methods of proof and provides several examples of using these methods.

2 Finding A Solution

As suggested by our analogy, the first step should be to find a solution. While there is no sure fired way to do so, the following steps will help you get started and provide you with some suggestion in case you get stuck.

1. **Read the problem** - Read it carefully!

2. **Determine what the problem is asking you to do.** Outline exactly what you have to do to answer this problem. Is it asking you for a formula? Do you have to prove that your formula is correct. Are there multiple parts?

3. **What information has been given?** It may help to write down all the definitions and their immediate implications. For example, if you are told that a and b are relatively prime, this means that a and b have no prime factors in common. It also means that the largest number that divides both a and b is 1, in other words, $gcd(a, b) = 1$. And lastly, it means that there exists integers r and s such that $ar + bs = 1$. In the end, you may not use all of these pieces of information, but it helps to remind yourself of what tools are at your disposal.

4. **What assumptions are you making, if any?** Are you introducing any new information that was not given in the problem? Is it possible to answer the question without introducing this new information? Are these additional assumptions valid. If you are introducing some valid assumptions, make sure to include this information in your solution.

5. **Try specific values.** If the problem is asking you to find a function, then before even attempting to guess the correct answer, try to determine what this function should evaluate to for specific and/or convenient values of the input variables. This will not only help get you started trying to figure out what the general formula is, but it may also give you a hint on how to prove that your formula is correct. Furthermore, this gives you a way to check that your answer is correct in specific cases.

   If the problem is asking you to prove an identity for all $n \geq 0$ and you are struggling to find a general argument, consider what the identity says for small values of n. Can you prove these specific cases? This may help you find a pattern which leads to a general argument.

6. **Formulate a possible solution.** The emphasis here should be on the word possible. Suppose that you are trying to find the number of permutations of $\{1, 2, 3, 4, 5\}$ that satisfy a certain condition. You know that there are $5! = 120$ total permutations to begin with, so your answer had better be no more than 120. Can you give a lower bound for the correct answer? Can you approximate what the correct answer should be? Does your proposed solution come close to this approximation?

7. **Determine a plan of attack.** Depending on the type of statement that you are trying to prove, you may try one of the following techniques: example/counterexample, direct proof, proof by contrapositive, proof by contradiction, proof by cases or proof by induction. See the section on "Methods of Proof" for specific examples regarding each of them methods.

8. **Implement.** Start writing up your proof based on the method you selected. Can you see how to complete the proof? Start combining the pieces of information to gather new information. Don't give up too easily. These things take time. If you can't see how to complete the proof, you might try working backwards. You know what the last line of your prove should be. What are some possible next-to-last lines? Can you see how to get to this next-to-last line?

   If all else fails, you may need to consider a different method of proof. And if no other method is working for you, you may have to reconsider your solution and select a new plan of attack.

9. **Can you simplify your proof/solution?** Make sure that you haven't repeated yourself anywhere and/or included any irrelevant information. Does your final answer simplify at all? If so, perhaps the simplified version suggests an easier way to solve the problem.

10. **Have you answered the question?** Double check to make sure that you have answered all parts of the problem. Does your final answer agree with the data you previously collected? Can you think of another way to do the problem? If you can, you should get the same answer. Do you?

3 Writing a Proof

The following is a list of things to keep in mind when writing your proof.

1. **Clearly state what you are going to prove and what method of proof you will to use.** It makes it much easier for the reader to follow along if they have some sense of the direction in which they are headed.

2. **Make sure each statement follows logically from the previous.** If you expect the reader to follow along, each statement should be an immediate consequence of the previous statement. Ultimately, by the time someone has finished reading your solution, they should know what the statement of the problem was.

3. **Say precisely what you mean and mean precisely what you say.** Be very careful in how you phrase each sentence. Use proper terminology. Many times there is a strong urge to paraphrase the statement of a definition or theorem. In the beginning, try to resist that urge until you truly understand it. Definitions and theorems are worded very precisely and hence changing one word could easily change its meaning and/or validity.

4. **Use complete sentences and correct grammar.** Writing a mathematical paper is no different from writing any other type of document. You should treat mathematical statements or symbols as if they were written in English. Make sure that when read, your statements involving mathematical formulas and symbols are in fact sentences.

5. **Define your notation.** If you introduce any new notation, you must define it. Even if you think it's clear from the context what your notation means, you cannot assume that it will be clear to the reader. Do not define new notation that conflicts with notation already established in class or in the text.

6. **Use examples appropriately.** During your proof, you may decide to introduce some new notation, make a definition, or describe an algorithm. If you are finding it difficult to describe precisely what you mean, an example can be a valuable tool to get your point across. However, never use an example as a substitute for a formal definition or proof.

7. **Never assume what you are trying to prove.** In your proof, restrict yourself to writing statements that you know to be true. These can be statements that are valid assumptions from the problem and/or the method of proof or statements that you have previously explained.

   For example: if you want to show that $(n+1)^2 - 1 = n(n+2)$, do not use the following technique:

   $$\begin{aligned} (n+1)^2 - 1 &\stackrel{?}{=} n(n+2) \\ (n^2+2n+1) - 1 &\stackrel{?}{=} n^2+2n \\ n^2+2n &\stackrel{?}{=} n^2+2n \end{aligned}$$

   but instead

   $$\begin{aligned} (n+1)^2 - 1 &= (n^2+2n+1) - 1 \\ &= n^2+2n \\ &= n(n+2) \end{aligned}$$

   In other words, start with one side of the equality, and show how to transform it into the other side. Not only does this look nicer, but each line corresponds to one algebraic manipulation, and thus makes it easier for the reader to follow or for you to further explain each step.

8. **The best way to prove something may not be the way you discovered it.** Your proof need not be a retelling of the way you happened upon the answer. While it's good to motivate each step and show the reader how they could have discovered the answer themselves, often times this can lead to a longer and more complicated proof than warranted.

9. **Conclude your proof with the vary statement you were trying to prove.** Do not leave the reader hanging. Let the reader know that you have arrived at the statement you were trying to prove and that you are now ready to move on to the next challenge.

4 Methods of Proof

4.1 Example/Counterexample

Many statements involving universal and/or existential quantifiers such as "for all" or "there exists" can be proved or disproved in a very straight forward manner. For example, the statement

$$\textit{there exists an } x \textit{ such that } p(x) \textit{ is true}$$

can be proved by giving a single value of x such that $p(x)$ is true.

Example: There exists integers x and y such that $23x + 15y = 1$

Proof: Let $x = 2$ and $y = -3$. Clearly $23 \cdot 2 + 15 \cdot -3 = 46 - 45 = 1$.

□

Notice that $x = -13$ and $y = 20$ also work, however all we had to do was present one such solution. In fact, there are infinitely many solutions. Can you describe them all?

Similarly, a statement of the form *for all x, $p(x)$ is true* can be disproved by giving one specific counterexample. In other words, the negation of the previous statement is *there exists an x such that $p(x)$ is not true.*

Example: For all integers x, a and b, if x divides ab then x divides a or x divides b.

Counterexample: Let $x = 6$, $a = 2$ and $b = 3$. Notice that 6 divides 2×3 however it does not divide 2 nor does it divide 3.

□

4.2 Direct Proof

A direct proof is used to prove any statement of the form

$$\textit{for all } x \in X \textit{ if } p(x) \textit{ is true then } q(x) \textit{ is true.}$$

A direct proof is generally considered the most desirable and therefore when attempting to prove a statement of this form, a direct proof should be your first option. The usual form of a direct proof is to let x be an arbitrary element of X, assume that $p(x)$ is true and through a series of logical deductions, conclude that $q(x)$ must also be true.

Example: Let x and y be integers. Show that if $x + y$ is even then $x - y$ is even.

Proof: Let x and y be arbitrary integers and assume that $x + y$ is even. That is, there exists an integer n such that

$$x + y = 2n.$$

Therefore

$$x - y = x + y - 2y = 2n - 2y = 2(n - y).$$

In other words, $x - y$ is even. □

Note that a statement of the form *p if and only if q* should be treated as *if p then q* and *if q then p*, which is known as the *converse* of *if p then q*.

4.3 Contrapositive

The contrapositive can also be used to prove statements of the form

$$\textit{for all } x \in X \textit{ if } p(x) \textit{ is true then } q(x) \textit{ is true.}$$

In this case however, one assumes that $q(x)$ is false and through a series of logical deductions, concludes that $p(x)$ must also be false. In other words, we are proving the statement *if* $q(x)$ *is false then* $p(x)$ *is false* using a direct proof. This is valid since *if p then q* is logically equivalent to *if not q then not p*.

Example: Let x,y and z be positive integers. If $x^2 + y^2 = z^2$ then at least one of x, y or z is even.

Proof: Let x, y and z be arbitrary odd integers. Then x^2, y^2 and z^2 are all odd as well. However $x^2 + y^2$ must be even since it is the sum of two odd integers. Therefore $x^2 + y^2 \neq z^2$.

□

4.4 Contradiction

A proof by contradiction is generally used when all other methods of proof have failed. It can be used to prove any statement, call it p. The idea is to assume that p is false and through a series of deductions, conclude something which is obviously false (this being the contradiction). Since p must be either true or false, and assuming p to be false leads to a contradiction, we must conclude that p is true.

Example: $\sqrt{2}$ is irrational.

Proof by contradiction: Assume that $\sqrt{2}$ is rational. Therefore there exists integers a and b such that

$$\sqrt{2} = \frac{a}{b}$$

where a and b do not have any factors in common. (If they do have a factor in common, say d, then $a = a'd$ and $b = b'd$ and $a/b = a'/b'$. In other words, we could use a' and b' instead of a and b.) Squaring both sides reveals that

$$2 = \frac{a^2}{b^2}$$

or $a^2 = 2b^2$. Now consider the number of factors of 2 in a^2. If a is even, then a^2 must be a multiple of 4. But since a and b do not have any factors in common, b must be odd and thus $2b^2$ is not a multiple of 4. Therefore $a^2 \neq 2b^2$, which contradicts our statement above. On the other hand, if a is odd, then a^2 is odd and is not a multiple of 2, but clearly $2b^2$ is a multiple of 2. Again, this implies that $a^2 \neq 2b^2$, which is a contradiction. Therefore, no such integers a and b exist, and thus $\sqrt{2}$ is irrational. □

Note that the negation of a statement of the form *if p then q* is

$$p \textit{ and not } q.$$

For example, the negation of the statement "If I have enough money then I will buy an ice cream cone" is "I have enough money and I'm not going to buy an ice cream cone."

4.5 Cases

It many instances, proving a statement in one fell swoop can be a bit much. Sometimes it can be worthwhile to break up your proof into several cases, where further assumptions may help prove the individual cases. Additionally, different methods of proof can be used in each case. Notice that in the proof that $\sqrt{2}$ is irrational, we considered the cases where a was even and where a was odd.

Example: For all integers n, $3n^4 + 2n^3 + n$ is divisible by 6.

Proof by cases: First we point out that

$$3n^4 + 2n^3 + n = n(n+1)(3n^2 - n + 1).$$

This done, we will consider the following cases depending on which number between n and $n+5$ is divisible by 6. Note that for any n, exactly one of these numbers must be divisible by 6.

Case 1 - n or $n+1$ is divisible by 6: If n or $n+1$ is divisible by 6 then clearly $3n^4 + 2n^3 + n$ is divisible by 6 since n and $n+1$ divide $3n^4 + 2n^3 + n$.

Case 2 - $n+2$ is divisible by 6: If $n+2$ is divisible by 6, then $n+2 = 6m$ for some integer m. Thus $n = 6m - 2$ is divisible by 2 and

$$3n^2 - n + 1 = 3(6m-2)^2 - 6m + 3 = 3((6m-2)^2 - 2m + 1)$$

is divisible by 3. Therefore $3n^4 + 2n^3 + n$ is divisble by both 2 and 3, and thus divisible by 6.

Case 3 - $n+3$ is divisible by 6: If $n+3$ is divisible by 6, then $n+3 = 6m$ for some integer m. Thus $n = 6m - 3$ is divisible by 3 and $n+1 = 6m - 2$ is divisible by 2. Therefore $3n^4 + 2n^3 + n$ is divisble by both 2 and 3, and thus divisible by 6.

Case 4 - $n+4$ is divisible by 6: If $n+4$ is divisible by 6, then $n+4 = 6m$ for some integer m. Thus $n = 6m - 4$ is divisible by 2 and $n+1 = 6m - 3$ is divisible by 3. Therefore $3n^4 + 2n^3 + n$ is divisble by both 2 and 3, and thus divisible by 6.

Case 5 - $n+5$ is divisible by 6: If $n+5$ is divisible by 6, then $n+5 = 6m$ for some integer m. Thus $n+1 = 6m - 4$ is divisible by 2 and

$$3n^2 - n + 1 = 3(6m-5)^2 - 6m + 6 = 3((6m-5)^2 - 2m + 2)$$

is divisible by 3. Therefore $3n^4 + 2n^3 + n$ is divisble by both 2 and 3, and thus divisible by 6.

Notice that in each case, $3n^4 + 2n^3 + n$ is divisible by 6, as claimed.

□

4.6 Mathematical Induction

Mathematical induction is used to prove statements of the form

$$\textit{for all } n \geq a,\ p(n).$$

A proof by induction consists of two steps. First, the *Base Step* shows that $p(a)$ is true. Second, the *Inductive Step* is where we will prove the statement *if* $p(n)$ *is true then* $p(n+1)$ *is true.* We will typically use a direct proof to prove this statement. The assumption that $p(n)$ is true is called the *inductive hypothesis.*

Example: For all $n \geq 1$, $3n^4 + 2n^3 + n$ is divisible by 6.

Proof: We will proceed by induction on n.
Base Step: $n = 1$

$$3 + 2 + 1 = 6$$

which is clearly divisible by 6.
Inductive Step: Assume that $3n^4+2n^3+n$ is divisible by 6. We will show that $3(n+1)^4+2(n+1)^3+(n+1)$ is also divisible by 6.

$$\begin{aligned} 3(n+1)^4 + 2(n+1)^3 + (n+1) &= 3n^4 + 14n^3 + 24n^2 + 19n + 6 \\ &= (3n^4 + 2n^3 + n) + (12n^3 + 24n^2 + 18n + 6) \\ &= (3n^4 + 2n^3 + n) + 6(2n^3 + 4n^2 + 3n + 1) \end{aligned}$$

Notice that each term is clearly divisible by 6. The first term is divisible by 6 by the inductive hypothesis and the second term is divisible by 6 since it is written as $6 \times m$ for some integer m. Therefore $3(n+1)^4 + 2(n+1)^3 + (n+1)$ is divisible by 6 since it is the sum of two numbers that are each divisible by 6.

□

It is crucial that at some point in the inductive step you use the inductive hypothesis. If you find that you didn't use the inductive hypothesis, then either your proof is incorrect or a proof by induction was not appropriate.