UT Martin's Minimal Proof Outlines

Department of Mathematics and Statistics

Abstract

The goal of this work is to provide a minimal agreed upon framework for proofs in our classes at UT Martin. Proofs written by different authors are not all the same, but there are minimal requirements for each type of proof.

1. Introduction

It is neither possible, nor desirable, to give outlines for proofs that should always be followed verbatim. However, it is both possible and desirable to give outlines which specify the minimum elements we seek in a proof. This is especially important as we evaluate proofs to assess our student learning objectives.

Notes:

1. You must indicate the beginning of your proof with the word **Proof.**; then clearly indicate the end with a symbol such as a square □ or a black square ■. (Some teachers might accept proofs which end with an appropriate Latin abbreviation such as QED and RAA.)

2. Parts of the outlines that are suggested, but not required by all teachers, are shown like this. These parts are more likely to be required in the lower level courses (such as Math 314), and will commonly be omitted by established provers (e.g., in Math 472 and Math 482).

3. Proofs are written to be read—this means that you should use correct capitalization, grammar, punctuation and spelling. In proofs, equations are part of the sentences in the narrative, so correct mathematical notation and correct punctuation should be used with equations also.

4. This is *not* a document on how to prove (take Math 314 to learn that).

5. A basic rule of life is "do it the way the boss wants." In class, always write proofs the way your teacher wants.

6. Some of the example proofs may be inconsistent with the definitions, theorems, etc., provided in the textbook you are using for a particular class. If in doubt, ask your teacher.

2. The four basic types of proof

In this section we will discuss the four proof types we test as part of our program assessment. For each type we first give a brief outline and example, followed by notes about these outlines. Always read the notes after the proof outlines.

In these proof outlines, the exact words are unimportant. A direct proof of "P implies Q" might start with "Assume P," "Suppose that P is true," "Given that P is true, . . . ". What is important is that you start with P, then work directly to Q.

2.1. Direct proof

A. Outline

Theorem 2.1. *If P, then Q.*

Proof. Suppose P.

$\vdots$

Therefore Q, completing the proof. ☐

B. Example

Theorem 2.2. *If a, b and c are integers and a divides b, then a divides bc.*

Proof. Suppose a, b and c are integers and a divides b; then by the definition of divides, there is an integer d such that $b{=}ad$. So it follows that $bc{=}(ad)c{=}a(dc)$. Since dc is an integer (closure), this shows a divides bc (definition of divides), completing the proof. ☐

C. Notes

1. The basic idea is very simple: start by assuming P, then without any additional assumptions, consecutively show a sequence of statements that end with Q.
2. In beginning proof classes, "Let P be as in the statement of the theorem" is not a sufficient start—restate the hypothesis. Sometimes, in senior level courses when the list of hypotheses is long, we skip this. Always follow your teacher's lead.
3. Notice that the heart of the proof is just given by the dots $\vdots$ above. These outlines just list minimal elements that a student proof must have to be considered correct. In the same way that two disconnected wings and a tail do not make a bird, several improperly connected statements do not make a proof.

2.2. Proof by contrapositive

A. Outline

Theorem 2.3. *If P, then Q.*

Proof. For proof by contraposition, suppose not Q.

$\vdots$

Therefore not P; completing the proof. ☐

B. Example

Theorem 2.4. *Let n be an integer. If n^2 is odd, then n is odd.*

Proof. For proof by contraposition, suppose n is an even integer. By the definition of even, $n = 2k$ for some integer k. It follows that

$$n^2 = (2k)(2k) = 2(2k^2),$$

so n^2 is even (by definition of even). This completes the proof. ☐

C. Notes

1. Contraposition can only be used on implications.

2.3. Proof by contradiction

A. Outline

Theorem 2.5. *P.*

Proof. For proof by contradiction suppose not P.

$\vdots$

Therefore C and not C; completing the proof. □

B. Example

Theorem 2.6. *Every integer greater than one has a prime divisor.*

Proof. For proof by contradiction, suppose there are positive integers, greater than one, with no prime divisors. By the well ordering principle, there must be a least such integer, call it n. If n is prime, then n is divisible by a prime (itself). Otherwise it is composite, so may be written as a product $n = ab$ where a, b are integers with $1 < a < n$. Since n is the least number not divisible by a prime, a must be divisible by a prime; but then that prime also divides $n = ab$ (transitivity property of divides). Either way, n is divisible by a prime which contradicts the choice of n. This contradiction completes the proof. □

C. Notes

1. If the statement is conditional, e.g., 'If P, then Q', then the proof starts 'Suppose P and not Q.'
2. Statement C is a statement that follows directly from P (and on rare occasions is P). For example, to prove that $\sqrt{3}$ is irrational, we assume it is rational, so there are relatively prime integers p and q for which $\sqrt{3} = p/q$. It is the statement that p and q are relatively prime that gets contradicted.
3. You must mention proof by contradiction at some point in the theorem. In lower level courses, it is common to mention proof by contradiction both at the beginning and at the end of the proof.

2.4. Proof by Induction

A. Outline

Theorem 2.7. *$P(n)$ is true for positive integers n.*

Proof. Note ... show $P(1)$ is true.

For proof by induction, suppose there is an integer k for which $P(k)$ is true.

$$\vdots$$

Therefore $P(k+1)$ is true. It follows by induction that $P(n)$ is true for all positive integers n. □

B. Example

Theorem 2.8. $(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)\cdots(2^{2^n}+1) = 2^{2^{n+1}}-1$ *for all non-negative integers n.*

Proof. Since $2^0=1$ and $2^1=2$, it follows that $2^{2^0}+1 = 2^{2^1}-1$, so the result is true for $n=0$.

For proof by induction, suppose there is an integer k for which

$$(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)\cdots(2^{2^k}+1) = 2^{2^{k+1}}-1$$

is true. Multiply both sides of this equation by $2^{2^{k+1}}+1$ to get

$$\begin{aligned}(2^{2^0}+1)\cdots(2^{2^k}+1)(2^{2^{k+1}}+1) &= (2^{2^{k+1}}-1)(2^{2^{k+1}}+1)\\ &= (2^{2^{k+1}})^2-1\\ &= 2^{2^{k+1}\cdot 2}-1.\end{aligned}$$

This shows the result is also true for the integer $k+1$:

$$(2^{2^0}+1)\cdots(2^{2^k}+1)(2^{2^{k+1}}+1) = 2^{2^{k+2}}-1,$$

and completes the proof by induction. □

C. Notes

1. Induction proofs vary in style more than the other types. However, the proof must indicate it is a proof by induction at some point. This is often done as the first line, instead of after the basis (or base) case, as was done in the outline.
2. It is not necessary for n to be changed to k in the induction step, but it is absolutely necessary to make it clear the induction step is an existence assumption. Make sure you understand this distinction between "there exists" and "for every" because we *never* assume what we are proving!
3. The first step, the basis (or base) case, should cover the first case (whether it be 1 as in the outline or 0 as in the example). Some proofs require multiple basis cases—do what is necessary.
4. For proof by strong induction, modify the induction step to read "For proof by induction, suppose there is an integer k for which $P(m)$ is true for $1 \le m \le k$."