Proof Strategies

MATH 24 — SPRING 2014

This document is designed to expose you to a variety of proof techniques. The margins are set wide to make it easier for you to take notes as you read. You will find some useful reading notes and pointers in the right margin.

As you read, pay attention to the structure of the statements and how that structure impacts their associated proofs. Here are a few structural features to look for:

- A *conjunction* is a compound statement of the form 'A and B' or any phrase that asserts that two (or more) given statements hold.
- A *disjunction* is a compound statement of the form 'A or B' or any phrase that asserts that at least one of two (or more) given statements hold.
- A *negation* is a statement of the form 'not A', 'it is not the case that A', or any phrase that denies a given statement.
- An *implication* is a compound statement of the form 'if A then B', 'A entails B', 'B whenever A', or any phrase that asserts that one statement is a logical consequence of another statement.
- An *equivalence* is a compound statement of the form 'A if and only if B', 'A exactly when B', 'A is necessary and sufficient for B', or any phrase that expresses that two (or more) given statements are logically equivalent to each other.

The majority of mathematical theorems are implications of the form 'if A then B'. However, the hypothesis A and the conclusion B are often compound statements. For example, the statement of Theorem 10 has the form 'if A then B and C'.

The basic method for proving an implication 'if A then B' is by *direct deduction*:

> First assume A.
> Then do some logical reasoning steps until you reach the conclusion that B holds.
> Conclude that if A then B.

As you will soon see, this is by no means the only way to prove an implication. The structure of A and B gives key clues regarding which method to use, so pay close attention how the structure of A and B leads to different styles of proof.

The most subtle proof method you will encounter here is when proving a negative 'not A'. The basic method for proving negative statements is by *contradiction*:

> First assume A.
> Then do some logical reasoning steps until you reach a contradictory conclusion.
> Conclude that not A.

The contradictory conclusion can be anything that is blatently false or that contradicts a fact you already established.

DEFINITION 1. An integer n is *even* if there is an integer m such that $n = 2m$.

The term being defined is usually typeset in a way that makes it stand out.

DEFINITION 2. An integer n is *odd* if there is an integer m such that $n = 2m + 1$.

THEOREM 3. *Suppose m and n are integers. If m is even then mn is also even.*

The first sentence of a theorem often serves to explain what kind of objects the variable symbols stand for.

Proof. To say that m is even means that there is an integer m such that $m = 2k$. After multiplying both sides by n, we obtain

$$mn = 2kn.$$

The first step of a proof is often to expand definitions, in this case the definition of 'even'.

Since kn is an integer, follows that mn is even. Therefore, if m is even then so is mn. □

The last step of a proof should match the conclusion of the theorem.

THEOREM 4. *Suppose m and n are integers. If m and n are both odd, then mn is odd.*

Proof. To say that m is odd means that there is an integer k such that $m = 2k + 1$; similarly, to say that n is odd means that there is an integer ℓ such that $n = 2\ell + 1$. In this case,

$$mn = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1,$$

or

$$mn = 2(2k\ell + k + \ell) + 1.$$

Notice how the use of parentheses clarifies the key step in this proof.

Since $2k\ell + k + \ell$ is an integer, it follows that mn is odd. Therefore, if m and n are both odd then so is mn. □

AXIOM 5 (Archimedean Property of the Real Numbers). *For every real number x there is an integer n such that $n \le x < n + 1$.*

An axiom is a basic assumption that we believe without proof. The properties (VS 1–8) of vector spaces are often called axioms since they are the basic assumptions that define vector spaces.

THEOREM 6. *Every integer is either even or odd.*

Proof. Let n be an arbitrary integer. By the Archimedean Property, there is an integer m such that

$$m \le \frac{n}{2} < m + 1.$$

The keyword 'arbitrary' means that we are not making any special assumptions about n.

Multiplying through by 2, we find that

$$2m \le n < 2(m + 1) = 2m + 2.$$

There are only two integers in the interval $[2m, 2m+2)$, namely $2m$ and $2m + 1$. Because n is an integer, we must either have $n = 2m$ and hence n is even, or have $n = 2m + 1$ and hence n is odd. Since n is an arbitrary integer, we conclude that every integer is either even or odd. □

Note that the proper use of punctuation is essential to properly parse this.

Theorem 7. *No integer is both even and odd.*

Proof. Suppose, for the sake of contradiction, that there is an integer n which is both even and odd. To say that n is even means that there is an integer p such that $n = 2p$; to say that n is odd means that there is an integer q such that $n = 2q + 1$. We then have

$$2p = 2q + 1,$$

or

$$2(p - q) = 1.$$

The phrase 'for the sake of contradiction' indicates that we are proving a negative and what follows is a contradictory assumption.

Since $p - q$ is an integer, we conclude that 1 is an even integer! This is a contradiction, so our assumption that there is an integer which is both even and odd must be false. □

An exclamation point is a good way to indicate that we have reached a contradiction.

Theorem 8. *An integer is odd if and only if it is not even.*

The phrase 'if and only if' is a very common way of expressing the equivalence of two statements. To prove an equivalence one must prove both the forward and the backward implications.

Proof. Let n be an integer. We must show that (a) if n is odd then n is not even and, conversely, that (b) if n is not even then n is odd.

For (a), suppose that n is odd. To see that n is not even, suppose instead that n is even. This contradicts Theorem 7, which says that n cannot be both even and odd. Therefore, if n is odd then n is not even.

The keyword 'instead' is a quick way to indicate that we are proving a negative and what follows is a contradictory assumption.

For (b), suppose that n is not even. By Theorem 6, either n is odd or n is even. Since n is not even, it must be that n is odd. Therefore, if n is not even then n is odd. □

Corollary 9. *An integer is even if and only if it is not odd.*

A corollary is an immediate consequence of a theorem whose proof is left to the reader.

Theorem 10. *Suppose m and n are integers. If mn is odd then m and n are both odd.*

Proof. We will prove the contrapositive: if m and n are not both odd then mn is not odd. By Corollary 9, to say that mn is not odd is the same as saying that mn is even. To say that m and n are not both odd is the same as saying that at least one of m and n is even. So, another way to state the contrapositive is: if m or n is even then mn is even.

The contrapositve of an implication 'if A then B' is 'if not B then not A'. The contrapositive is always logically equivalent to the original implication.

We prove this by cases:

- On the one hand, if m is even then mn is even by Theorem 3.

- On the other hand, if n is even then $mn = nm$ is even by Theorem 3.

Either way, we reach the conclusion that mn is even. Therefore, if m or n is even then mn is even. □

LEMMA 11. *An integer n is even if and only if its square n^2 is even.*

A lemma is a theorem with a very specialized purpose. This particular lemma will be used twice in Theorem 12 but it is of little interest on its own.

Proof. We must show that (a) if n is even then n^2 is also even and, conversely, that (b) if n^2 is even then n is also even.

Part (a) follows directly from Theorem 3 with $m = n$.

For part (b), we will prove the contrapositive: if n is not even then n^2 is also not even. By Theorem 8, another way to state the contrapositive is that: if n is odd then n^2 is also odd. This follows directly from Theorem 4 with $m = n$. □

THEOREM 12. *$\sqrt{2}$ is an irrational number.*

Note that an irrational number is one that is not rational, so this is a disguised negative statement.

Proof. Suppose, for the sake of contradiction, that $\sqrt{2}$ is a rational number. Say

$$\sqrt{2} = \frac{p}{q},$$

where p and q are integers with no common factors.

We're expanding the definition of rational number as well as the fact that fractions can always be reduced in such a way that the numerator and denominator have no common factors.

Squaring both sides of the above equality, we obtain

$$2 = \frac{p^2}{q^2}$$

or equivalently

$$2q^2 = p^2.$$

Since q^2 is an integer, we see that p^2 is an even integer. By Lemma 11, it follows that p is also even. Therefore, there is an integer r such that $p = 2r$.

Substituting $p = 2r$ in $2q^2 = p^2$, we see that

$$2q^2 = 4r^2$$

or, after dividing both sides by 2,

$$q^2 = 2r^2.$$

Since r^2 is an integer, we see that q^2 is an even integer. Since q^2 is even, it follows from Lemma 11 that q is also even. But p and q have no common factors, so they cannot both be even!

This is a contradiction, so we conclude that our original assumption that $\sqrt{2}$ is a rational number must have been false and therefore that $\sqrt{2}$ is an irrational number. □

Discussion

As you have observed, different types of statements lead to different types of proofs. There are no fixed rules or magic recipes for writing proofs but here are some helpful observations.

As mentioned in the introduction, many mathematical statements are implications of the form 'if A then B' (and variations). The most common way to prove such is by *direct deduction*:

> First assume A holds.
> Then do some logical reasoning steps until you reach the conclusion that B holds.
> Conclude that if A then B.

Another common method to prove 'if A then B' is to prove the contrapositive 'if not B then not A' instead. This method was used to prove Theorem 10 and part (b) of Lemma 11. A variation on proving the contrapositive is *indirect deduction*:

> First assume B fails (i.e. not B).
> Then do some logical reasoning steps until you reach the conclusion that A also fails.
> Conclude that if A then B.

Note that this is essentially direct deduction of the contrapositive, only the conclusion is the direct implication 'if A then B' rather than the contrapositive 'if not B then not A'.[1]

When an implication 'if A then B' has a compound hypothesis A or a compound conclusion B, then you get different refinements of the basic strategies. Conjunctions ('and') are typically easy to handle:

- If a conjunction occurs in a hypothesis 'if A and B then C' (as in Theorem 4) then you simply have two assumptions A and B to break down at the start of the proof.
- If a conjunction occurs in a conclusion 'if A then B and C' then you really have two facts to prove: 'if A then B' and 'if A then C'.

Disjunctions ('or') tend to be trickier:

- If a disjunction occurs in a hypothesis 'if A or B then C', cover all cases and prove both 'if A then C' and 'if B then C'. The reason is that while you know one of A and B is true, you don't know which one. By giving two proofs, one for each case, you know that one of them will work and reach the desired conclusion.
- If a disjunction occurs in a conclusion 'if A then B or C', the most common proof strategy is to assume that one of the two fails and use that (together with the hypothesis A) to derive the other conclusion. In other words, you can either prove 'if A and not B then C' or prove 'if A and not C then B' (your choice!).[2]

As a general alternative to the above, consider using the contrapositive. Taking a negative of a conjunction and a disjunction has an interesting effect, known as the *De Morgan Laws*:

'not (A and B)' is logically equivalent to '(not A) or (not B)'

[1] If you use the contrapositive or indirect deduction, remember to announce this ahead of time. Starting a proof of an implication by denying the conclusion, is an incredibly bold move! Be nice to the reader, this is not an action movie!

[2] If you use this method, remember to announce this ahead of time and explain which path you're choosing. You don't want to confuse the reader with a seemingly random assumption.

‘not (A or B)’ is logically equivalent to ‘(not A) and (not B)’

In other words, negation transforms conjunctions into disjunctions and vice versa! This is what happened in Theorem 10. The original statement is of the form ‘if A then B and C’ (where A is ‘mn is odd’, B is ‘m is odd’, C is ‘n is odd’) and we decided to prove the contrapositive ‘if not (B and C) then not A’. The first paragraph of the proof explains how ‘not (B and C)’ is the same as ‘(not B) or (not C)’, which is the first De Morgan Law. In the end we proved a statement of the form ‘if $\bar{\mathrm{B}}$ or $\bar{\mathrm{C}}$ then $\bar{\mathrm{A}}$’ (where $\bar{\mathrm{A}}$ is ‘mn is even’, $\bar{\mathrm{B}}$ is ‘m is even’, $\bar{\mathrm{C}}$ is ‘n is even’), for which we used a proof by cases as described above.

Negations are the trickiest of all. You may have heard the saying that “you can’t prove a negative” or “there is no evidence for absence.” While this is not the case, it is true that it can be very difficult to prove a negative. As mentioned in the introduction, the main strategy for proving a negative ‘not A’ is called *proof by contradiction*[3]

> First assume A.
> Then do some logical reasoning steps until you reach a contradictory conclusion.
> Conclude that not A.

In other words, to prove not A you need to prove that A is impossible since it leads to conclusions that are known to be false. Note that such a proof strategy is always an option since any statement A is logically equivalent to ‘not not A’, but since proofs by contradiction tend to be more difficult, it is often a good idea to first try a more direct method before this one.

Theorem 7 and Theorem 12 are both examples of proofs of negative statements. (Note that Theorem 12 is a slightly disguised negative since the negative is part of the word ‘irrational’, which is just another way of saying ‘not rational’.) The difficulty in these proofs is that the contradictory conclusion can be anything! In Theorem 7 the contradictory conclusion is ‘1 is even’, which is obviously false, and in Theorem 12 the contrary conclusion is that ‘p and q are even numbers with no common factors’, which is impossible since two even numbers always have the common factor 2. There is no way to predict what this contradictory conclusion will be just by looking at the statement of the theorems. Proofs of negatives always require a certain amount of insight, creativity, or just plain luck to see what the contradictory conclusion will be. Because there is no magic recipe for this, proofs of negatives are consistently more difficult than others…

Of course, this is not the end of the story for proofs, a lot of other ingredients go into the deductive steps in a proof. While the above discussion applies to any mathematical topic, these extra ingredients are generally specific to each topic. In Math 24, we will learn a lot of tools and techniques that are specific to linear algebra. In later courses, you will learn tools and techniques that are specific to other fields. However, the basic proof methods of proof that we just discussed as well as other general methods that we will discuss later in the course will follow you throughout your mathematical career. In fact, since the tools of linear algebra is used in almost all branches of mathematics, everything you learn in Math 24 will be useful for you later on!

[3] Needless to say, you should always give a clue that you are doing this. Starting a proof of ‘not A’ by assuming A sounds plainly wrong if you don’t know that this is a proof by contradiction.