Reading and Writing Proofs

Linear Algebra with Applications

Jeffrey Holt

Some taking a linear algebra course have little experience with formulating proofs. Since courses taught using *Linear Algebra with Applications* incorporate varying degrees of emphasis on proofs, this document is an attempt to fill the experience gap. I have not tried to give a complete treatment of proof-writing — there are a number of good books and numerous internet resources available if you want something more extensive. But I hope that this provides enough of an introduction to be useful.

Most of the focus here is on writing proofs, which is more challenging than reading proofs. But careful reading of proofs is also important and informative. Some text exercises call for a proof that is a modest modification of a proof already in the book, so there can be a direct benefit to studying text proofs. Beyond that, working to understand each step in the text proofs can serve as a guide for other proofs that you are asked to write, and will give you a better general sense of how proofs are constructed. As you read through the text, take the time to study the proofs — it will be worth your time!

Terminology

Below are a few mathematical terms that come up throughout the book (and other math books) that we will use regularly. These provide the organizational structure of the book.

Definition

In mathematics, *definitions* serve the same purpose they do in everyday language, to provide the specific meaning of words and phrases. The organization of linear algebra starts with definitions, with everything building from there. Here are several examples of definitions[1].

Definition 1 *The* ***integers*** *are the set of all positive and negative "counting numbers" together with 0,*

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Note: In what follows, each of k, m, n, and p will denote integers.

Definition 2 *An integer n is* ***even*** *if it can be expressed in the form $n = 2k$, where k is an integer.*

Note that an alternative definition of an even integer is that it ends in one of 0, 2, 4, 6, or 8. This may be more familiar, but turns out to be harder to work with so is less useful.

Definition 3 *An integer n is* ***odd*** *if it can be expressed in the form $n = 2k + 1$, where k is an integer.*

Definition 4 *An integer n is* ***prime*** *if its only positive integer divisors are 1 and n.*

Definition 5 *A 2×2 matrix A is* ***diagonal*** *if $A = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}$ for real a_1, a_2.*

[1]Many of the examples contained here are drawn from topics other than linear algebra, to make the discussion more self-contained.

Conjectures

A *conjecture* is a mathematical statement that has not yet been shown to be true or false. In this text there are "true or false" problems that ask for the reader to determine if each is true or false, and to provide justification for the response. The statements in each of these problems can be viewed as a conjecture. Below are three examples of conjectures.

Conjecture 1 *If m is even and n is odd, then $m+n$ is odd.*

Conjecture 2 *If $k \geq 0$, then $n = 2^{2^k} + 1$ is prime.*

Conjecture 3 *If A and B are 2×2 diagonal matrices, then the sum $A+B$ is also a 2×2 diagonal matrix.*

Mathematical theory is built up from statements that start as conjectures. To show that a statement is true, one must provide a rigorous mathematical proof that it is true for every possibility allowed by the statement. Thus, with respect to Conjecture 1, it is fine to note that

$$4+7=11, \qquad 14+9=23, \qquad \text{and} \qquad 24+13=37$$

all agree with the statement. However, this **does not prove** the statement. There are infinitely many possible combinations of an even integer m and an odd integer n, so we cannot individually check each of them. We need an general argument that applies to all possible combinations. More on this later.

Theorems

When a conjecture has been mathematically proved, it is promoted to the status of *theorem*. Theorems serve to state and organize mathematical results, including those in this book. Most theorems in this book have essentially one of two forms:

If-then Most of our theorems will have this form, which involve a *hypothesis* and a *conclusion*. For example,

> **Theorem**: If $p > 2$ is a prime number, then p is odd.

Here "$p > 2$ is a prime number" is the hypothesis and "p is odd" is the conclusion. When formulating a proof, we assume that the hypothesis is true, and from that assumption show that the conclusion must also be true.

Note that for this theorem, reversing the hypothesis and conclusion results in a statement that is not true:

> **False Statement**: If $p > 2$ is odd, then p is prime.

This shows that for some if-then theorems, reversing the order of hypothesis and conclusion produces a statement that is not true.

If-and-only-if Consider the following:

> **Theorem**: n is odd if and only if n^2 is odd.

The "if and only if" signals that this theorem is actually a combination of two "if-then" statements:

Statement 1: If n is odd, then n^2 is odd.

and the reverse

Statement 2: If n^2 is odd, then n is odd.

Both parts of an if-and-only-if theorem can play the role of the hypothesis, with the other part playing the role of the conclusion. In such cases, we sometimes say that the two parts are "equivalent" meaning that each follows from the other. To prove an if-and-only-if theorem, one must show that both "directions" (statements) are true.

Counterexamples

Although examples do not suffice to prove a conjecture is true, a single example is enough to show that a conjecture is false. Consider Conjecture 2, which states that $n = 2^{2^k} + 1$ is prime for $k = 0, 1, 2, \ldots$. Such numbers n are called *Fermat numbers* after Pierre de Fermat, a 17th century attorney and amateur mathematician who conjectured that numbers of this form are all prime. For the cases $0 \leq k \leq 4$ he was right, with

$$\begin{aligned}
k = 0 &\Rightarrow n = 2^{2^0} + 1 = 3 \quad \text{(prime)} \\
k = 1 &\Rightarrow n = 2^{2^1} + 1 = 5 \quad \text{(prime)} \\
k = 2 &\Rightarrow n = 2^{2^2} + 1 = 17 \quad \text{(prime)} \\
k = 3 &\Rightarrow n = 2^{2^3} + 1 = 257 \quad \text{(prime)} \\
k = 4 &\Rightarrow n = 2^{2^4} + 1 = 65537 \quad \text{(prime)}
\end{aligned}$$

However, in 1732 Leonhard Euler showed that

$$n = 2^{2^5} + 1 = 4294967297 = (641)(6700417)$$

so Conjecture 2 does not hold when $k = 5$.

In general, a *counterexample* is an example that shows a conjecture is not true. You only need one counterexample to disprove a conjecture. The above computation shows that $k = 5$ is a counterexample to Conjecture 2. (In fact, as of this writing it has been shown that $5 \leq k \leq 32$ are all counterexamples to Conjecture 2.)

Types of proofs

Below we outline the three main types that you are most likely to need to use, and give examples of each. As you read the book, pay attention to which type of proof is being used with each theorem. Also note that sometimes more than one method of proof is possible.

Throughout this section are "Tip"s that generally apply when writing proofs. Here is the first, which came up earlier:

Tip 1 *An example does not constitute a proof!*

That is, showing that a statement is true for a specific case does not show that it holds in general. Refer back to the discussion about Conjecture 1, and see Conjecture 2 for an example of the hazards of "proof by example."

The proofs in this book are shown in fairly efficient form, not in the way that they were originally conceived. Just like when writing an essay, writing a proof typically requires a rough draft. In the example proofs below, there will be included both "scratch work" (a form of rough draft) and the proof, which is the final version and the part that is actually turned in as homework or published.

Tip 2 *Use scratch work to figure out the required pieces of a proof, then write the final version of the proof.*

Direct proof

A *direct proof* is the most commonly used, and is typically the clearest, so is generally preferable when possible. This type of proof starts by assuming the statements in the hypothesis, and proceeds in a sequence of justified steps directly to the statement in the conclusion.

Theorem 1 *If m is even and n is odd, then $m+n$ is odd.*

Scratch work: When developing a proof, we need to know where we are starting, and where we want to go. It's almost always helpful to start with the definitions of the terms used in the hypothesis and conclusion. Referring back to the earlier definitions, we have

$$\begin{array}{lrcl} \text{Hypothesis:} & \text{“}m \text{ is even”} & \Longrightarrow & m = 2k_1 \text{ for some integer } k_1 \\ & \text{“}n \text{ is odd”} & \Longrightarrow & n = 2k_2 + 1 \text{ for some integer } k_2 \\ \text{Conclusion:} & \text{“}m+n \text{ is odd”} & \Longrightarrow & m+n = 2k_3 + 1 \text{ for some integer } k_3 \end{array}$$

Note that we use k_1, k_2, and k_3 to make it clear that these need not be the same integer. Combining the two parts of the hypothesis, we have

$$m+n = (2k_1) + (2k_2+1) = 2k_1 + 2k_2 + 1$$

To reach the conclusion, we need to show that $m+n$ has the form $2k_3+1$. It's clear that a bit of reorganizing will give us that,

$$m+n = 2k_1 + 2k_2 + 1 = 2(k_1+k_2) + 1$$

which shows that $m+n$ has the form $2k_3+1$ as required. Note that this argument works for *any* even m and odd n — no additional assumptions are made, so all possible cases covered by the hypothesis are included.

We're now ready for the proof.

Proof: Suppose that m is even and n is odd. Then $m = 2k_1$ and $n = 2k_2+1$ for some integers k_1 and k_2. Therefore

$$m+n = (2k_1) + (2k_2+1) = 2k_1 + 2k_2 + 1 = 2(k_1+k_2) + 1$$

Thus $m+n = 2k_3+1$ for some integer k_3, and hence $m+n$ is odd. ■

Tip 3 *Write down the definitions when starting scratch work for a proof.*

Theorem 2 *If A and B are 2×2 diagonal matrices, then so is $A + B$.*

Scratch work: Let's start again with definitions.

$$\begin{array}{lrcl} \text{Hypothesis:} & \text{“}A \text{ is a } 2 \times 2 \text{ diagonal matrix”} & \Longrightarrow & A = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \text{ for real } a_1, a_2 \\ & \text{“}B \text{ is a } 2 \times 2 \text{ diagonal matrix”} & \Longrightarrow & B = \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix} \text{ for real } b_1, b_2 \\ \text{Conclusion:} & \text{“}A + B \text{ is a } 2 \times 2 \text{ diagonal matrix”} & \Longrightarrow & A + B = \begin{bmatrix} c_1 & 0 \\ 0 & c_2 \end{bmatrix} \text{ for real } c_1, c_2 \end{array}$$

Matrix addition works by adding terms in corresponding entries (see Section 3.2), so that the two parts of the hypothesis gives us

$$A + B = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} + \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} (a_1 + b_1) & 0 \\ 0 & (a_2 + b_2) \end{bmatrix}$$

which is the required form. Note that the values of the entries does not matter, so this explanation holds for all cases covered by the hypothesis.

We're now ready for the proof.

Proof: Suppose that $A = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}$ and $B = \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}$ are 2×2 diagonal matrices. Then

$$A + B = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} + \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} (a_1 + b_1) & 0 \\ 0 & (a_2 + b_2) \end{bmatrix}$$

Hence it follows that $A + B$ is also a 2×2 diagonal matrix. ■

Indirect proofs

For an if-then statement, when the hypothesis is true, then either (a) the conclusion is true, or (b) the conclusion is false. Those are the only two possibilities. An *indirect proof*[2] starts by assuming that the hypothesis is true *and* the conclusion is false, then combines the two to arrive at a clear contradiction. This shows that the hypothesis being true cannot happen simultaneously with the conclusion being false, so when the hypothesis is true the only possibility remaining is for the conclusion to also be true.

Let's look at an example by proving a claim made earlier.

Theorem 3 *If $p > 2$ is a prime number, then p is odd.*

Scratch work: From the definitions,

$$\begin{array}{lrcl} \text{Hypothesis:} & \text{“}p > 2 \text{ is a prime number”} & \Longrightarrow & \text{the only positive divisors of } p \text{ are 1 and } p \\ \text{Conclusion:} & \text{“}p \text{ is odd”} & \Longrightarrow & p = 2k_1 + 1 \text{ for some integer } k_1 \end{array}$$

It is not easy to see how to get from the divisors of p being only 1 and p to $p = 2k_1 + 1$. But suppose that we try an indirect proof, which allows us to make the extra assumption that the conclusion is false:

[2] Also called a *proof by contradiction*.

Extra Assumption: p is *not* odd $\Longrightarrow$ p is even $\Longrightarrow$ $p = 2k_2$ for some integer k_2.

The extra assumption tells us that $p = 2k_2$, and since we know $p > 2$ it must be that $k_2 > 1$. Therefore 2 and k_2 are both divisors of p, which contradicts p being prime. Thus $p > 2$ being prime and p being even are incompatible, so it must be that p is odd.

We are ready for the proof.

Proof: Suppose that $p > 2$ is a prime number, and to the contrary[3] that p is even. Then $p = 2k_1$ for some integer k_1. Since $p > 2$, it must be that $k_1 > 1$ (otherwise $p = 2$). Hence 2 and k_1 are both divisors of p that are not equal to 1 or p. This implies that p is not a prime, contradicting the hypothesis. Therefore it must be that p is odd. ■

Tip 4 *Be careful not to accidentally assume that the conclusion of a statement is true when developing a proof.*

Theorem 4 *An integer n is odd if and only if n^2 is odd.*

Scratch work: Since this is an if-and-only-if theorem, we need to provide two proofs. One way to indicate this is with arrows $\Longrightarrow$ and $\Longleftarrow$ indicating the "direction" so that we can separate the hypothesis from the conclusion.

($\Longrightarrow$) Let's start with the definitions. For this direction, we have

Hypothesis: "n is odd" $\Longrightarrow$ $n = 2k_1 + 1$ for some integer k_1

Conclusion: "n^2 is odd" $\Longrightarrow$ $n^2 = 2k_2 + 1$ for some integer k_2

Since $n = 2k_1 + 1$, we have $n^2 = (2k_1 + 1)^2 = 4k_1^2 + 4k_1 + 1 = 2(2k_1^2 + 2k_1) + 1$. Thus n^2 has the form required to be odd, so a direct proof will work for this direction.

($\Longleftarrow$) For this direction, the role of hypothesis and conclusion reverse, so we have

Hypothesis: "n^2 is odd" $\Longrightarrow$ $n^2 = 2k_2 + 1$ for some integer k_2

Conclusion: "n is odd" $\Longrightarrow$ $n = 2k_1 + 1$ for some integer k_1

This time it is harder to proceed from $n^2 = 2k_2 + 1$ to saying something about the form of n, because the square root doesn't distribute as nicely as the square. Since a direct proof seems difficult, let's consider an indirect proof, adding the extra assumption that n is not odd, hence even.

Extra Assumption: n is even $\Longrightarrow$ $n = 2k_3 \Longrightarrow n^2 = (2k_3)^2 = 4k_3^2 = 2(2k_3^2)$

But this implies n^2 is even, contracting the hypothesis that n^2 is odd. Thus we see that an indirect proof will work.

We have all the required pieces for the proof.

Proof:
($\Longrightarrow$) Suppose that n is odd[4]. Then $n = 2k_1 + 1$ for some integer k_1. Thus

$$n^2 = (2k_1 + 1)^2 = 4k_1^2 + 4k_1 + 1 = 2(2k_1^2 + 2k_1) + 1$$

[3]The "to the contrary" signals to the reader that an indirect proof is coming.

[4]It is a good idea to clearly state the hypothesis for each direction so that the reader knows how the proof is organized.

so therefore n^2 is odd.

($\Longleftarrow$) Suppose that n^2 is odd, and to the contrary that n is even. Then $n = 2k_2$ for some integer k_2, and thus

$$n^2 = (2k_2)^2 = 4k_2^2 = 2(2k_2^2)$$

This implies n^2 is even, a contradiction. Therefore it follows that n is odd. ■

Induction

Proofs by *induction* are the most specialized considered here, and are used to prove statements that are indexed by positive integers. Here are two such statements:

Statement 1: If n is odd, then so is n^k for all $k \geq 1$.

Statement 2: $\displaystyle\sum_{m=1}^{k} m = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}$ for all $k \geq 1$.

Suppose that $S(k)$ denotes a mathematical statement indexed by the positive integer k. To use induction to prove that this statement is true for all such k, we have to verify two things:

Condition 1. That $S(1)$ is true.

Condition 2. If $S(k)$ is true, then $S(k+1)$ is also true.

Condition 1 shows that $S(k)$ is true when $k = 1$, and is usually not hard to verify. By Condition 2, since $S(1)$ is true, it follows that $S(2)$ is also true. Similarly, again by Condition 2, since $S(2)$ is true, it follows that $S(3)$ is also true. The same argument can be used again and again to show that $S(4)$, $S(5)$, ... are also all true.

A proof by induction requires that Condition 1 and Condition 2 be verified for a statement $S(k)$. Let's start with a silly application of induction. I like pizza, so much so that the following are true:

Claim 1. If I arrive at a party and pizza is available, I will always have a slice.

Claim 2. No matter how many slices of pizza I eat, I can always eat one more.

Now suppose that $S(k)$ denotes the statement "I can eat k pieces of pizza." We know that $S(1)$ is true due to Claim 1. Furthermore, by Claim 2 we know that if I have eaten k slices of pizza, I can always eat $k+1$ slices. Thus by induction, there is no limit to the number slices of pizza that I can eat. (The only constraint is the amount of pizza available.)

Now let's return to our previous statements.

Theorem 5 *If n is odd, then so is n^k for all $k \geq 1$.*

Scratch work: For this theorem, we set $S(k)$ be the statement "n^k is odd." Then $S(1)$ corresponds to "n is odd" which is exactly the hypothesis, thus is true.

Next we have to show that if $S(k)$ is true, then $S(k+1)$ is also true. This is an if-then statement, with

Hypothesis: "n^k is odd" (this is the *induction hypothesis*)

Conclusion: "n^{k+1} is odd"

We know n is odd (by the theorem hypothesis), so $n = 2k_1+1$. By the induction hypothesis, n^k is also odd so $n^k = 2k_2 + 1$. Thus

$$n^{k+1} = (n)(n^k) = (2k_1 + 1)(2k_2 + 1) = 4k_1k_2 + 2k_1 + 2k_2 + 1 = 2(2k_1k_2 + k_1 + k_2) + 1$$

which shows n^{k+1} is odd. This gives us all the pieces needed for the proof.

Proof: The proof is by induction[5]. For $k = 1$, $n^k = n$ which is odd by hypothesis, so the theorem holds for this case.

Now assume that the theorem holds for n^k, so that n^k is odd. (*This is the induction hypothesis.*) Since n is odd, we have $n = 2k_1 + 1$ for some k_1. Similarly, since n^k is odd, we have $n^k = 2k_2 + 1$ for some k_2. Therefore

$$n^{k+1} = (n)(n^k) = (2k_1 + 1)(2k_2 + 1) = 4k_1k_2 + 2k_1 + 2k_2 + 1 = 2(2k_1k_2 + k_1 + k_2) + 1$$

which shows n^{k+1} is odd. Thus by induction the theorem holds for all $k \geq 1$. ■

Theorem 6 $\displaystyle\sum_{m=1}^{k} m = \frac{k(k+1)}{2}$ *for all* $k \geq 1$.

Scratch work: This theorem also sets up well for induction. When $k = 1$, we have

$$\sum_{m=1}^{1} m = 1 \quad \text{and} \quad \frac{(1)(1+1)}{2} = 1$$

so the theorem holds in this case. For the second part of the induction proof, we start by assuming that $\sum_{m=1}^{k} m = \frac{k(k+1)}{2}$. The trick is to incorporate this information into the formula for the sum in the case $k + 1$, with the key being to note that we have the formula for the first k terms in the sum. Specifically,

$$\sum_{m=1}^{k+1} m = \left(\sum_{m=1}^{k} m\right) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

The last term at right is the formula when k is replaced by $k + 1$, so that is the last piece needed for the proof. (In fact, we pretty much have the proof. Just a little tidying is required.)

Proof: The proof is by induction. For $k = 1$, we have

$$\sum_{m=1}^{1} m = 1 \quad \text{and} \quad \frac{(1)(1+1)}{2} = 1$$

The sum matches the formula for $k = 1$, so the theorem holds in this case. Next assume the induction hypothesis, that $\sum_{m=1}^{k} m = \frac{k(k+1)}{2}$. Then

$$\begin{aligned}\sum_{m=1}^{k+1} m &= \left(\sum_{m=1}^{k} m\right) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}\end{aligned}$$

This confirms the formula for $k + 1$, and completes the proof. ■

[5]This explicit statement makes the method of proof clear.