An Introduction to Proof Techniques

Proof Technique: Direct Proof

EXAMPLE: Let $\mathbf{x}$ be a vector in $\mathbb{R}^n$. Prove that $\mathbf{x}\cdot\mathbf{x} = \|\mathbf{x}\|^2$.

Proof: Let $\mathbf{x} = [x_1, x_2, \ldots, x_n]$, then

$$\begin{aligned}
\mathbf{x}\cdot\mathbf{x} &= x_1x_1 + x_2x_2 + \ldots + x_nx_n \\
&= x_1^2 + x_2^2 + \ldots + x_n^2 \\
&= \left(\sqrt{x_1^2 + x_2^2 + \ldots + x_n^2}\right)^2 \\
&= \|\mathbf{x}\|^2 \quad \blacksquare
\end{aligned}$$

Working "Backward" to Discover a Proof

EXAMPLE: Let x_1, x_2, y_1, y_2 be any real numbers. Prove that

$$|x_1y_1 + x_2y_2| \le \sqrt{x_1^2 + x_2^2}\sqrt{y_1^2 + y_2^2}$$

Proof: We have

$$\begin{gathered}
|x_1y_1 + x_2y_2| \le \sqrt{x_1^2 + x_2^2}\sqrt{y_1^2 + y_2^2} \\
\Uparrow \\
\sqrt{(x_1y_1 + x_2y_2)^2} \le \sqrt{(x_1^2 + x_2^2)(y_1^2 + y_2^2)} \\
\Uparrow \\
(x_1y_1 + x_2y_2)^2 \le (x_1^2 + x_2^2)(y_1^2 + y_2^2) \\
\Uparrow \\
x_1^2y_1^2 + 2x_1y_1x_2y_2 + x_2^2y_2^2 \le x_1^2y_1^2 + x_1^2y_2^2 + x_2^2y_1^2 + x_2^2y_2^2 \\
\Uparrow \\
2x_1y_1x_2y_2 \le x_1^2y_2^2 + x_2^2y_1^2 \\
\Uparrow \\
0 \le x_1^2y_2^2 - 2x_1y_1x_2y_2 + x_2^2y_1^2 \\
\Uparrow \\
0 \le (x_1y_2 - x_2y_1)^2
\end{gathered}$$

"If A Then B" Proofs

Frequently, a theorem is given in the form "If A then B," where A and B represent statements. The entire "If A then B" statement is called an **implication**; A alone is the **premise**, and B is the **conclusion**.

EXAMPLE: Let $\mathbf{x}$ and $\mathbf{y}$ be nonzero vectors in $\mathbb{R}^n$ such that $\mathbf{x} \cdot \mathbf{y} > 0$. Prove that the angle between $\mathbf{x}$ and $\mathbf{y}$ is acute.

Proof: By the definition of the angle between two vectors,

$$\cos\theta = \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\|\|\mathbf{y}\|}$$

The numerator is > 0, since $\mathbf{x} \cdot \mathbf{y} > 0$. To show that the denominator is > 0, we note that since $\mathbf{x}$ and $\mathbf{y}$ are nonzero vectors, it follows that

$$\|\mathbf{x}\| > 0 \quad \text{and} \quad \|\mathbf{y}\| > 0$$

by Theorem 1.5, parts (2) and (3). So, the top and the bottom of $\dfrac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\|\|\mathbf{y}\|}$ are positive, therefore

$$\cos\theta > 0$$

This and the fact that $0 \leq \theta \leq \pi$ implies $0 < \theta < \pi/2$, that is, θ is acute. ■

EXAMPLE: Let $\mathbf{x}$ and $\mathbf{y}$ be vectors in $\mathbb{R}^n$ such that each coordinate of both $\mathbf{x}$ and $\mathbf{y}$ is equal to either 1 or -1. Prove that if $\mathbf{x}$ is orthogonal to $\mathbf{y}$, then n is even.

Proof: Since $\mathbf{x}$ is orthogonal to $\mathbf{y}$, it follows that

$$\mathbf{x} \cdot \mathbf{y} = 0 \tag{$*$}$$

Now

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$$

But each product $x_i y_i$ equals either 1 or -1. If exactly k of these products are equal to 1, then exactly $n-k$ of these products are equal to -1. Therefore

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= 1 \cdot k + (-1)(n-k) \\ &= k - n + k \qquad (**) \\ &= -n + 2k \end{aligned}$$

From $(*)$ and $(**)$ it follows that $-n + 2k = 0$, and so $n = 2k$. ■

"A If and Only If B" Proofs

Some theorems have the form "A if and only if B." This is really a combination of two statements: "If A then B" and "If B then A." Both of these statements must be shown true to fully complete the proof of the original statement.

EXAMPLE: Let $\mathbf{x}$ and $\mathbf{y}$ be nonzero vectors in $\mathbb{R}^n$. Prove that

$$\mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\|\|\mathbf{y}\|$$

if and only if $\mathbf{y}$ is a positive scalar multiple of $\mathbf{x}$.

Proof:

Part I: We suppose that $\mathbf{y} = c\mathbf{x}$ for some $c > 0$. Then,

$$\begin{aligned}
\mathbf{x} \cdot \mathbf{y} &= \mathbf{x} \cdot (c\mathbf{x}) && \text{because } \mathbf{y} = c\mathbf{x} \\
&= c(\mathbf{x} \cdot \mathbf{x}) && \text{Theorem 1.5, part (4)} \\
&= c\|\mathbf{x}\|^2 && \text{Theorem 1.5, part (2)} \\
&= \|\mathbf{x}\|(c\|\mathbf{x}\|) && \text{associative law of multiplication for real numbers} \\
&= \|\mathbf{x}\|(|c|\|\mathbf{x}\|) && \text{because } c > 0 \\
&= \|\mathbf{x}\|(\|c\mathbf{x}\|) && \text{Theorem 1.1} \\
&= \|\mathbf{x}\|\|\mathbf{y}\| && \text{because } \mathbf{y} = c\mathbf{x}
\end{aligned}$$

Part II: We assume that $\mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\|\|\mathbf{y}\|$ and show that there is some $c > 0$ such that $\mathbf{y} = c\mathbf{x}$. By Theorem 1.10, $\mathbf{y}$ can be expressed as $\mathbf{proj_x y} + \mathbf{w}$, where $\mathbf{w}$ is orthogonal to $\mathbf{x}$. Our strategy is first to show that $\mathbf{proj_x y}$ is a positive scalar multiple of $\mathbf{x}$ and then to show that $\mathbf{w} = \mathbf{0}$. For then, $\mathbf{y} = c\mathbf{x}$ with $c > 0$, and the proof is done.

First, note that

$$\begin{aligned}
\mathbf{proj_x y} &= \left(\frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\|^2}\right)\mathbf{x} && \text{formula for } \mathbf{proj_x y} \\
&= \left(\frac{\|\mathbf{x}\|\|\mathbf{y}\|}{\|\mathbf{x}\|^2}\right)\mathbf{x} && \text{because } \mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\|\|\mathbf{y}\| \\
&= \left(\frac{\|\mathbf{y}\|}{\|\mathbf{x}\|}\right)\mathbf{x}
\end{aligned}$$

Let $c = \|\mathbf{y}\|/\|\mathbf{x}\|$. Note that c is positive.

Finally, we conclude by showing $\mathbf{w} = \mathbf{0}$. Now,

$$\begin{aligned}
\|\mathbf{w}\|^2 &= \mathbf{w} \cdot \mathbf{w} && \text{Theorem 1.5, part (2)} \\
&= (\mathbf{y} - c\mathbf{x}) \cdot (\mathbf{y} - c\mathbf{x}) && \text{because } \mathbf{y} = c\mathbf{x} + \mathbf{w} \\
&= (\mathbf{y} \cdot \mathbf{y}) - 2c(\mathbf{x} \cdot \mathbf{y}) + c^2(\mathbf{x} \cdot \mathbf{x}) && \text{distributive law of dot product over addition} \\
&= \|\mathbf{y}\|^2 - 2c\|\mathbf{x}\|\|\mathbf{y}\| + c^2\|\mathbf{x}\|^2 && \text{Theorem 1.5, part (2), and } \mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\|\|\mathbf{y}\| \\
&= \|\mathbf{y}\|^2 - 2\frac{\|\mathbf{y}\|}{\|\mathbf{x}\|}\|\mathbf{x}\|\|\mathbf{y}\| + \frac{\|\mathbf{y}\|^2}{\|\mathbf{x}\|^2}\|\mathbf{x}\|^2 && \text{because } c = \frac{\|\mathbf{y}\|}{\|\mathbf{x}\|} \\
&= \|\mathbf{y}\|^2 - 2\|\mathbf{y}\|^2 + \|\mathbf{y}\|^2 \\
&= 0
\end{aligned}$$

and so $\mathbf{w} = \mathbf{0}$. The proof is complete. ■

“If A Then (B or C)” Proofs

Sometimes we must prove a statement of the form “If A then (B or C)”. This is an implication whose conclusion has two parts. Note that B is either true or false. Now, if B is true, there is no need for a proof, because we only need to establish that *either* B or C holds. For this reason, “If A then (B or C)” is equivalent to “If A is true and B is *false*, then C is true.” That is, we are allowed to assume that B is false, and then use this extra information to prove C is true.

EXAMPLE: Let $\mathbf{x}$ and $\mathbf{y}$ be vectors in $\mathbb{R}^n$. Prove that if $\|\mathbf{x}+\mathbf{y}\| = \|\mathbf{x}\|$, then $\mathbf{y} = \mathbf{0}$ or $\mathbf{x}$ is not orthogonal to $\mathbf{y}$.

Proof (version 1): Suppose $\mathbf{x}$ is orthogonal to $\mathbf{y}$, that is, $\mathbf{x}\cdot\mathbf{y} = 0$. We must show that $\mathbf{y} = \mathbf{0}$. We have

$$\begin{aligned}
\|\mathbf{x}\| &= \|\mathbf{x}+\mathbf{y}\| \\
\|\mathbf{x}\|^2 &= \|\mathbf{x}+\mathbf{y}\|^2 \\
&= (\mathbf{x}+\mathbf{y})\cdot(\mathbf{x}+\mathbf{y}) \\
&= \mathbf{x}\cdot\mathbf{x}+\mathbf{x}\cdot\mathbf{y}+\mathbf{y}\cdot\mathbf{x}+\mathbf{y}\cdot\mathbf{y} \\
&= \|\mathbf{x}\|^2 + 2\mathbf{x}\cdot\mathbf{y} + \|\mathbf{y}\|^2 \\
&= \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2
\end{aligned}$$

So, $\|\mathbf{x}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2$, hence $0 = \|\mathbf{y}\|^2$. Therefore $\mathbf{y} = \mathbf{0}$ by Theorem 1.5, parts (2) and (3). ■

Proof (version 2): Suppose $\mathbf{y} \neq \mathbf{0}$. We must show that $\mathbf{x}$ is *not* orthogonal to $\mathbf{y}$. We have

$$\begin{aligned}
\|\mathbf{x}\| &= \|\mathbf{x}+\mathbf{y}\| \\
\|\mathbf{x}\|^2 &= \|\mathbf{x}+\mathbf{y}\|^2 \\
&= (\mathbf{x}+\mathbf{y})\cdot(\mathbf{x}+\mathbf{y}) \\
&= \mathbf{x}\cdot\mathbf{x}+\mathbf{x}\cdot\mathbf{y}+\mathbf{y}\cdot\mathbf{x}+\mathbf{y}\cdot\mathbf{y} \\
&= \|\mathbf{x}\|^2 + 2\mathbf{x}\cdot\mathbf{y} + \|\mathbf{y}\|^2
\end{aligned}$$

So, $\|\mathbf{x}\|^2 = \|\mathbf{x}\|^2 + 2\mathbf{x}\cdot\mathbf{y} + \|\mathbf{y}\|^2$, therefore $0 = 2\mathbf{x}\cdot\mathbf{y} + \|\mathbf{y}\|^2$, which gives

$$\|\mathbf{y}\|^2 = -2\mathbf{x}\cdot\mathbf{y}$$

Since $\mathbf{y} \neq \mathbf{0}$, we have $\|\mathbf{y}\|^2 \neq 0$ by Theorem 1.5, parts (2) and (3). Therefore $\mathbf{x}\cdot\mathbf{y} \neq 0$. From this it follows that $\mathbf{x}$ is not orthogonal to $\mathbf{y}$ by the definition of orthogonality. ■

Proof Technique: Proof by Contrapositive

Related to the implication “If A then B” is its **contrapositive**: “If not B, then not A.” For example, for an integer n, the statement “If n^2 is even, then n is even” has the contrapositive “If n is odd (that is, not even), then n^2 is odd.” A statement and its contrapositive are always logically equivalent; that is, they are either both true or both false together. Therefore, proving the contrapositive of any statement (known as **proof by contrapositive**) has the effect of proving the original statement as well. In many cases, the contrapositive is easier to prove.

EXAMPLE: Let $\mathbf{x}$ and $\mathbf{y}$ be vectors in $\mathbb{R}^n$. Prove that if $\mathbf{x}\cdot\mathbf{y} \neq 0$, then

$$\|\mathbf{x}+\mathbf{y}\|^2 \neq \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2$$

Proof: Suppose that

$$\|\mathbf{x}+\mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 \tag{$*$}$$

Note that

$$\begin{aligned}\|\mathbf{x}+\mathbf{y}\|^2 &= (\mathbf{x}+\mathbf{y})\cdot(\mathbf{x}+\mathbf{y})\\ &= \mathbf{x}\cdot\mathbf{x}+\mathbf{x}\cdot\mathbf{y}+\mathbf{y}\cdot\mathbf{x}+\mathbf{y}\cdot\mathbf{y}\\ &= \|\mathbf{x}\|^2 + 2(\mathbf{x}\cdot\mathbf{y}) + \|\mathbf{y}\|^2\end{aligned}$$

From this and $(*)$ it follows that

$$\|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 = \|\mathbf{x}\|^2 + 2(\mathbf{x}\cdot\mathbf{y}) + \|\mathbf{y}\|^2$$

which implies that

$$2(\mathbf{x}\cdot\mathbf{y}) = 0$$

therefore $\mathbf{x}\cdot\mathbf{y} = 0$. ■

Proof Technique: Proof by Contradiction

Another common proof method is **proof by contradiction**, in which we assume the statement to be proved is false and use this assumption to contradict a known fact. In effect, we prove a result by showing that if it were false, it would be inconsistent with some other true statement.

DEFINITION: A **prime** is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

EXAMPLE: The numbers $2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47$ are prime.

THEOREM: There are infinitely many primes.

Proof: Suppose that there are only finitely many prime numbers,

$$p_1,\ p_2,\ldots,p_n \tag{$*$}$$

where n is a positive integer. Consider the integer

$$Q = p_1p_2\ldots p_n + 1 \tag{$**$}$$

Since all the prime numbers are listed in $(*)$, it follows that Q is divisible by some p_i with $1 \le i \le n$. Rewrite $(**)$ as

$$Q - p_1p_2\ldots p_n = 1$$

and divide both sides by p_i

$$\frac{Q}{p_i} - \frac{p_1p_2\ldots p_n}{p_i} = \frac{1}{p_i}$$

Since Q and $p_1p_2\ldots p_n$ are divisible by p_i, it follows that $\frac{Q}{p_i}$ and $\frac{p_1p_2\ldots p_n}{p_i}$ are integers. Therefore $\frac{1}{p_i}$ is an integer, which is impossible. This contradiction shows that there are infinitely many primes. ■

Proof Technique: Proof by Induction

The method of **proof by induction** is used to show that a statement is true for all values of an integer variable greater than or equal to some initial value i.

EXAMPLE: Prove that

$$1^2+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6} \qquad (*)$$

for any integer $n \geq 1$.
Proof:
STEP 1: For $n=1$ $(*)$ is true, since

$$1^2=\frac{1(1+1)(2\cdot 1+1)}{6}$$

STEP 2: Suppose $(*)$ is true for some $n=k\geq 1$, that is,

$$1^2+2^2+3^2+\ldots+k^2=\frac{k(k+1)(2k+1)}{6}$$

STEP 3: Prove that $(*)$ is true for $n=k+1$, that is,

$$1^2+2^2+3^2+\ldots+k^2+(k+1)^2\stackrel{?}{=}\frac{(k+1)(k+2)(2k+3)}{6}$$

We have

$$1^2+2^2+3^2+\ldots+k^2+(k+1)^2\stackrel{\textbf{ST.2}}{=}\frac{k(k+1)(2k+1)}{6}+(k+1)^2\stackrel{?}{=}\frac{(k+1)(k+2)(2k+3)}{6}$$

which is true, since

$$\frac{k(k+1)(2k+1)}{6}+(k+1)^2=\frac{(k+1)(k+2)(2k+3)}{6}$$

$$\Uparrow$$

$$k(k+1)(2k+1)+6(k+1)^2=(k+1)(k+2)(2k+3)$$

$$\Uparrow$$

$$(k^2+k)(2k+1)+6(k+1)^2=(k^2+3k+2)(2k+3)$$

$$\Uparrow$$

$$2k^3+k^2+2k^2+k+6k^2+12k+6=2k^3+3k^2+6k^2+9k+4k+6$$

$$\Uparrow$$

$$2k^3+9k^2+13k+6=2k^3+9k^2+13k+6 \quad \blacksquare$$

REMARK: We call Step 1 the **Base Step** and Steps 2, 3 the **Inductive Step**.

EXAMPLE: Let $\mathbf{x_1}, \ldots, \mathbf{x_k}$ be unit vectors in $\mathbb{R}^n$, and let $a_1, \ldots, a_k$ be real numbers. Then, for every $\mathbf{y}$ in $\mathbb{R}^n$,

$$\left(\sum_{i=1}^{k} a_i \mathbf{x_i}\right) \cdot \mathbf{y} \leq \left(\sum_{i=1}^{k} |a_i|\right) \|\mathbf{y}\| \tag{$*$}$$

Proof:

STEP 1: We must show

$$(a_1\mathbf{x_1}) \cdot \mathbf{y} \leq |a_1|\|\mathbf{y}\|$$

We have

$$\begin{aligned}
(a_1\mathbf{x_1}) \cdot \mathbf{y} &\leq |(a_1\mathbf{x_1}) \cdot \mathbf{y}| & \\
&\leq \|a_1\mathbf{x_1}\|\|\mathbf{y}\| & \text{Cauchy-Schwarz Inequality} \\
&\leq |a_1|\|\mathbf{x_1}\|\|\mathbf{y}\| & \text{Theorem 1.1} \\
&= |a_1|\|\mathbf{y}\| & \mathbf{x_1} \text{ is a unit vector}
\end{aligned}$$

STEP 2: Suppose $(*)$ is true for some $k \geq 1$, that is,

$$(a_1\mathbf{x_1} + \ldots + a_k\mathbf{x_k}) \cdot \mathbf{y} \leq (|a_1| + \ldots + |a_k|)\|\mathbf{y}\|$$

STEP 3: We prove that

$$(a_1\mathbf{x_1} + \ldots + a_k\mathbf{x_k} + a_{k+1}\mathbf{x_{k+1}}) \cdot \mathbf{y} \stackrel{?}{\leq} (|a_1| + \ldots + |a_k| + |a_{k+1}|)\|\mathbf{y}\|$$

We have

$$\begin{aligned}
(a_1\mathbf{x_1} + \ldots + a_k\mathbf{x_k} + a_{k+1}\mathbf{x_{k+1}}) \cdot \mathbf{y} &= (a_1\mathbf{x_1} + \ldots + a_k\mathbf{x_k}) \cdot \mathbf{y} + (a_{k+1}\mathbf{x_{k+1}}) \cdot \mathbf{y} \\
&\stackrel{\mathbf{ST.2}}{\leq} (|a_1| + \ldots + |a_k|)\|\mathbf{y}\| + (a_{k+1}\mathbf{x_{k+1}}) \cdot \mathbf{y}
\end{aligned} \tag{$**$}$$

But

$$\begin{aligned}
(a_{k+1}\mathbf{x_{k+1}}) \cdot \mathbf{y} &\leq |(a_{k+1}\mathbf{x_{k+1}}) \cdot \mathbf{y}| & \\
&\leq \|a_{k+1}\mathbf{x_{k+1}}\|\|\mathbf{y}\| & \text{Cauchy-Schwarz Inequality} \\
&\leq |a_{k+1}|\|\mathbf{x_{k+1}}\|\|\mathbf{y}\| & \text{Theorem 1.1} \\
&= |a_{k+1}|\|\mathbf{y}\| & \mathbf{x_{k+1}} \text{ is a unit vector}
\end{aligned}$$

Using this in $(**)$, we get

$$\begin{aligned}
(a_1\mathbf{x_1} + \ldots + a_k\mathbf{x_k} + a_{k+1}\mathbf{x_{k+1}}) \cdot \mathbf{y} &\leq (|a_1| + \ldots + |a_k|)\|\mathbf{y}\| + |a_{k+1}|\|\mathbf{y}\| \\
&\leq (|a_1| + \ldots + |a_k| + |a_{k+1}|)\|\mathbf{y}\| \quad \blacksquare
\end{aligned}$$