Examples of useful proof techniques

Shikhara Bhat

1 Proof by Contradiction

Proof by contradiction is a widely used proof technique that can be very successful in convincing you *why* your theorem should be true by exploring the consequences of the theorem being false. The basic idea goes back (at least) to ancient Greek philosophy, and is known in philosophical circles as *reductio ad absurdum*.

> **Big Idea:** Assume the focal statement is false. Show that this assumption leads to a contradiction, inconsistency, or other absurdity. Conclude that the focal statement must thus be true.

Some Examples

Theorem 1.1

There are infinitely many primes

Proof. Assume the contrary. Let us say the finitely many primes are $p_1, p_2, \ldots, p_n$. Consider the number $p \coloneqq 1 + (\Pi_{i=1}^{n} p_i)$. The number p is clearly larger than all of $p_1, \ldots, p_n$, but is not divisible by any of them and thus must be a prime. Thus, the assumption that we can have a finite list of primes $p_1, \ldots, p_n$ must be wrong. □

Theorem 1.2

$\sqrt{2}$ is irrational

Proof. Assume the contrary. If $\sqrt{2}$ is indeed rational, then, by definition, we can find two integers p and $q \neq 0$ such that they share no common factors and

$\sqrt{2} = p/q$. We now calculate

$$\sqrt{2} = \frac{p}{q} \tag{1.1}$$

$$\Rightarrow 2 = \left(\frac{p}{q}\right)^2 \tag{1.2}$$

$$\Rightarrow 2p^2 = q^2 \tag{1.3}$$

From equation 1.3, we can conclude that q^2 is twice an integer and is, therefore, an even number. If q^2 is even, q must also be even. Thus, we can find an integer r such that $q = 2r$. Substituting this into Eq. 1.3, we obtain

$$2p^2 = (2r)^2 \tag{1.4}$$

$$\Rightarrow 2p^2 = 4r^2 \tag{1.5}$$

$$\Rightarrow p^2 = 2r^2 \tag{1.6}$$

Thus, p^2 is also an even number, and therefore, so is p.

We have now found that p and q are both even numbers and thus share 2 as a common factor. However, we initially assumed that p and q shared no common factors. Thus, we have arrived at a logical contradiction. Since our assumption that $\sqrt{2}$ was rational has led to a contradiction, we conclude that $\sqrt{2}$ is irrational. □

Theorem 1.3

The set of real numbers in the interval $[0, 1]$ contains more elements than the set of natural numbers $\mathbb{N} = 1, 2, 3, 4, \cdots$

Proof. Assume the contrary. If $[0, 1]$ and $\mathbb{N}$ have the same number of elements, it must be possible to create a pairing between each element of $[0, 1]$ and each element of $\mathbb{N}$. Let us use r_i to denote the element of $[0, 1]$ that has been paired with the i^{th} natural number.

Each element of $[0, 1]$ can be represented by its decimal expansion in the form $0.d_1d_2d_3d_4\ldots$, where $d_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is the number at the j^{th} decimal point. Thus, we have the representation $r_i = 0.r_{i1}r_{i2}r_{i3}\ldots$ for every r_i in $[0, 1]$. Consider the number $c = 0.c_1c_2\ldots \in [0, 1]$ given by choosing $c_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \setminus \{r_{ii}\}$. In words, we choose the number in the i^{th} position of the decimal expansion of c such that it is different from the number

in the i^{th} position of the decimal expansion of i^{th} real number r_i:

$$\begin{aligned}
r_1 &= 0.r_{11}r_{12}r_{13}r_{14}r_{15}\ldots \\
r_2 &= 0.r_{21}r_{22}r_{23}r_{24}r_{25}\ldots \\
r_3 &= 0.r_{31}r_{32}r_{33}r_{34}r_{35}\ldots \\
r_4 &= 0.r_{41}r_{42}r_{43}r_{44}r_{45}\ldots \\
r_5 &= 0.r_{51}r_{52}r_{53}r_{54}r_{55}\ldots \\
\vdots \quad &= \qquad\quad \vdots
\end{aligned}$$

For every $i \in \mathbb{N}$, the number c differs from r_i in the i^{th} position. In other words, c cannot equal any r_i. However, we had assumed that every number in $[0, 1]$ can be associated with a natural number via the pairing $n \to r_n$. We have arrived at a contradiction. We thus conclude that our initial assumption that such a pairing exists is false, and therefore see that the set $[0, 1]$ has more elements than the set $\mathbb{N}$. □

2 Proof by Induction

Proof by induction works well when we want to prove that some statement $P(n)$ holds for all natural numbers n. The idea is to prove that if the statement holds for a number n, it must hold for the next number, and thus, we have a sort of 'domino effect'.

Big Idea: Suppose you have a statement $P(n)$ concerning a number n. To prove that $P(n)$ holds for all n, we use a two step process.

Step 1 (base case): Prove $P(1)$, i.e. that the statement holds for 1.

Step 2 (induction step): Show that if $P(k)$ is true, then $P(k+1)$ must also be true.

The two steps together prove that $P(1)$ is true, and therefore $P(1+1) = P(2)$ is true, and therefore $P(2+1) = P(3)$ is true, and....

Some Examples

Theorem 2.1

A formula for the sum of the first n natural numbers:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \;\forall\; n \in \mathbb{N}$$

Proof. Let $S_n \coloneqq 1 + 2 + 3 + \ldots + n$. Then, our claim is that $S_n = n(n+1)/2$ for any natural number n.

Step 1 (base case)

$$S_1 = 1 = \frac{1(1+1)}{2}$$

Thus, the statement is true for $n = 1$.

Step 2 (induction step)

Assume the statement is true for $n = k$. Thus, $S_k = k(k+1)/2$. This is our 'induction hypothesis'. We can now calculate S_{k+1} as

$$S_{k+1} = \underbrace{1+2+3+\ldots+k}_{S_k} + (k+1) \tag{2.1}$$

$$= \frac{k(k+1)}{2} + (k+1) \quad \text{(by induction hypothesis)} \tag{2.2}$$

$$= \frac{k(k+1)+2(k+1)}{2} \tag{2.3}$$

$$= \frac{(k+1)(k+2)}{2} \tag{2.4}$$

$$\Rightarrow S_{k+1} = \frac{(k+1)(k+1+1)}{2} \tag{2.5}$$

Thus, if our statement is true for some $n = k$, we have proven that it is also true for $n = k+1$.

Since we already proved that the statement holds for $n = 1$, it thus holds for every $n \in \mathbb{N}$. □

Theorem 2.2

(Bernoulli's inequality) Given any real number $x \geq -1$,

$$(1+x)^n \geq 1 + nx \;\forall\; n \in \mathbb{N}$$

Proof. Step 1 (base case)

$$(1+x)^1 = 1 + x = 1 + (1) * x \forall x \geq 1$$

Thus, the statement is true for $n = 1$.

Step 2 (induction step)

Assume the statement is true for $n = k$. Thus, $(1+x)^k \geq 1 + kx \forall x \geq -1$.

We now observe that

$$(1+x)^{k+1} = (1+x)^k(1+x) \tag{2.6}$$
$$\geq (1+kx)(1+x) \quad \text{(by induction hypothesis)} \tag{2.7}$$
$$= 1 + kx + x + kx^2 \tag{2.8}$$
$$\geq 1 + kx + x = 1 + (k+1)x \tag{2.9}$$

Thus, if our statement is true for some $n = k$, we have proven that it is also true for $n = k + 1$.

Since we already proved that the statement holds for $n = 1$, it thus holds for every $n \in \mathbb{N}$. □

Theorem 2.3

Let $f(x) = xe^x$, and let $f^{(n)}(x)$ denote the n^{th} derivative $\frac{d^n f}{dx^n}$. Then,

$$f^{(n)}(x) = (x+n)e^x \ \forall \ n \in \mathbb{N}$$

Proof. Step 1 (base case)

$$f^{(1)}(x) = \frac{df}{dx} = \frac{d}{dx}(xe^x) = x\frac{de^x}{dx} + e^x\frac{dx}{dx} = xe^x + e^x = (x+1)e^x$$

Thus, the statement is true for $n = 1$.

Step 2 (induction step)

Assume the statement is true for $n = k$. Thus, $f^{(k)}(x) = (x+k)e^x$. We now observe that

$$f^{(k+1)}(x) = \frac{d}{dx}f^{(k)}(x) \tag{2.10}$$
$$= \frac{d}{dx}\left((x+k)e^x\right) \tag{2.11}$$
$$= \frac{d}{dx}(xe^x) + k\frac{de^x}{dx} \tag{2.12}$$

We already calculated the first term on the RHS when computing the base case above. Using that result, we obtain

$$f^{(k+1)}(x) = (x+1)e^x + ke^x = (x+k+1)e^x \tag{2.13}$$

which is the desired expression. Thus, if our statement is true for some $n = k$, we have proven that it is also true for $n = k + 1$. Since we already proved that the statement holds for $n = 1$, it thus holds for every $n \in \mathbb{N}$. □

Exercise 1

What is wrong with the following proof?

Claim: All birds are the same color.

Proof:

Let $P(n)$ denote the statement that any collection of n birds are the same color. We seek to prove that $P(n)$ is true for every $n \in \mathbb{N}$. We will proceed by induction.

Step 1 (base case): Clearly, a bird is the same color as itself, and thus a collection of 1 birds all have the same color. Thus, $P(1)$ is true.

Step 2 (induction step:) Let us assume that any collection of k birds are the same color. Let $B = \{b_1, b_2, \ldots, b_{k+1}\}$ denote a collection of $k+1$ birds. Let $B_0 = \{b_1, b_2, \ldots, b_k\}$. Since B_0 is a collection of k birds, by our induction hypothesis, we conclude that all birds in B_0 are the same color. Now let let $B_1 = \{b_2, \ldots, b_k, b_{k+1}\}$. B_1 is also a collection of k birds, and thus every bird in B_1 is also the same color by the induction hypothesis. Since the bird b_2 occurs in both B_0 and B_1, we conclude that every bird in $B_0 \cup B_1$ is the same color. Since $B_0 \cup B_1 = B$ (in words: every bird in our collection B is either in B_0, in B_1, or both), we conclude that our collection of $k+1$ birds are all the same color.

Thus, if our statement is true for some $n = k$, we have proven that it is also true for $n = k+1$. Since we already proved that the statement holds for $n = 1$, it thus holds for every $n \in \mathbb{N}$. We have thus proved that all birds are the same color. □

Since empiricists have already gathered evidence for the existence of both blackbirds and bluebirds, a corollary of the above proof is that blue and black are the same color.

3 The Pigeonhole Principle

The pigeonhole principle is essentially a counting argument. It arises from the following simple observation

> **Big Idea:** If n pigeons live in m holes and $n > m$, then at least one hole must have more than one pigeon.

This elementary observation can be astonishingly useful when proving statements about discrete objects.

Some Examples

Theorem 3.1

Let G be a graph on n vertices with no self-loops (i.e. a vertex cannot connect to itself) and no multi-edges (i.e. two vertices may share at most one edge). If $n \geq 2$, at least two vertices in G have the same number of edges.

Proof. Let $v_1, v_2, \ldots, v_n$ be the vertices of G. Since the graph does not have self-loops or multi-edges, each vertex can only have at most $n-1$ edges. Thus, we need to assign one of $n-1$ possible choices of the number of edges (the 'holes') to each of n vertices (the 'pigeons'). By the pigeonhole principle, we conclude that at least two vertices must have the same number of edges. □

Theorem 3.2

(Dirichlet approximation theorem) Let α be any irrational number. It is possible to find infinitely many integers $p, q \in \mathbb{Z}$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

. In words, any irrational number α can be approximated arbitrarily well by rationals p/q.

Proof. Let $N > 0$ be a positive integer. For each $k = 0, 1, 2, \ldots, N$, we can rewrite the number $k\alpha$ as $k\alpha = z_k + x_k$, where $z_k \in \mathbb{Z}$ is the integer part of $k\alpha$ and $0 \leq x_k < 1$ is the non-integer part.

Divide the interval $[0, 1]$ into N intervals via the partition $0, 1/N, 2/N, \ldots, 1$. There are now $N+1$ numbers x_k and N intervals. By the pigeonhole principle, at least one interval must therefore contain two of the numbers x_k. Let x_{k_i}, x_{k_j} be the two numbers that share the same interval, and without loss of generality, assume $k_i < k_j$. Since they are within the same interval, we must have $|x_{k_j} - x_{k_i}| < 1/N$. We now observe that

$$|(k_j - k_i)\alpha - (z_{k_j} - z_{k_i})| = |(k_j\alpha - z_{k_j}) - (k_i\alpha - z_{k_i})| = |x_{k_j} - x_{k_i}| < \frac{1}{N}$$

Dividing both sides by $k_j - k_i$ (which can be taken inside the modulus since we assumed $k_j - k_i > 0$), we obtain

$$\left|\alpha - \frac{z_{k_j} - z_{k_i}}{k_j - k_i}\right| < \frac{1}{N(k_j - k_i)} < \frac{1}{(k_j - k_i)^2}$$

Letting $p = z_{k_j} - z_{k_i}$ and $q = k_j - k_i$, we obtain the desired result. □

4 Clever non-constructive proofs

Big Idea: To prove a statement of the form 'there exists an object satisfying certain properties', it is not necessary to explicitly find or construct such an object.

Theorem 4.1

It is possible to find two irrational numbers n and m such that n^m is rational.

Proof. Let $x = (\sqrt{2})^{\sqrt{2}}$. We already know that $\sqrt{2}$ is irrational. If x is rational, then we are done, with $n = m = \sqrt{2}$. Thus, assume x is irrational. We have

$$x^{\sqrt{2}} = \left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2$$

which is rational, and thus $n = (\sqrt{2})^{\sqrt{2}}, m = \sqrt{2}$ provide the desired pair of irrationals. □

Theorem 4.2

Color a sphere such that 90% of its surface area is red and the remaining 10% is blue. Regardless of the pattern you choose for the coloring, it is always possible to inscribe a cube in this sphere such that no vertex of the cube is blue.

Proof. Surprisingly, we will prove this statement using probability theory. Given the focal sphere S^2, let Ω be the set of all possible ways to inscribe a cube on S^2. We are interested in the probabilistic experiment of choosing an orientation ω uniformly at random from Ω (in words, just picking an arbitrary orientation of the cube at random).

For $i = 1, 2, \ldots, 8$, let X_i be the random variable given by

$$X_i(\omega) = \begin{cases} 1 & ; \ i^{\text{th}} \text{ vertex of the cube is red in the orientation } \omega \\ 0 & ; \ \text{otherwise} \end{cases}$$

Since 90% of the area of the sphere is red, we have $\mathbb{E}[X_i] = 0.9$. The expected number of red vertices associated with a random orientation of the cube is then

$$\mathbb{E}\left[\sum_{i=1}^{8} X_i\right] = \sum_{i=1}^{8} \mathbb{E}[X_i] = 8\mathbb{E}[X_i] = 8 \times 0.9 = 7.2$$

Since the number of red vertices is always integer-valued and $7.2 > 7$, we conclude that there must exist at least one orientation $\omega \in \Omega$ such that all 8 vertices are red. □

5 Some advanced clever proofs

The theorems/proofs in this section are slightly more advanced and may not be accessible if you are relatively new (< undergraduate) to mathematics.

Theorem 5.1

The harmonic series diverges:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots = \infty$$

Proof. Assume the contrary. Let $H(x) = \sum_{i=1}^{\infty} 1/n$. Let $f_n(x) \coloneqq \frac{1}{n}\chi_{[0,n]}(x)$. Note that $\lim_{n\to\infty} f_n(x) = 1$ and $f_n(x) \leq H(x) < \infty \ \forall \ x$. However,

$$\int_{\mathbb{R}} \lim_{n\to\infty} f_n(x)dx = \int_{\mathbb{R}} 0 \ dx = 0$$

and

$$\lim_{n\to\infty} \int_{\mathbb{R}} f_n(x)dx = \lim_{n\to\infty} 1 = 1$$

which contradicts Lebesgue's dominated convergence theorem. Thus, $H = \infty$. □

Exercise 2

Why can't we adapt the proof of theorem 5.1 to show that $\sum_{i=1}^{\infty} 2^{-n}$ diverges?

Theorem 5.2

Let $f, g, h \in L^2(\mathbb{R})$ and let $*$ denote convolution. Then, convolution is associative, i.e.

$$(f * g) * h = f * (g * h)$$

Proof. Let $\hat{\phi}$ denote the Fourier transform of $\phi \in L^2(\mathbb{R})$. We have

$$((f * g) * h)\hat{} = (f * g)\hat{}\hat{h} = \hat{f}\hat{g}\hat{h} = \hat{f}(g * h)\hat{} = (f * (g * h))\hat{}$$

Since the Fourier transform is a bounded operator on the Hilbert space $L^2(\mathbb{R})$, it is invertible, thus yielding the desired result. □

Theorem 5.3

(Uniqueness of solutions to the heat equation) Let $\Omega \subset \mathbb{R}^n$ be open and bounded. Let $\Omega_T \coloneqq \Omega \times (0, T]$ for any $T > 0$, and use $\Gamma_T \coloneqq \overline{\Omega}_T \setminus \Omega_T$ to denote the boundary. Let $u, v \in C_1^2(\Omega_T)$ satisfy the heat equation on Ω_T, i.e.

$$\begin{aligned} u_t - \Delta u = v_t - \Delta v = f \text{ on } \Omega_T \\ u(\cdot, 0) = v(\cdot, 0) = g \text{ on } \Gamma_T \end{aligned}$$

where $f \in C_1^1(\Omega_T) \cap L^\infty(\Omega_T)$, $g \in C^1(\Gamma_T) \cap L^\infty(\Gamma_T)$, and subscript indicates partial differentiation. Then, $u = v$.

Proof. Define $w \coloneqq u - v$. Since u and v satisfy the given heat equation, w satisfies

$$w_t - \Delta w = 0 \text{ on } \Omega_T \tag{5.1}$$

$$w = 0 \text{ on } \Gamma_T \tag{5.2}$$

Let

$$E(t) \coloneqq \frac{1}{2} \int_{\Omega_T} w^2(x, t) dx \tag{5.3}$$

Differentiating both sides with respect to time, we find

$$E'(t) = \int_{\Omega_T} w w_t dx = \int_{\Omega_T} w \Delta w dx \tag{5.4}$$

where we have substituted w_t from Eq. 5.1. Using integration by parts, we now find

$$\int_{\Omega_T} w \Delta w dx = -\int_{\Omega_T} \nabla w \nabla w dx + \underbrace{\int_{\Gamma_T} w \Delta w \gamma_i dx}_{=0 \text{ by Eq. 5.2}} \tag{5.5}$$

Substituting Eq. 5.5 into Eq. 5.4, we obtain

$$E'(t) = -\int_{\Omega_T} (\nabla w)^2 dx \leq 0 \tag{5.6}$$

and thus see that $E(t)$ is a decreasing function of time. From the definition 5.3, E is the integral of a non-negative function and therefore $E(t) \geq 0$. Further, from the initial condition 5.2, we obtain $E(0) = 0$. We hence conclude that $E(t) \equiv 0$. However, from the definition (5.3), this can only happen if $u = v$ almost everywhere. Since u and v are $C_1^2(\Omega_T)$, a.e. equality implies pointwise equality. □

The next proof provides an example of a technique that requires the axiom of choice.

Theorem 5.4

Let $(\mathbb{R}, \mathscr{M}, \mu)$ denote the reals equipped with the Lebesgue measure and the usual σ-algebra. Then, $\mathscr{M} \neq 2^{\mathbb{R}}$. In other words, non-measurable sets exist.

Proof. Define a relation $\sim$ from $[0,1]$ to $[0,1]$ by $x \sim y \iff x - y \in \mathbb{Q}$. It is easy to see that $\sim$ is an equivalence relation. Let $\{E_\alpha\}_{\alpha \in I}$ be the set of equivalence classes of $[0,1]$ with respect to $\sim$.

By the axiom of choice, we can choose exactly one element x_α from each equivalence class E_α. Let $V = \{x_\alpha | \alpha \in I\}$ be this set of choices. We will show that V is not measurable.

Let $\{r_i\}_{i \in \mathbb{N}}$ be an enumeration of the rationals in $[-1,1]$, and define $E_n = \{r_n + x | x \in E\}$. Clearly, $E_n \cap E_m = \emptyset \ \forall \ n \neq m$. Since $E \subset [0,1]$, we can also see that $E_n \subset [-1,2] \ \forall \ n$.

Claim. $[0,1] \subset E_k$ for some $k \in \mathbb{N}$

Proof. Let $x \in [0,1]$. Since $\{E_\alpha\}$ is obtained from an equivalence relation on $[0,1]$, we have $[0,1] = \bigcup\limits_{\alpha \in I} E_\alpha$. Thus, $x \in E_\alpha$ for some $\alpha \in I$. But

$$x \in E_\alpha \Rightarrow x \sim x_\alpha \Rightarrow x - x_\alpha \in \mathbb{Q}$$

Since we additionally also have $x, x_\alpha \in [0,1]$, we conclude that $x - x_\alpha \in \mathbb{Q} \cap [-1,1]$. Thus, $x - x_\alpha$ must be in the enumeration $r_1, \ldots, r_n$. Let us say $x - x_\alpha = r_k$. Rearranging, we obtain $x = x_\alpha + r_k$ and thus conclude that $x \in E_k$. □

We now have

$$[0,1] \subset \bigcup_{n=1}^{\infty} E_n \subset [-1,2] \tag{5.7}$$

Assume $V \in \mathscr{M}$. Since μ is translation invariant and $\mu(\mathbb{Q}) = 0$, we must have $E_n \in \mathscr{M} \ \forall \ n$ and $\mu(E_n) = \mu(V) \ \forall \ n$.

Case 1. $\mu(V) = 0$

If $\mu(V) = 0$, we find

$$\mu(\bigcup_{n=1}^{\infty} E_n) = \sum_{n=1}^{\infty} \mu(E_n) = 0$$

However, from Eq. 5.7, we know that $[0,1] \subset \bigcup\limits_{n=1}^{\infty} E_n$. Further, $\mu([0,1]) = 1 > 0$. This is a contradiction, since $A \subset B \Rightarrow \mu(A) \leq \mu(B)$.

Case 2. $\mu(V) > 0$

If $\mu(V) > 0$, we instead have

$$\mu(\bigcup_{n=1}^{\infty} E_n) = \sum_{n=1}^{\infty} \mu(E_n) = \mu(V) \sum_{n=1}^{\infty} 1 = \infty$$

However, from Eq. 5.7, we know that $\bigcup_{n=1}^{\infty} E_n \subset [-1, 2]$ and thus must also have $\mu(\bigcup_{n=1}^{\infty} E_n) \leq \mu([-1, 2])$. Our calculation of $\mu(\bigcup_{n=1}^{\infty} E_n)$ thus yields $\infty < 3$, which is a contradiction,

Since both cases lead to a contradiction, we conclude that $V \notin \mathscr{M}$. $\square$