Mathematical Proofs: Portfolio

Illinois Wesleyan University

Ted Yap

April 15, 2018

Contents

1 Introduction

Currently taking Techniques of Mathematical Proofs at Illinois Wesleyan University, I put together a portfolio of basic mathematical proofs to demonstrate some of the best works that I have completed. To ensure that I have covered the breadth and depth of the subject matter, I selected proofs based on difficulty and method of proving. For each method of proof, I included a summary discussing about the method, and consequently, listed out a few proofs that I solved.

2 Direct Proof

A true mathematical statement whose truth is accepted without proof is referred to as an **axiom**, while a true mathematical statement whose truth can be verified is referred to as a **theorem**. In nearly all theorems, we will encounter the implication $P(x) \Rightarrow Q(x)$, where P and Q are **open sentences** with variable x whose domain is S.

In a **direct proof** of $P(x) \Rightarrow Q(x)$ for all $x \in S$, we assume $P(x)$ is true for some element $x \in S$ and show that $Q(x)$ is true for this element x. Theorem is proved below using direct proof.

Theorem 1. *If $A \subseteq B$ and $B \subseteq C$ and $C \subseteq A$, then $A = B$ and $B = C$.*

Proof. Assume $A \subseteq B$ and $B \subseteq C$ and $C \subseteq A$. We consider two parts.

Part 1: Prove $A = B$.

> To prove $A = B$, show $B \subseteq A$, given that $A \subseteq B$. Since $B \subseteq C$, if $x \in B$, then $x \in C$. However, since $C \subseteq A$, then $x \in A$. Hence, $x \in B \Rightarrow x \in A$, and $B \subseteq A$.

Part 2: Prove $B = C$.

> To prove $B = C$, show $C \subseteq B$, given that $B \subseteq C$. Since $C \subseteq A$, if $x \in C$, then $x \in A$. However, since $A \subseteq B$, then $x \in B$. Hence, $x \in C \Rightarrow x \in B$, and $C \subseteq B$.

Hence, from Part 1 and 2, $A = B$ and $B = C$. □

As one can see, to prove Theorem 1, it is assumed that $A \subseteq B$ and $B \subseteq C$ and $C \subseteq A$, and using the definition of subsets, we show $A = B$ and $B = C$. This proof might seem trivial, but one needs to understand the definitions in order to correctly prove the result.

3 Proof by Cases

When the variable x in $P(x)$ and $Q(x)$ possesses more than one properties, such as if x can be even or odd, it is useful to divide the proof into multiple cases with each case for each property of x. Such technique of proof is called **proof by cases**.

Theorem 2. *Let $a, b \in \mathbb{Z}$. If a is even or b is even, then ab is even.*

Proof. Consider three cases.

Case 1: a and b are both even.

> Assume a and b are both even, then $a, b = 2k$, where $k \in \mathbb{Z}$. Thus, $ab = (2k)(2k) = 2(2k^2)$. Since $2k^2 \in \mathbb{Z}$, it follows that ab is even.

Case 2: a is even and b is odd.

> Assume a is even and b is odd, then $a = 2k$ and $b = 2k + 1$, where $k \in \mathbb{Z}$. Thus, $ab = (2k)(2k + 1) = 2[k(2k + 1)]$. Since $k(2k + 1) \in \mathbb{Z}$, it follows that ab is even.

Case 3: a is odd and b is even.

> Then $a = 2k + 1$ and $b = 2k$, where $k \in \mathbb{Z}$. Thus, $ab = (2k + 1)(2k) = 2[k(2k + 1)]$. Since $k(2k + 1) \in \mathbb{Z}$, it follows that ab is even.

Hence, in all cases, it has been shown that if a is even or b is even, then ab is even.

Note that in all three cases, subsets of the pair (a, b) do not intersect. Hence, the cases are determined by a partition. □

Since the premise a is even or b is even is a disjunction, there are three cases for which the disjunction can be true. Therefore, it is a good idea to use proof by cases for this theorem.

4 Proof by Contrapositive

The **contrapositive** of the implication $P(x) \Rightarrow Q(x)$ is the implication $\sim Q(x) \Rightarrow \sim P(x)$ It can be shown that the contrapositive of the implication is logically equivalent to the implication. Hence, in **proof by contrapositive**, we assume $\sim Q(x)$ is true for some $x \in S$ and show $\sim P(x)$ is true for this element x.

Theorem 3. *Let $x \in \mathbb{Z}$. $(3x+1)$ is even if and only if $5x-2$ is odd.*

Proof. Assume, by way of contrapositive, $(3x+1)$ is odd if and only if $5x-2$ is even. This contrapositive is a bi-conditional statement. Therefore, we need to prove two parts:

Part 1: Prove that if $(3x+1)$ is odd, then $5x-2$ is even.

Assume $(3x+1)$ is odd, then $(3x+1) = 2k+1$ where $k \in \mathbb{Z}$. Thus,

$$\begin{aligned} 5x-2 &= 2x + (3x+1) - 3 \\ &= 2x + 2k - 2 \\ &= 2(x+k-1) \end{aligned} \tag{1}$$

Since $(x+k-1) \in \mathbb{Z}$, then $5x-2$ is even because it can be written in the form of $2p$ where $p \in \mathbb{Z}$.

Part 2: Prove that if $5x-2$ is even, then $(3x+1)$ is odd.

Assume $5x-2$ is even, then $5x-2 = 2k$ where $k \in \mathbb{Z}$. Thus,

$$\begin{aligned} 3x+1 &= (5x-2) - 2x + 3 \\ &= 2(k-x+1) + 1 \end{aligned} \tag{2}$$

Since $(k-x+1) \in \mathbb{Z}$, then $3x+1$ is odd because it can be written in the form of $2p+1$ where $p \in \mathbb{Z}$.

Now that the contrapositive is proven to be true, it must also be true that $(3x+1)$ is even if and only if $5x-2$ is odd. □

Here, the implication is $(3x+1)$ is even if and only if $5x-2$ is odd. Since this is a bi-conditional statement, its contrapositive, $(3x+1)$ is odd if and only if $5x-2$ is even, is also a bi-conditional statement. Therefore, both directions of implication must be proved.

5 Proof by Contradiction

It can sometimes be useful to use **proof by contradiction** to show the implication $P(x) \Rightarrow Q(x)$ for all $x \in S$ is true. In such technique of proof, we first assume $P(x)$ and the negated conclusion $\sim Q(x)$. However, such assumptions lead to a contradiction. Therefore, $Q(x)$ must be true.

Theorem 4. *A is any set and $\emptyset$ is the empty set, then $\emptyset \subseteq A$.*

Proof. Consider two cases.

Case 1:

Let A be an empty set. Then, A $= \emptyset$. Hence, by definition of equivalent sets, $A \subseteq \emptyset$ and $\emptyset \subseteq A$.

Case 2:

Let A be a nonempty set. By way of contradiction, assume that $\emptyset \subsetneq A$. Then, if $x \in \emptyset$, then $x \notin A$. Since there is no element in the empty set, it contradicts that there is an element in the empty set such that the element is not in A. Therefore, $\emptyset \subseteq A$, for any set A.

□

Theorem 5. *Let R be an equivalence relation defined on a nonempty set A. Then the set*

$$P = \{[a] : a \in A\}$$

of equivalence classes resulting from R is a partition of A.

Proof. A set P of equivalence classes forms a partition of A if and only if every element of A belongs to exactly one subset of P. Assume, by contradiction, that some element $x \in A$ belongs to two distinct equivalence classes, say $[a]$ and $[b]$. Since $x \in [a]$ and $x \in [b]$, it follows that xRa and xRb. Because R is symmetric, aRx. Thus, aRx and xRb. Since R is transitive, aRb. It follows that $[a] = [b]$, which contradicts the assumption that $[a]$ and $[b]$ are two distinct classes. Therefore, x belongs to a unique equivalence class and the set P forms a partition of A. □

In almost all cases where uniqueness must be shown, we will always use proof by contraction.

6 Proof by Induction

Proof by Induction is used to prove that a statement $P(n)$ is true for all $n \in \mathbb{N}$. According to the Principle of Mathematical Induction, the base case proves that $P(n)$ is true for $n = 1$, while the inductive step proves that if $P(k)$ is true for all $k \in \mathbb{N}$, then $P(k+1)$ is true. If both the base case and inductive step are true, then $P(n)$ is true for all $n \in \mathbb{N}$. Other variants of the Principle of Mathematical Induction include the Generalized Principle of Mathematical Induction and Strong Principle of Mathematical Induction.

Theorem 6. *For every $n \geq 1$ positive real numbers $a_1, a_2, \cdots, a_n$,*

$$(\sum_{i=1}^{n} a_n)(\sum_{i=1}^{n} \frac{1}{a_n}) \geq n^2$$

Proof. For $n = 1$, $(\sum_{i=1}^{1} a_n)(\sum_{i=1}^{1} \frac{1}{a_n}) = \frac{a_1}{a_1} = 1 \geq 1$ Hence, the inequality if true for $n = 1$. Assume it is true for every $k \geq 1$ positive real numbers $a_1, a_2, \cdots, a_k$ that

$$(\sum_{i=1}^{k} a_k)(\sum_{i=1}^{k} \frac{1}{a_k}) \geq k^2$$

Show the inequality is true for $k+1$. Observe that

$(\sum_{i=1}^{k+1} a_{k+1})(\sum_{i=1}^{k+1} \frac{1}{a_{k+1}}) = (\sum_{i=1}^{k} a_k)(\sum_{i=1}^{k} \frac{1}{a_k}) + \sum_{i=1}^{k}(\frac{a_{k+1}}{a_k} + \frac{a_k}{a_{k+1}}) + 1 \geq k^2 + (\frac{a_{k+1}}{a_k} + \frac{a_k}{a_{k+1}}) + 1$

Since $(\frac{a_{k+1}}{a_k} + \frac{a_k}{a_{k+1}}) \geq 2k$, then

$$k^2 + (\frac{a_{k+1}}{a_k} + \frac{a_k}{a_{k+1}}) + 1 \geq k^2 + 2k + 1 = (k+1)^2$$

Hence, by Principle of Mathematical Induction, the claim is true. □

Theorem 7. *If $a_1 = 1, a_2, = 2, a_3 = 3$, and $a_n = 2a_{n-1} - a_{n-3}$ for $n \geq 4$, then $a_n = a_{n-1} + a_{n-2}$ for every integer $n \geq 3$.*

Proof. We use strong induction. Let P(n) be if $a_1 = 1, a_2, = 2, a_3 = 3$, and $a_n = 2a_{n-1} - a_{n-3}$ for $n \geq 4$, then $a_n = a_{n-1} + a_{n-2}$ for every integer $n \geq 3$.

For P(3), $a_3 = a_2 + a_1 \Rightarrow a_3 = 3$. Given that $a_3 = 3$, P(3) is true.

Assume P(i) is true where $3 \leq i \leq k$. We show P(k+1) is true, where $a_{k+1} = a_k + a_{k-1}$. Observe that $a_{k+1} = 2a_k - a_{k-2} = a_k + a_k - a_{k-2} = a_k + a_{k-1} + a_{k-2} - a_{k-2} = a_k + a_{k-1}$. Hence, P(k+1) is true.

By the Strong Principle of Mathematical Induction, if $a_1 = 1, a_2, = 2, a_3 = 3$, and $a_n = 2a_{n-1} - a_{n-3}$ for $n \geq 4$, then $a_n = a_{n-1} + a_{n-2}$ for every integer $n \geq 3$. □

7 Others

Proof Involving Equivalence Relations

Theorem 8. *The relation R on $\mathbb{R}$ if $a - b = k\pi,\ a, b \in \mathbb{R},\ k \in \mathbb{Z}$, is an equivalence relation.*

Proof. To show R is an equivalence relation, we show R is reflexive, symmetric, and transitive.

Assume $a \in R$, then $a - a = 0 \cdot \pi$. It follows that aRa, and R is reflexive.

Assume aRb, then $a - b = k\pi$ for some $k \in \mathbb{Z}$. Then, $b - a = -k\pi$. Since $-k \in \mathbb{Z}$, it follows that bRa whenever aRb, and R is symmetric.

Assume aRb and bRc, then $a - b = k\pi$ and $b - c = k\pi$ for some $k \in \mathbb{Z}$. Observe that $a - c = (a - b) + (b - c) = k\pi + k\pi = (2k)\pi$. Since $2k \in \mathbb{Z}$, it follows that aRc whenever aRb and aRc, and R is transitive.

Hence, R is an equivalence relation because it is reflexive, symmetric, and transitive. □

Proof Involving Sets and De Morgan's Laws

Theorem 9. *If $A_1, A_2, \cdots, A_n$ are any $n \geq 2$ sets, then*

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}.$$

Proof. We proceed by induction. For $n = 2$, the result is De Morgan's law and is therefore true. Assume that the result is true for any k sets, where $k \geq 2$; that is, assume that if $B_1, B_2, \cdots, B_k$ are any k sets, then

$$\overline{B_1 \cap B_2 \cap \cdots \cap B_k} = \overline{B_1} \cup \overline{B_2} \cup \cdots \cup \overline{B_k}$$

We show that it is also true for $k + 1$. Observe that

$$\overline{B_1 \cap B_2 \cap \cdots \cap B_{k+1}} = \overline{B_1} \cup \overline{B_2} \cup \cdots \cup \overline{B_{k+1}}$$

Then, let $S = B_1 \cup B_2 \cdots \cup B_k$.

$$\overline{B_1 \cap B_2 \cap \cdots \cap B_{k+1}} = \overline{S \cup B_{k+1}} = \overline{S} \cap \overline{B_{k+1}}$$

Since $\overline{S} = \overline{B_1 \cup B_2 \cdots \cup B_k} = \overline{B_1} \cap \overline{B_2} \cdots \overline{B_k}$, then

$$\overline{S} \cap \overline{B_{k+1}} = \overline{B_1} \cap \overline{B_2} \cdots \overline{B_k} \cap \overline{B_{k+1}}$$

Hence, by the Principle of Mathematical Induction, if $A_1, A_2, \cdots, A_n$ are any $n \geq 2$ sets, then $\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$. □

Proof Involving Divisibility of Integers

Theorem 10. $7 \mid [3^{4n+1} - 5^{2n-1}]$ *for every positive integer* n.

Proof. We use induction. Let $\mathrm{P}(n)$ be $7 \mid [3^{4n+1} - 5^{2n-1}]$. For $n = 1$, $3^{4(1)+1} - 5^{2(1)-1} = 238 = 7(34)$. Thus, $\mathrm{P}(1)$ is true. Assume $\mathrm{P}(k)$, which is $3^{4k+1} - 5^{2k-1} = 7p$ where p is any integer. We show $\mathrm{P}(k+1)$ is true, which is $3^{4(k+1)+1} - 5^{2(k+1)-1} = 7p$. Observe that

$$\begin{aligned} 3^{4(k+1)+1} - 5^{2(k+1)-1} &= 3^4 \cdot 3^{4k+1} - 5^2 \cdot 5^{2k-1} \\ &= 3^4 \cdot (7p + 5^{2k-1}) - 5^2 \cdot 5^{2k-1} \\ &= 7 \cdot 81p + 56 \cdot 5^{2k-1} \\ &= 7(81p + 8 \cdot 5^{2k-1}) \end{aligned} \tag{3}$$

Since p and k are both integers, $81p + 8 \cdot 5^{2k-1}$ is also an integer. Therefore, $3^{4k+1} - 5^{2k-1}$ is a multiple of 7 and $\mathrm{P}(k+1)$ is true. Hence, by mathematical induction, $7 \mid [3^{4n+1} - 5^{2n-1}]$ for every positive integer n. □

Proofs Involving Cardinalities of Sets

Theorem 11. $| \mathbb{Z} | = | \mathbb{Z} - \{2\} |$.

Proof. To prove that the cardinalities of $\mathbb{Z}$ and $\mathbb{Z} - \{2\}$ are the same, we show that there exists a bijective function f such that $f : \mathbb{Z} \to \mathbb{Z} - \{2\}$. $\mathbb{Z}$ is denumerable since there exists a bijective function $f : \mathbb{N} \to \mathbb{Z}$. Since $\mathbb{Z} - \{2\} \subseteq \mathbb{Z}$, $\mathbb{Z} - \{2\}$ is denumerable. A bijective function $f : \mathbb{Z} \to \mathbb{Z} - \{2\}$ exists such that

$$\ldots, f(0) = 0, f(1) = 1, f(2) = 3, f(3) = 4, \ldots$$

Hence, $| \mathbb{Z} | = | \mathbb{Z} - \{2\} |$. □

Theorem 12. *The set of irrational numbers* $\mathbb{I}$ *is uncountable.*

Proof. Assume, by contradiction, that the set of irrational numbers $\mathbb{I}$ is countable. This implies $\mathbb{I}$ is denumerable. Let $\mathbb{Q}$ be the set of rational numbers. It has been shown that $\mathbb{Q}$ is denumerable. Observe that $\mathbb{Q} \cap \mathbb{I} = \emptyset$. Then, $\mathbb{Q} \cup \mathbb{I}$ is also denumerable. However, $\mathbb{Q} \cap \mathbb{I} = \mathbb{R}$. This implies $\mathbb{R}$ is denumerable, which is a contradiction. Hence, the set of irrational numbers is not denumerable and uncountable. □

Proof Involving Well Ordering Principle

Theorem 13. *If A is a well ordered set and B is a nonempty subset of A, then B is well ordered.*

Proof. To prove that B is well ordered, we show every nonempty subset of B has a least element. Assume A is a well ordered set and B is a nonempty subset of A. By definition of subsets, every subset of B is also a subset of A. Since A is a well-ordered set, every non-empty subset of A has a least element. Therefore, every subset of B has a least element. Hence, B is a well-ordered set. □

Existence Proof

Theorem 14. *There is no positive integer x such that $2x < x^2 < 3x$.*

Proof. Assume, by contradiction, $2x < x^2 < 3x$ and that x is a positive integer. Since $x \in \mathbb{N}$, $2x < x^2 < 3x \Rightarrow 2 < x < 3$. Clearly, x is not an integer, which contradicts the assumption that x is a positive integer. Therefore, by way of contradiction, there is no positive integer x such that $2x < x^2 < 3x$. □

8 Conclusion

Through this writing intensive course on mathematical proofs, I developed my own proof writing style and mastered various techniques of proof. Like writing any other essays, writing proofs require the author to understand the vocabulary and definitions, to identify the audience, to develop a clear and concise structure, and most importantly, to present a logically sound proof for a given statement. This portfolio serves as a reflection on my knowledge in mathematics and my skills in writing mathematical proofs. In the future, as I obtain more mathematical maturity, I will add some of my best works in this portfolio.