A Primer on Mathematical Proof

A *proof* is an argument to convince your audience that a mathematical statement is true. It can be a calculation, a verbal argument, or a combination of both. In comparison to computational math problems, proof writing requires greater emphasis on mathematical rigor, organization, and communication.

A typical theorem may have the form:

Theorem. *Under Conditions A, Statement B is true.*

Here, A is called the *hypothesis* or *assumptions*, and B is called the *conclusion*. Note that mathematicians use the word "hypothesis" differently than it is used in the scientific method. For a mathematician, a 'hypothesis' is not an statement with an absolute 'true' or 'false' value, it is a description of a situation in which the conclusion of the theorem holds.

For example:

Theorem 1. *Suppose that $f(x)$ and $g(x)$ are differentiable real-valued functions, and that $g(x)$ is never equal to zero. Then the quotient $\frac{f(x)}{g(x)}$ is differentiable.*

In this example, the hypotheses are that $f(x)$ and $g(x)$ are differentiable functions and that $g(x)$ is never zero. The conclusion is that $\frac{f(x)}{g(x)}$ is a differentiable function.

A *proof* of a theorem is a series of statements, each following logically from the previous, to reach the conclusion – using only the hypotheses, definitions, and known true statements.

Examples of Theorems and Proofs

Theorem 2. *Suppose that a and n are positive integers such that a^n is divisible by 2. Then a^n is divisible by 2^n.*

Proof. We know that products of odd numbers are odd, so if a were an odd number, then a^n would be an odd number too. Since a^n is even, the integer a must be even. Therefore we can factor $a = 2b$ for some integer b, and

$$a^n = (2b)^n = 2^n b^n.$$

We conclude that a^n is divisible by 2^n.

$\square$

Theorem 3. *Let a and b be real numbers. Suppose that $0 < a \leq b$. Then $\sqrt{a} \leq \sqrt{b}$.*

Note that, for a nonnegative real number x, $\sqrt{x}$ denotes the nonnegative square root of x.

Proof. Since $a \leq b$ by assumption, it follows that

$$(b - a) \geq 0.$$

We know that a and b are both positive, so their square roots are defined. Thus, we can use a difference of squares expansion to write:

$$(\sqrt{b} - \sqrt{a})(\sqrt{b} + \sqrt{a}) = (b - a) \geq 0.$$

Since a and b are strictly positive, so are $\sqrt{a}$ and $\sqrt{b}$. Thus $(\sqrt{b} + \sqrt{a}) > 0$, and we can divide through the above expression without changing the direction of the inequality. We get:

$$(\sqrt{b} - \sqrt{a}) = \frac{(b - a)}{(\sqrt{b} + \sqrt{a})} \geq \frac{0}{(\sqrt{b} + \sqrt{a})} = 0$$

and so we conclude that $\sqrt{b} \geq \sqrt{a}$. $\square$

There is some discretion involved in writing proofs in deciding which statements are well-known or self-evident and which need further justification. For example, in the above proof, we used the fact that positive numbers have positive square roots without justification.

Common Mistakes in Proof-Writing

Common Mistake #1. Starting with the conclusion, and working backwards toward the hypotheses.

This approach can be a good way to brainstorm how the proof will work – but it is *not* appropriate for the final write-up of the proof. At best, such arguments are poor exposition, and at worst they are logically unsound. Always start a proof with the hypotheses and known truths, and work toward the conclusion.

Common Mistake # 2. Checking the conclusion in a few specific examples, and extrapolating that it always holds.

A proof must give a rigorous argument that the conclusion holds in *all* situations satisfying the hypotheses.

For example, if you want to prove that some property holds for all real numbers, then assign a variable (such as x) to represent an arbitrary real number, and prove that property holds for this arbitrary number x. Because x can represent any real number, you can conclude that the property holds for every real number. It is not enough to simply plug in a few numbers for x and check in those cases.

In contrast, you can *disprove* a statement by finding a single example where the hypotheses hold but the statement fails.

Common Mistake #3. Assuming the conclusion.

Suppose, for example, you want to prove that two quantities or expressions A and B are equal. It is a common error to start this proof by equating $A = B$ and then simultaneously manipulating both sides of the equation. This is *not* a valid approach to the proof. Do not start a proof that $A = B$ with the statement $A = B$. It is possible to "prove" false statements this way. Instead, choose one side of the equation (A or B) and work through a sequence of equalities until you arrive at the other side.

For example, the following is a proof that $(x - y)^2 + 4xy = (x + y)^2$ for all real numbers x and y:

$$\begin{aligned}
(x-y)^2 + 4xy &= (x^2 - 2xy + y^2) + 4xy \\
&= x^2 + y^2 - 2xy + 4xy \\
&= x^2 + y^2 + 2xy \\
&= (x+y)^2
\end{aligned}$$

Common Mistake #4. Making steps in the proof without adequate justification.

For this course, you should give justification for any facts that aren't obvious. If you invoke a result that was proved earlier in the course, then you should cite the result and explicitly verify that its hypotheses are satisfied. As a general guideline, the arguments in your proof should be detailed enough to convince someone with the background of a student in this course. Use your judgment about how much to write.

Be sure, too, that the overall structure of the proof is clear. A series of statements or computations are not a complete proof unless it is explained how they connect and why they imply the final result. Most proofs should include full English sentences. Keep in mind that the main goal of the proof is to *communicate* a mathematical argument to the reader.

Common Mistake #5. Overlooking special cases.

For example, if a step in the proof involves dividing by an unknown real number x, you will need to separately treat the case that $x = 0$.

Common Mistake #6. Undeclared variables and undefined notation.

A symbol such as x is meaningless until it is assigned a meaning. A proof should include a declaration of all the objects involved, for example "let x be a real number", or "let f be a continuous function from $\mathbb{R}$ to $\mathbb{R}$". Similarly, any nonstandard notation or shorthand should be defined. Communicate!

Common Mistake # 7. Imprecise statements.

An argument cannot be rigorous if it involves ambiguous or poorly defined statements. Be specific. Use mathematical terminology, and use it correctly.

For example,

Imprecise Sentence: "The sine function looks the same every 2π."

Better Sentences:
"The sine function takes on the same value at any two points in its domain that have a difference of 2π."
"For every real number x, $\sin(x) = \sin(x + 2\pi)$."
"The sine function is periodic with period 2π."

Common Mistake #8. General bad communication.

If you were writing an essay, you would not invent your own words, symbols, or shorthand. You would not write idea fragments without context or support. You would not write a chaotic jumble of ideas across the page with a network of arrows directing your reader in circles.

Please treat your proofs the same way. Remember that the primary purpose of your write-up is to communicate your reasoning to your reader. Please write neatly, grammatically, and in a sensible linear order. The proofs in the textbook (and in class) are good models for proper formatting.

It is good practice to re-read your proofs, imagining how they would look to someone else. Is it clear what all the words and symbols represent? Is it clear what order the proof should be read in? Is it clear which statements are assumptions, which are statements that you are about to prove, and which are deductions? Is the purpose of each line clear – what is being deduced, and why this deduction is logically sound? Does the proof start with known facts, and progress toward the desired conclusion? Or, alternatively, start with one side of a desired equation, and progress through a sequence of equalities toward the other side? Consider having a second person proofread your work, and tell you which aspects need clarification.

Example of a False Statement and Counterexample

To prove that a statement is true, you must show that the conclusion holds in **every** situation that satisfies the hypotheses. You can, however, prove that a statement is **false** by finding a single instance where the hypotheses hold but the conclusion fails. This is called a *counterexample* to the statement.

False Statement. *For all real numbers a and b, $|a + b| = |a| + |b|$.*

Counterexample. Consider the example $a = 1$, $b = -1$. Then

$$|a+b| = |0| = 0 \qquad \text{but} \qquad |a| + |b| = 1 + 1 = 2.$$

It is therefore not always true that $|a+b| = |a| + |b|$.

Logic: Conditional Statements and Equivalence

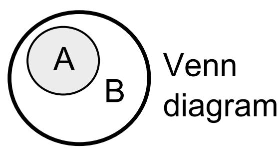
Implication

Let A and B denote properties or mathematical statements. The following notation means "A implies B":

$$A \implies B.$$

Other ways to write this:

- If A is true, then B is true.
- A is true only if B is true.
- B is true whenever A is true.
- B is true if A is true.
- Everything with property A also has property B.
- The set of things with property A is contained in the set of things with property B.



We write $A \not\Longrightarrow B$ to mean "A does not imply B". This means that there is *at least one* example where A holds, but B fails.

Examples of Conditional Statements

"An integer n must be even if it is divisible by 4."

$$\Big(n \text{ is divisible by } 4\Big) \implies \Big(n \text{ is even}\Big)$$

"A real number r can be greater than 10 only if it is strictly positive."

$$\Big(\, r > 10 \,\Big) \implies \Big(r > 0 \Big)$$

"The composition $g \circ f$ of two functions f and g is continuous whenever both functions are continuous."

$$\Big(\, f \text{ and } g \text{ are continuous} \Big) \implies \Big(g \circ f \text{ is continuous} \Big)$$

"Any differentiable function f is continuous."

$$\Big(\, f \text{ is differentiable} \,\Big) \implies \Big(f \text{ is continuous} \Big)$$

Contrapositive

The conditional statement

$$\text{Property } A \text{ holds} \implies \text{Property } B \text{ holds}$$

is logically equivalent to its *contrapositive*, the statement that

$$\text{Property } B \text{ fails} \implies \text{Property } A \text{ fails}$$

Both of these implications mean precisely that there is no situation where A holds and B fails.

Example of a Statement and its Contrapositive

For example, the statement

"If n is an integer, then n is a rational number"

has precisely the same meaning as the statement

"If n is not a rational number, then n cannot be an integer".

Both say that the set of integers is contained in the set of rational numbers.

An example we saw earlier:

"Let n be a positive integer. If a is an odd integer, then a^n is an odd integer."

is equivalent to:

"Let n be a positive integer. If a^n is an even integer, then a is an even integer."

Converse

The conditional statement

$$A \implies B$$

is *not* equivalent to the statement

$$B \implies A,$$

which is called its *converse*.

Example of a True Implication with a False Converse

Let N be an integer. It is true that:

$$\Big(N \text{ is divisible by } 6\Big) \implies \Big(N \text{ is divisible by } 3\Big)$$

. The converse statement, however, is false.

$$\Big(N \text{ is divisible by } 3\Big) \not\Longrightarrow \Big(N \text{ is divisible by } 6\Big)$$

.

Be careful not to confuse a conditional statement with its converse!

Two-Way Implication

We write

$$A \iff B$$

to mean "A is true if and only if B is true". We say that A and B are *equivalent*.

Proving an "if and only if" statement requires two steps: showing $A \implies B$, and showing $B \implies A$.

Examples of Two-Way Implication

Theorem 4. *Let $P(x)$ be a polynomial in x, and let r be a real number. Then $P(r) = 0$ if and only if $(x - r)$ is a factor of P.*

Theorem 5. *Let a and b be real numbers. Then $|a + b| = |a| + |b|$ if and only if $(ab) \geq 0$.*

Theorem 6. *An integer m is divisible by 3 if and only if the sum of its digits is divsible by 3.*

Theorem 7. *An integer p (with $p \neq -1, 0, 1$) is prime if and only if it satisfies the following conditional statement: Whenever p divides a product of integers $a_1 a_2 a_3 \cdots a_n$, p must divide at least one of the factors a_i.*

A Warning About Definitions

There is an unfortunate convention in mathematics to write definitions as "if" statements, even though they should be interpreted as meaning "if and only if".

For example, the statement

"An interval I is called *open* if it does not contain its endpoints"

should be understood to mean

"An interval I is open if and only if it does not contain its endpoints".

Inclusive "or"

By convention, mathematicians use the word "or" to be *inclusive*, that is, the statement "A or B" means either A is true, B is true, or both A and B are true.

For example, the statement

"Every real number is nonnegative or nonpositive."

asserts that every real number x is nonnegative, nonpositive, or both (as is the case with $x = 0$).

The statement:

"Let a, b, p be integers such that p is prime and ab is divisible by p. Then p divides a or b."

asserts that at least one of a and b is divisible by p, and they may both be divisible by p.

An *exclusive 'or'* must be written out explicitly, for example:

"Every integer is either even or odd, but not both."

A second example:

"Let a, b, p be integers such that p is prime and ab is divisible by p but not p^2. Then p divides exactly one of a and b."

Negation

The *negation* of a statement is its logical opposite, sometimes also called the *logical complement*. That is, a statement A is true precisely if its negation is false, and vice versa.

The negation of the statement ”A and B are true” is ”A or B is false”. Remember that ”A or B is false” this means that at least one of A or B is false, and both may be false.

The negation of ”A or B is true” is ”A and B are both false”.

The negation of a statement of the form ”For all x, proposition $P(x)$ holds” has the form ”There exists an x such that proposition $P(x)$ fails.”

The negation of the statement ”There exists an x such that proposition $P(x)$ holds” is ”For every x, proposition $P(x)$ does not hold”.

The negation of the statement ”A implies B” is ”It is possible for A to hold and B to fail”.

Some examples:

(C)	Every polynomial $p(x)$ has a real root.
Negation of (C)	There exists a polynomial with no real roots.
(D)	There exists a function $f(x)$ with derivative $\dfrac{1}{x}$.
Negation of (D)	No function has derivative $\dfrac{1}{x}$.
(E)	Any triangle T is either acute or obtuse.
Negation of (E)	There exists triangles T that are not acute and are not obtuse.
(F)	For all integers m there exists an integer n which is not divisible by m.
Negation of (F)	There exists an integer m such that every integer n is divisible by m.
(G)	If a, b are nonzero integers with $a > b$, then $\dfrac{a}{b} > 0$.
Negation of (G)	There nonzero exists integers a, b such that $a > b$ and $\dfrac{a}{b} \leq 0$.

(**Exercise:** Which of the above statements are true?)

Proof Techniques

Technique #1: Proof by Contradiction

Suppose that the hypotheses are true, but that the conclusion is false. Reach a contradiction. Deduce that if the hypotheses are true, the conclusion must be true too.

Example of a Proof by Contradiction

Theorem 8. *If $|x| < \epsilon$ for* every *real number $\epsilon > 0$, then $x = 0$.*

Proof. Suppose for the sake of eventual contradiction that $|x| < \epsilon$ for every positive number ϵ, but $x \neq 0$.

Since $x \neq 0$, necessarily $\frac{|x|}{2} > 0$, so in particular $|x| < \epsilon$ for the positive number $\epsilon = \frac{|x|}{2} > 0$. This means

$$|x| < \frac{|x|}{2}.$$

But, $|x| \neq 0$ by assumption, so we can divide both sides by $|x|$ to conclude that $1 < \frac{1}{2}$, a contradiction!

Thus, if $|x| < \epsilon$ for every real number $\epsilon > 0$, it must be the case that $x = 0$. □

Technique #2: Proof by Exhaustion

This involves breaking down the proof into a number of cases. Argue that any instance of the theorem falls into one of the cases, and show that the theorem is true in every case.

Example of a Proof by Exhaustion

Theorem 9. *For any real number a, $|a|^2 = a^2$.*

Proof. Since a must satisfy either $a \geq 0$ or $a < 0$, it suffices to prove the result for these two cases.

If $a \geq 0$, then $|a| = a$, so

$$|a|^2 = a^2.$$

If $a < 0$, then $|a| = -a$, so

$$|a|^2 = (-a)^2 = (-1)^2 a^2 = a^2.$$

In all cases, $|a|^2 = a^2$. □

Technique #3: Proof by Induction

This is a technique used to prove a mathematical proposition $P(n)$ involving a natural number n is true for every value of n. $P(n)$ might be a formula

$$\text{for example,} \qquad 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

or a statement involving a variable n

for example, "For every natural number n, $n^3 + 2n$ is divisible by 3."

A proof by induction is structured as follows:

1. **The Base Case.** Prove that the proposition holds when $n = 1$
2. **The Inductive Step.** Prove that, under the assumption that proposition holds for $n = k$ for some natural number k, it follows that it holds for the subsequent number $n = k + 1$.

   The inductive step involves proving a *conditional* statement:

   If $P(n)$ holds when $n = k$, *then* $P(n)$ holds when $n = k + 1$.
3. **Conclusion.** Conclude that the proposition holds for every natural number n.

   Because the proposition holds when $n = 1$, the inductive step implies that it must hold when $n = 2$, and therefore it must hold when $n = 3$, and when $n = 4$, and so forth, for every natural number n.

The reasoning behind a proof by induction is often compared to 'the domino effect'.

Example of a Proof by Induction

Theorem 10. *For any integer $n \geq 1$,*

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Proof. We begin the base case, when $n = 1$. In this case, the left hand side of the equation has a single term,

$$2n - 1 = 2(1) - 1 = 1,$$

and the right-hand side of the equation is

$$n^2 = 1^2 = 1.$$

These qauntities agree, so equality holds when $n = 1$.

Next we make the inductive step. Let k be a fixed positive integer, and assume the formula holds when $n = k$. Specifically, we assume that

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2 \qquad \text{(Inductive hypothesis).}$$

Our goal is to show that, under this assumption, the formula holds when $n = (k + 1)$. Specifically we want to show that:

$$1 + 3 + 5 + \cdots + \big(2(k + 1) - 1\big) = (k + 1)^2.$$

We expand left-hand side:

$$\begin{aligned} &1 + 3 + 5 + \cdots + (2k - 1) + \big(2(k + 1) - 1\big) \\ =&\Big(1 + 3 + 5 + \cdots + (2k - 1)\Big) + \big(2(k + 1) - 1\big) \end{aligned}$$

The quantity $\Big(1 + 3 + 5 + \cdots + (2k - 1)\Big)$ is, by the inductive hypothesis, equal to k^2, so we have:

$$\begin{aligned} &\Big(1 + 3 + 5 + \cdots + (2k - 1)\Big) + \big(2(k + 1) - 1\big) \\ =&\Big(k^2\Big) + \big(2(k + 1) - 1\big) \\ =&k^2 + 2k + 1 \\ =&(k + 1)^2 \qquad \text{as desired,} \end{aligned}$$

and so we conclude that (under the inductive hypothesis) the formula holds when $n = (k + 1)$.

Conclusion: Our base case demonstrates that the equation holds when $n = 1$. Thus, the inductive step implies that it must hold when $n = 2$, and therefore it must hold when $n = 3$, and when $n = 4$, etc, and in this way we conclude that the proposition holds for any integer $n \geq 1$. $\square$

Homework

1. Read through this handout. Make note of any questions you have, or parts of the handout you found confusing.
2. Briefly explain why a mathematical statement of the form "Under conditions A, conclusion B is true" cannot be proven with a single example, but it can be disproven with a single example.
3. Briefly explain why a conditional statement $A \implies B$ is equivalent to its contrapositive.
4. Suppose we know that $A \implies B$ and and we are in a situation where A is false. What can we conclude about B? (Trick question!)

5. Write the following conditional statements in the form $A \implies B$, and write the converses. For each statement, indicate whether the statement is true or false, and indicate whether its converse is true or false.
   (a) If n is an integer, then $2n$ is an integer.
   (b) A number $5n$ is rational only if n is rational.
   (c) Let a and b be real numbers. If $|a| < |b|$, then $a < b$.
6. Write the negation of the following statements.
   (a) The integer p is prime.
   (b) The integers m and n are divisible by 12.
   (c) If $5n$ is an integer then n is an integer.
7. Write an explicit proof of the assertion made in Theorem 2: if an integer a is odd, then any positive power of a is odd. *Hint:* You can define an odd integer to be an integer of the form $(2b+1)$ for some $b \in \mathbb{Z}$. You could complete this proof using the binomial theorem, or, alternatively, by mathematical induction.
8. (a) Prove by induction that for every $n \geq 1$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

   (b) Prove by induction that for any integer $n > 1$, a set of n elements has exactly 2^n distinct subsets. (Note that we always consider the empty set $\varnothing$ to be a subset.)