Proof Methods

Selim Kaan Ozsoy, Middle East Technical University

Proof Methods and Strategies

Formal Proof vs. Informal Proof

In mathematical practice, proofs are written in the daily English (informal), even though we have built a formal system to handle these. Why?

- Formal proofs are too long.
- Informal proofs are easier to read and communicate ideas.

However, every informal proof must be translatable into a formal proof.

Now, we shall learn various Proof Methods.

1. Direct Proof

Most mathematical statements are of the form $P \to Q$.

Method: Assume P is true. Show that Q is true using definitions, axioms, and previously proven theorems.

Example: Parity of Product

Proposition: Let m and n be integers. If m and n are odd, then mn is odd.

Proof: Assume m and n are odd integers. By the definition of odd integers, there exists $k \in \mathbb{Z}$ such that $m = 2k + 1$, and there exists $l \in \mathbb{Z}$ such that $n = 2l + 1$.

Since $k, l \in \mathbb{Z}$, setting $s = 2kl + k + l$. Hence,

$$\begin{aligned} mn &= (2k+1)(2l+1) \\ &= 4kl + 2k + 2l + 1 \\ &= 2(2kl + k + l) + 1 \\ &= 2s + 1 \end{aligned}$$

For $s \in \mathbb{Z}$, $mn = 2s + 1$. Hence, mn is odd. □

2. Proof by Contrapositive

Given a statement of the form $P \to Q$. A proof by contrapositive of $P \to Q$ is a proof of the contrapositive statement $\neg Q \to \neg P$.

Theorem: Let $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.

Proof: We shall do a proof by contrapositive. Assume n is not odd. Then n is even. And so, there exists $k \in \mathbb{Z}$ such that $n = 2k$. Then:

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Since $k \in \mathbb{Z}$, let $m = 2k^2 \in \mathbb{Z}$. Hence, $n^2 = 2m$. Thus, n^2 is not odd (it is even). By contrapositive, if n^2 is odd, then n is odd. □

Example 2: Let $p, q \in \mathbb{Z}^+$. If $n = pq$, then $p \leq \sqrt{n}$ or $q \leq \sqrt{n}$.

Proof: We will prove by contrapositive. Suppose that $\neg(p \leq \sqrt{n} \vee q \leq \sqrt{n})$. This is equivalent to $p > \sqrt{n} \wedge q > \sqrt{n}$ (by De Morgan). Then:

$$p \cdot q > \sqrt{n} \cdot \sqrt{n} = n$$

$$p \cdot q > n$$

Hence $n \neq pq$. Therefore, if $n = pq$, then $p \leq \sqrt{n}$ or $q \leq \sqrt{n}$. □

3. Proof By Contradiction

In a proof by contradiction of a statement P, one assumes $\neg P$ (the negation of P) as hypothesis and works towards a contradiction (like $1 = 0$ or $Q \wedge \neg Q$). This shows that P must be true. A typical format is as follows:

- **Theorem:** P.
- **Proof:** Assume towards a contradiction that $\neg P$.
- ... (logical steps) ...
- ... a contradiction.
- Then P. □

A Famous Example: Irrationality of $\sqrt{2}$

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume towards a contradiction that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. (It follows that the fraction is in simplest form). Squaring both sides:

$$2 = \frac{m^2}{n^2} \implies 2n^2 = m^2$$

By Euclid's Lemma (or previous theorem), since m^2 is even $(2n^2)$, m must be even. So, $m = 2k$ for some $k \in \mathbb{Z}$. Substitute $m = 2k$ back into the equation:

$$\begin{aligned} 2n^2 &= (2k)^2 \\ 2n^2 &= 4k^2 \\ n^2 &= 2k^2 \end{aligned}$$

Since $n^2 = 2k^2$, n^2 is even. By Euclid's Lemma, n is even. So $n = 2l$ for some $l \in \mathbb{Z}$. But if m is even and n is even, then $2|m$ and $2|n$. So $\gcd(m, n) \geq 2$. This contradicts the assumption that $\gcd(m, n) = 1$. Hence $\sqrt{2}$ is irrational. □

Theorem: Infinitude of Primes

Theorem: There are infinitely many prime numbers.

Proof: Suppose for a contradiction that there are finitely many prime numbers. Say, $p_1, p_2, \ldots, p_k$ are all the prime numbers. Let $n = p_1 p_2 \ldots p_k + 1$. By a theorem (Fundamental Theorem of Arithmetic), every integer must be divisible by a prime number. In particular, n is divisible by a prime number q. Since $p_1, \ldots, p_k$ are *all* primes, q must be in the list $p_1, p_2, \ldots, p_k$. So $q|n$ and $q|(n-1)$ (since $n - 1 = p_1 \ldots p_k$). Then $q|(n-(n-1)) \implies q|1$. A contradiction. So there are infinitely many prime numbers. □

Case by Case Proofs

Given a statement P, a case-by-case proof of P is done by splitting into cases covering all possibilities within a proof and obtaining the statement in each case separately.

$$\begin{array}{l} \text{Case I} \ --- \ \text{then } P. \\ \text{Case II} \ --- \ \text{then } P. \\ \vdots \\ \text{Case X} \ --- \ \text{then } P. \end{array}$$

Theorem (Monotonicity from Calculus)

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be a differentiable function. Note that

$$sgn(x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases}$$

If $sgn(f'(x))$ is the same for all $x \in \mathbb{R}$ (constant), then f is monotone.

Proof. Assume that $sgn(f'(x))$ is constant. We split into the following cases:

Case I: ($sgn(f'(x)) = 1$). In this case, $f'(x) > 0$ for all $x \in \mathbb{R}$. By a theorem from Calculus, f must be increasing everywhere, if $a > b$, then $f(a) > f(b)$. Hence f is monotone.

Case II: ($sgn(f'(x)) = 0$). In this case $f'(x) = 0$ for all $x \in \mathbb{R}$, then by a theorem, f must be constant. However, f must be constant. However, constant functions are monotone. (Note: Handwritten text implies logical flow: Constant → Monotone).

Case III: ($sgn(f'(x)) = -1$). In this case $f'(x) < 0$ for all $x \in \mathbb{R}$. Then by a theorem, f must be decreasing everywhere, therefore f is monotone.

This case cannot happen by the assumption of $f(x)$ is not constant? (Note: There is a scratched out box or text here, concluding the proof). Hence, f is monotone. □ □

Proofs of "If and only If" Statements

Given a statement of the form $P \iff Q$, one way to prove the statement(s) is to prove the statements $P \to Q$ and $Q \to P$ separately.

Theorem (Absolute Values)

Theorem: Let a, b be nonzero integers. Then,

$$|a| = |b| \iff a = b \vee a = -b$$

Proof. **(⇒) Direction:** By contrapositive, suppose $a \neq b$ and $a \neq -b$. Then, $|a| \neq |b|$. We split into cases:

Case I: $(|a| < |b|)$. In this case $|a| \neq |b|$.

Case I: $(|a| > |b|)$? (Handwriting seems to reiterate cases or imply trichotomy). In this case $|a| \neq |b|$. (The notes imply: logical argument derived S or Q).

(⇐) Direction: Assume $a = b$ or $a = -b$. Then consider two cases:

Case I: $(a = b)$. Then, since $a = b$, $|a| = |b|$.

Case II: $(a = -b)$. Then, since $a = -b$. Then $|a| = |-b|$. Since $|-b| = |b|$ and $b = |a|(-1)$? (Handwriting: $|a| = |-b| = |b|$). And so $|a| = |b|$.

Hence $|a| = |b|$.

□

How to Prove Statements that involve Quantifiers

Universal Statements

Given a statement of the form $\forall x \in A, P(x)$, one usually proves this statement by picking an **arbitrary** element $x \in A$ and then showing that $P(x)$ holds.

Existential Statements

Given a statement of the form $\exists x \in A, P(x)$, we usually prove the statement by:

- **Construct/choose** an object $a \in A$, such that $P(a)$ holds.
- **Show** that such an object a in A with $P(a)$ holding exists.

Theorem: Let $a, b \in \mathbb{Z}^+$ be given. Then, there exists integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Theorem: For every positive integer n, there exists $a, b, c \in \mathbb{Z}^+$ such that $a^2 + b^2 = c^2$. (Note: Handwritten diagram indicates $\forall n \in \mathbb{N}, \exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, \exists c \in \mathbb{Z}$ s.t. $(a^2 + b^2 = c^2 \wedge a, b, c > n)$).

Proof: Let $n \in \mathbb{Z}^+$. Choose:

- $a = 2n + 1$
- $b = \frac{(2n+1)^2 - 1}{2}$
- $c = \frac{(2n+1)^2 + 1}{2}$

Since we have $a^2 + b^2 = c^2 \iff (c - b)(c + b) = a^2$, notice that $(c - b) = 1$ and $(c + b) = (2n + 1)^2$. So $1 \cdot (2n + 1)^2 = (2n + 1)^2$. So $a^2 + b^2 = c^2$. Moreover, $a = 2n + 1 > n$, $b = \frac{(2n+1)^2 - 1}{2} = \frac{4n^2 + 4n}{2} = 2n^2 + 2n > n$. And $c = 2n^2 + 2n + 1 > n$. Then the theorem follows.

How to Prove Equivalence of Several Statements

Given statements $P_1, P_2, \ldots, P_n$, one way to prove that all these statements are logically equivalent is to prove the implications:

$$P_1 \implies P_2, \quad P_2 \implies P_3, \quad \ldots, \quad P_{n-1} \implies P_n, \quad P_n \implies P_1.$$

Example: Let $a, b \in \mathbb{Z}^+$. Then the following are equivalent (TFAE):

(i) a and b are relatively prime.

(ii) a and $a+b$ are relatively prime.

(iii) a and $a-b$ are relatively prime.

Proof: $(i) \implies (ii)$**:** By contrapositive, suppose a and $a+b$ are not relatively prime. Then there exists $d = \gcd(a, a+b) \geq 2$. Then, by a theorem, $d|a$ and $d|a+b$, then $d|b$. Since $d|a$ and $d|b$ and $d \geq 2$, this means a and b are not relatively prime.

$(ii) \implies (iii)$**:** By contrapositive, suppose a and $a-b$ are not relatively prime. Then $\gcd(a, a-b) = d \geq 2$. For some $d \in \mathbb{Z}^+$. Since $d|a$ and $d|a-b$, then $d|a-(a-b) = b$. Since $d|a$ and $d|b$, then $d|a+b$. Then $\gcd(a, a+b) = d \geq 2$. So a and $a+b$ are not relatively prime.

$(iii) \implies (i)$**:** By contrapositive, suppose that a and b are not relatively prime. Then $d = \gcd(a, b) \geq 2$ for some $d \in \mathbb{Z}^+$. Then $d|a$ and $d|b$ and so $d|a-b$. Since $d|a-b$ and $d|a$ and $d \geq 2$, it follows that $\gcd(a-b, a) = d \geq 2$. So $a-b$ and a are not relatively prime. □

Uniqueness Proofs

Given a statement of the form "There exists a unique $x \in A$ such that $P(x)$", one way to prove this statement is the following:

Step I: **Prove** that such $x \in A$ exists. (**Existence**)

Step II: **Put** two arbitrary $x, y \in A$ such that $P(x)$ and $P(y)$ and show that $x = y$.

$$\exists! x \in A \quad P(x) \iff (\exists x \in A \quad P(x)) \wedge (\forall x, y \in A \quad (P(x) \wedge P(y) \to x = y))$$

Theorem

Let $a \geq 1$ be an integer. Then there exists a **unique** pair of positive integers m, n such that

$$a = 2^m \cdot n \quad \text{and} \quad n \text{ is odd.}$$

Proof (Existence): Consider the set $S = \{2^k \mid k \in \mathbb{N} \text{ and } 2^k|a\}$. Since $2^0 = 1$ and $1|a$, S is non-empty. Since S is a set of integers and it is bounded above (by a), then by the **Well Ordering Principle** (or its consequence), there exists a **largest** element.

Let k_0 be the **largest** element of S. Choose $m = k_0$. Then $2^m|a$. This means $a = 2^m \cdot n$ for some $n \in \mathbb{Z}^+$.

We claim that n is odd. Suppose towards a contradiction that n is even. If it were that $2|n$, then we would have $n = 2l$ for some $l \in \mathbb{Z}^+$. Then:

$$a = 2^m \cdot n = 2^m \cdot (2l) = 2^{m+1} \cdot l$$

This implies $2^{m+1}|a$, which means $2^{m+1} \in S$. However, $2^{m+1} > 2^m$, which contradicts that 2^m is the **largest** element of S. Therefore, n is not even, so n is odd. □