Proof

Xiaofeng Gao

Department of Computer Science and Engineering
Shanghai Jiao Tong University, P.R.China

October 31, 2016

Outline

What is proof?

A proof of a statement is essentially a convincing argument that the statement is true. A typical step in a proof is to derive statements from

- assumptions or hypotheses.
- statements that have already been derived.
- other generally accepted facts, using general principles of logical reasoning.

Types of Proof

- Proof by Construction
- Proof by Contrapositive
  - Proof by Contradiction
  - Proof by Counterexample
- Proof by Cases
- Proof by Mathematical Induction
  - The Principle of Mathematical Induction
  - Minimal Counterexample Principle
  - The Strong Principle of Mathematical Induction

Proof by Construction ($\forall x, P(x)$ holds)

Example: For any integers a and b, if a and b are odd, then ab is odd.

Proof: Since a and b are odd, there exist integers x and y such that $a = 2x + 1$, $b = 2y + 1$. We wish to show that there is an integer z so that $ab = 2z + 1$. Let us therefore consider ab.

$$\begin{aligned} ab &= (2x+1)(2y+1) \\ &= 4xy + 2x + 2y + 1 \\ &= 2(2xy + x + y) + 1 \end{aligned}$$

Thus if we let $z = 2xy + x + y$, then $ab = 2z + 1$, which implies that ab is odd. $\square$

Proof by Contrapositive ($p \to q \Leftrightarrow \neg q \to \neg p$)

Example: $\forall i, j, n \in \mathbb{N}$, if $i \times j = n$, then either $i \leq \sqrt{n}$ or $j \leq \sqrt{n}$.

Proof: We change this statement by its logically equivalence:
$\forall i, j, n \in \mathbb{N}$, if it is not the case that $i \leq \sqrt{n}$ or $j \leq \sqrt{n}$, then $i \times j \neq n$.

If it is not true that $i \leq \sqrt{n}$ or $j \leq \sqrt{n}$, then $i > \sqrt{n}$ and $j > \sqrt{n}$.

Since $j > \sqrt{n} \geq 0$, we have

$$i > \sqrt{n} \Rightarrow i \times j > \sqrt{n} \times j > \sqrt{n} \times \sqrt{n} = n.$$

It follows that $i \times j \neq n$. The original statement is true. $\square$

Proof by Contradiction (p is true $\Leftrightarrow \neg p \to$ *false* is true)

Example: For any sets A, B, and C, if $A \cap B = \emptyset$ and $C \subseteq B$, then $A \cap C = \emptyset$.

Proof: Assume $A \cap B = \emptyset$, $C \subseteq B$, and $A \cap C \neq \emptyset$.

Then there exists x with $x \in A \cap C$, so that $x \in A$ and $x \in C$.

Since $C \subseteq B$ and $x \in C$, it follows that $x \in B$.

Therefore $x \in A \cap B$, which contradicts the assumption that $A \cap B = \emptyset$. $\square$

Proof by Cases (Divide domain into distinct subsets)

Example: Prove that if $n \in \mathbb{N}$, then $3n^2 + n + 14$ is even.

Proof: Let $n \in \mathbb{N}$. We can consider two cases: n is even and n is odd.

Case 1. n is even. Let $n = 2k$, where $k \in \mathbb{N}$. Then

$$\begin{aligned} 3n^2 + n + 14 &= 3(2k)^2 + 2k + 14 \\ &= 12k^2 + 2k + 14 \\ &= 2(6k^2 + k + 7) \end{aligned}$$

Since $6k^2 + k + 7$ is an integer, $3n^2 + n + 14$ is even if n is even.

Proof by Cases (Cont.)

Case 2. n is odd. Let $n = 2k + 1$, where $k \in \mathbb{N}$. Then

$$\begin{aligned} 3n^2 + n + 14 &= 3(2k+1)^2 + (2k+1) + 14 \\ &= 3(4k^2 + 4k + 1) + (2k+1) + 14 \\ &= 12k^2 + 12k + 3 + 2k + 1 + 14 \\ &= 12k^2 + 14k + 18 \\ &= 2(6k^2 + 7k + 9) \end{aligned}$$

Since $6k^2 + 7k + 9$ is an integer, $3n^2 + n + 14$ is even if n is odd.

Since in both cases $3n^2 + n + 14$ is even, it follows that if $n \in \mathbb{N}$, then $3n^2 + n + 14$ is even. □

The Principle of Mathematical Induction

Suppose $P(n)$ is a statement involving an integer n. Then to prove that $P(n)$ is true for every $n \geq n_0$, it is sufficient to show these two things:

- $P(n_0)$ is true.
- For any $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

An Example for Mathematical Induction

Example: Let $P(n)$ be the statement $\sum_{i=0}^{n} i = n(n+1)/2$. Prove that $P(n)$ is true for every $n \geq 0$.

Proof: We prove $P(n)$ is true for $n \geq 0$ by induction.

Basis step. $P(0)$ is $0 = 0(0+1)/2$, and it is obviously true.

Induction Hypothesis. Assume $P(k)$ is true for some $k \geq 0$. Then $0 + 1 + 2 + \cdots + k = k(k+1)/2$.

Proof of Induction Step. Now let us prove that $P(k+1)$ is true.

$$\begin{aligned} 0 + 1 + 2 + \cdots + k + (k+1) &= k(k+1)/2 + (k+1) \\ &= (k+1)(k/2+1) \\ &= (k+1)(k+2)/2 \end{aligned}$$ □

The Minimal Counterexample Principle

Example: Prove $\forall n \in \mathbb{N}$, $5^n - 2^n$ is divisible by 3.

Proof: If $P(n) = 5^n - 2^n$ is not true for every $n \geq 0$, then there are values of n for which $P(n)$ is false, and there must be a smallest such value, say $n = k$.

Since $P(0) = 5^0 - 2^0 = 0$, which is divisible by 3, we have $k \geq 1$, and $k - 1 \geq 0$.

Since k is the smallest value for which $P(k)$ false, $P(k-1)$ is true. Thus $5^{k-1} - 2^{k-1}$ is a multiple of 3, say $3j$.

The Minimal Counterexample Principle (Cont.)

However, we have

$$\begin{aligned} 5^k - 2^k &= 5 \times 5^{k-1} - 2 \times 2^{k-1} \\ &= 5 \times (5^{k-1} - 2^{k-1}) + 3 \times 2^{k-1} \\ &= 5 \times 3j + 3 \times 2^{k-1} \end{aligned}$$

This expression is divisible by 3. We have derived a contradiction, which allows us to conclude that our original assumption is false. □

An Example for the Weakness of Mathematical Induction

Example: Prove that $\forall n \in \mathbb{N}$ with $n \geq 2$, it has prime factorizations.

Proof: Define $P(n)$ be the statement that "n is either prime or the product of two or more primes". We will try to prove that $P(n)$ is true for every $n \geq 2$.

Basis step. $P(2)$ is true, since 2 is a prime. ✓

Induction hypothesis. $P(k)$ for $k \geq 2$. (as usual process)

Proof of induction step. Let's prove $P(k+1)$.

If $P(k+1)$ is prime, ✓
If $P(k+1)$ is not a prime, then we should prove that $k+1 = r \times s$, where r and s are positive integers greater than 1 and less than $k+1$.

However, from $P(k)$ we know nothing about r and s $\longrightarrow$???

The Strong Principle of Mathematical Induction

Suppose $P(n)$ is a statement involving an integer n. Then to prove that $P(n)$ is true for every $n \geq n_0$, it is sufficient to show these two things:

- $P(n_0)$ is true.
- For any $k \geq n_0$, if $P(n)$ is true for every n satisfying $n_0 \leq n \leq k$, then $P(k+1)$ is true.

Also called the principle of complete induction, or course-of-values induction.

To Complete the Example

Example: Prove that $\forall n \in \mathbb{N}$ with $n \geq 2$, it has prime factorizations.

Continue the Proof:
Induction hypothesis. For $k \geq 2$ and $2 \leq n \leq k$, $P(n)$ is true. (Strong Principle)

Proof of induction step. Let's prove $P(k+1)$.

If $P(k+1)$ is prime, ✓
If $P(k+1)$ is not a prime, by definition of a prime, $k+1 = r \times s$, where r and s are positive integers greater than 1 and less than $k+1$.

It follows that $2 \leq r \leq k$ and $2 \leq s \leq k$. Thus by induction hypothesis, both r and s are either prime or the product of two or more primes. Then their product $k+1$ is the product of two or more primes. $P(k+1)$ is true.

Giuseppe Peano (1858-1932)

- In 1889, Peano published the first set of axioms.
- Build a rigorous system of arithmetic, number theory, and algebra.
- A simple but solid foundation to construct the edifice of modern mathematics.
- The fifth axiom deserves special comment. It is the first formal statement of what we now call the “induction axiom" or “the principle of mathematical induction".

Peano Five Axioms

- Axiom 1. 0 is a number.
- Axiom 2. The successor of any number is a number.
- Axiom 3. If a and b are numbers and if their successors are equal, then a and b are equal.
- Axiom 4. 0 is not the successor of any number.
- Axiom 5. If S is a set of numbers containing 0 and if the successor of any number in S is also in S, then S contains all the numbers.

Peano Axioms vs Theorem of Mathematical Induction

Let $S(n)$ be a statement about $n \in \mathbb{N}$. Suppose

1. $S(1)$ is true, and
2. $S(t+1)$ is true whenever $S(t)$ is true for $t \geq 1$.

Then $S(n)$ is true for all $n \in \mathbb{N}$.

Can use contradiction and Peano Axiom to prove the correctness of $S(n)$.