Proof Techniques

Dr. Shatrughan
Modi

What is a proof?

- A proof is a sequence of logical statements, one implying another, which gives an explanation of why a given statement is true.
- Previously established theorems may be used to deduce the new ones.
- We may also refer to axioms, which are the starting points, “rules” accepted by everyone.
- Mathematical proof is absolute, which means that once a theorem is proved, it is proved for ever.

Methods of proofs

- There are many techniques that can be used to prove the statements.
- **Direct proofs**: assumes a given hypothesis, or any other known statement, and then logically deduces a conclusion.
- **Indirect proof:** also called proof by contradiction, assumes the hypothesis (if given) together with a negation of a conclusion to reach the contradictory statement.
- It is often equivalent to proof by contrapositive, though it is subtly different.
- Both direct and indirect proofs may also include additional tools to reach the required conclusions, namely proof by cases or mathematical induction.

Direct Proof

- The easiest approach to establish the theorems, as it does not require knowledge of any special techniques.
- The argument is constructed using a series of simple statements, where each one should follow directly from the previous one
- To prove the hypothesis, we may use axioms, as well as the previously established statements of different theorems.
- Propositions of the form $A \Rightarrow B$ are shown to be valid by starting at A by writing down what the hypothesis means and consequently approaching B using correct implications.

Example

- Let n and m be integers. If n and m are both even, then prove that $n + m$ is even

Proof:

- If n and m are even, then there exist integers k and j such that $n = 2k$ and $m = 2j$.
- Then $n + m = 2k + 2j = 2(k + j)$.
- And since $k, j \in Z, (k + j) \in Z$. $\therefore$ $n + m$ is even.

Example

- If m and n are both square numbers, then prove that m n is also a square number

Proof

Counterexample

- A counterexample is an example that disproves a universal statement.
- One counterexample is enough to say that the statement is not true, even though there will be many examples in its favor.

Example:

Conjecture: let $n \in N$ and suppose that n is prime. Then $2^n - 1$ is prime.

- Counterexample: when $n = 11$
- $\Rightarrow 2^{11} - 1 \Rightarrow 23 \times 89$.

Fallacious Proofs

- Study the sequence of sentences below and try to find what went wrong. We prove that 1 = 2.
- $a = b$

$\Rightarrow a^2 = ab$

$\Rightarrow a^2 + a^2 = ab + a^2$

$\Rightarrow 2a^2 = ab + a^2$

$\Rightarrow 2a^2 - 2ab = ab + a^2 - 2ab$

$\Rightarrow 2a^2 - 2ab = a^2 - ab$

$\Rightarrow 2(a^2 - ab) = 1(a^2 - ab)$

$\Rightarrow 2 = 1.$

Sometimes we do a mistake unknowingly while proving a statement.

Proof by cases

- Proof by cases is sometimes also called proof by exhaustion, because the aim is to exhaust all possibilities.
- The problem is split into parts and then each one is considered separately
- Example: Let $n \in Z$. Then $n^2 + n$ is even.
- CASE I: n is even
- CASE II: n is odd

Example

- If an integer n is not divisible by 3, then prove that $n^2 = 3k + 1$ for some integer k

Proof by contradiction

- The basic idea is to assume that the statement we want to prove is false, and then show that this assumption leads to a contradiction

Example

- Let a be rational number and b irrational. Then prove that $a + b$ is irrational

Proof

- Suppose that $a + b$ is rational, so $a + b := m/ n$.
- Now, as a is rational, we can write it as $a := p /q$.
- $b= (a + b) – a$
- $= (m/n)-(p/q)$
- $=(mq-pn)/qn$
- hence b is rational, which contradicts the assumption.

Proof by contrapositive

- To prove a statement of the form “If A, then B,” do the following:

1. Form the contrapositive. In particular, negate A and B.
2. Prove directly that $\neg B$ implies $\neg A$.

Example

- Prove by contrapositive: Let $x \in Z$. If $x^2 - 6x + 5$ is even, then x is odd.

Proof:

- Suppose that x is even. Then we want to show that $x^2 - 6x + 5$ is odd.
- Write $x = 2a$ for some $a \in Z$, then

$$x^2 - 6x + 5$$

$$= (2a)^2 - 6(2a) + 5$$

$$= 4a^2 - 12a + 5 = 2(2a^2 - 6a + 2) + 1.$$

Thus $x^2 - 6x + 5$ is odd

Example

- If $3n + 2$ is an odd integer, then prove that n is odd.

Proof by Induction

Mathematical induction

- Mathematical induction is a very useful mathematical tool to prove theorems on natural numbers.
- Three parts:
  - Base case(s): show it is true for one element
  - Inductive hypothesis: assume it is true for any given element
  - Show that if it true for the next highest element

Principle of Mathematical Induction

Let $P(n)$ be an infinite collection of statements with $n \in \mathbb{N}$. Suppose that

(i) $P(1)$ is true, and

(ii) $P(k) \Rightarrow P(k+1)$, $\forall k \in \mathbb{N}$.

Then, $P(n)$ is true $\forall n \in \mathbb{N}$.

- INDUCTION BASE check if $P(1)$ is true, i.e. the statement holds for $n = 1$,
- INDUCTION HYPOTHESIS assume $P(k)$ is true, i.e. the statement holds for $n = k$,
- INDUCTION STEP show that if $P(k)$ holds, then $P(k+1)$ also does.

Example 1

- Prove by mathematical induction that for all positive integers n

  $1+2+3+\ldots\ldots+n=n(n+1)/2$

Example 2

- Prove by mathematical induction that for all positive integers n

$$1\times 2 + 2\times 3 + 3\times 4 + \ldots\ldots\ldots + n\times(n+1) = n(n+1)(n+2)/3$$

Example 3

- Show that $n! < n^n$ for all $n > 1$

Strong Induction

Strong induction

- Weak mathematical induction assumes P(k) is true, and uses that (and only that!) to show P(k+1) is true
- Strong mathematical induction assumes P(1), P(2), …, P(k) are all true, and uses that to show that P(k+1) is true.

Example 1

- Prove that if n is an integer greater than 1, then it is either a prime or can be written as the product of primes.
- Base case (n=2): Since 2 is a prime number, P(2) holds.
- Inductive step: Assume each of 2, 3, . . . , k is either prime or product of primes.
- Now, we want to prove the same thing about k+1
- There are two cases:
  - k+1 is prime
  - k+1 is composite

Strong induction vs. non-strong induction

- Show that every postage amount 12 cents or more can be formed using only 4 and 5 cent stamps

Answer via mathematical induction

- Show base case: P(12):
  - $12 = 4 + 4 + 4$
- Inductive hypothesis: Assume P(k) is true
- Inductive step: Show that P(k+1) is true
  - If P(k) uses a 4 cent stamp, replace that stamp with a 5 cent stamp to obtain $P(k+1)$
  - If P(k) does not use a 4 cent stamp, it must use only 5 cent stamps
    - Since $k >= 12$, there must be at least three 5 cent stamps
    - Replace these with four 4 cent stamps to obtain $k+1$
- Note that only $P(k)$ was assumed to be true

Answer via strong induction

- Show base cases: P(12), P(13), P(14), and P(15)
  - $12 = 4 + 4 + 4$
  - $13 = 4 + 4 + 5$
  - $14 = 4 + 5 + 5$
  - $15 = 5 + 5 + 5$
- Inductive hypothesis: Assume P(12), P(13), …, P(k) are all true
  - For $k \geq 15$
- Inductive step: Show that P(k+1) is true
  - We will obtain P(k+1) by adding a 4 cent stamp to P(k+1-4)
  - Since we know P(k+1-4) = P(k-3) is true, our proof is complete
- Note that P(12), P(13), …, P(k) were all assumed to be true

THANK YOU

Structural Induction

Structural Induction

- Structural induction is a proof methodology similar to mathematical induction, only instead of working in the domain of positive integers (N) it works in the domain of recursively defined structures.

Recursively defined functions

- Assume f is a function with the set of nonnegative integers as its domain
- We use two steps to define f.
  - Basis step:

    Specify the value of f(0).
  - Recursive step:

    Give a rule for f(x) using f(y) where $0 \le y < x$
- Such a definition is called a recursive or inductive definition

Methodology

- Assume we have recursive definition for the set S. Let $n \in S$.
- Show P(n) is true using **structural induction**:

Basis step:

- Assume j is an element specified in the basis step of the definition.
- Show $\forall j\ P(j)$ is true.

Recursive step: Let x be a new element constructed in the recursive step of the definition.

Assume $k_1, k_2, \ldots, k_m$ are elements used to construct an element x in the recursive step of the definition.

Show $\forall k_1, k_2, \ldots, k_m\ ((P(k_1) \wedge P(k_2) \wedge \ldots \wedge P(k_m)) \rightarrow P(x))$.

Example

- Show that well-formed formulae for compound propositions contains an equal number of left and right parentheses.

Proof by structural induction:

Define P(x)

P(x) is “well-formed compound proposition x contains an equal number of left and right parentheses”

Basis step: (P(j) is true, if j is specified in basis step of the definition.)

T, F and propositional variable p is constructed in the basis step of the definition.

Since they do not have any parentheses, P(T), P(F) and P(p) are true.

Contd..

- **Recursive step:**
- Assume p and q are well-formed formulae.
- Let lp be the number of left parentheses in p.
- Let rp be the number of right parentheses in p.
- Let lq be the number of left parentheses in q.
- Let rq be the number of right parentheses in q.
- Assume lp= rp and lq= rq.