Methods of Proofs

Peter Lo

Predicate Logic

- ∀ and ∃ are known as **Predicate Quantifiers**
  - ∀ means **FOR ALL**
  - ∃ means **THERE EXIST**
- Example:
  - If we have 1 computer for all students, we say:
    - ∃ one computer ∀ students
  - If each student has a separate computer
    - ∀ students ∃ one computer

Odd and Even Numbers

- Odd Number
  - We donated as $\{x \mid x=2p+1, \forall x, p \in Z\}$
- Even Number
  - We denoted as $\{x \mid x=2p, \forall x, p \in Z\}$

Absolution Value

- The Absolution Value of a number x, denote by the symbol |x|, is defined by the rules:
  - $|x| = x, \forall x \geq 0$
  - $|x| = -x, \forall x < 0$

Divisibility

- If a divides b, we write a | b.
  - i.e. b/a = c { $\forall a,b,c \in Z$}
- Example:
  - 3 | 18 is True
    - Because 18 = 3 x 6.

Types of Numbers

- **Natural numbers** are the counting number and the set of Natural Numbers is the set {1, 2, 3, … }.
- A **Prime Number** is a natural number greater than 1 that is divisible only by itself and 1.
- A **Composite Number** is a natural Number greater than 1 that is not a prime number.
  - Note that 1 is the only natural number that is neither prime number nor composite number

Types of Numbers

- **Whole Numbers** is the union of 0 and the set of natural number. The set of whole number is the set {0, 1, 2, 3, … }.
- **Integer** is the union of the set of whole numbers and the set of negative numbers. The set of Integer is the set {…, -3, -2, -1, 0, 1, 2, 3, … }.

Types of Numbers

- A **Rational Number** is any number that can be written in the form a/b, and denoted as
  - {x | x = a / b, $\forall a,b \neq 0, a,b \in Z$ }
- An **Irrational Number** is a decimal that cannot be written in the form a/b, where a and b are integers and $b \neq 0$.
- **Real Number** is the union of the set of rational numbers and the set of irrational numbers. The set real number is denoted by the symbol $\Re$.

Recurrence Relation

- A Recurrence Relation is an equation that defines the i^{th} value in a sequence of numbers in terms of the preceding i-1 values.
- For example,
  - $n! = n(n-1)!$
    $= n(n-1)(n-2)\ldots\ldots 3\times2\times1$
- (Do Ex. 1)

Sequences

- A sequence is a list in which order is taken into account.
  - Finite Sequence: 1, 2, 3,4, 5, 6, … n
  - Infinite Sequence: 1, 2, 3, 4, 5, 6, …
- (Do Ex. 2 – 3)

Series

- A series is the summation of a sequence such as $a_1 + a_2 + a_3 + \ldots + a_n$
- (Do Ex. 4)

Summation Properties

Summation Properties

1. $\sum_{i=a}^{b} i = \sum_{i=a+k}^{b+k} (i-k) \quad k \in N$
2. $\sum_{i=a}^{b} i = \sum_{i=a-k}^{b-k} (i+k) \quad k \in N$
3. $\sum_{i=a}^{b} cx_i = c\sum_{i=a}^{b} x_i \quad c$ is a constant, x_i is an expression involving i.
4. $\sum_{i=a}^{b} (x_i + y_i) = \sum_{i=a}^{b} x_i + \sum_{i=a}^{b} y_i \quad x_i$ and y_i are expressions involving i.
5. $\sum_{i=1}^{n} c = nc \quad c$ is a constant.
6. $\sum_{i=a}^{a} x_i = x_a \quad x_i$ is an expression involving i.

Exponents

The Rules of Exponents
$x^r \cdot x^n = x^{r+n}$
$\frac{x^n}{x^m} = x^{n-m}$
$(x^n)^m = x^{nm}$
$x^0 = 1,\ x \neq 0$
$x^{-n} = \frac{1}{x^n}$
$(xy)^n = x^n \cdot y^n$
$\left(\frac{x}{y}\right)^n = \frac{x^n}{y^n}$

Logic

- Given a statement $p \rightarrow q$
  - The **Inverse** of $p \rightarrow q$ is $\sim p \rightarrow \sim q$.
  - The **Converse** of $p \rightarrow q$ is $q \rightarrow p$.
  - The **Contrapositive** of $p \rightarrow q$ is $\sim q \rightarrow \sim p$
- (Do Ex. 5 – 6)

Method of Proofs

- Direct Proofs
- Contrapositive Proofs
- Proofs by Contradiction
- Counterexamples
- Mathematical Induction

Direct Proofs

- A **Direct Proof** assumes that $p(x_1, x_2, \ldots x_n)$ is true and then, using $p(x_1, x_2, \ldots x_n)$ as well as other axioms, definitions and theorem, to show that $q(x_1, x_2, \ldots x_n)$ is true.

Example

- Give a direct proof that the sum of three consecutive integers is divisible by 3.
- Answer

  Let the three consecutive integers be n, n+1 and n+2.

  Sum = n + (n+1) + (n+2)

  = 3n + 3

  = 3(n+1), which is divisible by 3.

Contrapositive Proofs

- **Contrapositive**, is based on the fact that $\sim Q \Rightarrow \sim P$ is logically equivalent to $P \Rightarrow Q$
  - i.e. $(\sim q \rightarrow \sim p) \leftrightarrow (p \rightarrow q)$

Example

- Consider the statement 'If it is cold then Tony will wear a coat.' Write down the contrapositive of this statement.
- Answer:
  - 'If Tony is not wearing a coat, then it is not cold.'

Proofs by Contradiction

- A **Proof by Contradiction** is a proof of an implication that shows that joining the assumption "Q is False" together with the premise "P is True" leads to a contradiction.

Example

- Let n be a positive integer. Given a proof by contradiction that if n is a prime number different from 2, then n is odd.

The contrapositive form of the statement "If n is a prime number different from 2, then n is odd" is "If n is even, then either $n = 2$ or n is a not a prime number." We suppose that n is even. Then $n = 2 \cdot p$ for a positive integer, $p < n$. Now, either $p = 1$ or $p > 1$. If $p = 1$, then $n = 2$. If $p > 1$, then n is not prime because n is divisible by p and $p \neq n$ or $p \neq 1$. In either case, we have proven the contrapositive. Therefore, the initial implication is *true*.

Counterexamples

- The universally quantified statement P(x) is False if for at least one x in the domain of discourse, the proposition P(x) is False. A value x in the domain of discourse that makes P(x) false is called Counterexample to the statement P(x).
- (Do Ex. 7)

Example 1

- Disprove the following statements by giving a counterexample.
  - The product of any two prime numbers is prime.
  - The difference of any two odd integers is odd.
  - For all integers n, n^2 - n + 11 is a prime number.

(i) E.g. 3 and 5 are both prime numbers, but $3 \times 5 = 15$ is not prime.

(ii) E.g. 5 and 3 are odd integers, but $5 - 3 = 2$ is even.

(iii) E.g. When $n = 11$, $n^2 - n + 11 = 121$ is not prime.

Example 2

- Let R be the relation on the set Z+ of positive integers defined by aRb if and only if a=b. Prove or give a counter-example to determine the following properties:
  - Reflexivity
  - Symmetry
  - Transitivity

(i) $a \leq a \forall a \in \mathbb{Z}^+$, so aRa, and so R is reflexive .

(ii) $1 \leq 2$, but $2 \leq 1$ and so R is not symmetric .

(iii) $a \leq b, b \leq c \Rightarrow a \leq c$, so $aRb, bRc \Rightarrow aRc$, and so R is transitiv e.

Mathematical Induction

- Mathematical induction is a method of proving a law or theorem by showing that it holds in the first case and showing that, if it holds for all case preceding a given one, then it also holds for this case.
- The essential steps of the proof:
  - Prove the theorem for the first case.
  - Prove that if the theorem is true for the n^{th} case (or for the fist through n^{th} case), then it is true for the $(n+1)^{th}$ case.

Principle of M.I.

Prove: $P(n)$ for all integers $n \geq k$

Principle of Mathematical Induction

Let P(n) be a proposition that is valid for $n \geq k$, n, k integers.

If (1) P(k) is true, and

(2) $\forall n \geq k, P(n) \Rightarrow P(n+1)$

then P(n) is true $\forall n \geq k$

Example 1

- Use Mathematical Induction to prove that

$$3\sum_{k=0}^{n} 5^k = \frac{3}{4}(5^{n+1}-1)$$

whenever n is a nonnegative integer.

Let $P(m)$ be the statement $3\sum_{k=0}^{m} 5^k = 3(5^{m+1}-1)/4$.
Step 1. Prove $P(0)$.
$3\sum_{k=0}^{0} 5^k = 3$
$3(5^{0+1}-1)/4 = 3$ *One mark.*

Step 2. Assume $P(m)$ and prove $P(m+1)$.

$$\begin{aligned} 3\sum_{k=0}^{m+1} 5^k &= 3\sum_{k=0}^{m} 5^k + 3\times 5^{m+1} \\ &= \frac{3(5^{m+1}-1)}{4} + 3\times 5^{m+1} \\ &= \frac{3(5^{m+1}-1+4\times 5^{m+1})}{4} \\ &= \frac{3(5^{m+2}-1)}{4} \end{aligned}$$

Example 2

- Use mathematical induction to prove that

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

whenever n is a nonnegative integer.

Step 1: show that statement is true for $n = 1$. When $n = 1$, LHS=1, RHS=1.

Step 2: Prove that if it is true for n then it is true for $n+1$.

$$\begin{aligned} \sum_{j=1}^{n+1} j &= n+1+\sum_{j=1}^{n} j \\ &= n+1+\frac{n(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

Example 3

- A function, f (n), defined for positive integers n, satisfies the following conditions:

  $f(1) = 2$

  $f(n + 1) = 2f(n)$ for n = 1,2,3,...

  Use Mathematical Induction to prove that $f(n) = 2n$ for n = 1,2,3,....

First step, prove true for $n = 1$.
When $n = 1$, $f(1) = 2$, and $2^1 = 2$ and so $f(n) = 2^n$ for $n = 1$.
Second step, assume true for $n = k$. Prove that it is then true for $n = k + 1$.
Suppose that $f(k) = 2^k$. Then

$$\begin{aligned} f(k+1) &= 2f(k) \\ &= 2 \times 2^k \\ &= 2^{k+1} \end{aligned}$$

so it is also true for $k + 1$.
Then, by induction, it is true for any $n = 1,2,3,....$

Example 4

- Prove by mathematical induction that

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

for n=1,2,3,...

Prove true for n=1

LHS = $\sum_{k=1}^{1} k^2 = 1$

RHS = $\frac{(1)(2)(3)}{6} = 1$

So statement true for n=1.

Assume true for n=N, prove true for n=N+1

$$\sum_{k=1}^{N+1} k^2 = \sum_{k=1}^{N} k^2 + (N+1)^2$$

$$= \frac{N(N+1)(2N+1)}{6} + (N+1)^2$$

$$= \frac{(N+1)}{6}(N(2N+1) + 6(N+1))$$

$$= \frac{(N+1)}{6}(2N^2 + 7N + 6)$$

$$= \frac{(N+1)(2(N+1)+1)((N+1)+1)}{6}$$

So true for n=N+1, so true by induction.

Example 5

- Prove by mathematical induction that $U_n = n^2 + n - 1$ for all integers $n \geq 1$.
- Answer

  Let P(n) be the statement $U_n = n^2 + n - 1$

  Step 1: Prove true for n=1.

  LHS=1,RHS=1, so true for n=1

  Step 2: Prove that if P(n) is true, then P(n+1) is true.

  $U_{n+1} = U_n + 2n + 2$

  $= n^2 + n - 1 + 2n + 2$

  $= (n+1)^2 + (n+1) - 1$

  And so if P(n) is true, P(n+1) is true

Example 6

- Prove by mathematical induction that

$$\sum_{j=1}^{n} 2^j = 2^{n+1} - 2$$

whenever *n* is a positive integer.

Let P(n) be the statement

$$\sum_{j=1}^{n} 2^j = 2^{n+1} - 2$$

for n=1,2,3,...

Step 1: show that P(1) is true.
LHS of P(1)=2, RHS of P(1)=4-2=2 and so P(1) is true

Step 2: show that P(n) implies P(n+1)

$$\sum_{j=1}^{n+1} 2^j = \sum_{j=1}^{n} 2^j + 2^{n+1}$$

$$= 2^{n+1} - 2 + 2^{n+1}$$

$$= 2^{n+2} - 2$$