Discrete Mathematics

Lecture 12

Introduction to Mathematical Proofs

Lecturer: Kahenya N.P

Introduction to Lecture 12

The lecture will introduce methods of direct and indirect mathematical proof. Mathematical proofs are important in developing your logical and analytical skills relevant to programming. This lecture builds on concepts learnt in the lectures on logic and validity, propositional and predicate logic.

References and Further readings

The lecture notes have been derived from relevant topics from (Kahenya, 2017; Murray & Robert, 2009; Rosen, 2012; Stewart, 2012) and lecture 13 from *mathematics for science* (Kahenya, 2022).

Intended Learning Outcomes

At the end of this lecture, you will be able to;

(a) Explain the direct and indirect methods of mathematical proofs.

(b) Apply the methods of direct and indirect proofs to prove theorems.

Definition of Terms

We need to define key terminologies used in mathematics. Some of the terms were defined in previous lectures.

Definition 1: A proposition is a statement that can be assigned a truth value e.g., It is raining, A car has four wheels, $8 < 11$, etc. The statement is either true or false.

Definition 2: A theorem is a proposition that has been proved to be true e.g., Bezout's theorem.

Definition 3: Axiom is a statement that is assumed to be true e.g., $b + c = c + b$

Definition 4: Reasoning can be viewed as drawing of inferences or conclusions from known or assumed facts. Deductive reasoning is the type of logic (science of correct reasoning that is fundamental to critical thinking and problem solving) that involves the application of a general statement to a specific case i.e., from general to specific. On the other hand, inductive reason is drawing conclusions from a specific case i.e., from specific to general (Kahenya, 2022).

Example 1: An example of deductive reasoning (from GENERAL to SPECIFIC) is the use of a formula to solve a particular problem e.g., we use the general quadratic formula to solve specific problems involving quadratic equations (Kahenya, 2022).

Example 2. An example of inductive reasoning is where we use a blood SAMPLE to make a conclusion or generalization of the entire blood.

Definition 4: An argument is a structure that consists of premises or assumptions and a conclusion. Proof is an argument that is used to establish the truth of a theorem.

We have different methods of mathematical proofs for establishing the truth of statements or theorems or claims. There exist direct and indirect methods of proof used depending on the nature of the statement, theorem, or claim.

Methods of Direct Proof

In methods of direct proof, one starts with the hypothesis of an implication and then shows that the conclusion is true. One assumes the hypothesis is true and then presents a logical chain of reasoning to directly establish the truth of the conclusion.

The steps in the proof flows logically and it utilizes axioms, definitions, and previously proved theorems. One establishes the truth of a statement through a logical deduction and reasoning process.

The method of direct proof is applied to implication or conditional statements or propositions. That is, propositions of the form 'if p then q' or $p \rightarrow q$. It used to establish that the logical connection between the antecedent p and the consequent q. Demonstrating that the consequent q follows logically from the antecedent p.

There exist different methods of direct proof among them.

a) Constructive proof

b) Method of exhaustion

c) Method of counter example

d) Method of proof by cases

a) Constructive Proof

The method seeks to establish the truth of a statement and goes further by providing explicit evidence (constructive procedure) to demonstrate the validity of the conclusion. This method provides practical insights and methods.

One can use this method of proof in areas such as number theory, optimization etc. where explicit solutions are important.

Constructive proof tackles theorems of the form; $\exists\, x: p(x)$ i.e., there exist an x such that p(x) is true. This theorem guarantees the existence of at least one x for which the predicate $p(x)$ is true. The proof by constructive involves finding a particular x that makes the predicate $p(x)$ true. One can also establish a formula for finding x.

Example 1: Show that: $\exists x : x^2 = y^2 + z^2$, where $x, y, z \in \mathbb{Z}^+$

Proof: In our case $p(x) = x^2 = y^2 + z^2$ we only need to find an x, y, z that makes $p(x)$ true.
Consider $5^2 = 3^2 + 4^2$

Example 2: Show that: $\exists x : x^2 = 16, \forall\, x \in \mathbb{Z}$

Proof: $\sqrt{x} = \pm\sqrt{16} \Rightarrow x = \pm 4$

b) **Method of Exhaustion**

It establishes that if the proposition holds true for every possible approximation within a finite range, then it must be true for the limiting case.

It is used for theorems of the form; $\forall x \in \mathbb{D}, P(x) \to Q(x)$, where $P(x)$ is the hypothesis and $Q(x)$ is the conclusion. If domain $\mathbb{D}$ is a finite set, then we check the truth value of $P(x)$ for each $x \in \mathbb{D}$.

Example 1: Show that for each integer; $1 \leq n \leq 4$ then $n^2 - n + 5$ is a prime number.

Solution: We can rewrite the above as; $\forall n \in \mathbb{N}, p(n) \Rightarrow q(n)$ where $p(n) = 1 \leq n \leq 4$ and $q(n) = n^2 - n + 5$. We must check for all n in the domain $\mathbb{D}$ i.e.,

n	$n^2 - n + 5$
1	$1 - 1 + 5 = 5$
2	$2^2 - 2 + 5 = 7$
3	$3^2 - 3 + 5 = 11$
4	$4^2 - 4 + 5 = 17$

c) **Method of Counterexample**

It involves using logical reasoning to disprove a claim by providing a specific example or scenario where the claim fails to hold true. You only need to provide a single instance that contradicts the given proposition. This instance must demonstrate the invalidity of the given proposition.

In this method, to show that $\forall x \in \mathbb{D}$, if $p(x)$ then $q(x)$ is false, it suffices to find an element $x \in \mathbb{D}$ where $p(x)$ is true but $q(x)$ is false. Such an x is called a counterexample.

Example 1: Disprove $\forall x, y \in \mathbb{R}$ if $x < y$ then $x^2 < y^2$

Solution: Let $x = -7, y = -3$ then $x < y$ but $x^2 > y^2$

Example 2: Prove: Every computer science student owns a laptop.

Solution: It suffices to find at least one computer science student who owns no laptop.

d) Method of Proof by Cases

This method involves splitting the statement into distinct cases and proceeding by proving each case individually, demonstrating that the statement holds true under each case specific circumstance. It is appropriate when one is interested in identifying key scenarios that encompass all possible situations and hence proving the claim separately for each case rather than considering all possibles cases exhaustively.

Method of proof by cases is therefore a direct method of proving the conditional proposition

$$p_1 \vee p_2 \vee \cdots \vee p_n \to q.$$

The method is used to prove the conditional proposition $p_1 \to q, p_2 \to q, \cdots p_n \to q$.

Example 1: Show that if n is a positive integer then $n^3 + n$ is even.

Solution: The positive integers can either be odd p_1 or even p_2 i.e., 'if $p_1 \vee p_2 \Rightarrow q = n^3 + n \in 2\mathbb{N}$'. That is;

(i) If n is even, then $n^3 + n$ is even.

(ii) If n is odd, then $n^3 + n$ is even

Now if n is even, there exists a $k \in \mathbb{N}$ such that;

$n = 2k$ then $n^3 + n = 8k^3 + 2k = 2(4k^3 + k)$ which is clearly an even number.

Next, if n is odd then there is a $k \in \mathbb{N}$ such that $n = 2k + 1$ then

$$n^3 + n = (2k + 1)^3 + (2k + 1) = 8k^3 + 12k^2 + 8k + 2 = 2(4k^3 + 6k^2 + 4k + 1)$$

Which is even.

Methods of Indirect Proof

Some statements or claims may be difficulty to prove directly and hence the importance of methods of indirect proof. Some important methods of indirect proofs include proof by contradiction, proof by contrapositive, and proof by mathematical induction.

a) Proof by Contradiction

It is a method of proof where the validity of a theorem is established by assuming the negation of the statement and then deriving a contradiction or inconsistency or absurdity from that assumption. Implying that the original statement must be true.

In this method if one wants to show that p is true, we assume it is not and therefore $\neg p$ is true.

Example 1: Prove that $\sqrt{2}$ is irrational.

Proof: Suppose the contrary i.e., $\sqrt{2}$ is rational. It then implies that there exist two integers x and y such that $\gcd(x, y) = 1$ and hence; $\sqrt{2} = \frac{x}{y}$

Squaring both sides of the equation we get; $2 = \frac{x^2}{y^2} \Rightarrow 2y^2 = x^2 \cdots (i) \therefore x^2$ is even.

Since x^2 is even, so is x and therefore there exists an integer k such that $x = 2k$ *(it can be proved that if x^2 is even for $x \in \mathbb{Z}$ then x is even).*

Therefore from (i) $2y^2 = 4k^2 \Rightarrow y^2 = 2k^2$ which means that y^2 is even and so is y.

We can see 2 divides both x and y i.e., gcd (x,y) = 2, and thus contradicts the assumption that the gcd(x,y) = 1 (a condition for rational numbers). Hence $\sqrt{2}$ must be irrational.

Example 2: Prove that $\sqrt{3} + \sqrt{7} < \sqrt{26}$.

Proof: Assume the contradiction i.e., $\sqrt{3} + \sqrt{7} \geq \sqrt{26}$.

Squaring both sides to get; $\left(\sqrt{3} + \sqrt{7}\right)^2 \geq \sqrt{26}^2$ to get $3 + 2\sqrt{21} + 7 \geq 26$

$$10 + 2\sqrt{21} \geq 26$$

$$2\sqrt{21} \geq 16 \Rightarrow \ 84 \geq 256$$

This is a contradiction, indeed $\sqrt{3} + \sqrt{7} < \sqrt{26}$ is true.

b) **Proof by Contrapositive**

In the lecture on propositional logic, we noted that given the implication law (conditional proposition) $p \rightarrow q$, then its contrapositive is $\neg q \rightarrow \neg p$, and that the conditional proposition is logically equivalent to its contrapositive i.e., $p \rightarrow q \equiv \neg q \rightarrow \neg p$.

Therefore, to prove $p \rightarrow q$ we sometimes instead prove the contrapositive $\neg q \rightarrow \neg p$. If the contrapositive is shown to be true, then the original statement must also be true. The method establishes the truth of a proposition by proving the contrapositive statement.

Example 1: Prove that if n is an integer such that n^2 is odd then n is also odd.

Proof: Our proposition is $n^2 \rightarrow n$. We know that it is equivalent to its contrapositive $\neg n \rightarrow \neg n^2$. That is, $n^2 \rightarrow n \equiv \neg n \rightarrow \neg n^2$.

Suppose that n is an integer that is even. Then there exists a k such that $n = 2k$

Hence $n^2 = 4k^2 = 2(2k^2)$ i.e. n^2 is even.

Then if n is an integer such that n^2 is odd then n is also odd.

Example 2: Prove if n^2 is an even integer so is n

Proof: Suppose the contrary i.e., suppose n is odd, then there exists an integer k such that $n = 2k + 1$. Hence; $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

If we let, $2k^2 + 2k = K$ then $n^2 = 2K + 1$ i.e., it is odd.

This proves the claim that if n^2 is even so is n.

Example 3: If ab is even, then a and b are even.

Proof: Assume that a and b are odd then for some integers k_1, k_2, $a = 2k_1 + 1$, $b = 2k_2 + 1$

Now, $ab = (2k_1 + 1)(2k_2 + 1) = 4k_1k_2 + 2k_1 + 2k_2 + 1 = 2(2k_1k_2 + k_1 + k_2) + 1$

Let $2k_1k_2 + k_1 + k_2 = K$ then $ab = 2K + 1$ i.e., an odd number.

So, by contrapositive, *If ab is odd, then a and b are odd* is equivalent to *If ab is even, then a and b are even.*

c) Mathematical Induction

This method is discussed in the course *Mathematics for science* lecture 13 (Kahenya, 2022).

Definition 1: A set X is called an inductive set if it satisfies the following conditions;

(i) $1 \in X$

(ii) If $x \in X$, then $(x+1) \in X$

Definition 2: The set of natural number $\mathbb{N} = \{1,2,3,4,\cdots\}$ is an inductive set.

Definition 3: Principle of mathematical induction

Let $p(n)$ be a proposition for each positive integer. If the following two conditions are satisfied;

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

(ii) Whenever for $n = k$, $p(k)$ is true implies $p(k+1)$ is true.

Then $p(n)$ is true for all positive integers n.

Steps to follow when proving by mathematical induction

Two unique steps to follow:

Step 1: Show by actual substitution that the proposed theorem or formula is true for some natural number n. For instances as $n = 1$, or $n = 2$, or $n = 3$ and so on.

Step 2: Assume that the proposed theorem or formula is true for $n = k$ (where k is an arbitrary positive integer or natural number). Then prove that is true for $n = k + 1$.

Then conclude that the proposed theorem or formula is true for all positive integers or natural numbers greater than or equal to the n selected in step 1 (Kahenya, 2022).

Example 1: Prove that for all positive integers n then;

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

Proof:

Step 1: Is the formula true for $n = 1$?

For $n = 1$ we have $\frac{1^2(1+1)^2}{4} = 1$. Hence it is true for $p(1)$.

Remark : We can check for $n = 2$ i.e., $\frac{2^2(2+1)^2}{4} = \frac{4 \cdot 9}{4} = 9$

The LHS: $1^3 + 2^3 = 9$

For $n = 3$ we have the LHS as $1^3 + 2^3 + 3^3 = 36$

This is equal to the RHS; $\frac{3^2(3+1)^2}{4} = \frac{9 \cdot 16}{4} = 36$. Clearly the LHS = RHS.

Step 2: We assume that the formula is true for $n = k$.

$$1^3 + 2^3 + 3^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4}$$

Then we prove that it is true for $(k+1)$ integer, we add $(k+1)$ term to both sides i.e.

$$1^3 + 2^3 + 3^3 + \cdots + k^3 + (k+1)^3 = \frac{k^2(k+1)^2}{4} + (k+1)^3$$

We now simplify the RHS to get;

$$\frac{k^2(k+1)^2}{4} + (k+1)^3 = \frac{k^2(k+1)^2 + 4(k+1)^3}{4}$$

$$= \frac{(k+1)^2[k^2 + 4(k+1)]}{4}$$

$$= \frac{(k+1)^2(k^2 + 4k + 4)}{4}$$

$$= \frac{(k+1)^2(k+2)^2}{4}$$

Now $\frac{(k+1)^2(k+2)^2}{4}$ is the value of $\frac{n^2(n+1)^2}{4}$ when n is replaced with $(k+1)$. Therefore, we can conclude that the formula is true for all positive integers.

For more examples see lecture 13 in mathematics for science available (Kahenya, 2022).

Exercise

1) Prove that for all positive integers n then;

   a) $a + (a + d) + (a + 2d) + (a + 3d) + \cdots + [a + (n - 1)d] = \frac{n}{2}[2a + (n - 1)d]$

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

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

2) Prove the if $n \in \mathbb{Z}$ then $n^2 + n$ is even.

3) Show that for each integer; $1 \leq n \leq 10$ then $n^2 - n + 11$ is a prime number.

4) Prove that if $x, y \in \mathbb{Q}$ then $(x + y) \in \mathbb{Q}$

5) Prove the triangle inequality; $|x + y| = |x| + |y|$ (use Prove by cases)

6) Prove that for any integer n the product $n(n + 1)$ is even.

7) Prove that for any integer n; $n(n^2 - 1)(n + 2)$ is divisible by 4.

8) Prove that $\sqrt{3}$ is irrational.

9) Prove that the difference between any rational number and any irrational number is irrational.

10) Explain with an example the method of proof by generalizing from the generic particular.

11) Explain the difference between the method of exhaustion and proof by cases.

12) Compare and contrast the following methods of proof: proof by contradiction, proof by uniqueness, proof by infinite descent, and proof by impossibility.

References

Kahenya, P. (2017). *Foundation Maths*. LAP Lambert Academic Publishers.

Kahenya, P. (2022). *Mathematics for Science*. https://www.hufocw.org/Course/932

Murray, S., & Robert, M. (2009). *College Algebra*. McGraw-Hill.

Rosen, K. (2012). *Discrete mathematics and its application* (7th ed.). McGraw-Hill.

Stewart, J. (2012). *Calculus* (7th ed.). Brooks/Cole Cengage Learning.

https://www.mathcentre.ac.uk/resources/uploaded/mathcentre-direct.pdf retrieved on 21/5/2023

Proof-and-Reasoning.pdf (birmingham.ac.uk) retrieved on 21/5/2023

math-299-lecture.pdf (scranton.edu) retrieved on 21/5/2023