

MATH221 Mathematics for Computer Science

Unit 3 Methods of Proof

1

What Is An Argument?

An **argument** is a sequence of statements. All the statements in an argument, except the final one are called **assumptions** (or **premises** or **hypotheses**). The final statement is called the **conclusion**.

An argument is **valid** if no matter what particular statements are substituted for the statement variables in its assumptions, if the resulting assumptions are all true, then the final conclusion is also true. Otherwise, the argument is invalid. Truth table can be used to test the validity of an argument.

3

OBJECTIVES

- Understand the formal definition of argument and proof in Mathematics.
- Understand the rule of Modus Ponens and the Law of Syllogism.
- Understand all the methods of proof.
- Apply the appropriate methods for proving and disproving universal and existential statements.

2

Example: Testing the Validity of an Argument

- An Argument:

$$P \vee (Q \vee R)$$

$$\sim R$$

$$\text{Therefore } P \vee Q$$
- In this argument:
 The assumptions are:

$$P \vee (Q \vee R)$$

$$\sim R$$
 The conclusion is:

$$P \vee Q$$
- Next we shall test the validity of this argument.

4

Example: Testing the Validity of an Argument

- Testing the validity of the Argument:

P	Q	R	$P \vee (Q \vee R)$	$\sim R$	$P \vee Q$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	T
T	F	F	F	T	T
F	T	T	T	F	T
F	T	F	T	T	T
F	F	T	T	F	F
F	F	F	F	T	F

Since in all the rows that all the assumptions are true - 2nd and 6th rows – the conclusion is also true, Hence, the argument is a valid argument.

5

What Is A Proof?

A proof is a valid argument – a sequence of statements - that used to establish a result.

Each statement is

- an assumption
- an axiom
- follows from previous statements by mathematical or logical rule (or definition)
- follows from previously proved theorem

6

Assumptions

All statements in a proof except the final one, are called **assumptions**.

The final statement is called the **conclusion**.

7

Assumptions: Examples

If you want to prove

“If $x \in \mathbb{R}$ and $n \in \mathbb{N}$ is even, then $x^n > 0$ ”

Your proof should start with the assumptions that

$x \in \mathbb{R}$ and $n \in \mathbb{N}$ is even.

Further, you can use the “definition” of an even number, and write the assumptions as follows.

Let $x \in \mathbb{R}$, and $n \in \mathbb{N}$ is even, that is $\exists p \in \mathbb{N}, n = 2p$.

Given (points to $x \in \mathbb{R}$ and $n \in \mathbb{N}$ is even)
Definition (points to $\exists p \in \mathbb{N}, n = 2p$)

Assumptions are often thought to be “given information” or information we “know”.

8

Assumptions: Note

Note when proving statement of the form

$$P \Rightarrow Q,$$

the assumption is the statement P (which could be a list of things).

9

Axioms

Axioms are laws in Mathematics that hold true and require no proof.

10

Axioms: Examples

Three properties of equality: for all objects A , B and C ,

- (1) $A = A$
- (2) If $A = B$ then $B = A$
- (3) If $A = B$ and $B = C$, then $A = C$.

Existence of Identity Elements:

$$0 + a = a + 0 = a \text{ and } 1 \cdot a = a \cdot 1 = a$$

Existence of Additive Inverses:

$$a + (-a) = (-a) + a = 0$$

11

Mathematical Rules

Mathematical Rules are known rules that are often used in each branches of mathematics.

12

Mathematical Rules: Examples

- If $x = y$ then $x + z = y + z$.
- Principle of mathematical Induction (will be introduced shortly and will be studied in detailed in Unit 7).

13

Logical Rules

The two commonly used **Logical rules** are rules such as

- Modus Ponens
- Law of Syllogism

that we will discuss after this.

14

Rule of Modus Ponens

Rule of Modus Ponens: If P and $P \Rightarrow Q$ are **both true**, then so is Q . This rule is based on the tautology $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$.

In other words, Modus Ponens simply says that if we know P to be true, and we know that P implies Q , then Q must also be true. It has the following form:

If P then Q .
 P
 $\therefore Q$

The following exercise demonstrates how Modus Ponens works.

15

Discussion: the use of Modus Ponens

1. We have " $n \in \mathbb{N}$ is even $\Rightarrow n^2$ is even" from previously proved theorem

Let $n = 98374$.

98374^2 is even? True or False?

$n \in \mathbb{N}$ is even $\Rightarrow n^2$ is even

98374 is even

98374^2 is even

16

Discussion: the use of Modus Ponens

2. The Principle of Mathematical Induction says that when you have a statement, CLAIM(n), that concerns $n \in \mathbb{N}$, if
- CLAIM(1) is true, AND
 - CLAIM(k) \Rightarrow CLAIM($k + 1$) for all $k \in \mathbb{N}$,
- then CLAIM(n) is true for all $n \in \mathbb{N}$.

Question: According to Modus Ponens, what must we establish so we can apply this principle to the following statement and be able to say "CLAIM(n) is true for all $n \in \mathbb{N}$ "?

CLAIM(n): $4^n - 1$ is a multiple of 3.

Answer: We must show that:

- CLAIM(1) is true, AND
- CLAIM(k) \Rightarrow CLAIM($k + 1$) for all $k \in \mathbb{N}$

17

Law Of Syllogism

An argument consisting two assumptions and a conclusion is called a **syllogism**. Modus ponens is the most famous form of syllogism.

Law of Syllogism: If $P \Rightarrow Q$ and $Q \Rightarrow R$ are both true, then so is $P \Rightarrow R$. This law is based on the tautology $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$.

Most results in Mathematics that require proof are of the form
 $P \Rightarrow R$.

The Law of Syllogism provides the most common structure for proofing of such statements.

18

Law Of Syllogism: Method

To use the Law of Syllogism, we set up a string of

$$\begin{aligned} P &\Rightarrow P_1, \\ P_1 &\Rightarrow P_2, \\ P_2 &\Rightarrow P_3, \\ &\dots \\ P_n &\Rightarrow R. \end{aligned}$$

Then, by successive applications of the law, we have $P \Rightarrow R$.

19

Law Of Syllogism: Example

We wish to prove that for $n \in \mathbb{N}$, if n is even, then n^2 is even; in logic notation, we wish to prove

$$n \text{ is even} \Rightarrow n^2 \text{ is even.}$$

This has the form

$$P \Rightarrow Q$$

and we note that our assumption includes

$$n \in \mathbb{N},$$

and

$$P: n \text{ is even.}$$

20

Law Of Syllogism: Example

Proof:

$$\begin{array}{lll}
 n \text{ is even} & \Rightarrow \exists p \in \mathbb{N}, n = 2p & (P \Rightarrow P_1) \\
 \exists p \in \mathbb{N}, n = 2p & \Rightarrow n^2 = 4p^2 & (P_1 \Rightarrow P_2) \\
 n^2 = 4p^2 & \Rightarrow n^2 = 2(2p^2) & (P_2 \Rightarrow P_3) \\
 n^2 = 2(2p^2) & \Rightarrow n^2 \text{ is even.} & (P_3 \Rightarrow Q)
 \end{array}$$

By applying the Law of Syllogism three times, we get
 $n \text{ is even} \Rightarrow n^2 \text{ is even.}$

21

Law Of Syllogism: Note

The use of the connective \Rightarrow in the previous proof seems a little repetitive.

For variety, the connective can be replaced by words such as
 therefore,
 thus,
 so we have,
 and
 hence.

23

Law Of Syllogism: Note

In our work, we shall abbreviate the proofs by applying the Law of Syllogism in a more subtle way as follows:

Proof:

$$\begin{array}{lll}
 n \text{ is even} & \Rightarrow \exists p \in \mathbb{N}, n = 2p & (P \Rightarrow P_1) \\
 & \Rightarrow n^2 = 4p^2 & (P_1 \Rightarrow P_2) \\
 & \Rightarrow n^2 = 2(2p^2) & (P_2 \Rightarrow P_3) \\
 & \Rightarrow n^2 \text{ is even.} & (P_3 \Rightarrow Q)
 \end{array}$$

Therefore, if n is even, n^2 is even.

We shall use the Law of Syllogism without direct reference.

22

Methods of Proof - Types

- (i) Proving for one Value
- (ii) Method of Exhaustion: this method will show for each x in D , $P(x)$ is true
- (iii) Generalized Proof: there are three methods for generalized proof:
 - Method 1: Direct Proof
 - Method 2: Indirect Proof
 - ❑ Proof by Contradiction
 - ❑ Proof by Contrapositive
 - Method 3: Proof by Cases

24

Proving \exists Statements

The statement $\exists x \in D, P(x)$ is true if and only if $P(x)$ is true for at least one $x \in D$.

To prove this kind of statement, we need to find one $x \in D$, that makes $P(x)$ true – use the method, **proving for one value**.

25

Proving \exists Statements: Example

Prove that there exists an even integer that can be written two ways as the sum of two primes.

Essentially, to find the appropriate number, we have to “guess”.

Consider $14 = 7 + 7$ [7 is prime];
and $14 = 3 + 11$ [3 and 11 are prime.]

Therefore, there exists an even integer that can be written two ways as the sum of two primes.

26

Example:

1. Prove $\exists x \in \mathbb{R}, x + 5 = 0$.

Let $x = -5$,
then $x + 5 = 0$.
Therefore, $\exists x \in \mathbb{R}, x + 5 = 0$.

27

Proving \forall Statements

Most mathematical statements to be proved are \forall statements of the form

$$\forall x \in D, P(x).$$

To prove such statement, if D is finite and small, we can use **Method of Exhaustion** that requires checking that $P(x)$ is true for every x in D . But this method is not useful when D is large, and impossible if D is an infinite set.

Unfortunately, in most cases the method of exhaustion cannot be used.

For example, how long would it take to prove the statement for all even values of $n \in \mathbb{N}$?

In this case, we have to use methods for generalized proof.

28

Proving \forall Statements: Example

Prove the following statement: Every even number between 2 and 16 can be written as a sum of two prime numbers.

$$4 = 2 + 2 \quad 6 = 3 + 3 \quad 8 = 3 + 5$$

$$10 = 5 + 5 \quad 12 = 5 + 7 \quad 14 = 7 + 7$$

Therefore, by the method of exhaustion, the statement is true.

29

Disproving \forall Statements

To disprove the statement $\forall x \in D, P(x)$, we must *prove* its negation, that is prove

$$\sim (\forall x \in D, P(x)) \equiv \exists x \in D, \sim P(x).$$

Note that to disprove a “ \forall ” statement, we are required to prove a “ \exists ” statement.

Therefore, it is enough to use the method, proving for one value, to find one $x \in D$ that satisfies $\sim P(x)$, that is, one value that makes $P(x)$ false.

This is also called *counterexample*.

31

Disproving \exists Statements

To disprove the statement $\exists x \in D, P(x)$, we must *prove* its negation, that is prove

$$\sim (\exists x \in D, P(x)) \equiv \forall x \in D, \sim P(x).$$

Hence, to prove this statement, we must use a generalized proof as mentioned earlier, to prove that $\sim P(x)$ is true.

30

Example:

Disprove the statement $\forall x \in \mathbb{R}, (x > 0 \vee x < 0)$.

The negation is

$$\exists x \in \mathbb{R}, (x \leq 0 \wedge x \geq 0).$$

We can use a *counterexample*.

$$\text{Let } x = 0.$$

$$\text{But } 0 \leq 0 \wedge 0 \geq 0.$$

Hence, the statement is false.

32

Discussion:

Prove or disprove the statement $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0$.

Given $x \in \mathbb{R}$, we choose $y = -x$.

This implies that $x + y = 0$.

Therefore, $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0$.

33

The Direct Proof

A direct proof is one in which we work in a straightforward fashion to the answer.

34

Examples:

1. Prove that if $3x - 9 = 15$ then $x = 8$.

The statement is of the form $P \Rightarrow Q$.

Now, $3x - 9 = 15$

$$\Rightarrow 3x = 15 + 9$$

$$\Rightarrow 3x = 24$$

$$\Rightarrow x = 8$$

Therefore, if $3x - 9 = 15$ then $x = 8$.

35

Exercise:

2. Prove that if $a, b \in \mathbb{Z}$, then $10a + 8b$ is divisible by 2 (ie., is even).

Form: $a, b \in \mathbb{Z} \Rightarrow 10a + 8b$ is divisible by 2

Let a and b be integers.

Now,

$$10a + 8b = 2 \cdot 5a + 2 \cdot 4b$$

$$= 2(5a + 4b)$$

$$= 2k \text{ where } k = 5a + 4b, k \in \mathbb{Z}$$

Therefore, if $a, b \in \mathbb{Z}$, then $10a + 8b$ is divisible by 2.

36

Handy Hint:

Before proving a statement, it is of great use to write the statement using logic notation, including quantifiers, where appropriate.

Doing this means you have clearly written in front of you the assumptions you can make AND where you are eventually trying to get.

37

Forwards And Backwards Process

To develop a proof, it is often helpful to work in a forwards and backwards manner, with the hope that the steps will “meet u” in the middle.

38

Forwards And Backwards Process: Example

When approaching a proof of the statement,

“ n is even $\Rightarrow n^2$ is even”,

it is useful to not only consider what it means for n to be even, but also what we must show to be able to say n^2 is even.

Forward working: n is even $\Rightarrow \exists p \in \mathbb{N}, n = 2p$
 $\Rightarrow n^2 = 4p^2$
 $\Rightarrow n^2 = 2(2p^2)$
 $\Rightarrow \exists k \in \mathbb{N}, n^2 = 2k$ (Since $2p^2 \in \mathbb{N}$)

Backward working: $\exists k \in \mathbb{N}, n^2 = 2k \Rightarrow n^2$ is even.

Can “match up” the two sets of working? Yes, it is as follows to form the proof:

n is even $\Rightarrow \exists p \in \mathbb{N}, n = 2p$
 $\Rightarrow n^2 = 4p^2$
 $\Rightarrow n^2 = 2(2p^2)$
 $\Rightarrow \exists k \in \mathbb{N}, n^2 = 2k$ (Since $2p^2 \in \mathbb{N}$)
 $\Rightarrow n^2$ is even.

39

Forwards And Backwards Process: Example

Prove that for $x \in \mathbb{R}$, $(-x^2 + 2x + 1) \leq 2$.

Forward: (nothing can be drawn)

Backward: $-x^2 + 2x + 1 \leq 2$

$$\Leftarrow x^2 - 2x + 1 \geq 0$$

(Since $x^2 - 2x + 1 = (x - 1)^2 \geq 0$)

$$\Leftarrow (x - 1)^2 \geq 0$$

(Since the square of any real number is always non-negative)

We can now put the proof together:

$$(x - 1)^2 \geq 0$$

(Since the square of any real number is always non-negative)

$$\Rightarrow x^2 - 2x + 1 \geq 0 \quad (\text{Since } x^2 - 2x + 1 = (x - 1)^2 \geq 0)$$

$$\Rightarrow (-x^2 + 2x + 1) \leq 2$$

40

Forwards And Backwards Process: Note

In the previous example, we must NOT start with the statement

$$(-x^2 + 2x + 1) \leq 2,$$

as we technically do not know whether it is true or not.

We started our proof with a statement we know to be true from basic algebra.

The steps drawn from backward process CANNOT be used as a proof. These steps are just for helping us to construct a proof from assumptions and/or well-known facts to conclusion.

41

Proof By Contradiction: Method

We assume the negation of what we are trying to prove ($\sim Q$) is true, then use a logical argument to show that we would then have a contradiction with either P or some other well-known truth.

42

Proof By Contradiction: Example

Prove that for $n \in \mathbb{N}$, if n^2 is even, then n is even,

This is of the form

$$\forall n \in \mathbb{N}, (P \Rightarrow Q),$$

where P is " n^2 is even"

and Q is " n is even".

Thus, we must give a general proof and we start with the premise that n^2 is even.

If we try a direct proof, we start with $n^2 = 2p$ for some $p \in \mathbb{N}$... but then we get "stuck"!

43

Proof By Contradiction: Example

A proof by contradiction proceeds as follows:

Let n^2 be even. (The "usual" assumption P)

Suppose that n is an odd number. (Assume $\sim Q$)

Then $n = 2p + 1$ for some $p \in \mathbb{N}$

Now, $n^2 = (2p + 1)^2$

$$= 4p^2 + 4p + 1$$

$$= 2(2p^2 + 2p) + 1$$

$$\Rightarrow n^2 = 2k + 1 \quad \text{where } k = 2p^2 + 2p, k \in \mathbb{N}.$$

Thus, n^2 is odd. (Show $\sim P$)

Therefore, we have a contradiction, and so n is even.

44

Example:

Complete the following proof by contradiction that if y is irrational, then $y + 7$ is also irrational.

Let y be an irrational number. Suppose $y + 7$ is rational.
Therefore, $y + 7$ can be written as a fraction, that is $y + 7 = p/q$
where $p, q \in \mathbb{Z}$ and $q \neq 0$.
Simplifying,

$$\begin{aligned} y &= (p/q) - 7 \\ &= (p - 7q)/q \\ &= k/q \quad \text{where } k = p - 7q, k \in \mathbb{Z}. \end{aligned}$$

Thus, y is rational, which is a contradiction.
Therefore, if y is irrational, then $y + 7$ is also irrational.

45

Proof By Contrapositive: Method

Given the statement to be proved in the form $P \Rightarrow Q$.

Rewrite the statement in the contrapositive form $\sim Q \Rightarrow \sim P$.

Prove the contrapositive by a direct proof.

In other words, we assume the negation of what we are trying to prove ($\sim Q$), then use a logical argument to prove $\sim P$.

46

Proof By Contrapositive: Example

Prove for all integers n , if n^2 is even then n is even.

Rewrite the statement in the contrapositive form:
For all integers n , if n is odd then n^2 is odd.

Suppose n is any odd integer.

Hence, $n = 2k + 1$ for some integers k .

$$\begin{aligned} \text{Thus, } n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2l + 1 \text{ where } l = 2k^2 + 2k \in \mathbb{Z} \end{aligned}$$

Since n^2 is odd, therefore, the statement is true.

47

When to use Proof By Contrapositive and Proof by Contradiction

For proving $P \Rightarrow Q$:

- When we have difficulty with direct proof, we should consider the use of Proof by Contradiction or Proof by Contrapositive.
- The method of Contrapositive has the advantage that your goal is clear: Prove Not P .
- In the method of Contradiction, your goal is to prove a contradiction. Though at the start, it is not always clear what the contradiction is going to be, but usually it is also Not P .

48

Discussion:

How would you go about proving the following statement?

If $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$.

You have to show:

- (1) If $x \neq 0$, then $x^2 + y^2 > 0$
- (2) If $y \neq 0$, then $x^2 + y^2 > 0$

49

Proof By Cases

The method for proving the statement discussed is *proof by cases*. The method is used whenever you wish to prove a statement of the form

$$(P \vee Q) \Rightarrow R.$$

The rationale behind a proof by cases is based on a generalization of the following logical equivalence.

$$(P \Rightarrow R) \wedge (Q \Rightarrow R) \equiv (P \vee Q) \Rightarrow R.$$

The only problem with this method of proof is that it is not always obvious that this is the technique required and how to dividing into cases.

50

Proof By Cases: Example

To prove the statement " $\forall m \in \mathbb{N}, m^2 + m + 1$ is odd", we should use a proof by cases, that is when m is even and when m is odd.

Let m be even. Then $m = 2p$, for some $p \in \mathbb{N}$.

Hence,

$$\begin{aligned} m^2 + m + 1 &= (2p)^2 + 2p + 1 \\ &= 4p^2 + 2p + 1 \\ &= 2(2p^2 + p) + 1 \\ &= 2k + 1 \quad \text{where } k = 2p^2 + p, k \in \mathbb{N}. \end{aligned}$$

Therefore, when m is even, $m^2 + m + 1$ is odd.

51

Proof By Cases: Example

Let m be odd. Then $m = 2q + 1$, for some $q \in \mathbb{N}$.

Hence,

$$\begin{aligned} m^2 + m + 1 &= (2q + 1)^2 + (2q + 1) + 1 \\ &= 4q^2 + 4q + 1 + (2q + 1) + 1 \\ &= 4q^2 + 6q + 3 \\ &= 2(2q^2 + 3q + 1) + 1 \\ &= 2l + 1 \end{aligned}$$

where $l = 2q^2 + 3q + 1, l \in \mathbb{N}$.

Therefore, when m is odd, $m^2 + m + 1$ is odd.

Thus, $\forall m \in \mathbb{N}, m^2 + m + 1$ is odd.

52

Identifying Appropriate Methods of Proof

- First, always try Direct Proof.
- If you get “stuck”, next, try Proof by Contradiction. Usually, after this, you should be able to identify the methods. However, if you are more comfortable with Proof by Contrapositive, before trying Proof by Contradiction, you can try Proof by Contrapositive first.
- Note that Proof by Cases can be used in Direct Proof, Proof by Contradiction and Proof by Contrapositive.
- Mathematical Induction is only suitable for proofing an infinite family of statements based on integers n . All the methods of proof can be used within the structure of Mathematical Induction.

53

Working on a Proof

- In general, proving a statement is a creative task, and therefore, there is no fixed steps. However, the following guidelines are useful.
- Always start from the assumption (either given assumption or assumptions from a selected method of proof).
- Then, based on the assumption and/or well-known facts, draw statements from definition or theorem, again, based on the statements drawn, draw further statements from definition or theorem, and so on..., until a proof is formed.
- During the previous step, always match what you need to prove with what you have currently to draw further statements for bridging the gap between them.

54

End of Unit 3

55