Logic, Proofs, and Counting

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

April 9, 2021

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

2

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Outline

1. Introduction
   - Syllabus
     - References

2. The Foundations: Logic and Proofs
   - Propositional Logic
   - Proofs
     - Direct Proof
     - Proof by Contradiction
     - Proof by Contrapositive
     - Constructive Proofs, Counterexamples, and Vacuous Proofs

3. Counting

Outline

1. Introduction
   - Syllabus
     - References

2. The Foundations: Logic and Proofs
   - Propositional Logic
   - Proofs
     - Direct Proof
     - Proof by Contradiction
     - Proof by Contrapositive
     - Constructive Proofs, Counterexamples, and Vacuous Proofs

3. Counting

What is Discrete Mathematics?

- Discrete mathematics is the part of mathematics devoted to the study of discrete (as opposed to continuous) objects.
- **Examples of discrete objects:** integers, steps taken by a computer program, distinct paths to travel from point A to point B on a map along a road network, ...
- A course in discrete mathematics provides the mathematical background needed for all subsequent courses in computer science and for all subsequent courses in the many branches of discrete mathematics.

Types of Problems We Solve Using Discrete Maths

- How many ways can you choose a password following specific rules?
- How many valid Internet addresses are there?
- How can we prove that there are infinitely many prime numbers?
- How can a list of integers be sorted so that the integers are in increasing order?
- Is there a link between two computers in a network?
- How can I encrypt a message so that no unintended recipient can read it?
- What is the shortest path between two cities using a transportation system?

Goals of This Course

- **Mathematical Reasoning:** Ability to read, understand, and construct mathematical arguments and proofs.
- **Combinatorial Analysis:** Techniques for counting objects of different kinds.
- **Discrete Structures:** Abstract mathematical structures that represent objects and the relationships between them. Examples are sets, permutations, relations, graphs, and trees.

Goals of This Course

- **Algorithmic Thinking:** One way to solve many problems is to specify an algorithm.

  An algorithm is a sequence of steps that can be followed to solve any instance of a particular problem.

  Algorithmic thinking involves specifying algorithms, analyzing the memory and time required by an execution of the algorithm, and verifying that the algorithm will produce the correct answer.

Discrete Maths in CS, Maths, . . .

- **Computer Science:** Computer Architecture, Data Structures, Algorithms, Programming Languages, Compilers, Computer Security, Theory of Computation, Networking, . . .
- **Mathematics:** Logic, Set Theory, Number Theory, Abstract Algebra, Combinatorics, Graph Theory, Probability, Game Theory, Network Optimization, . . .

Discrete Maths in CS, Maths, ...

- **Computer Science:** Computer Architecture, Data Structures, Algorithms, Programming Languages, Compilers, Computer Security, Theory of Computation, Networking, ...
- **Mathematics:** Logic, Set Theory, Number Theory, Abstract Algebra, Combinatorics, Graph Theory, Probability, Game Theory, Network Optimization, ...

  The concepts learned will also be helpful in continuous areas of mathematics.
- **Other Disciplines:** It is also useful in courses in philosophy, economics, linguistics, and other disciplines.

Syllabus

- Logic, Proofs, and Counting
- Basic Structures
- Introduction to Abstract Algebra
- Introduction to Number Theory
- Introduction to Graph Theory

References

- **Textbook**
  - Kenneth H. Rosen,
    Discrete Mathematics and Its Applications, McGraw-Hill Education, Eighth Edition, 2019.
  - I. N. Herstein,
    Topics in Algebra, John Wiley & Sons, 1975.
  - Tom M. Apostol,
    Introduction to Analytic Number Theory, Springer 1976.
  - Frank Harary,
    Graph Theory, CRC Press, 2018.

References

- **Supplementary Reading**

- Owen D. Byer, Deirdre L. Smeltzer, & Kenneth L. Wantz, *Journey into Discrete Mathematics*, AMS/MAA Textbooks, volume 41, 2018.
- Harry Lewis, & Rachel Zax, *Essential Discrete Mathematics for Computer Science*, Princeton University Press, 2019.
- Gerard O'Regan, *Guide to Discrete Mathematics: An Accessible Introduction to the History, Theory, Logic and Applications*, Springer 2016.
- Kenneth H. Rosen, *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, Second Edition, 2018.

Outline

1. Introduction
   - Syllabus
     - References

2. The Foundations: Logic and Proofs
   - Propositional Logic
   - Proofs
     - Direct Proof
     - Proof by Contradiction
     - Proof by Contrapositive
     - Constructive Proofs, Counterexamples, and Vacuous Proofs

3. Counting

Propositions

Definition

A proposition is a declarative sentence that is either true or false but not both.

Propositions

Definition

A proposition *is a declarative sentence that is either true or false but not both.*

Example (Propositions)

1. *Lucknow is the capital of UP.*
2. *Guwahati is the capital of Assam*
3. $2 \times 3 = 5$

Propositions

Definition

A ***proposition*** *is a declarative sentence that is either true or false but not both.*

Example (Propositions)

1. *Lucknow is the capital of UP.*
2. *Guwahati is the capital of Assam*
3. $2 \times 3 = 5$

Example (Not Propositions)

1. *What is the time now?*
2. $x + y = a$

Propositional Logic

- **Constructing Propositions**
  - **Propositional Variables:** $p, q, r, s, \ldots$
  - The proposition that is always *true* is denoted by T and the proposition that is always *false* is denoted by F.
  - **Compound Propositions** – constructed from logical connectives and other propositions
    - Negation $\neg$
    - Conjunction $\wedge$
    - Disjunction $\vee$
    - Implication $\rightarrow$ or $\implies$
    - Biconditional $\leftrightarrow$ or $\iff$

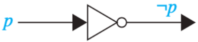
Compound Propositions: Negation

Many mathematical statements are constructed by combining one or more propositions. New propositions, called **compound propositions**, are formed from existing propositions using logical operators.

- The negation of a proposition p is denoted by $\neg p$

$\mathbf{p}$	$\neg\mathbf{p}$
T	F
F	T

Table: Truth Table



Example

p – *you are students of* 1^{st} *year BTech*

$\neg p$ –

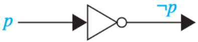
Compound Propositions: Negation

Many mathematical statements are constructed by combining one or more propositions. New propositions, called **compound propositions**, are formed from existing propositions using logical operators.

- The negation of a proposition p is denoted by $\neg p$

$\mathbf{p}$	$\neg\mathbf{p}$
T	F
F	T

Table: Truth Table



Example

p – *you are students of* 1^{st} *year BTech*

$\neg p$ – *you are not students of* 1^{st} *year BTech*

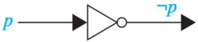
Compound Propositions: Negation

Many mathematical statements are constructed by combining one or more propositions. New propositions, called **compound propositions**, are formed from existing propositions using logical operators.

- The negation of a proposition p is denoted by $\neg p$

$\mathbf{p}$	$\neg\mathbf{p}$
T	F
F	T

Table: Truth Table



Example

p – *you are students of* 1^{st} *year BTech*

$\neg p$ – *you are not students of* 1^{st} *year BTech*

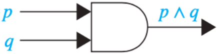
Remark: Other notations for negation are $\bar{p}, \sim p, -p, Np, p'$ or $!p$.

Conjunction

- The conjunction of propositions p and q is denoted by $p \wedge q$

p	**q**	$\mathbf{p \wedge q}$
T	T	T
T	F	F
F	T	F
F	F	F

Table: Truth Table



Example

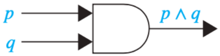
p – you are listening this lecture from home
q – it is raining
$p \wedge q$ –

Conjunction

- The conjunction of propositions p and q is denoted by $p \wedge q$

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{p \wedge q}$
T	T	T
T	F	F
F	T	F
F	F	F

Table: Truth Table



Example

p – *you are listening this lecture from home*

q – *it is raining*

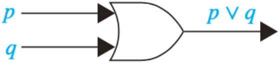
$p \wedge q$ – *you are listening this lecture from home* *and* *it is raining*

Disjunction

- The conjunction of propositions p and q is denoted by $p \vee q$

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

Table: Truth Table



Example

p – *you are listening this lecture from home*

q – *you are watching TV*

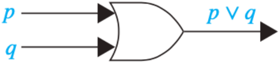
$p \vee q$ –

Disjunction

- The conjunction of propositions p and q is denoted by $p \vee q$

p	**q**	**p ∨ q**
T	T	T
T	F	T
F	T	T
F	F	F

Table: Truth Table



Example

p – *you are listening this lecture from home*
q – *you are watching TV*
$p \vee q$ – *you are listening lecture from home or watching TV*

Exclusive or (Xor)

- In English ‘or’ has two distinct meanings.
  - **Inclusive or –** “Students who have taken Linear Algebra or Basic Computer class may take this class,"

Exclusive or (Xor)

- In English ‘or’ has two distinct meanings.
  - **Inclusive or –** “Students who have taken Linear Algebra or Basic Computer class may take this class,"

    we assume that students need to have taken one of the prerequisites, but may have taken both.

    This is the meaning of **disjunction**.

Exclusive or (Xor)

- In English ‘or’ has two distinct meanings.
  - **Inclusive or –** “Students who have taken Linear Algebra or Basic Computer class may take this class,"

    we assume that students need to have taken one of the prerequisites, but may have taken both.

    This is the meaning of **disjunction**.
  - **Exclusive or (Xor) –** “Soup or salad comes with the main course of a meal,"

Exclusive or (Xor)

- In English ‘or’ has two distinct meanings.
  - **Inclusive or –** “Students who have taken Linear Algebra or Basic Computer class may take this class,"

    we assume that students need to have taken one of the prerequisites, but may have taken both.

    This is the meaning of **disjunction**.
  - **Exclusive or (Xor) –** “Soup or salad comes with the main course of a meal," you do not expect to be able to get both soup and salad.

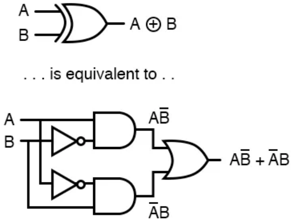
    This is the meaning of **Exclusive Or (Xor)**.

    It is denoted by $\oplus$. E.g., $p \oplus q$, one of p and q must be true, but not both.

Exclusive or (Xor)

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{p \oplus q}$
T	T	F
T	F	T
F	T	T
F	F	F

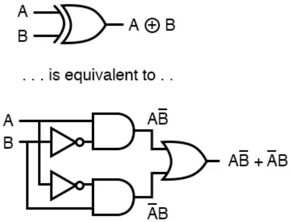
Table: Truth Table



Exclusive or (Xor)

p	**q**	$\mathbf{p \oplus q}$
T	T	F
T	F	T
F	T	T
F	F	F

Table: Truth Table



Theorem

$$p \oplus q \iff (p \wedge \neg q) \vee (\neg p \wedge q).$$

Conditional Statements: Implication

- If p and q are propositions, then $p \rightarrow q$ is a conditional statement or implication which is read as "if p, then q".
- The conditional statement $p \rightarrow q$ is false when p is true & q is false, and true otherwise.

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{p \rightarrow q}$
T	T	T
T	F	F
F	T	T
F	F	T

Table: Truth Table

Conditional Statements: Implication

- If p and q are propositions, then $p \to q$ is a conditional statement or implication which is read as "if p, then q".
- The conditional statement $p \to q$ is false when p is true & q is false, and true otherwise.

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{p \to q}$
T	T	T
T	F	F
F	T	T
F	F	T

Table: Truth Table

In $p \to q$, p is called the **hypothesis** and q is called the **conclusion**.

Understanding Implication

- If n is an even integer, then $n = 2 \cdot k$, where $k \in \mathbb{Z}$.
- In $p \rightarrow q$ there does not need to be any connection between the hypothesis or the conclusion.
  The “meaning" of $p \rightarrow q$ depends only on the truth values of p and q.
- These implications are perfectly fine, but would not be used in ordinary English.
  - If color the moon is green, then you have more money than Mukesh Ambani.
  - If $1 + 1 = 3$, then you are wearing leather jacket.
- One way to view the logical conditional is to think of an obligation or contract.
  - If you get 85% on the final, then you will get an A.

Converse, Contrapositive, and Inverse

- From $p \rightarrow q$ we can form new conditional statements
  - $q \rightarrow p$ is the **converse** of $p \rightarrow q$
  - $\neg q \rightarrow \neg p$ is the **contrapositive** of $p \rightarrow q$
  - $\neg p \rightarrow \neg q$ is the **inverse** of $p \rightarrow q$
- We first show that the contrapositive, $\neg q \rightarrow \neg p$, of a conditional statement $p \rightarrow q$ always has the same truth value as $p \rightarrow q$.

Converse, Contrapositive, and Inverse

- From $p \to q$ we can form new conditional statements
  - $q \to p$ is the **converse** of $p \to q$
  - $\neg q \to \neg p$ is the **contrapositive** of $p \to q$
  - $\neg p \to \neg q$ is the **inverse** of $p \to q$

- We first show that the contrapositive, $\neg q \to \neg p$, of a conditional statement $p \to q$ always has the same truth value as $p \to q$.
- Note that the contrapositive is false only when
  - $\neg p$ is false and $\neg q$ is true, that is, only when p is true and q is false.
- You show that neither the converse, $p \to q$, nor the inverse, $\neg p \to \neg q$, has the same truth value as $p \to q$ for all possible truth values of p and q.

Converse, Contrapositive, and Inverse

- When two compound propositions always have *the same truth values*, regardless of the truth values of its propositional variables, we call them **equivalent**.
- Hence, a *conditional statement* and *its contrapositive* are **equivalent.**
- The *converse* and the *inverse* of a conditional statement are also equivalent.
  However neither is equivalent to the original conditional statement.

Theorem

$$p \to q \iff \neg p \vee q.$$

Biconditional/Equivalence

- If p and q are propositions, then we can form the biconditional proposition $p \leftrightarrow q$, read as
  "p if and only if (iff) q".

p	q	$\mathbf{p} \leftrightarrow \mathbf{q}$
T	T	T
T	F	F
F	T	F
F	F	T

Table: Truth Table

- Some alternative ways "p iff q" is expressed in English:
  - p is necessary and sufficient for q
  - if p then q, and conversely

Propositional Logic

Example	Name	Meaning
$\neg p$	Negation	Not p
$p \vee q$	(Inclusive) Or	Either p or q or both
$p \wedge q$	And	Both p and q
$p \oplus q$	XOR	Either p or q, but not both
$p \rightarrow q$	Implies	If p, then q
$p \leftrightarrow q$ / $p \iff q$	Biconditional / Equivalence	p if and only if q

Truth Tables for Compound Propositions

- A truth table presents the truth values of a compound propositional formula in terms of the truth values of the components.

Precedence of Logical Operators

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Example of Truth Table

Construct a truth table for $p \vee q \rightarrow \neg r$

Example of Truth Table

Construct a truth table for $p \vee q \rightarrow \neg r$

p	q	r	$\neg r$	$p \vee q$	$p \vee q \rightarrow \neg r$
T	T	T	F	T	F
T	T	F	T	T	T
T	F	T	F	T	F
T	F	F	T	T	T
F	T	T	F	T	F
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	T	F	T

Tautologies, Contradictions, and Contingencies

Definition

- *A **tautology** is a proposition which is always true.*

$$p \lor \neg p$$

- *A **contradiction** is a proposition which is always false.*

$$p \land \neg p$$

- *A **contingency** is a proposition which is neither a tautology nor a contradiction.*

De Morgan's Laws

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

Truth table for De Morgan's Second Law:

p	q	$\neg p$	$\neg q$	$(p \vee q)$	$\neg(p \vee q)$	$\neg p \wedge \neg q$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
T	F	T	T	F	T	T

Key Logical Equivalences

- Identity Laws: $p \wedge T \equiv p$, $p \vee F \equiv p$
- Domination Laws: $p \vee T \equiv T$, $p \wedge F \equiv F$
- Idempotent laws: $p \wedge p \equiv p$, $p \vee p \equiv p$
- Double Negation Law: $\neg(\neg p) \equiv p$
- Negation Laws: $p \vee \neg p \equiv T$, $p \wedge \neg p \equiv F$
- Commutative Laws: $p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$

Key Logical Equivalences

- Associative Laws: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
  $(p \vee q) \vee r \equiv p \vee (q \vee r)$
- Distributive Laws: $(p \vee (q \wedge r)) \equiv (p \vee q) \wedge (p \vee r)$
  $(p \wedge (q \vee r)) \equiv (p \wedge q) \vee (p \wedge r)$
- Absorption Laws: $p \vee (p \wedge q) \equiv p$
  $p \wedge (p \vee q) \equiv p$

Logic Puzzles

- In Lucknow, there are two kinds of inhabitants, Type-1, who always tell the truth, and Type-2, who always lie.
- You come to Lucknow and meet A and B.
  - A says “B is a Type-1."
  - B says “The two of us are of opposite types."

Example

What are the types of A and B?

Logic Puzzles

Solution

Let p and q be the statements that A is a Type-1 and B is a Type-1, respectively. So, then $\neg p$ represents the proposition that A is a Type-2 and $\neg q$ that B is a Type-2.

- *If A is a Type-1, then p is true. Since Type-1s tell the truth, q must also be true. Then $(p \wedge \neg q) \vee (\neg p \wedge q)$ would have to be true, but it is not. So, A is not a Type-1 and therefore $\neg p$ must be true.*
- *If A is a Type-2, then B must not be a Type-1 since Type-2 always lie. So, then both $\neg p$ and $\neg q$ hold since both are Type-2.*

Proofs of Mathematical Statements

- A proof is a valid argument that establishes the truth of a statement.
- In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.
  - More than one rule of inference are often used in a step.
  - Steps may be skipped.
  - The rules of inference used are not explicitly stated.
  - Easier for to understand and to explain to people.
  - But it is also easier to introduce errors.
- Proofs have many practical applications:
  - verification that computer programs are correct
  - establishing that operating systems are secure
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent

Some Terminology

- A **theorem** is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - axioms (statements which are given as true)
  - rules of inference
- A **lemma** is a ‘helping theorem’/‘little theorem‘ or a result which is needed to prove a theorem.
- A **corollary** is a result which follows directly from a theorem.
- Less important theorems are sometimes called **propositions**.

Some Terminology

- A **conjecture** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a *theorem*. It may turn out to be false.
- A **proof** is an argument that begins with a proposition and proceeds using logical rules to establish a conclusion.

Conversion of Plain English into Mathematical Form

Everybody loves somebody

Conversion of Plain English into Mathematical Form

Everybody loves somebody

For every person A, *there is a* person B such that A loves B.
or
There is a person B such that for *every person* A, A loves B.

Conversion of Plain English into Mathematical Form

Everybody loves somebody

For every person A, *there is a* person B such that A loves B.
or
There is a person B such that for *every person* A, A loves B.

- The phrases '*for all*', '*for any*', '*for every*', '*for some*', & '*there exists*' are called **quantifiers**
- Their careful use is an important part in mathematics.
- The symbol $\forall$ stands for '*for all*', '*for any*', or '*for every*'
- The symbol $\exists$ stands for '*there exists*' or '*for some*'.

Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
- Often the *universal quantifier* (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

Example

The statement:

If $x > y$, where x & y are positive real numbers, then $x^2 > y^2$ really means

For all positive real numbers x & y, if $x > y$, then $x^2 > y^2$.

Proving Theorems

- Many theorems have the form:
  $\forall\ x\ (P(x) \rightarrow Q(x))$
- To prove them, we show that where c is an arbitrary element of the domain,

$$P(c) \rightarrow Q(c)$$

- By universal generalization the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$.

Theorem

Every odd integer is equal to the difference between the squares of two integers.

Methods of Proof

- **Direct Proof**
- **Proof by Contradiction**
- **Proof by Contrapositive**
- **Constructive Proofs, Counterexamples, and Vacuous Proofs**
- **Mathematical Induction**

Direct Proof

- To prove a statement of the form "if A, then B" directly, begin by assuming that A is true.
- Then, making use of *axioms*, *definitions*, *previously proven theorems*, and *rules of inference*, proceed directly until B is reached as a conclusion.
- Direct proofs are most easily employed when establishing the general form of the antecedent is straightforward.

Example

Theorem

The square of an integer is odd if and only if the integer itself is odd.

For any integer n, n^2 is odd iff n is odd.

Example

Theorem

The square of an integer is odd if and only if the integer itself is odd.

For any integer n, n^2 is odd iff n is odd.

The statement “n^2 is odd iff n is odd" is really two statements in one:

Example

Theorem

The square of an integer is odd if and only if the integer itself is odd.

For any integer n, n^2 is odd iff n is odd.

The statement “n^2 is odd iff n is odd" is really two statements in one:

1. if n is odd then n^2 is odd
2. if n^2 is odd then n is odd

Example

Proof.

First, we show that if n is odd then n^2 is odd.
If n is odd, then we can write $n = 2k + 1$ where $k \in \mathbb{Z}$. Then

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2.j + 1 \qquad\qquad where\ \ j = (2k^2 + 2k) \in \mathbb{Z} \end{aligned}$$

Thus, n^2 is odd.

□

Proof by Contradiction

- The technique known as proof by contradiction is one type of **indirect proof**.
- In a proof by contradiction, in order to prove a statement of the form “If A, then B", one assumes that both A and ¬B are true.
- The goal is then to reach a contradiction, which allows one to conclude that A and ¬B can never both be true.
- That is, whenever A is true, B must also be true.
- This method of proof is useful when assuming ¬B allows you to easily utilize a definition or theorem.

Example

Only if part of previous theorem:

Proof.

Now, we have to show that if n^2 is odd, then n must be odd.
Suppose this is not true for all n, and that n is a particular integer s/t n^2 is odd but n is not odd.
Now if n is even, we can write $n = 2k$ where $k \in \mathbb{Z}$

Example

Only if part of previous theorem:

Proof.

Now, we have to show that if n^2 is odd, then n must be odd.
Suppose this is not true for all n, and that n is a particular integer s/t n^2 is odd but n is not odd.
Now if n is even, we can write $n = 2k$ where $k \in \mathbb{Z}$

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2) \\ &= 2.j, \qquad\qquad where\ \ j = 2k^2 \end{aligned}$$

Thus, n^2 is even which contradicts our assumption.

That is, the assumption, n is an integer s/t n^2 is odd but n is not odd, was false.

Corollary

Corollary

If n is odd, then n^4 is odd.

Corollary

Corollary

If n is odd, then n^4 is odd.

Proof.

Note that $n^4 = (n^2)^2$.

Since n is odd, by previous theorem, n^2 is also odd.

Then since n^2 is odd, again the theorem, n^4 is odd. □

Proof by Contrapositive

- Proof by contrapositive makes use of the fact, which relies on the equivalence of an implication with its contrapositive.
- The proof begins by assuming $\neg B$ is true.
- Referencing *axioms*, *definitions*, *previously proven theorems*, and *rules of inference*, the proof ultimately reaches the conclusion that $\neg A$ is true.
- In other words, this is a direct proof on the contrapositive of the original statement $A \rightarrow B$.

Example

Theorem

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Example

Theorem

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Proof.

1. The first step in a proof by contraposition is to assume that the conclusion of the conditional statement “If $3n + 2$ is odd, then n is odd" is false.
2. Then $n = 2k$ for some $k \in \mathbb{Z}$.
3. We find that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.
4. This tells us that $3n + 2$ is even.
5. This is the negation of the premise of the theorem.

We have proved that if $3n + 2$ is odd, then n is odd. □

Constructive Proofs

- While proofs of universally quantified statements are more commonly encountered, knowing how to prove an existentially quantified statement is essential.
- Recall that an existentially quantified statement simply makes a claim about the existence of a particular entity.
- If a single example of the desired object can be produced, the statement has been proven.
- Such a proof is often called a constructive proof.

Example

Exercise

Prove that there exists an integer n s/t

$$\frac{n^2 + n}{3n + 8} = 1.$$

Solution

- *First Thoughts – find such n*
- *Prove the statement for those n.*

Counterexamples

- One is presented with a statement that may or may not be true and is asked to prove or disprove the given statement.
- In this case, experimentation may be required in order to decide whether to attempt a proof or a disproof.
- To disprove a universally quantified statement, providing a single **counterexample** is sufficient.
- Thus disproof of a universally quantified statement is constructive.
- On the other hand, disproving an existentially quantified statement amounts to proving a quantified statement:
  one must show that the given statement does not hold for any elements of the domain of discourse.

Example

Exercise

Prove that the irrational numbers are not closed under multiplication.

Example

Exercise

Prove that the irrational numbers are not closed under multiplication.

Solution

First Thoughts. *The statement p : irrational numbers are closed under multiplication is a universal statement.*

$\neg p$: *It is not the case that the irrational numbers are closed under multiplication.*

This means the given statement is logically equivalent to an existential statement.

We can prove it false if we can produce two irrational numbers whose product is rational.

Example

Exercise

Prove that the irrational numbers are not closed under multiplication.

Solution

First Thoughts. *The statement p : irrational numbers are closed under multiplication is a universal statement.*

$\neg p$: *It is not the case that the irrational numbers are closed under multiplication.*

This means the given statement is logically equivalent to an existential statement.

We can prove it false if we can produce two irrational numbers whose product is rational.

Let $x = \sqrt{2}$ & $y = \sqrt{8}$. Then x & y are both irrational, but $xy = 4$ is rational.
Thus the irrational numbers are not closed under multiplication.

Counterexamples

In summary,

- A single example cannot prove a universally quantified statement (unless the domain of discourse contains only one element);
- a single counterexample can disprove a universally quantified statement;
- a single example can prove an existentially quantified statement;
- a single counterexample cannot disprove an existentially quantified statement (unless the domain of discourse contains only one element).

Vacuous Proofs

- Now, we consider the situation in which a statement of the form “if A, then B" is to be proven, but the statement A is never true.
- Since a conditional statement is always true when the antecedent is false.
- We would regard such a statement as vacuously true.

Example

Exercise

For all $x \in \mathbb{R}$, *if* $x^2 < 0$ *then* $3x^2 + 5 = -7x$

Solution

For any $x \in \mathbb{R}, x^2 \geq 0$.

Thus, since the antecedent ($x^2 < 0$) *is always false, the implication is* ***vacuously true***.

Proof by Mathematical Induction

- Mathematical induction is an important proof technique, and it is often used to establish the truth of a statement for all natural numbers.
- There are two parts to a proof by induction:
  - the **base step**
  - the **inductive step**
- In the base step, we show that the statement is true for some natural number (usually the number 1).
- In the inductive step, we assume the statement is true for some natural number $n = k$ (*inductive hypothesis*), then the statement is true for its successor $n = k + 1$. This is often written as $P(k) \to P(k + 1)$.

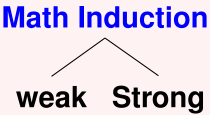
Proof by Mathematical Induction

- Mathematical induction is an important proof technique, and it is often used to establish the truth of a statement for all natural numbers.
- There are two parts to a proof by induction:
  - the **base step**
  - the **inductive step**
- In the base step, we show that the statement is true for some natural number (usually the number 1).
- In the inductive step, we assume the statement is true for some natural number $n = k$ (*inductive hypothesis*), then the statement is true for its successor $n = k + 1$. This is often written as $P(k) \to P(k + 1)$.

$$(P(1) \land \forall k\ (P(k) \to P(k + 1))) \to \forall n\ P(n).$$

Mathematical Induction

Induction


Math Induction

weak **Strong**

Definition

- ***Weak Induction:*** $(P(1) \land \forall k\ (P(k) \to P(k+1))) \to \forall n\ P(n)$.
- ***Strong Induction:*** $(P(1) \land \forall k(P(1) \land P(2) \land \ldots \land (P(k) \to P(k+1))) \to \forall n\ P(n)$.

Example of Weak Induction

Exercise

Show that the sum of the first n natural numbers is $\frac{n(n+1)}{2}$

Example of Weak Induction

Exercise

Show that the sum of the first n natural numbers is $\frac{n(n+1)}{2}$

Solution

1. *First, we consider the case when $n = 1$ and clearly $1 = \frac{1.(1+1)}{2}$.*
2. *Next, we assume that it is true for $n = k$, i.e.,*

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

3. *Prove it for $n = k + 1$*

Importance of Base Step

Let us try to prove $n + 1 < n \ \forall n \in \mathbb{N}$.

- First we assume that the above inequality is true for $n = k$ for some $k \in \mathbb{N}$, i.e.,

$$k + 1 < k.$$

- Now, we try to prove this is true for $n = k + 1$.

$$\begin{aligned}(k+1)+1 &< k+1 \\ k+2 &< k+1\end{aligned}$$

- Thus, induction step is true.
- However, it is not true for $n = 1$.

Thus, the given inequality is not true.

Example of Strong Induction

Proposition

Every integer greater than 1 can be written as the product of prime numbers.

Proof.

- Let $P(n)$ be the statement that n can be written as the product of prime numbers.
- $P(n)$ is true for each integer greater or equal to 2.
- For $n = 2$, $P(n)$ is true.
- Now, assume that for some $k \geq 2$, each integer n with $2 \leq n \leq k$ may be written as a product of primes. We need to prove that $k + 1$ is a product of primes.

□

Example of Strong Induction

Proof.

- **Case (a):** Suppose $k + 1$ is a prime. Then we are done.
- **Case (b):** Suppose $k + 1$ is a not prime. Then by our assumption, $\exists$ integers a & b with $2 \leq a, b \leq k$ s/t

$$k + 1 = ab.$$

By the strong inductive hypothesis, since $2 \leq a, b \leq k$, both a & b are the product of primes. Thus,

$k + 1 = ab$ is the product of primes.

Example of Strong Induction

Proof.

- **Case (a):** Suppose $k+1$ is a prime. Then we are done.
- **Case (b):** Suppose $k+1$ is a not prime. Then by our assumption, $\exists$ integers a & b with $2 \le a, b \le k$ s/t

$$k+1 = ab.$$

By the strong inductive hypothesis, since $2 \le a, b \le k$, both a & b are the product of primes. Thus,

$k+1 = ab$ is the product of primes.

This is proved by strong induction. □

Outline

1. Introduction
   - Syllabus
     - References
2. The Foundations: Logic and Proofs
   - Propositional Logic
   - Proofs
     - Direct Proof
     - Proof by Contradiction
     - Proof by Contrapositive
     - Constructive Proofs, Counterexamples, and Vacuous Proofs
3. Counting

Basic Counting Principles: The Product Rule

The Product Rule: A procedure can be broken down into a sequence of two tasks.

There are n_1 ways to do the first task and n_2 ways to do the second task.

Then there are $n_1 \times n_2$ ways to do the procedure.

Example

How many different number plates can be made if each plate contains a sequence of 2 uppercase English letters followed by 4 digits?

Basic Counting Principles: The Product Rule

The Product Rule: A procedure can be broken down into a sequence of two tasks.
There are n_1 ways to do the first task and n_2 ways to do the second task.
Then there are $n_1 \times n_2$ ways to do the procedure.

Example

How many different number plates can be made if each plate contains a sequence of 2 uppercase English letters followed by 4 digits?

Solution

There are $26^2 \times 10^4$ *many different number plates*

Counting Functions

Example

How many functions are there from a set with m elements to a set with n elements?

Counting Functions

Example

How many functions are there from a set with m elements to a set with n elements?

Solution

There are $\underbrace{n \times n \times \ldots \times n}_{m\text{-times}} = n^m$ *such functions.*

Example

How many one-to-one functions are there from a set with m elements to a set with n elements?

Counting Functions

Example

How many functions are there from a set with m elements to a set with n elements?

Solution

There are $\underbrace{n \times n \times \ldots \times n}_{m\text{-times}} = n^m$ such functions.

Example

How many one-to-one functions are there from a set with m elements to a set with n elements?

Solution

There are $n(n-1)(n-2)\ldots(n-m+1)$ such functions.

Basic Counting Principles: The Sum Rule

The Sum Rule: If a task can be done either in one of n_1 ways or in one of n_2, where none of the set of n_1 ways is the same as any of the n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Basic Counting Principles: The Sum Rule

The Sum Rule: If a task can be done either in one of n_1 ways or in one of n_2, where none of the set of n_1 ways is the same as any of the n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Example

The IIITL must choose either a student from CS, a student from CSAI, or a student from IT as a representative for students' committee.

The Sum Rule

Counting Passwords

Exercise

A password consists of 6 to 8 characters, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible ways you can choose your passwords?

Counting Passwords

Solution

Let P be the total number of passwords, and let $P_6, P_7,\ \&\ P_8$ be the passwords of length 6, 7, and 8.

- *By the sum rule* $P = P_6 + P_7 + P_8$.
- *We find that:* $P_6 = 36^6 - 26^6$
- $P_7 = 36^7 - 26^7$
- $P_8 = 36^8 - 26^8$

Consequently, we have $P = P_6 + P_7 + P_8$

Basic Counting Principles: Subtraction Rule

Subtraction Rule: If a task can be done either in one of n_1 ways or in one of n_2 ways,

then the total number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.

- This is also known as, the principle of *inclusion-exclusion*:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Counting Bit Strings

Exercise

How many bit strings of length 8 either start with a 1 bit or end with the two bits 00?

Counting Bit Strings

Exercise

How many bit strings of length 8 either start with a 1 bit or end with the two bits 00?

Solution

- *Number of bit strings of length 8 that start with a 1 bit:* $2^7 = 128$
- *Number of bit strings of length 8 that end with bits 00:* $2^6 = 64$
- *Number of bit strings of length 8 that start with a 1 bit and end with bits 00 :* $2^5 = 32$

Thus, the number is $128 + 64 - 32 = 160$.

The Pigeonhole Principle

Principle

If one places n pigeons into m pigeonholes, and $n > m$, then at least one pigeonhole will contain more than one pigeon.

The Pigeonhole Principle

Principle

If one places n pigeons into m pigeonholes, and $n > m$, then at least one pigeonhole will contain more than one pigeon.

– familiar version

The Pigeonhole Principle

Principle

If one places n pigeons into m pigeonholes, and $n > m$, then at least one pigeonhole will contain more than one pigeon.

– familiar version

Proof.

We use a proof by contraposition.

Suppose none of the m pigeonholes, has more than one pigeon.

Then the total number of pigeons would be at most m.

This contradicts the statement that we have n pigeons and $n > m$.

Thus, our assumption was wrong. Hence proved! □

The Pigeonhole Principle

Corollary

A function f from a set with $k+1$ elements to a set with k elements is not one-to-one.

The Pigeonhole Principle

Corollary

A function f from a set with $k + 1$ elements to a set with k elements is not one-to-one.

Example

Among any group of 366 people, there must be at least 2 having the same birthday.

The Pigeonhole Principle

Corollary

A function f from a set with $k+1$ elements to a set with k elements is not one-to-one.

Example

Among any group of 366 people, there must be at least 2 having the same birthday.

Problem

Let there be $m+1$ people $\{P_1, P_2, \ldots, P_{m+1}\}$ in a room. What should be the value of m so that the probability that atleast one of the persons $\{P_2, P_3, \ldots, P_{m+1}\}$ shares birthday with P_1 is greater than $\frac{1}{2}$?

The Pigeonhole Principle

Corollary

A function f from a set with $k+1$ elements to a set with k elements is not one-to-one.

Example

Among any group of 366 people, there must be at least 2 having the same birthday.

Problem

Let there be $m+1$ people $\{P_1, P_2, \ldots, P_{m+1}\}$ in a room. What should be the value of m so that the probability that atleast one of the persons $\{P_2, P_3, \ldots, P_{m+1}\}$ shares birthday with P_1 is greater than $\frac{1}{2}$?

Problem

How many people must be there in a room, so that the probability of atleast 2 of them sharing the same birthday is greater than $\frac{1}{2}$?

The Pigeonhole Principle

Theorem

Let A be a finite set, partitioned into finite subsets $S_1, S_2, \ldots, S_m$. If $|A| = n > m$, then at least one of these m subsets contains more than one element.

The Pigeonhole Principle

Theorem

Let A be a finite set, partitioned into finite subsets $S_1, S_2, \ldots, S_m$. If $|A| = n > m$, then at least one of these m subsets contains more than one element.

Principle (Generalized Pigeonhole)

If one places n pigeons into m pigeonholes with respective capacities of $c_1, c_2, \ldots, c_m$ and $n > c_1 + c_2 + \ldots + c_m$ then at least one of the pigeonholes will contain more pigeons than its capacity.

Principle (Extended Pigeonhole)

If one places n pigeons into m pigeonholes, then one of the pigeonholes will contain at least $\lfloor \frac{n-1}{m} \rfloor + 1$ pigeons.

The Pigeonhole Principle

Exercise

1. *Prove that in any set of 99 natural numbers, there is a subset of 15 of them with the property that the difference of any two numbers in the subset is divisible by 7.*
2. *There are 75 students in a class. Each got an A, B, C, or D on a test. Show that there are at least 19 students who received the same grade.*

The End

Thanks a lot for your attention!