Discrete Mathematics

Dhananjoy Dey

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

July 28, 2020

Disclaimers

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

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

Outline

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.

Outline

Syllabus

- Logic, Proof, 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.

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

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 $\Longrightarrow$
    - Biconditional $\leftrightarrow$ or $\Longleftrightarrow$

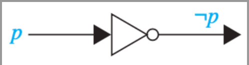
Compound Propositions: Negation

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 $\neg p$

p	$\neg$**p**
T	F
F	T

Table: Truth Table



Example

p – *you are students of* 3^{rd} *year BTech*

$\neg p$ –

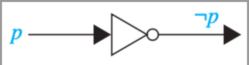
Compound Propositions: Negation

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* 3^{rd} *year BTech*

$\neg p$ – *you are not students of* 3^{rd} *year BTech*

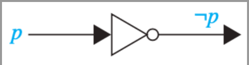
Compound Propositions: Negation

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* 3^{rd} *year BTech*

$\neg p$ – *you are not students of* 3^{rd} *year BTech*

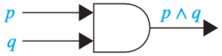
Remark: Other notations for negation are $\bar{p}, \sim p, -p, Np, p'$ or $!p$.

Conjunction

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

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

Table: Truth Table



Example

p – *you are watching this lecture from home*

q – *it is raining*

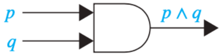
$p \wedge q$ –

Conjunction

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

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 watching this lecture from home*

q – *it is raining*

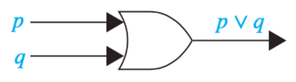
$p \wedge q$ – *you are watching this lecture from home and it is raining*

Disjunction

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

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

Table: Truth Table



Example

p – *you are watching this lecture from home*

q – *you are watching TV*

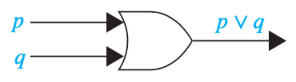
$p \wedge q$ –

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 watching this lecture from home*

q – *you are watching TV*

$p \wedge q$ – *you are watching this 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.

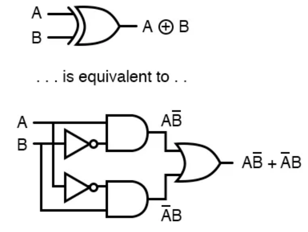
    This is the meaning of **Exclusive Or (Xor)**.

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

Exclusive or (Xor)

p	q	p ⊕ q
T	T	F
T	F	T
F	T	T
F	F	F

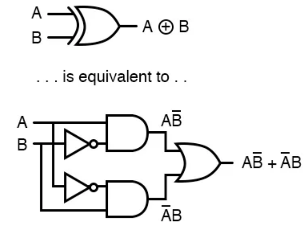
Table: Truth Table



Exclusive or (Xor)

p	**q**	**p ⊕ 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 $p \to q$ 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

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.

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

Table: Truth Table

In $p \rightarrow q$, 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**	$\mathbf{p \leftrightarrow q}$
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

विद्या ददाति विनयं विनयाद् याति पात्रताम्

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.*

$$p \vee \neg p$$

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

$$p \wedge \neg p$$

- *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 tablefor 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

The End

Thanks a lot for your attention