Why Do We Study a Discrete Mathematics course ?

As engineering students, you all should be able to think logically and Mathematically.

And Discrete Mathematics provide you with the necessary tools required to read, comprehend and construct mathematical logic.

* Give example of some random programming problem & conditions.

In addition, there are several other importances for studying Discrete Mathematics —

① Mathematical maturity :

You will act like a more mature engineer!

⇓

improves ability to understand and create mathematical arguments.

② Gateway to many other advanced courses

Algorithms | data structures | database | Computer Security

Criptography

⊞ Ciphers & codes use a lot of tools that are part of discrete mathematics!

RSA algorithm

- encryption Key is public
- decryption Key is Kept secret.

RSA ~~er~~ in ~~bf~~ brief.

$p \longrightarrow$ Prime number 1

$q \longrightarrow$ Prime number 2

$pq \longrightarrow$ Product of the two primes and is made public.

$e \longrightarrow$ The other number that is also made public.

e is relatively prime to $(p-1)*(q-1)$

That's gcd = (greatest common Divisor) between e & $(p-1)*(q-1) = 1$.

How the encryption happens:

$\boxed{\text{Message}} \xrightarrow{\text{convert to}} \boxed{\text{sequence of Integers } x_1 x_2 x_3 x_4 x_5 \ldots x_n} \xrightarrow[\text{known}]{p,\,q,\,e} \boxed{\begin{aligned} x_1^* &= x_1^e \bmod pq \\ x_2^* &= x_2^e \bmod pq \\ &\vdots \\ x_n^* &= x_n^e \bmod pq \end{aligned}} \rightarrow \boxed{\text{encrypted Message}}$

Example: $p=5$, $q=11$
$e=21$
So, $(p-1)*(q-1) = 4 \times 10 = 40$
So, $\gcd(21, 40) = 1$

For $p=5$, $q=11$, $e=21$. Encryption of any x could be done as follows.

$$x^* = x^e \bmod pq$$

↳ calculation of this kind of modular exponentiation is done using fast and efficient algorithms.

Early History of Cryptography

One of the first encryption systems whose details survives:

Polybius square

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- Created by Greek historian Polybius around the second century BCE.

- For example, You want to transmit below message:

THE ATHENIANS BESEECH YOU TO HASTEN TO THEIR AID

44 23 15 11 44 23 ...

- Each letter in the message can be represented by holding between one & Five torches in each hand.

↓

Allows a message to be passed quickly over long distance.

Consider a few questions/issues

* In how many ways you can choose a valid password?

* What is your probability of winning a lottery?

* You are given a list of numbers, and you are asked to sort the numbers in an ascending or descending order.

  How will you do that?

  How many steps will it take?

One ~~f~~ common thing in all the above questions is that — They all ~~deal~~ deal with discrete objects.

By discrete objects we mean that —

- Objects are countable, or counted.
- Relationships between those countable objects
- Processes involving finite/countable steps.

  etc.

And Discrete mathematics is primarily focused to study all these discrete objects.

More importantly, all the computers, digital gadgets etc. stores information discretely, and they are manipulated by computing machines in a discrete fashion.

So, you all are here, precisely, to learn how your computers, gadgets etc, at some point of time in your life, be designed/developed by yourselves.

Goodluck, & welcome.

Upon completion, you may be able to

- understand formal statements & proofs of Mathematics.
- demonstrate rigorous proof by yourselves
- reach a certain level of mathematical maturity.

"THE" LOGIC

Socrates — one of the greatest thinkers, philosophers of all times.

He invented a method, comprises of series of interrogative questions to discover contradiction in one's understanding/belief on something.

↓ This method is known as

Method of Elenchus, elenctic Method

→ Ask questions until you run out of answers or Knowledge

→ Then according to Socrates, you will understand at some point of time that you know nothing

Anyway,

Great Grand student of Socrates, That is Aristotle,

He was the first thinker who came up with ~~a~~ ~~to~~ well devised logical system.

In short, Aristotle emphasized on —

- ✓ Claims about propositional structure & negation in Parmenid and plato.
- ✓ Argumentative techniques found in legal reasoning and geometric proof

☐ Analysis of Logical form, opposition and conversion are syllogistic.

Applies deductive reasoning.

→ A form of reasoning in which conclusion is drawn from two or more given or assumed propositions.

→ Man is mortal; we all are humans; so, we all will die.

→ You all have enrolled in CSE program at NSU;

Discrete Mathematics course is mandatory to obtain CSE degree at NSU;

so, you all will do Discrete Mathemat at NSU.

So, here we obtain the notion of propositions.

What do you mean by Proposition?

[Take student's input]

By definition,

Propositions: It is a declarative sentence that is either true or false.

By declarative, we mean that a sentence that declares a fact.

Examples:

* Dhaka is the capital of Bangladesh.
* $1 + 1 = 2$

Sentences	Proposition YES	Proposition NO
* $2 + 3 = 10$	✓	
* $5 + 8 = 13$	✓	
* Where are you going?		✓
* Be attentive in class?		✓
* $x + 7 = 14$		✓

↳ because, it is neither true nor false

Propositional variable:

- Variables that represent propositions; frequently, letters are used.
  - → p, q, r, s are more commonly used.

- True and False propositions are represented as T and F respectively.

Now, the question is — Given that you have a proposition, how can you produce new proposition from it?

Any guess?

In short,

Many mathematical statements are produced by combining one or more propositions.

New propositions constructed from existing propositions are known as compound propositions.

AND,

We need logical operators to combine existing propositions.

LOGICAL OPERATORS

Devising new propositions using existing propositions is first discussed by English mathematician George Boole.

- Boolean Algebra is named after him

A few logical operators are -

(1) Negation:

- If P is a proposition, negation of P is $\neg P$ or $\overline{P}$

$\neg P \Rightarrow$ It is not the case that P

Example:

Proposition: Today is Friday
Negation: It is the case that today is Friday.

P	$\neg P$
0 T	1 F
1 F	0 T

P:

- All CSE 173 students get "A" in final exam.

$\neg$P: It is not the case that all CSE173 students get "A" in the final exam.

- To summarize, negation of a proposition can also be considered as the result of the operation of the negation operator on a proposition.

Negation operator constructs new proposition from a single existing proposition. But, there are other logical operators that are used to form new propositions from <u>two or more</u> propositions.

Conjunction

Definition:

- Let p and q are two propositions. The conjunction of p and q is the proposition "p and q".

It is denoted as "$p \wedge q$"

TRUTH TABLE

$p \wedge q$ is true when both p and q are true.

$p \wedge q$ is false if at least one of the two propositions is false.

- Consider two propositions —

① The sun is shining
② It is raining

Using conjunction:

✓ The sun is shining and it is raining.

✓ The sun is shining, but it is raining.

TRUTH TABLE:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction

Definition:

Let p and q are two propositions. The disjunction of p and q is the proposition $p \vee q$.

* Here, the connective is "or"

* When one of the two propositions is true, the disjunction becomes true.

Example :

p : Today is Friday

q : It is raining today

So, $p \vee q$ is —

Today is Friday or it is raining today.

Inclusive "Or" and Exclusive "Or"

Let's take an example

- Students who have enrolled in Mathematics or computer science, at NSU, can do CSE 173 course.

↓ This implies

Any one who's enrolled in Math
Any one who's enrolled in CS
Any one who has double major in Math & CS
can take CSE 173 course.

inclusive

- Students who have enrolled in Mathematics or CS, but not both, at NSU, can do CSE 173 course.

Exclusive

A disjunction is true when at least one of the two propositions is true. Thus, the truth table for a disjunction looks as below:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

* Ask students to fill the 3rd column.

That is, disjunction $p \vee q$ is false when both the propositions are false.

Another connective : Exclusive or

Suppose p and q are the two propositions. The "exclusive or" suggests that—

* the proposition is true when exactly one of p and q is true
AND
false otherwise

Or is used here as "exclusive"

So, * Exclusive or is denoted as $p \oplus q$

p	q	$p \oplus q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
T	T	F	$(T \wedge F) \vee (F \wedge T) = F \vee F = F$
T	F	T	$(T \wedge T) \vee (F \wedge F) = T \vee F = T$
F	T	T	$(F \wedge F) \vee (T \wedge T) = F \vee T = T$
F	F	F	$(F \wedge T) \vee (\cancel{T} F \wedge F) = F \vee F = F$

Conditional Statements ;

Propositions can be combined using conditional statement as well.

Definition :

Let p and q be propositions.

conditional statement $p \rightarrow q$ is the proposition

if "p", then "q"

The conditional statement $p \rightarrow q$ is false when p is true and q is false.

Here, p is hypothesis/premise

q is conclusion/consequence

$p \rightarrow q$ conditional statement, because q is true on the condition that p holds.

Truth table

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

* Ask students for the 3rd column.

This compound proposition is also known as implication.

$p \rightarrow q$ continues ...

* Confusion

p	q	$p \rightarrow q$
T	F	F

Case 2 ⟵ T F | F ⟶ how

Let's take an example — Say, you want to by shares from Dhaka Stock Exchange (DSE)

Now, p denotes

I buy shares of * company

q denotes

I will be rich

So $p \rightarrow q$ means

If I buy shares of * company then I will be rich.

$\underbrace{\text{I buy shares}}_{p}$ $\underbrace{\text{I will be rich}}_{q}$

$\equiv$ if p then q

Case 1: "I buy shares of * Company (p is T) and I will be (q is T)

Case 2 "I buy shares" and I won't be rich (q is F)
↳ P(T)
↳ so, "$p \rightarrow q$" F

Case 3 & 4: "I don't buy shares" and this doesn't contradict our proposition $p \rightarrow q$

More about $p \rightarrow q$

Proposition "p implies q" or, "if p then q" is represented $\underbrace{p \rightarrow q}$

↳ called an "Implication", or a "Conditional"

- Proposition $p \rightarrow q$ is false only when the antecedent "p" is true and the consequent q is false.

- $p \rightarrow q$ does not assert that its antecedant p is true; nor it does say that its consequent q is true.

- Instead, it only says that if antecedent is true then its consequent is true also.

According to definition of implication —

There are two valid principles of $p \rightarrow q$ that, nevertheless, are sometimes considered paradoxical.

A. A False antecedent "p" implies any proposition q

example:

If 1981 is leap year (p), then Isaac Newton discovered America. (q)

More on Implication ($p \to q$)

In English,

a sentence of the form "if A then B" can have different meanings.

Typically there is a causal realationship between A and B, which is not required logic.

We are often implying more than simply that if A holds then B holds.

Example:

If I finish my work early, then I will pick you up before lunch

inverse

If I do not finish my work, then I will not pick you up before lunch.

But, this is not implied by the logical implication

$$p \longrightarrow q$$

Here, "p": I finish my work early

"q": I will pick you up before lunch

English is not as precise as logic.

Biconditional Statement $p \leftrightarrow q$

It is the proposition

"p if and only if q"
" p iff "

The statement $p \leftrightarrow q$ is true when p and q both have same truth values.

TRUE FALSE

and is false otherwise

Truth Table

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

* $p \leftrightarrow q$ has the same truth table as $(p \to q) \wedge (q \to p)$

Example:

You can take flight $\equiv p$
You buy a ticket $\equiv q$

$p \leftrightarrow$

You can take a flight if and only if you buy a ticket.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

$\wedge$

p	q	$q \to p$
T	T	T
T	F	T
F	T	F
F	F	T

$\equiv$

T
F
F
T

$\equiv$

$p \leftrightarrow q$
T
F
F
T

Converse:

$q \rightarrow p$ is the converse of $p \rightarrow q$

Let's assume the compound proposition $p \rightarrow q$ is

" If Maradona scores by hand, then Argentina wins "

So, Converse is,

" If Argentina wins, then Maradona scores by hand "

Inverse:

Proposition $p \rightarrow q$, inverse is $\neg p \rightarrow \neg q$

Example: $p \rightarrow q$ "If FIFA favors Brazil, then they move to finals "

So, $\neg p \rightarrow \neg q$ is.

" If FIFA does not favor Brazil, then they do not move to finals "

Contrapositive:

For $p \rightarrow q$, " $\neg q \rightarrow \neg p$ "

If students do homework well, then they do well in exam.

contrapositive

$\neg q \rightarrow \neg p$

If students do not do well in exam, then students do not do homework well.

Translate English sentence

* There are different ways to translate a sentence into logical expression.

① treating as single propositional variable

* This may not be useful for further reasoning.

② Use multiple propositional variables to treat different parts of a long sentence as separate propositional variables.

Example : You can access the internet from campus only if you are a computer science student/instructor or you are not a freshman.

→ a : You can access the internet from campus

→ c : You are a computer science students/instructor

→ f : You are a freshman.

So, considering "only if", we represent using conditional,

$$a \longrightarrow (c \lor \neg f)$$

Precedence of Operators :

Let us take an example —

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

↓ if represented as

$$p \vee q \wedge \neg r$$

What operator do we apply first ?

So, there's a precedence of operators.

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

Logic and bit operations

* There are two possible truth values
  - → TRUE 1
  - → FALSE 0
* Bit operations correspond to the logical connectives.
* We define

Bitwise OR

$$\begin{array}{r} 01\ 1011\ 0110 \\ 11\ 0001\ 1101 \\ \hline 11\ 1011\ 1111 \end{array}$$

Bitwise AND

$$\begin{array}{r} 01\ 1011\ 0110 \\ 11\ 0001\ 1101 \\ \hline 01\ 0001\ 0100 \end{array}$$

Bitwise XOR

$A'B + AB'$

$$\begin{array}{r} 01\ 1011\ 0110 \\ 11\ 0001\ 1101 \\ \hline 10\ 1010\ 1011 \end{array}$$

Propositional equivalence

Replacing a compound proposition, by a proposition that has the same truth values, is often necessary for the construction of mathematical arguments.

Tautology:

A compound proposition that is always true, no matter what the truth values of the propositions.

Contradiction:

A compound proposition that is always false is called a contradiction.

Tautology

p		$p \vee \neg p$
T	F	T
F	T	T

contradiction

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

A compound proposition that is neither a tautology nor a contradiction

Known as

" Contingency "

Consider three propositions p, q, r. Find out a compound proposition involving p, q, r, that is true when p and q are true and r is false. The compound proposition is false otherwise.

$$(p \land q) \land \neg r$$

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

true only when p and q are true and r is false

Logical Equivalence:

Let's assume that p and q are two compound positions.

If truth values in all possible cases for the compound propositions p and q are same

Then, p and q are logically equivalent.

- The notation $p \equiv q$ denotes that p and q are logically equivalent.
- p and q are logically equivalent if $p \leftrightarrow q$ is a tautology.

Example:

$p \to q$ and $\neg p \vee q$ are logically equivalent

p	q	$\neg p$	$p \to q$	$\neg p \vee q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

* As the truth tables are same, $p \to q$ and $\neg p \vee q$ are logically equivalent.

De Morgan's Law [example of logical equivalence]

- Tells us how to negate conjunctions, and
- How to negate disjunctions.

The laws are:

1. $\neg(p \vee q) \equiv \neg p \wedge \neg q$
2. $\neg(p \wedge q) \equiv \neg p \vee \neg q$

* We can use Truth Table to show that they are logicall equivalent. Homework

De Morgan's Law continues ...

For "n" propositional variables, the laws are

$$\neg(P_1 \vee P_2 \vee P_3 \ldots \vee P_n) \equiv \neg P_1 \wedge \neg P_2 \wedge \neg P_3 \ldots \wedge \neg P_n$$

and

$$\neg(P_1 \wedge P_2 \wedge P_3 \ldots \wedge P_n) \equiv \neg P_1 \vee \neg P_2 \vee \neg P_3 \ldots \vee \neg P_n$$

New Logical Equivalence :

- Existing logical equivalence can be used to construct new logical equivalence.

For instance, we know $(p \rightarrow q) \equiv \neg p \vee q$ and we use to show logical equivalence between $\neg(p \rightarrow q)$ and $(p \wedge \neg q)$

So,

$$\neg(p \rightarrow q) \equiv \neg(\neg p \vee q) \quad \text{Using the given one.}$$

$$\equiv \neg(\neg p) \wedge \neg q \quad \text{De morgan: negation of disjunction}$$

$$\equiv p \wedge \neg q \quad \text{Double negation}$$

Prove $(p \wedge q) \rightarrow (p \vee q)$ is a tautology

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

$$\equiv (\neg p \vee \neg q) \vee (p \vee q) \quad \text{De Morgan Law}$$

$$\equiv (\neg p \vee p) \vee (\neg q \vee q) \quad \text{Associative commutative}$$

$$\equiv T \vee T \quad \text{Commutative \& Negation}$$

$$\equiv T$$

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

List of logical equivalence.

Table 6 in the book

$p \wedge T \equiv p$ Identity

$p \vee F \equiv p$

$p \vee T \equiv T$ Domination

$p \wedge F \equiv F$

$(p \vee q) \vee r = p \vee (q \vee r)$ Associative laws

$(p \wedge q) \wedge r = p \wedge (q \wedge r)$

$p \vee q \equiv q \vee p$ commutive laws

$p \wedge q \equiv q \wedge p$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ distributed laws

$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$

Show that

$$\text{" } (p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r) \text{ "}$$

is a tautology.

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

So, this is a tautology

Consider a truth table for

$$((p \to q) \to r) \to s$$

p	q	$p \to q$	r	$(p - q) \to r$	s	$((p \to q) \to r) \to s$
~~T~~	~~T~~		~~T~~		~~T~~	
~~T~~	~~T~~		~~F~~		~~F~~	
~~T~~	~~F~~		~~F~~			
~~T~~	~~F~~		~~F~~			
p	q		r		s	
T	T	T	T	T	T	T
T	T	T	T	T	F	F
T	T	T	F	F	T	T
T	T	T	F	F	F	T
T	F	F	T	T	T	T
T	F	F	T	T	F	F
T	F	F	F	T	T	T
T	F	F	F	T	F	F
F	T	T	T	T	T	T
F	T	T	T	T	F	F
F	T	T	F	F	T	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T
F	F	T	T	T	F	F
F	F	T	F	F	T	T
F	F	T	F	F	F	T