LECTURE # 1

Course Introduction: Discrete structures.

(Based on John Howat's course notes && Jit's course notes).

Discrete structures - study of structures that are fundamentally discrete rather than continuous. (domain of Calculus).

- discrete structures - abstract mathematical structures used to represent discrete objects and relationships between these objects. (Wikipedia defn)
- discrete from word 'distinct'.

Course Topics

1. Logic - building block
   - how we specify meanings of mathematical statements.
   - has application to
     - design of computers
     - system specifications
     - programming.

2. Algorithms
   - Algorithms: a finite set of precise instructions for performing a computation or for solving a problem.
   - how long does an algorithm take?
     - if we have two different algorithms (sets of instructions), which one will take longer.
     - how long will an algorithm if we try to solve a problem with a large input.
   - How do we measure this?

3. Counting
   - harder than what you covered in kindergarten.
   - how to compute the amont of memory we will need.
   - how to generate all objects of a certain type (eg. all valid passwords).

4. Graphs

- a discrete structure that is used to solve a huge range of problems.
- shortest paths (Google / Bing maps)
- colouring maps.
- the links between all sites on the internet
- computer networks.

Common thread - proofs and proper mathematical rigor.
- understanding & how to develop
- what constitues a valid mathematical proof.

Topic 1: Logic (1.1 - Propositional Logic)

- Logic gives precise meaning to mathematical statements.
  - ▷ tells us exactly what statements mean.
  - ▷ allows computers to reason without ambiguities of natural languages.
  - ▷ rules allow us to distinguish between valid and invalid mathematical arguments.

The basic building block of logic is the proposition
- a declarative statement that is either TRUE or FALSE.

Examples
- Pigs can fly.
- Ottawa is in Canada.
- $2 + 2 = 4$
- $1 + 1 = 3$

Scentences that are not declarative are not propositions.

eg "How are you today?"

"Go outside and play"

Scentences that are not true, or false, are not propositions.

eg. "$x + y = z$"

"This sentence is false".

We can assign propositions names (a, b, c ...) for short.

a = "The sky is blue"

The <u>truth value</u> of a proposition is either T (true) or F (false).

It is best if a single proposition expresses a single fact:

"It is cold today and I am wearing green socks and I am not feeling well."

Can be expressed as the propositions

"It is cold today."

"I am wearing green socks"

"I am not feeling well".

How would we assert all three statements at once?

- we use <u>connectives</u> to create <u>compound propositions</u>.

1. Negation :

Let 'p' be a proposition; we say the <u>negation</u> of p is the statement

" it is not the case that p is true"

This is a compound proposition called negation and we write it $\neg p$ (read as "not p").

p "I am sick"

$\neg p$ "It is not the case that I am sick"

"I am not sick"

As a rule, the original propositions should not contain a negation.

Truth Tables: Useful tool for determining the possible values of a proposition.

p	$\neg p$
T	F
F	T

② Conjunction ("and")

For propositions p, q then the sentence

"p and q"

is the compound proposition called the conjunction of p and q.

write $p \wedge q$ - read "p and q"

p "I am sick"

q "I am wearing green socks"

$p \wedge q$ "I am sick and I am wearing green socks"

Truth Table for $\wedge$

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

Conjunction can be expressed in many ways:

"and", "but", "also"

3 Disjunction ("or")

For propositions p and q the disjunction is the sentence

"p or q"

write: "$p \vee q$" - read "p or q"

It is true when either proposition, or both, are true.

Truth Table

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

p "I work hard"

q "I fail"

$p \vee q$ "I work hard or I fail"

This definition of "or" is more rigorous than in the English language, where or can be inclusive or exclusive.

Inclusive: "Students must have taken CS or calculus to enroll in this class"

Exclusive: "You can buy a Ford or a Toyota". (one or the other, not both).

The disjunction $\vee$ is always inclusive (see TT), for the exclusive or we write $p \oplus q$

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

④ Implication ("if.. then")

Given the propositions p and q, then the implication "if p then q" is a compound proposition.

p - the hypothesis, q - conclusion

write: $p \to q$

eg. p "I attend class"
q "I will pass the final exam"

$p \to q$

"If I attend class then I will pass the final exam".

[This implication is not necessarily true for this class]

TT

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

Note: When p is false, the implication is always true! So if you don't attend class, then this statement is still true, but if you attend class and fail it is false.

Many ways to express $p \to q$ in English.

"if p then q" "p is sufficient for q"

"p implies q" "q follows from p"

"p only if q" "q whenever p"

Given $p \to q$, we define a few special propositions

converse: $q \to p$

contrapositive: $\neg q \to \neg p$

inverse: $\neg p \to \neg q$

The contrapositive is true exactly when $p \to q$ is true, and the others are not - more on this later.

5 Biconditional ("if and only if")

If p, q are propositions then "$p \leftrightarrow q$" is the biconditional compound proposition

Read: "p if and only if q" Write: $p \leftrightarrow q$

"p iff q"

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

It is true when p & q have the same truth values.

p "I get eaten by a bear"

q "I kept donuts in my tent"

We can say

"p is necessary and sufficient for q"

"if p, then q, and conversely"

Thus we can think of $p \leftrightarrow q$ as: $(p \to q) \wedge (q \to p)$

"If I get eaten by a bear if and only if I keep donuts in my tent".

Precedence

- use brackets to make things clear
- negation applies to the proposition (or compound proposition) immediately to its right

This should be about 1.5 hrs

BREAK TIME

Translating Sentences

Given, propositions a, b, c, let

a be "the computer lab uses Linux"

b be "a hacker breaks into the computer"

c be "the data on the computer is lost"

What is $(a \rightarrow \neg b) \wedge (\neg b \rightarrow \neg c)$?

"If the computer lab uses Linux then a hacker will not break into the computer, AND, if a hacker does not break into the computer then the data on the computer is not lost"

What is : $\neg(a \vee \neg b)$?

"It is not the case that either the computer lab uses Linux or a hacker will not break into the computer"

(Awkward - we will learn better ways to phrase this.

What is : $c \leftrightarrow (\neg a \wedge b)$?

"The data on the computer is lost if and only if the computer lab does not use Linux AND a hacker breaks into the computer."

Translate (English to logical propositions)

Translate: "IF the hard drive crashes then the data is lost"

h : "the hard drive crashes"

d : "the data is lost"

$h \rightarrow d$

"The sensor detects motion only if the intruder is in the room or the scanner is defective"

m : "the sensor detects motion."

i : "the intruder is in the room"

d : "the sensor is defective"

$m \rightarrow (i \vee d)$

Truth Table for $p \rightarrow (\neg q \vee r)$

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

we knew immediately due to $p \rightarrow$ that those will be true, since hypothesis is false.

If there are n variables there will be 2^n different combinations/rows.

Strategy for large tables...

> fill first $\frac{2^n}{2}$ rows with T, second half with F.

> second repeat in each half.

> so . . on.

Truth table.

$\neg(a \vee b) \leftrightarrow (\neg a \wedge \neg b)$ $\boxed{\text{TAUTOLOGY}}$

a	b	$\neg a$	$\neg b$	$\neg(a \vee b)$	$(\neg a \wedge \neg b)$	$\neg(a \vee b) \leftrightarrow (\neg a \wedge \neg b)$
T	T	F	F	F	F	T
T	F	F	T	F	F	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T

Note - the result for this compound proposition is always TRUE, regardless of what we pick for a or b is called a TAUTOLOGY.

Now consider $a \wedge \neg a$: this compound proposition is always FALSE - such a proposition is called a CONTRADICTION

a	$\neg a$	$a \wedge \neg a$
T	F	F
F	T	F

A <u>CONTINGENCY</u> is dependent on the values selected for its constituent propositions.

<u>Examples</u>:

what is: $((a \vee b) \wedge (\neg a \wedge c)) \rightarrow (b \vee c)$: <u>TAUTOLOGY</u>.

$\neg(a \wedge b) \leftrightarrow ((a \vee b) \wedge \neg(a \vee \neg b))$: <u>Contingency</u>

PROPOSITIONAL EQUIVALENCES

- Refer back to our first TAUTOLOGY ... it is a

Two compound propositions p and q are <u>LOGICALLY EQUIVALENT</u> if $p \leftrightarrow q$ is a tataulogy.

Denote this $p \equiv q$ or $p \Leftrightarrow q$

we will use this in this course.

How do we determine if two expressions are logically equivolent?

M1 : truth tables. - do they have same truth values. (ie. prev example).

If time permits show truth tables

<u>Example</u>: $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$ De Morgan's Law (1).

the negation of a disjunction can be formed by taking the conjunction of the negations of the component propositions.

<u>Example</u>: $\neg(p \wedge q) \equiv \neg p \vee \neg q$ - De Morgans Law (2)

the negation of a conjunction can be formed by taking the disjunction of the negations of the component propositions.

M2: Use existing, known logical equivalences to transform one proposition into the other.

What are known logical equivalences (many are listed in Tables 6, 7, 8 on p. 24-25 of textbook), a few of the key ones are (Table 6). - Laws

$p \wedge T \equiv p$, $p \vee F \equiv p$ } Idenity Laws.

$p \vee T \equiv T$, $p \wedge F \equiv F$ } Domination Laws

$p \vee p \equiv p$, $p \wedge p \equiv p$ } Idempotent Laws

$\neg(\neg p) \equiv p$ Double Negation.

$p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$ } Commutative

$(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ } Associative

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ } Distributive

$\neg(p \wedge q) \equiv \neg p \vee \neg q$ De Morgan's

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

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

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

$p \vee \neg p \equiv T$ Negation.

$p \wedge \neg p \equiv F$

There are more in the book, but these you should know.

Table 7

Implication Equivalence.

$p \rightarrow q \equiv \neg p \vee q$

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Table 8: Biconditional

Are $\neg(p \vee (\neg p \wedge q))$ and $(\neg p \wedge \neg q)$ logically equivalent?

take this, try & turn it into this

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge (\neg(\neg p \wedge q)) && \text{De Morgans Law.} \\
&\equiv \neg p \wedge (\neg\neg p \vee \neg q) && \text{De Morgans Law} \\
&\equiv \neg p \wedge (p \vee \neg q) && \text{Double Negation} \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{Distributive} \\
&\equiv F \vee (\neg p \wedge \neg q) && \text{Negation} \\
&\equiv \neg p \wedge \neg q && \text{Identity.}
\end{aligned}$$

We can also use logical equivalences to classify statements as tautologies or contradiction by checking for logical equivalence with T or F.

<u>Example</u> $(p \wedge q) \rightarrow (p \vee q)$ - what is it.

$$\begin{aligned}
(p \wedge q) \rightarrow (p \vee q) &\equiv \neg(p \wedge q) \vee (p \vee q) && \text{Implication Equivalence.} \\
&\equiv (\neg p \vee \neg q) \vee (p \vee q) && \text{De Morgans (Conj).} \\
&\equiv (\neg p \vee p) \vee (\neg q \vee q) && \text{Assoc. Law, Commutative Law} \\
&\equiv T \vee T && \text{Negation} \\
&\equiv T && \text{Identity.}
\end{aligned}$$

$\therefore$ <u>tautology</u>

<u>Example</u> : Are $(p \to q) \to r$ and $p \to (q \to r)$ logically equivalent?

$(p \to q) \to r \equiv \neg(\neg p \lor q) \lor r$ Implication Equivalence (x2).

$\equiv (\neg\neg p \land \neg q) \lor r$ De Morgans (Disjunction).

$\equiv (p \land \neg q) \lor r$ Double Negation

- - - - - - - - - - - - - - - - - -

$p \to (q \to r) \equiv \neg p \lor (\neg q \lor r)$ Implication Equivalence (x2)

$\equiv (\neg p \lor \neg q) \lor r$ Associative

$\equiv \neg(p \land q) \lor r$ De Morgans (Conjunction Inverse).

So we reduce problem to determing are $(p \land \neg q)$ and $\neg(p \land q)$ logically equivalent?

Now, since there is no clear way to prove this, use a truth table:

p	q	$\neg q$	$(p \land \neg q)$	$\neg(p \land q)$
T	T	F	F	F
T	F	T	T	T
F	T	F	F	T
F	F	T	F	T

$\therefore (p \to q) \to r \not\equiv p \to (q \to r)$.

END of LECTURE #1