MATH221
Mathematics for Computer Science

Course Overview

Lecturer/Tutor: Dr Tan Hee Beng Kuan
(email: hbktan@uow.edu.au)

Course Overview

- Logic
- Predicate Logic
- Methods of Proof
- Set Theory
- Relations & Functions
- Number Systems
- Mathematical Induction
- Elementary Number Theory
- Modular Arithmetic
- Introduction to Combinatorics and Probability
- Probability
- Graphs

Why This Course?

- Propositional logic – digital circuit design
- Sets/relations - databases (Oracle, MS Access, etc.)
- Predicate logic - Artificial Intelligence, compilers
- Proofs - Artificial Intelligence, compilers
- Modular arithmetic – Cryptography
- Elementary Number Theory – Cryptography
- Probability – Data mining, machine learning
- Graph Theory – network analysis

MATH221
Mathematics for Computer Science

Unit 1
Logic

OBJECTIVES

- Understand statements and compound statements
- Using logical connectives to form compound statements
- Using the truth table to evaluate the truth values of compound statements
- Understand what is tautology, contradiction and contingent.
- Using logical equivalences to simplify compound statements
- Using truth table and logical equivalences to prove/disprove tautologies (logical formulas)

What is Logic?

Mathematical logic is a tool for dealing with formal reasoning.

Numerous application in design of computer circuits, construction of computer programs and verification of correctness of programs.

What is Logic?

You are familiar with using numbers in arithmetic and symbols in algebra. You are also familiar with the 'rules' of arithmetic and alegebra.

Examples:

$$\begin{aligned}(3 + 4) + 6 &= 3 + (4 + 6)\\ &= 3 + 10\\ &= 13\end{aligned} \qquad \begin{aligned}3x - 5x &= (3 - 5)x\\ &= -2x\end{aligned}$$

In a similar way, Logic deals with statements. We shall define statements later.

What is Logic?

Roughly speaking, in arithmetic an *operation* is a rule for producing new numbers from a pair of given numbers, like addition (+) or multiplication (×).

In Logic, we form new statements by combining short statements using **connectives**, like words *and*, *or*.

Examples:

This room is hot *and* I am tired.

MATH221 lectures are fun *or* I am dreaming.

Statement

A ***statement*** is a sentence that is true or false but not both.

A ***statement*** is also called a ***proposition***

Statement: Examples

True statements:

$2 + 2 = 4$

The sun rises in the east.

False statements:

$2 + 2 = 7$

There are twenty planets in the Solar system.

Non-Statement: Examples

Non-statements are questions, commands, exclamations, or sentences with undefined words such as:

Study logic.

$x + y > 0$: because it is neither true nor false

Do you speak French?

Do your homework now.

Good!

Read this carefully.

Examples:

Which of the following are statements?

(i)	$2 + 3 = 5$	Statement, True
(ii)	It is raining outside.	Statement
(iii)	$2 + 3 = 6$	Statement, False
(iv)	Is it raining?	Non-statement
(v)	Go away!	Non-statement
(vi)	There exists an even prime number.	Statement, True
(vii)	There are six people here.	Statement
(viii)	Seven is?	Non-statement
(ix)	For some real number x, $x < 2$.	Statement

Examples:

Which of the following are statements?

(x)	$x < 2$	Statement
(xi)	$2 = =$	Statement, False
(xii)	$x + y = y + x$	Statement, True

Strictly speaking, as we don't know what x and y are in parts (x) and (xii), these should not be statements. In Mathematics, x and y usually represent real numbers and we will assume this is the case here.

Logical Connectives and Compound Statements

A ***compound statement*** (or statement form) is an expression made up of statement variables (such as P, Q, and R) and logical connectives ($\sim$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$) that becomes a statement when actual statements are substituted for the component statement variables. For example, $(P \vee Q) \wedge R$ is a compound statement.

From now onwards, the word ***statement*** may refer to simple or compound statement.

Connectives

If P and Q are statements, then so are

In words	*In symbols*	*Formal Name*
not P	$\sim P$	**Negation** of P
P or Q	$P \vee Q$	**Disjunction** of P and Q
P and Q	$P \wedge Q$	**Conjunction** of P and Q
P implies Q	$P \Rightarrow Q$	**Conditional** of P, Q
P if and only if Q	$P \Leftrightarrow Q$	**Biconditional** of P, Q

Logical Connectives and Compound Statements

Recall that each statement must either be true or false. We will therefore, assign to each statement a ***truth value*** of

T for true

or **F** for false.

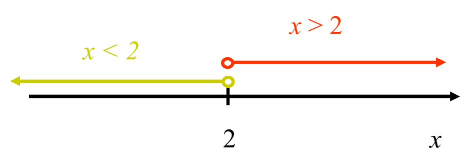
The truth value of a compound statement depends only on the truth values of the member statements and the connectives that form it. We represent this dependence by means of ***truth tables***.

Negation: $\sim P$

The negation of a statement is simply the opposite of what it says.

Negation: Examples

If P is:	It is raining outside.
then $\sim P$ is:	$\sim$ (It is raining outside.)
or	It is not raining outside.
If Q is:	$x > 2$ or $x < 2$
then $\sim Q$ is:	$\sim (x > 2$ or $x < 2)$
	Can this be simplified? Yes, it is x =2



Negation: Truth Table

Truth table for negation:

Let P be a statement.

P	$\sim P$
T	F
F	T

Negation: Notes

1. In some books 1 is used for T and 0 is used for F.

2. The truth table for $\sim$ tells us that for any statement P, exactly one of P or $\sim P$ is true.

   So if we want to prove P is true, we have two methods:

   Direct: Start with some facts and end up proving P in a direct step-by-step manner.

   Indirect: Don't prove P is true directly, but prove that $\sim P$ is false.

   This is how logic is used in 'doing' Mathematics.

Negation: Notes

3. Generally, brackets are left out around '$\sim P$'. Thus

$\sim P \vee Q$ means $(\sim P) \vee Q$

and not $\sim (P \vee Q)$.

This is similar to arithmetic where $-x + y$ means $(-x) + y$ and not $-(x + y)$.

Disjunction: $P \vee Q$

Disjunction is when the two statements are connected with the word 'or', that is, one or the other is considered.

Disjunction: Examples

P: $2 + 3 = 5$

Q: $2 + 3 = 6$

$P \vee Q$: $2 + 3 = 5$ or $2 + 3 = 6$

or $(2 + 3 = 5) \vee (2 + 3 = 6)$

Examples:

1. Write the following statement using the connective $\vee$.

   I am catching the bus or train home.

   I am catching the bus home $\vee$ I am catching the train home.

   Note that connectives are allowed only between complete statements, and not between sentence fragments.

Examples:

2. For the statements P and Q, write down $P \vee Q$.

(i) P: $x \geq 0$

Q: $x \leq 1$

$P \vee Q$: $x \geq 0$ or $x \leq 1$

$P \vee Q$: $x \geq 0 \vee x \leq 1$

(ii) P: x is the square of an integer.

Q: x is prime.

$P \vee Q$: x is the square of an integer or prime.

$P \vee Q$: x is the square of an integer $\vee$ x is prime.

Disjunction: Truth Table

Truth table for Disjunction:

Let P and Q be statements.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Disjunction: Notes

1. It is important that you notice the order of the rows in a truth table. We will **always** start our truth tables with the maximum number of T's in the top left of the table.

Examples:

Write down the truth value of the following statements.

(i) $2 > 1 \vee (x + 1)^2 = x^2 + 2x + 1$ True

(ii) 2 is odd $\vee$ 5 is odd True

(iii) $2 < 1 \vee 22 < 11$ False

Conjunction: $P \wedge Q$

Conjunction is when the two statements are connected with the word ‘and’, that is, both statements are considered.

Conjunction: Examples

P:	$x < 2$
Q:	$x > -1$
$P \wedge Q$:	$x < 2$ and $x > -1$
or	$(x < 2) \wedge (x > -1)$
	Can this be simplified?
yes	$-1 < x < 2$?

Examples:

1. Write the following statements using connective $\wedge$.

   (i) It is hot and sticky here.

   It is hot here $\wedge$ it is sticky here.

   (ii) I like rock and roll.

   I like rock $\wedge$ I like roll.

Examples:

2. For the statements P and Q write down $P \wedge Q$.

   (i) P: $x \geq 0$

   Q: $x \leq 1$

   $P \wedge Q$: $x \geq 0$ and $x \leq 1$

   $P \wedge Q$: $x \geq 0 \wedge x \leq 1$

   (ii) P: x is the square of an integer.

   Q: x is prime.

   $P \wedge Q$: x is the square of an integer and prime.

   $P \wedge Q$: x is the square of an integer $\wedge$ x is prime.

Conjunction: Truth Table

Truth table for Conjunction:

Let P and Q be statements.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Examples:

Write down the truth value of the following statements.

(i) $3 < 5 \wedge 6 > \pi$ True

(ii) $3 > 5 \wedge 6 > \pi$ False

(iii) $1 = 2 \wedge 4 = 7$ False

Truth Tables for Compound Statements

The truth table for a given compound statement displays the truth values that correspond to all possible combinations of truth values for its constituent parts.

The method for computing the truth values for a compound statement is similar to the evaluation of algebraic expressions:

- First, evaluate those in the innermost parentheses
- Next, evaluate those in the next innermost parentheses, and so forth, until you have the truth values for the complete compound statement.

Next, we shall discuss the order to evaluate logical connectives all within only a single parentheses (without further parentheses).

Order for Evaluating Logical Connectives

Order	Logical Connective
1	$\sim$
2	$\wedge$, $\vee$
3	$\Rightarrow$, $\Leftrightarrow$

That is, first, evaluate $\sim$, next, evaluate $\wedge$ and $\vee$ (if both are present, parentheses is needed) , then evaluate $\Rightarrow$ and $\Leftrightarrow$ (if both are present, parentheses is needed).

Truth Tables For Compound Statements: Example

(i) Construct the truth table for the compound statement $P \vee \sim P$.

P	$\sim P$	$P \vee \sim P$
T	F	T
F	T	T

Truth Tables For Compound Statements: Example

(ii) Construct the truth table for the compound statement $\sim P \vee Q$.

P	Q	$\sim P$	$\sim P \vee Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Truth Tables For Compound Statements: Example

(iii) Construct the truth table for the compound statement $(P \vee Q) \wedge \sim (P \wedge Q)$.

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

We can 'see' from the table that $(P \vee Q) \wedge \sim (P \wedge Q)$ is true if P is true or Q is true but not both.

Conditional: $P \Rightarrow Q$

The conditional of two statements is an "if … then…" statement, or an "implication".

In this case,

P is called the ***antecedent*** or ***hypothesis*** or ***condition***, while Q is the ***consequent*** or ***conclusion***.

Conditional: $P \Rightarrow Q$

The statement "$P \Rightarrow Q$" can be read in any of the following ways.

* P implies Q	* P only if Q
* If P then Q	* P is a sufficient condition for Q
* Q if P	* Q is a necessary condition for P
* Q provided P	* Q whenever P

Examples

1.

P:	I work hard.
Q:	I do well.
$P \Rightarrow Q$:	If I work hard then I do well.
or	I work hard $\Rightarrow$ I do well.
P:	x is 2.
Q:	x^2 is 4.
$P \Rightarrow Q$:	x being 2 implies that x^2 is 4.
or	$x = 2 \Rightarrow x^2 = 4$

Would the meaning change if the arrow were backwards?

Examples:

2. Write the following statement using connective.

If x^2 is 4, then x is plus or minus 2.

$x^2 = 4 \Rightarrow x = \pm 2$

Conditional: Truth Table

Truth table for Conditional:

Let P and Q be statements.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note that $P \Rightarrow Q$ is false only when P = T and Q = F.

Example:

Complete the truth table for the statement $P \Rightarrow (Q \Rightarrow P)$.

P	Q	$Q \Rightarrow P$	$P \Rightarrow (Q \Rightarrow P)$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	T	T

What do you notice about the truth value of this statement?
For all cases of P and Q, the truth value of $P \Rightarrow (Q \Rightarrow P)$ is True.

Biconditional: $P \Leftrightarrow Q$

A biconditional statement is a statement of the form "P if and only if Q", and is true only when each of the operands have the same truth value. The statement "$P \Leftrightarrow Q$" can be read in any of the following ways.

* P if and only if Q
* P is equivalent to Q
* P implies and is implied by Q
* P is a necessary and sufficient condition for Q

In many books, the statement 'P if and only if Q' is written "P iff Q" or "$P \equiv Q$".

Examples

1. P: $x^3 = -8$.
   Q: $x = -2$.
   $P \Leftrightarrow Q$: $x^3 = -8$ if and only if $x = -2$.
   or $x^3 = -8 \Leftrightarrow x = -2$.

Biconditional: Note

$$x^3 = -8 \Leftrightarrow x = -2$$

means

both $x^3 = -8 \Rightarrow x = -2$ and $x = -2 \Rightarrow x^3 = -8$.

That is, $P \Leftrightarrow Q$

means

both $P \Rightarrow Q$ and $Q \Rightarrow P$

Examples:

2. For the statements P and Q, write down $P \Leftrightarrow Q$.

(i) P: $x^2 - 1 = 0$

Q: $x = 1$ or $x = -1$

$P \Leftrightarrow Q$: $(x^2 - 1 = 0) \Leftrightarrow (x = 1 \text{ or } x = -1)$

(ii) P: $\sqrt{x} > 1$

Q: $x > 1$

$P \Leftrightarrow Q$: $\sqrt{x} > 1 \Leftrightarrow x > 1$

Biconditional: Truth Table

Truth table for Biconditional:

Let P and Q be statements.

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Examples:

Write down the truth value of the following statements.

(i) $x^2 = 1 \Leftrightarrow (x = 1 \vee x = -1)$ True

(ii) I get wet $\Leftrightarrow$ it is raining False

Evaluating Compound Statements

From the order that logical connectives are evaluated, it is clear that "$P \Leftrightarrow Q \wedge \sim R$" means "$P \Leftrightarrow (Q \wedge \sim R)$" but not "$(P \Leftrightarrow Q) \wedge \sim R$".

When constructing compound statements, we should use parentheses to specify the order of evaluation if it is not implied directly from the order that logical connectives are evaluated. For example, $P \vee Q \wedge R$.

Examples:

Examine the order in which the following are evaluated:

(i) $(P \vee \sim Q) \Rightarrow (P \wedge R)$

(ii) $P \Rightarrow (Q \Rightarrow (R \vee \sim R))$

(iii) $\sim ((P \wedge Q) \vee (\sim P \wedge Q))$

Tautology

Any compound statement that is always true regardless of the truth values of the of the individual statements substituted for its statement variables is called a ***tautology*** or ***tautological statement***.

Examples

(i) We saw earlier that the truth value for $P \vee \sim P$ is always T. Therefore, $P \vee \sim P$ is a tautology.

(ii) From the truth table for $P \Rightarrow (Q \Rightarrow P)$ drawn earlier, we see that this statement is also a tautology.

Contradiction

Any compound statement that is always false regardless of the truth values of the of the individual statements substituted for its statement variables is called a ***contradiction*** or ***contradictory statement***.

Example

Consider the truth table for the statement $P \wedge \sim P$.

P	$\sim P$	$P \wedge \sim P$
T	F	F
F	T	F

As the truth value for $P \wedge \sim P$ is always F, the statement is a contradiction.

Contingent

Any statement that is not a tautology and not a contradiction is ***contingent*** or ***intermediate***.

Contingent: Example

If P is a statement variable, then it is contingent.

Note that a statement variable is a statement that can be True or False.

Example: Determining tautology, contradiction or contingent statement

Determine from its truth table whether the following statement is a tautology, contradiction or contingent statement.

$$\sim((\sim P \wedge Q) \wedge P)$$

P	Q	$\sim P$	$\sim P \wedge Q$	$(\sim P \wedge Q) \wedge P$	$\sim((\sim P \wedge Q) \wedge P)$
T	T	F	F	F	T
T	F	F	F	F	T
F	T	T	T	F	T
F	F	T	F	F	T

Therefore, it is a tautology.

Logical Equivalence

Two (compound) statements P and Q are said to be ***logically equivalent***, written $P \equiv Q$, if and only if they have identical truth values for each possible substitution of statements for their variables.

That is, they have the same truth table.

Note that:

- A compound statement E is a tautology if and only if E ≡ T (true). For example, $P \vee \sim P \equiv$ T.
- A compound statement E is a contradiction if and only if E ≡ F (false). For example, $P \wedge \sim P \equiv$ F.

Logical Equivalence: Notes

1. To say P is logically equivalent to Q is the same as saying "$P \Leftrightarrow Q$ is a tautology".
2. Two statements are logically equivalent if they have identical truth tables.
3. Logically equivalent statements can be substituted in statement forms (compound statements) without changing their truth values.

Substitution

1. Based on logical equivalences, we can substitute a statement with an equivalence statement in any compound statements in the same way as in algebra with "≡" treated as "=".
2. Hence, substitution can be used for the following purposes:
   - Proving tautology or contradiction as an alternative method to the truth table method.
   - Simplifying compound statements

Next few slides show the logical equivalences that are commonly used in substitution. All these equivalences can be proved using the truth table method.

And, after that we shall show some examples on using substitution method.

Some Logical Equivalences

1. Commutative Laws:

$$(P \vee Q) \equiv (Q \vee P)$$
$$(P \wedge Q) \equiv (Q \wedge P)$$
$$(P \Leftrightarrow Q) \equiv (Q \Leftrightarrow P)$$

2. Associative Laws:

$$((P \vee Q) \vee R) \equiv (P \vee (Q \vee R))$$
$$((P \wedge Q) \wedge R) \equiv (P \wedge (Q \wedge R))$$
$$((P \Leftrightarrow Q) \Leftrightarrow R) \equiv (P \Leftrightarrow (Q \Leftrightarrow R))$$

Some Logical Equivalences

3. Distributive Laws:
   $(P \vee (Q \wedge R)) \equiv ((P \vee Q) \wedge (P \vee R))$
   $(P \wedge (Q \vee R)) \equiv ((P \wedge Q) \vee (P \wedge R))$
   $(P \Rightarrow (Q \vee R)) \equiv ((P \Rightarrow Q) \vee (P \Rightarrow R))$
   $(P \Rightarrow (Q \wedge R)) \equiv ((P \Rightarrow Q) \wedge (P \Rightarrow R))$
4. Double Negation Laws:
   $\sim\sim P \equiv P$

Some Logical Equivalences

5. DeMorgan's Laws:
   $\sim (P \vee Q) \equiv (\sim P \wedge \sim Q)$
   $\sim (P \wedge Q) \equiv (\sim P \vee \sim Q)$
6. Other Implication Laws:
   $(P \Leftrightarrow Q) \equiv ((P \Rightarrow Q) \wedge (Q \Rightarrow P)$
   $(P \Rightarrow Q) \equiv (\sim P \vee Q)$
   $(P \Rightarrow Q) \equiv (\sim Q \Rightarrow \sim P)$
   $\sim (P \Rightarrow Q) \equiv (P \wedge \sim Q)$

Other Logical Equivalences

7. Identity Laws:
   $P \vee \mathrm{F} \equiv P$
   $P \wedge \mathrm{T} \equiv P$
8. Idempotent Laws:
   $P \wedge P \equiv P$
   $P \vee P \equiv P$
9. Domination Laws:
   $P \vee \mathrm{T} \equiv \mathrm{T}$
   $P \wedge \mathrm{F} \equiv \mathrm{F}$

Other Logical Equivalences

10. Absorption Laws:
    $P \vee (P \wedge Q) \equiv P$
    $P \wedge (P \vee Q) \equiv P$
11. Inverse Laws:
    $P \vee \sim P \equiv \mathrm{T}$
    $P \wedge \sim P \equiv \mathrm{F}$

Using Substitution: Example - Proving Tautology

Use substitution to prove that $S \Rightarrow (\sim R \vee S)$ is a tautology

Proof:

$S \Rightarrow (\sim R \vee S)$

$\equiv \sim S \vee (\sim R \vee S)$	Implication Law
$\equiv (\sim R \vee S) \vee \sim S$	Commutative Law
$\equiv \sim R \vee (S \vee \sim S)$	Associative Law
$\equiv \sim R \vee T$	Inverse Law
$\equiv T$	Domination Law

Using Substitution: Example - Simplification

Simplify the following statement:

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

$\sim(\sim p \wedge q) \wedge (p \vee q)$	$\equiv (\sim(\sim p) \vee \sim q) \wedge (p \vee q)$	DeMorgan's Law
	$\equiv (p \vee \sim q) \wedge (p \vee q)$	Double negation Law
	$\equiv p \vee (\sim q \wedge q)$	Distributive law
	$\equiv p \vee (q \wedge \sim q)$	Commutative Law
	$\equiv p \vee \mathbf{F}$	Inverse Law
	$\equiv p$	Identity Law

End of Unit 1