MACM 101

Discrete Mathematics I

A Course Overview

Jeffrey Leung

Table of Contents

Related Topics and Introduction

- Continuous mathematics
    - Fifth Euclid's Postulate

- Discrete mathematics (not requiring continuity)
    - Asymptotics (approximation using a continuous function)

- Logic:
    - Formal logic & syllogisms
    - Mathematical logic & formal reasoning
    - Computational logic & formal verification

- Set theory:
    - Naïve (informally in native languages)
    - Axiomatic (formally with formal logic)

- Graphs:
    - Toy graph theory
    - Seven Bridges of Königsberg

- Number theory:
    - Began in Middle Ages
    - Arithmetic
    - Algebraic geometry

Propositional Logic

- Logic:
  - Math and rhetoric:
    - Precise meaning to statements
    - Distinguish between valid/invalid arguments
    - Rules of correct reasoning
  - **Mathematical logic**: Computing everything with just symbols
  - Computing:
    - Compose new data from existing facts
    - Design computer circuits (modeled on a formula)
    - Construction of computer programs
    - Verification of correctness of programs and circuit design
    - Specification of the ideal – must be fully understood
- Statements/propositions:
  - **Propositional logic**: Deals with statements and their truth values (true/false)
  - **Statement**: Declarative sentence which can be true/false
    - Exclamation mark ≠ statement
    - Uncertainty ≠ statement
  - Primitive/compound statements:
    - **Primitive statements**: Simple statements without a set true/false value
      - Denoted by propositional variables (p, q, r, etc.)
    - **Compound statements/formulae**: Primitive statements combined by logic connectives
      - Discover how the truth value of the compound statement depends on the truth values of the primitive statements
      - Denoted by Greek capitals (Φ, Ψ, etc.)
- **Logical connectives**: Symbol used to grammatically connect two statements

Connective:	**Said as:**	**Symbol:**
Negation	Not	$\neg$
Conjunction	And	$\wedge$
Disjunction	Or	$\vee$
Implication	If/then	$\rightarrow$
Exclusive or	Either/or	$\oplus$ OR $\veebar$
Biconditional / equivalence	If and only if	$\leftrightarrow$

- **Truth tables**: Way to determine/specify the exact dependence of the truth value of a compound statement through the values of primitive statements involved

Truth value of primitive statement	Truth value of primitive statement	Truth value of compound statement
…	…	…

- *Negation:*

p	¬p
F (0)	T (1)
T (1)	F (0)

- *Conjunction:*

p	q	p ∧ q
0	0	0
0	1	0
1	0	0
1	1	1

(2^x rows, where x = # of primitive statements)

- *Disjunction:*

p	q	p ∨ q
0	0	0
0	1	1
1	0	1
1	1	1

- *Exclusive:*

p	q	p ⊕ q
0	0	0
0	1	1
1	0	1
1	1	0

- *Implication:*

p	**q**	**p → q**
0	0	1
0	1	1
1	0	0
1	1	1

- Does not assume a casual connection
- Can be thought of as a promise: "If I am elected, then I will lower taxes."
    - Not elected (0) & taxes not lowered (0): Promise kept (1)
    - Not elected (0) & taxes lowered (1): Promise kept (1)
    - Elected (1) & taxes not lowered (0): Promise not kept (0)
    - Elected (1) & taxes lowered (1): Promise kept (1)
- Converse/contrapositive/inverse:
    - $p \rightarrow q$

      "The home team wins whenever it is raining."

      "If it is raining then the home team wins."
    - **Converse**: $q \rightarrow p$

      "If the home team wins, then it is raining."
    - **Contrapositive**: $\neg q \rightarrow \neg p$

      "If the home team does not win, then it is not raining."
    - **Inverse**: $\neg p \rightarrow \neg q$

      "If it is not raining, then the home team does not win."
- "Only if" means "if – then" (not "then – if")
    - E.g. "I will go swimming only if it is sunny" – If I go swimming, then it is sunny. The weather being sunny does not necessarily mean I will go swimming.

- *Biconditional/equivalence:*

p	**q**	**p ↔ q**
0	0	1
0	1	0
1	0	0
1	1	1

- ***Tautology***: Compound statement which is true for all combinations of truth values of its propositional variables

$(p \rightarrow q) \vee (q \rightarrow p)$

p	q	(p → q) ∨ (q → p)
0	0	1
0	1	1
1	0	1
1	1	1

- ***Contradiction**:* Compound statement which is false for all combinations of truth values of its propositional variables

(p ⊕ q) ∧ (p ⊕ ¬ q)

p	q	(p ⊕ q) ∧ (p ⊕ ¬ q)
0	0	0
0	1	0
1	0	0
1	1	0

- Contingency: Compound statement which is neither a tautology or a contradiction

- *Example: Construct the truth table of the following compound statement:* p → (q ∨ ¬p)

p	q	p → (q ∨ ¬p)
0	0	1
0	1	1
1	0	0

1	**1**	**1**

- *Example: Write the following as propositional formulas and construct the truth tables of the resulting compound statements.*
  - *"An inhabitant of a castle in Transylvania is either sane or insane, and is a human or vampire."*

    p – Sane q – Human

$(p \oplus \neg p) \wedge (q \oplus \neg q)$

p	**q**	$\mathbf{(p \oplus \neg p) \wedge (q \oplus \neg q)}$
0	0	1
0	1	1
1	0	1
1	1	1

(Tautology)

  - *"If a person is an insane vampire then he believes only in false things and always lies."*

    r – False beliefs

    s – Always lies

p	**q**	**r**	**s**	$\mathbf{(\neg p \wedge \neg q) \rightarrow (r \wedge s)}$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

- **Logic equivalences**:
    - Compound statements Φ and Ψ are said to be logically equivalent if the statement Φ is true/false if and only if Ψ is true/false
        - I.e. Truth tables of Φ and Ψ are equal
    - Shown by $\Leftrightarrow$
    - Must have the same propositional variables
    - Purpose:
        - To simplify compound statements
        - To convert complicated compound statements to 'conjunctive normal form' to be easier to handle
            - **Conjunctive normal form**: Compound statement which only contains connectives of AND, OR, and/or NOT
    - Example equivalences:
        - Implication and its contrapositive:

p	**q**	$\mathbf{p \rightarrow q}$	$\mathbf{\neg q \rightarrow \neg p}$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

        - All tautologies and contradictions
    - Equivalences and tautologies:
        - Example theorem: Compound statements Φ and Ψ are logically equivalent if and only if $\Phi \leftrightarrow \Psi$ is a tautology.

p	**q**	**…**	Φ	Ψ	$\Phi \leftrightarrow \Psi$
0	1	…	1	1	1
…	…	…	…	…	1
1	0	…	0	0	1
…	…	…	…	…	1

Proof: Suppose that $\Phi \Leftrightarrow \Psi$. Then these have equal value:

Suppose now that $\Phi \leftrightarrow \Psi$ is a tautology. If Φ is true, then Ψ must also be true. If Φ is false, then to make the formula $\Phi \leftrightarrow \Psi$ true, Ψ must also be false. Q.E.D.

- **Laws of logic**
  - Double negation law:
    - $\neg\neg p \Leftrightarrow p$

p	¬q	¬¬p
0	1	0
1	0	1

  - De Morgan's Laws:
    - $\neg (p \wedge q) \Leftrightarrow \neg p \vee \neg q$

p	**q**	$\neg (p \wedge q)$	$\neg p \vee \neg q$	$\neg (p \vee q)$	$\neg p \wedge \neg q$
0	0	1	1	1	1
0	1	1	1	0	0
1	0	1	1	0	0
1	1	0	0	0	0

- $\neg (p \vee q) \Leftrightarrow \neg p \wedge \neg q$

- *Example: Construct the negations of:*
  - *"Miguel has a cell phone and he has a laptop."*

p – 'He has a cell phone'   q – 'He has a laptop'

$p \wedge q$

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

"Miguel does not have a cell phone or he does not have a laptop."

- *"Heather will go to the concert or Steve will go to the concert."*

p – 'Heather will go to the concert' q – 'Steve will go to the concert'

$p \vee q$

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

"Heather will not go to the concert and Steve will not go to the concert."

- Algebraic Laws:
  - Commutative laws:
    - $p \wedge q \Leftrightarrow q \wedge p$
    - $p \vee q \Leftrightarrow q \vee p$
  - Associative laws:
    - $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
    - $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$
  - Distributive laws:
    - $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
    - $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
  - Idempotent laws:
    - $p \wedge p \Leftrightarrow p$
    - $p \vee p \Leftrightarrow p$
- Logic Laws:
  - Identity laws:
    - $p \wedge T \Leftrightarrow p$
    - $p \vee F \Leftrightarrow p$

- Inverse laws:
  - $p \wedge \neg p \Leftrightarrow F$ *(Law of Contradiction)*
  - $p \vee \neg p \Leftrightarrow T$ *(Law of Excluded middle)*
- Domination laws:
  - $p \wedge F \Leftrightarrow F$
  - $p \vee T \Leftrightarrow T$
- Absorption laws:
  - $p \wedge (p \vee q) \Leftrightarrow p$
  - $p \vee (p \wedge q) \Leftrightarrow p$

- *Example: Simplify the following statement:*

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

$\mathbf{(\neg q \wedge \neg r)} \vee \neg (\neg q \vee p) \vee r \vee p$ DeMorgan's Law

$(\neg q \wedge \neg r) \vee \mathbf{(\neg\neg q \wedge \neg p)} \vee r \vee p$ DeMorgan's Law

$(\neg q \wedge \neg r) \vee (\mathbf{q} \wedge \neg p) \vee r \vee p$ Double negation

$\mathbf{r \vee} (\neg q \wedge \neg r) \vee \mathbf{p \vee} (q \wedge \neg p)$ Commutative law

$\mathbf{[}\ r \vee (\neg q \wedge \neg r)\ \mathbf{]} \vee \mathbf{[}\ p \vee (q \wedge \neg p)\ \mathbf{]}$ Associative law

$[\ \mathbf{(r \vee \neg q) \wedge (r \vee \neg r)}\ ] \vee [\ \mathbf{(p \vee q) \wedge (p \vee \neg p)}\ ]$ Distributive law

$[\ (r \vee \neg q) \wedge \mathbf{T}\ ] \vee [\ (p \vee q) \wedge \mathbf{T}\ ]$ Excluded middle law

$[\ (r \vee \neg q)\ ] \vee [\ (p \vee q)\ ]$ Identity law

$r \vee \neg q \vee p \vee q$ Associative law

$r \vee p \vee \mathbf{q \vee \neg q}$	Commutative law
$r \vee p \vee \mathbf{T}$	Excluded middle law
T (Tautology)	Domination law

- Expressing connectives:
  - Some connectives can be expressed through others:
    - $p \oplus q \Leftrightarrow \neg(p \leftrightarrow q)$
    - $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$
    - $p \rightarrow q \Leftrightarrow \neg p \vee q$
  - Example theorem: Every compound statement is logically equivalent to a statement that uses only conjunction, disjunction, and negation.
  - *Example: "If you are a computer science major or a freshman, and you are not a computer science major or you are granted access to the internet, then you are a freshman or have access to the internet."*

    p – 'You can access the internet from campus'
    q – 'You are a computer science major'
    r – 'You are a freshman'

    $[\,(q \vee r) \wedge (\neg q \vee p)\,] \rightarrow (r \vee p)$

$\Leftrightarrow$ $\neg [(q \vee r) \wedge (\neg q \vee p)] \vee r \vee p$ Expressing implication

$\Leftrightarrow$ $\neg (q \vee r) \vee \neg (\neg q \vee p) \vee r \vee p$ DeMorgan's law

Identical to the example above

$\Leftrightarrow$ T (Tautology)

- *Example: Simplify the statement:* $(p \vee q) \leftrightarrow (p \rightarrow q)$

$\Leftrightarrow$ $[(p \vee q) \rightarrow (p \rightarrow q)] \wedge [(p \rightarrow q) \rightarrow (p \vee q)]$ Expressing biconditional

$\Leftrightarrow$ $[\neg(p \vee q) \vee (p \rightarrow q)] \wedge [\neg(p \rightarrow q) \vee (p \vee q)]$ Expressing implication

$\Leftrightarrow$ $[\neg(p \vee q) \vee (\neg p \vee q)] \wedge [\neg(\neg p \vee q) \vee (p \vee q)]$ Expressing implication

$\Leftrightarrow$ $[(\neg p \wedge \neg q) \vee \neg p \vee q] \wedge [(\neg\neg p \wedge q) \vee p \vee q]$ DeMorgan's law

$\Leftrightarrow$ $[(\neg p \wedge \neg q) \vee \neg p \vee q] \wedge [(p \wedge q) \vee p \vee q]$ Double negative law

$\Leftrightarrow$ $(\neg p \vee q) \wedge (p \vee q)$ Absorption law

$\Leftrightarrow$ $(\neg p \wedge p) \wedge q$ Distributive law

$\Leftrightarrow$ $F \wedge q$ Contradiction law

$\Leftrightarrow$ q Identity law

- **First Law of Substitution**: Suppose that the compound statement Φ is a tautology. If p is a primitive statement that appears in Φ and we replace each occurrence of p by the same statement q, then the resulting compound statement Ψ is also a tautology.

Let $\Phi = (p \rightarrow q) \vee (q \rightarrow p)$ and we substitute p by $p \vee (s \oplus r)$.

Therefore, $((p \vee (s \oplus r)) \rightarrow q) \vee (q \rightarrow (p \vee (s \oplus r))$ is a tautology.

- **Second Law of Substitution**: Let Φ be a compound statement, p an arbitrary statement (not necessarily primitive) which appears in Φ, and let q be a statement such that $p \Leftrightarrow q$. If we replace one or more occurrences of p by q, then for the resulting compound statement Ψ we have $\Phi \Leftrightarrow \Psi$.

Let $\Phi = (p \rightarrow q) \vee (q \rightarrow p)$ and we substitute the first occurrence of p by $p \vee (p \wedge q)$ by the absorption law. Recall that $p \Leftrightarrow p \vee (p \wedge q)$ by the absorption law.

Therefore, $(p \rightarrow q) \vee (q \rightarrow p) \Leftrightarrow (p \vee (p \wedge q) \rightarrow q) \vee (q \rightarrow p)$.

- Logic inference:
  - One of the main goals of logic is to distinguish valid and invalid arguments
  - *Example: Write these arguments in symbolic form:*

    1. "If you have a current password, then you can log onto the network. You have a current password. Therefore, you can log onto the network."
    2. "If you have a current password, then you can log onto the network. You can log onto the network. Therefore, you have a current password."

    p – 'You have a current password   q – 'You can log onto the network'

    1. Valid

    $$\begin{array}{l} p \rightarrow q \\ \underline{p \qquad\quad} \\ \therefore q \end{array}$$

    2. Invalid

    $$\begin{array}{l} p \rightarrow q \\ \underline{q \qquad\quad} \\ \therefore p \end{array}$$

  - Inferences & tautologies:
    - *Example: Check that $\Phi = ((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology.*

      If $(p \rightarrow q) \wedge p$ is false (that is, if one of $p \rightarrow q$ and q is false), then Φ is true.

If $(p \rightarrow q) \wedge p$ is true, then both $p \rightarrow q$ and q are true. Since the implication $p \rightarrow q$ is true and p is true, q must also be true. Therefore, Φ is true.

Therefore, whatever values of p and q are, if $(p \rightarrow q) \wedge p$ is true, q is also true.

This is a **valid** argument.

p	**q**	**$((p \rightarrow q) \wedge p)$**	**Ψ**
0	0	0	1
0	1	1	**0**
1	0	0	1
1	1	1	1

- Let us try $\Psi = ((p \rightarrow q) \wedge p) \rightarrow p$

In the case $p = 0$ and $q = 1$, both conditions $((p \rightarrow q) \land p)$ are true, but p is false.

Therefore this is **not** a valid argument.

- General definition of inference:
  - General form of an argument in symbolic form is

$$\text{Premise} \land \text{Premise} \land \ldots \land \text{Premise} \rightarrow \text{Conclusion}$$

  - Argument is valid if, whenever all of the premises are true, the conclusion is true
  - Argument is valid if and only if the following compound statement is a tautology:

$$(p_1 \land p_2 \land p_3 \land \ldots \land p_n) \rightarrow q$$

- Rules of inference:
  - Verifying if a complicated statement is a tautology is nearly impossible
  - General arguments can be replaced with simpler ones
  - **Modus ponens**:

    "If you have a current password, then you can log onto the network."

    "You have a current password. Therefore, you can log onto the network."

$$\begin{array}{l} p \rightarrow q \\ \underline{p \qquad\quad} \\ \\ \therefore q \end{array}$$

- **Rules of Syllogism**:

$$\begin{array}{l} p \rightarrow q \\ \underline{q \rightarrow r} \\ \therefore p \rightarrow r \end{array}$$

The corresponding tautology: $((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$

"If you send me an email, then I'll finish writing the program. If I finish writing the program, I'll go to sleep early."
p – 'You will send me an email'
q – 'I will finish writing the program'
r – 'I will go to sleep early'
"Therefore, if you send me an email, I'll go to sleep early."

- **Modus Tollens**:

$$\begin{array}{l} p \rightarrow q \\ \underline{\neg q} \\ \therefore \neg p \end{array}$$

The corresponding tautology: $((p \rightarrow q) \land \neg q) \rightarrow \neg p$

"If today is Friday, then tomorrow I'll go skiing. I will not go skiing tomorrow."
p – 'Today is Friday' q – 'I will go skiing tomorrow'
"Therefore, today is not Friday.
(Contrapositive)

- **Rule of Disjunctive Syllogism**:

$$\begin{array}{l} p \lor q \\ \underline{\neg p} \end{array}$$

$\therefore q$

The corresponding tautology: $((p \lor q) \land \neg p) \rightarrow q$

“I’ll go skiing this weekend. I will not go skiing on Saturday.”
p – ‘I will go skiing on Saturday’ q – ‘I will go skiing on Sunday’
“Therefore, I will go skiing on Sunday.”

- **Rule of Proof by Cases**:

$$\begin{array}{l} p \rightarrow r \\ \underline{q \rightarrow r \qquad\qquad} \\ \therefore (p \lor q) \rightarrow r \end{array}$$

The corresponding tautology: $((p \rightarrow q) \land (q \rightarrow r)) \rightarrow ((p \lor q) \rightarrow r)$

“If today is Saturday, then I’ll go skiing.”
“If today is Sunday, then I’ll go skiing.”
p – ‘Today is Saturday’ q – ‘Today is Sunday’ r – ‘I’ll go skiing’
“Therefore, if today is Saturday or Sunday, then I will go skiing.”

- Rules of Contradiction, Simplification, and Amplification
  - **Rule of Contradiction** (Reductio ad Absurdum):

$$\begin{array}{l} \underline{\neg p \rightarrow F \qquad} \\ \therefore p \end{array}$$

Corresponding tautology: $(\neg p \rightarrow F) \rightarrow p$

  - **Rule of Simplification**:

$p \wedge q$

$\therefore p$

Corresponding tautology: $(p \wedge q) \to p$

- **Rule of Amplification**:

$\underline{p}$

$\therefore p \vee q$

Corresponding tautology: $p \to (p \vee q)$

- Logic inference:
  - Goal of an argument is to infer the required conclusion from the given premises
  - Formally: An argument is a sequence of statements, each of which is either a premise or obtained from preceding statements by means of a rule of inference
  - *Example:*

    Premises: “It is not sunny this afternoon and it is colder than yesterday. We will go swimming only if it is sunny. If we do not go swimming, then we will take a canoe trip. If we take a canoe trip, we will be home by sunset.”
    Conclusion: “We will be home by sunset.”

    Notation:

    p – ‘It is sunny this afternoon’
    r – ‘We will go swimming’
    q – ‘It is colder than yesterday
    t – ‘We will be here by sunset’
    s – ‘We will take a canoe trip’

Premises: $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$

Conclusion: t

	Step	Reason
1.	$\neg p \wedge q$	Premise
2.	$\neg p$	Rule of Simplification
3.	$r \rightarrow p$	Premise
4.	$\neg r$	Modus tollens
5.	$\neg r \rightarrow s$	Premise
6.	s	Modus ponens
7.	$s \rightarrow t$	Premise
8.	t	Modus ponens

- *Logic puzzle: A prisoner must choose between two rooms, each of which contains either a lady or a tiger. If he chooses a room with a lady, he marries her; if he chooses a room with a tiger, he gets eaten by the tiger. The rooms have signs on them:*

I	II
At least one of these rooms contains a lady	A tiger is in the other room

It is known that either both signs are true or both are false.
Determine what each room contains.

Notation:

p – 'First room contains a lady'   q – 'Second room contains a lady'

Premises: Sign 1: $p \vee q$ Sign 2: $\neg p$

$(p \vee q) \leftrightarrow \neg p$

$(p \vee q) \rightarrow \neg p$, $\neg p \rightarrow (p \vee q)$

	Step	Reason
1.	$\neg p \rightarrow (p \vee q)$	Premise
2.	$p \vee p \vee q$	Expressing implication
3.	$p \vee q$	Idempotent law
4.	$(p \vee q) \rightarrow \neg p$	Premise
5.	$\neg p$	Modus ponens
6.	q	Rule of disjunctive syllogism to 3 and 5

Room I contains a tiger; room II contains a lady.

- Conjunctive Normal Form (CNF) (will not be tested):
    - Literal: Primitive statement (propositional variable) or its negation
        - E.g. p, $\neg p$, q, $\neg q$
    - Clause: Disjunction of one or more literals

    - E.g. $p \vee q$, $\neg s \vee s \vee \neg r \vee \neg q$

  - Statements are said to be in CNF if it is a *conjunction* of clauses

    - E.g. $p \wedge (p \vee \neg q) \wedge (\neg r \vee \neg p)$, $\neg r$

  - CNF Theorem: Every statement is logically equivalent to a certain CNF
    - Proof (Sketch): Let Φ be a (compound) statement.

      Step 1: Express all logic connectives in Φ through negation, conjunction, and disjunction. Let Ψ be the obtained statement.

      Step 2: Using DeMorgan's laws, move all the negations in Ψ to individual primitive statements. Let Θ denote the updated statement.

      Step 3: Using distributive laws, transform Θ into CNF.

    - *Example: Find a CNF logically equivalent to $(p \rightarrow q) \rightarrow r$.*

      Step 1: $\neg (\neg p \vee q) \vee r$

      Step 2: $(p \wedge \neg q) \vee r$

      Step 3: $(p \vee r) \wedge (\neg q \vee r)$

- Rule of Resolution:

$p \vee q$

$\neg p \lor r$

$\therefore q \lor r$

$q \lor r$ is called *resolvent*

Resolvent: The result from applying the rule of resolution

The corresponding tautology: $((p \lor q) \land (\neg p \lor r)) \rightarrow (q \lor r)$

"Jasmine is skiing or it is not snowing. It is snowing or Bart is playing hockey."
p – 'It is snowing' q – 'Jasmine is skiing' r – 'Bart is playing hockey'
"Therefore, Jasmine is skiing or Bart is playing hockey."

- Computerized Logic Inference:
  - Convert the premises into CNF
  - Convert the negation of the conclusion into CNF
  - Consider the collection consisting of all the clauses that occur in the obtained CNFs
  - Use the rule of resolution to obtain the empty clause (Ø).

    If it is possible, then the argument is valid; otherwise, it is not.

    Why an empty clause? The only way to produce the empty clause is to apply the resolution rule to a pair of clauses of the form p and ¬p. Therefore, the collection of clauses is contradictory. In other words, for any choice of truth values for the primitive statements, if the premises are true, the conclusion cannot be false.

  - *Example: A prisoner must choose between two rooms, each of which contains either a lady or a tiger. The rooms have signs on them:*

I	II
At least one of these rooms contains a lady	A tiger is in the other room

It is known that either both signs are true or both are false.

Determine what each room contains.

Premises: $\neg p \to (p \lor q)$, $(p \lor q) \to \neg p$

Negation of the conclusion: $\neg q$

$\neg p \to (p \lor q)$	$(p \lor q) \to \neg p$
$\Leftrightarrow \neg\neg p \lor (p \lor q)$	$\Leftrightarrow \neg(p \lor q) \lor \neg p$
$\Leftrightarrow p \lor p \lor q$	$\Leftrightarrow (\neg p \land \neg q) \lor \neg p$
$\Leftrightarrow p \lor q$	$\Leftrightarrow \neg p$

Clauses: $\neg p$, $p \lor q$, $\neg q$

Argument:

Step	**Reason**

1.	$p \vee q$	Premise
2.	$\neg q$	Premise
3.	p	Resolvent
4.	$\neg p$	Premise
5.	Ø	Resolvent

Predicates and Quantifiers

- Propositional logic cannot do some things:
  - Some declarative statements are not statements without specifying the value of 'indeterminates'
    - Examples: "x + 2 is an even number", "If x + 1 > 0 then x > 0", "A man has a brother"
  - Some valid arguments cannot be expressed with all our machinery of tautologies, equivalences, and rules of inference

Every man is a mortal.
Socrates is a man.

∴ Socrates is mortal.

- Open statements/predicates:
  - Sentences like 'x is greater than 3' or 'person x has a brother' are neither true nor false unless the variable is assigned some particular value
  - **Open statement/Predicate**: Sentence with a specific structure (subject and predicate)
    - E.g. Sentence 'x is greater than 3' consists of 2 parts:
    - **Variable/subject**: First part of the open statement
      - In this case, 'x'
    - **Predicate**: States a property the subject can have
      - In this case, 'greater than 3'
  - We write P(x) to denote a predicate with variable x

- Unary, binary, ternary, etc:
  - **Unary predicate**: Contains only 1 variable
    - Denoted by P(x)
    - 'x is greater than 3'

      'x is my brother'

      'x is a human being'
  - **Binary predicate**: Contains 2 variables
    - Denoted by Q(x, y)
    - 'x is greater than y'

      'x is the mother of y'

      'Car x has colour y'
  - **Ternary predicate**: Contains 3 variables
    - Denoted by R(x, y, z)
    - 'x divides y + z'

      'x sits between y and z'

'x is a son of y and z'

- Assigning a value:
  - When a variable is assigned a value, the predicates turn into a statement, whose truth value can be evaluated
  - *E.g. P(x) = 'x is greater than 3'*
    - If x = 2, P(2) = '2 is greater than 3' (False)
    - If x = 4, P(4) = '4 is greater than 3' (True)
  - *E.g. Q(x, y) = 'Car x has colour y'*
    - If x = 'my car' and y = 'red', Q(my car, red) = 'My car is red' (FALSE)
    - If x = 'my car' and y = 'grey', Q(my car, grey) = 'My car is grey' (True)

- **Universe (of discourse)**: Values which can logically belong to the variable of a predicate
  - Cannot assign any value to a predicate of a variable
    - E.g. 'x is greater than 3' P('my cat')
  - *Examples:*
    - 'x is greater than 3' x is a number
    - 'x is my brother' x is a human
    - 'Car x has colour y' x is a car; y is a colour
  - Every variable of a predicate is associated with a universe and its values are taken from this universe

- **Relational database**: Collection of tables:
  - E.g.

No.	**Name**	**Student ID**	**Thesis title**
1.	John Doe	30101234	Algebraic graph theory
...	...	...	...

  - Table consists of a schema and an instance
    - **Schema**: Collection of attributes where each attribute has an associated universe of possible values
    - **Instance**: Collection of rows where each row is a mapping which associates with each attribute of the schema a value in its universe
  - Every table is a predicate that is true for the rows of the instance and false otherwise
- **Quantifiers**: A way to obtain a statement from a predicate by assigning all of its variables some values
  - Examples of quantification: 'Every man is a mortal'; 'There is an x such that x > 3'
  - **Universal quantifier**: For all x, p(x); All x are p(x)
    - Notation: $\forall x\ p(x)$
    - Can be expressed as: For all _, for any _, every _, each _, etc.
    - Asserts that a predicate is true for all values from the universe
    - Examples: 'Every man is mortal', 'For any x, $x^2 \geq 0$', 'Every car is red'
    - False if and only if there is at least one value a (from the universe) such that P(a) is false

- **Counterexample**: Demonstration that there is at least one value a from the universe such that P(a) is false, therefore declaring that ∀x p(x) is false

- **Existential quantifier**: For some x, p(x); There exists an x such that p(x)
  - Notation: ∃x p(x)
  - Can be expressed as: For some _, for at least one _, there is _, there exists _, etc.
  - Asserts that a predicate is true for at least one value from the universe
  - Examples: 'There is a living king', 'There is x such that $x^2 \geq 10$'
  - False if and only if for all a from the universe, P(a) is false
  - Disproving an existential statement is difficult

- Quantifiers and negations:
  - Summarizing universal and existential quantifiers:

	True	**False**
∀x p(x)	For every value a from the universe, P(a) is true.	There is a value a from the universe such that P(a) is false.
∃x p(x)	There is a value a from the universe such that P(a) is true.	For every value a from the universe, P(a) is false.

∀x p(x) is false if and only if ∃x ¬p(x) is true. $\neg \forall x\, p(x) \Leftrightarrow \exists x\, \neg p(x)$

∃x p(x) is false if and only if ∀x ¬p(x) is true. $\neg \exists x\, p(x) \Leftrightarrow \forall x\, \neg p(x)$

- *Examples: What is the negation of each of the following statements?*

Statement	Negation
All lions are fierce $\forall x\ p(x)$	There is a peaceful lion
Everyone has 2 legs $\forall x\ p(x)$	There is a person with more than or less than 2 legs
Some people like coffee $\exists x\ p(x)$	All people hate coffee
There is a lady in one of these rooms $\exists x\ p(x)$	There is a tiger in every room

- Multiple quantifiers:
  - Often predicates have multiple variables, so we need multiple quantifiers
  - *Example: $P(x, y)$ - 'car x has colour y'*

    $\forall x \forall y\ P(x, y)$ – 'Every car is painted all colours'

    $\exists x \exists y\ P(x, y)$ – 'There is a car that is painted some specific colour'

$\forall x \exists y\ P(x, y)$ – 'Every car is painted some specific colour'

$\exists x \forall y\ P(x, y)$ – 'There is a car that is painted all colours'

- To negate multiple quantifiers, change both of them
  - Examples:
    - $\neg \forall x \forall y\ P(x, y) = \exists x \exists y \neg P(x, y)$
    - $\neg \exists x \exists y\ P(x, y) = \forall x \forall y \neg P(x, y)$
    - $\neg \forall x \exists y\ P(x, y) = \neg \exists x \forall y\ P(x, y)$
    - $\neg \exists x \forall y\ P(x, y) = \neg \forall x \exists y\ P(x, y)$

- Open/bound variables :
  - In the statement 'car x has some colour' $\exists y\ P(x, y)$, variables x and y play completely different roles
  - Variable y is bound by the existential quantifier (essentially disappears from the statement), while variable x is not bound – it is free
  - *Example: 'x is the least number'*

    $Q(x, y)$ – 'x is less than y'

    $\forall y\ Q(x, y)$ or $\forall y\ (x \le y)$

        - ‘x is the greatest number’: $\forall x\, Q(y, x)$ or $\forall x\, (y \leq x)$

- Defining new predicates:
    - Quantifying some variables helps to create new predicates
        - E.g. “Car x has some colour” $Q(x) = \exists y\, P(x, y)$
    - *Example: Let P(x, y) mean ‘Lion x likes y’*

$Q(y) = \forall x\, P(x, y)$ ‘Every lion likes y’ Q(meat) is true; Q(apples) is false

$R(x) = \forall y\, P(x, y)$ ‘Lion x likes everything’ R(x) is false

$S(x) = \exists y\, P(x, y)$ ‘Lion x has a favourite food’

- Quantifiers can be used together with logic connectives:
    - *Example: “Every car is red or blue”*

      P(x) – ‘Car x is red’ Q(x) – ‘Car x is blue’

$\forall x\, [\, P(x) \wedge Q(x)\,]$

- *Example: "Everyone who knows a current password can log onto the network"*

  P(x) – 'x has a current password' Q(x) – 'x can log onto the network'

  $\forall x\, [\, P(x) \rightarrow Q(x)\,]$

- Logic connectives can be placed between quantified statements:
  - *Example: "Every car is blue or there is a red car"*

    P(x) – 'Car x is blue' Q(x) – 'Car x is red'

    $[\, \forall x\, P(x)\,] \vee [\, \exists x\, Q(x)\,]$

  - *Example: "For every number there is a smaller one, or there is a smallest number'*

    P(x) – 'x is smaller than y"

    $[\, \forall x \exists y\, P(x, y)\,] \vee [\, \exists x \forall y\, [\, P(x, y) \wedge (x \neq y)\,]\,]$

- Definitions:
  - Can be created with predicates and quantifiers:
  - *Examples:*
    - *"The mother of x is the female parent of x"*

      P(x, y) – 'y is a parent of x' Q(x) – 'x is a female' M(x, y) -'y is the mother of x'

      $M(x, y) \leftrightarrow P(x, y) \wedge Q(y)$

    - *"A cow is a big rectangular animal with horns and four legs in the corners"*

      A(x) – 'x is an animal' H(x) – 'x has horns'

$R(x)$ – 'x is rectangular' $L(x)$ – 'x has 4 legs in the corners

$Cow(x) \leftrightarrow A(x) \wedge H(x) \wedge R(x) \wedge L(x)$

- *Definition of a limit: "A number A is a limit of a sequence $\{a_n\}$ if for any number $\varepsilon > 0$ there is N such that for any $n > N$ we have $| a_n - A | < \varepsilon$"*

$\forall\varepsilon\ \exists N\ \forall n\ [\ (\varepsilon > 0) \wedge (n > N) \rightarrow (\ | a_n - A | < \varepsilon)\ ]$

- Rules:
  - Predicates and quantifiers are implicitly present in all rules and laws
  - Example: "Everyone having income more than $20,000 must file a tax report"

    $P(x)$ – 'x has an income greater than $20,000 must file a tax report'

    $Q(x)$ – 'x must file a tax report'

    $\forall x\ [\ P(x) \rightarrow Q(x)\ ]$

- Theorems:
  - Every theorem includes predicates and quantifiers:
  - *Examples:*
    - *"For every statement there is an equivalent CNF"*

      $C(x)$ – 'x is a CNF' $\forall x \exists y\ [\ C(y) \wedge (x \Leftrightarrow y)\ ]$

    - *"A parallelogram is a rectangle if all its angles are equal"*

      $R(x)$ = 'Parallelogram x is a rectangle' $A(x)$ = 'All angles of x are equal'

      $\forall x\ [\ A(x) \rightarrow R(x)\ ]$

- **Interpretation**: Specification of a universe and a particular meaning of the predicate

- A logic statement by itself is meaningless (e.g. $\forall x\, P(x)$) and only makes sense if we

  specify an interpretation
- E.g. Universe – animals; P(x) – 'x has horns'
- E.g. Universe – cars; P(x) – 'x is red'

- **Logical equivalence of predicates**: States that for two predicates P(x) and Q(x), for any value a from the universe, P(a) and Q(a) are equivalent

  - States that $\forall x\, [\, P(x) \leftrightarrow Q(x)\,]$ is true in the given universe

  - *Example: "A parallelogram is a rectangle if and only if all its angles are equal"*

    P(x) – 'x is a rectangle'   Q(x) – 'all angles of x are equal'

    $\forall x\, [\, P(x) \leftrightarrow Q(x)\,]$

    $P(x) \Leftrightarrow Q(x)$ (in the universe of parallelograms)

- **Logical equivalence of quantified statements**: States that two quantified statements are equivalent for any given universe
  - *Examples:*
    - *Prove that these are not logically equivalent:*

      $\exists x\, [\, P(x) \wedge Q(x)\,]$ and $[\, \exists x\, P(x)\,] \wedge [\, \exists x\, Q(x)\,]$

      Find a universe in which they are not equivalent.

      Let the universe consist of integers, let P(x) mean $x > 5$, and let Q(x) mean $x < 3$.

$[\exists x\, P(x)] \wedge [\exists x\, Q(x)]$ claims that "there is a number greater than 5, and there is a number less than 3". This is true, as 6 witnesses the first claim and 2 witnesses the second claim.

$\exists x\, [P(x) \wedge Q(x)]$ claims that "there exists a number which is both greater than 5 and less than 3", which is impossible and false. Therefore, the two statements are not logically equivalent.

- *Prove that these are logically equivalent:*

$\exists x\, [P(x) \vee Q(x)]$ and $[\exists x\, P(x)] \vee [\exists x\, Q(x)]$

We must prove that in any universe and interpretation, if the first statement is true then the second statement is true, and if the second statement is true then the first statement is true.

Since we cannot consider every possible universe, we consider an arbitrary universe, meaning that although we look at a certain universe, no assumptions or properties are assigned, except for those that follow from the problem.
In our case, $P(x)$ and $Q(x)$ are interpreted somehow.

Suppose that $\exists x\, [P(x) \vee Q(x)]$ is true in a certain universe. This means that there is a value a in the universe such that $P(a)$ is true or $Q(a)$ is true.

If $P(a)$ is true, then a witnesses that $\exists x\, P(x)$ is true. By the rule of amplification we

conclude that $[\, \exists x\, P(x)\,] \vee [\, \exists x\, Q(x)\,]$ is also true.

The case when $Q(a)$ is true is similar.

Suppose that $[\, \exists x\, P(x)\,] \vee [\, \exists x\, Q(x)\,]$ is true in a certain universe. This means that

either $\exists x\, P(x)$ or $\exists x\, Q(x)$ are true, or both are true.

If $\exists x\, P(x)$ is true, then there is a value a in the universe such that $P(a)$ is true.

By the rule of amplification, we conclude that $P(a) \vee Q(a)$ is true. Therefore, a

witnesses that $\exists x\, [\, P(x) \vee Q(x)\,]$ is also true.

The case when $\exists x\, Q(x)$ is true is similar.

- If $\Phi \Leftrightarrow \Psi$ is a pair of logically equivalent compound statements, and $\Phi(x)$, $\Psi(x)$

  denote the open compound statements obtained from Φ and Ψ by replacing every propositional variable occurring in these statements (p, q, r, etc.) with open statements (P(x), Q(x), R(x), etc.), then:

  $\forall x\, \Psi(x) \Leftrightarrow \forall x\, \Phi(x)$ and $\exists x\, \Psi(x) \Leftrightarrow \exists x\, \Phi(x)$

  - $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ (The distributive law)

    $\forall x \{ P(x) \wedge [Q(x) \vee R(x)] \} \Leftrightarrow \forall x \{ [P(x) \wedge Q(x)] \vee [P(x) \wedge R(x)] \}$

  - $\exists x \neg [P(x) \wedge Q(x)] \Leftrightarrow \exists x [\neg P(x) \vee \neg Q(x)]$

    $\neg (p \wedge q) \Leftrightarrow \neg p \vee \neg q$ (DeMorgan's law)

- $\forall x\, [\, P(x) \vee \neg\, P(x)\,] \Leftrightarrow T$

- Logic equivalences for statements with multiple quantifiers are similar:

$$\forall x \forall y \{ P(x) \wedge [Q(x) \vee R(x, y)] \} \Leftrightarrow \forall x \forall y \{ [P(x) \wedge Q(x)] \vee [P(x) \wedge R(x, y)] \}$$

- Permutation of quantifiers:
  - If the quantifiers are all existential or all universal, then permutation does not matter:
    - $\forall x \forall y\, P(x, y) \Leftrightarrow \forall y \forall x\, P(x, y)$
    - $\exists x \exists y\, P(x, y) \Leftrightarrow \exists y \exists x\, P(x, y)$
  - If the quantifiers are different, then permutation does matter:
    - If $P(x, y)$ means 'y is the mother of x':
      - $\forall x \exists y\, P(x, y)$ means "Everyone has a mother"
      - $\exists y \forall x\, P(x, y)$ means "There is a person who is the mother of everyone"

Theorems and Proofs

- **Theorem**:
    - Definitions:
        - Mathematical statement of certain importance
            - E.g. "Every statement is equivalent to a certain CNF" or

              "A quadratic equation $ax^2 + bx + c = 0$ has at most 2 solutions"
        - Statement inferred within an axiomatic theory
            - E.g. "Prove that the computer chip design is correct"
    - **Axioms**: Starting points of inferring a theorem
        - Self-evident truth
            - E.g. "Two non-parallel lines intersect" or

              "There is something outside me"
            - Usually not quite truths; not such a useful meaning
                - E.g.
        - Statements we assume as true, facts from experiment or observation,

          something we suggest to see implications
- Proving theorems:
    - Use rules of inference (usually implicitly)
        - Explicitly in axiomatic theories:
            - Specify axioms
            - Specify rules of inference
    - Elementary geometry is an axiomatic theory
    - Euclid's postulates are axioms