Mathematical Foundation of Computer Science

(or)

Mathematics for Computer Science

(Discrete Mathematics or Discrete Structures)

Why to study Discrete Maths?

- Proof
  - Ability to understand and create mathematical argument
- Gateway to more advanced CS courses
  - Data Structures, Algorithms, Automata Theory and Formal Languages, Database, Networks, Operating system, Security

Guide for Successful Study

- No minimalist approach
  - Homework would be sufficient! NOPE!!!
  - Read relevant sections before coming to class
  - Do the homework (of course!!!)
  - Solve much more problems (odd numbered)
- Work regularly
  - Most chapters are building blocks for other chapters
    - So you cannot catch up 2 week lectures in 2 days
  - On average 3 hours EVERY week!
- Creativity
  - No questions will require you to put just numbers to formula.
  - Need to know how to apply! This can be improved by practice!
- Learning ≠ Book, class, note, homework
  - It is combination of everything!
- Think yourself, discuss with your friends, write your own answer!

Course content

very approximately in temporal order

- Unit.1: Propositional / Predicate Logic and Proofs
- Unit.2: Sets, Relation and Functions
- Unit.3: Number Theory
- Unit.4: Algebraic Structures
- Unit.5: Counting Principles

Note: Learning to do proofs from watching the slides is like trying to learn to play tennis from watching it on TV! So, do the exercises!

Discrete vs. Continuous Mathematics

Continuous Mathematics

It considers objects that vary continuously;

Example: analog wristwatch (separate hour, minute, and second hands).

From an analog watch perspective, between 1 :25 p.m. and 1 :26 p.m. there are infinitely many possible different times as the second hand moves around the watch face.

Real-number system --- core of continuous mathematics;

Continuous mathematics --- models and tools for analyzing real-world phenomena that change smoothly over time. (Differential equations etc.)

Discrete vs. Continuous Mathematics

Discrete Mathematics

The study of discrete mathematical structures and objects (as opposed to continuous objects).

It considers objects that vary in a discrete way.

Example: digital wristwatch.

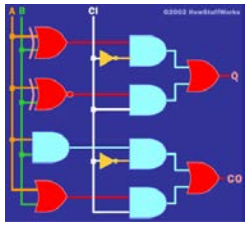
On a digital watch, there are only finitely many possible different times between 1 :25 P.M. and 1:27 P.M. A digital watch does not show split seconds: - no time between 1 :25:03 and 1 :25:04. The watch moves from one time to the next.

Integers --- *core of discrete mathematics*

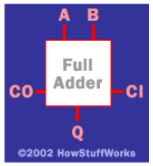
Discrete mathematics --- models and tools for analyzing real-world phenomena that change discretely over time and therefore ideal for studying computer science – computers are digital! (numbers as finite bit strings; data structures, all discrete! Historical aside: earliest computers were analogue.)

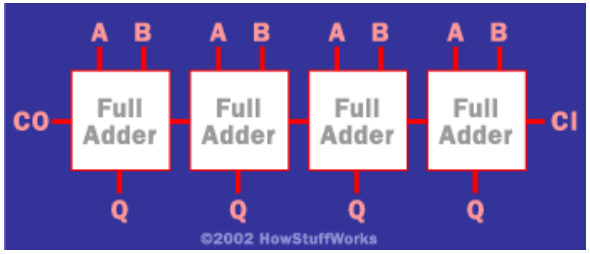
Why is it in computer science? (examples)

Logic:
Hardware and software specifications



One-bit Full Adder with Carry-In and Carry-Out





4-bit full adder

Formal: Input_wire_A
value in {0, 1}

Example 1: Adder

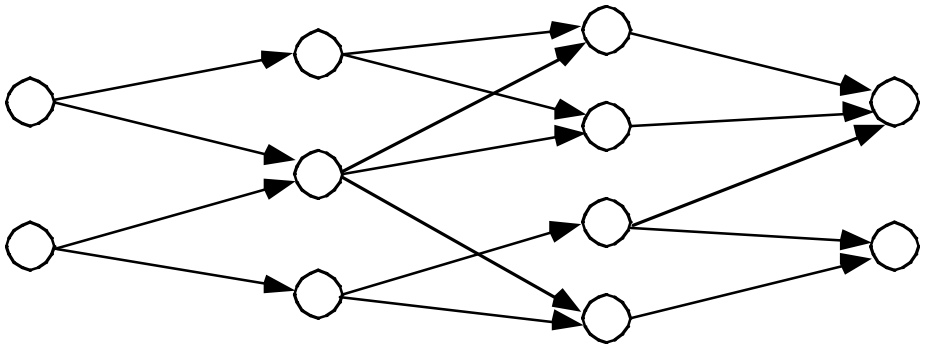
Example 2: System Specification:

–The router can send packets to the edge system only if it supports the new address space.
– For the router to support the new address space it's necessary that the latest software release be installed.
–The router can send packets to the edge system if the latest software release is installed.
–The router does not support the new address space.

How to write these specifications in a rigorous / formal way? ***Use Logic.***

Graphs and Networks

♈Many problems can be represented by a graphical network representation.

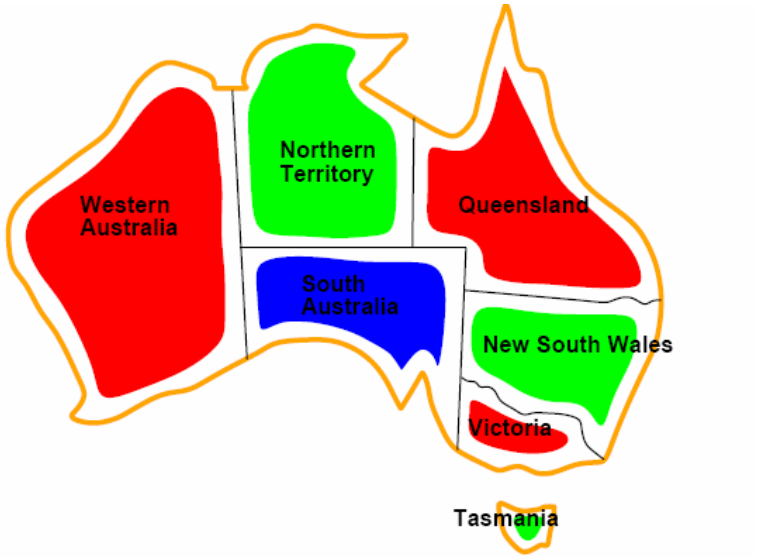


•Examples:

- Distribution problems
- Routing problems
- Maximum flow problems
- Designing computer / phone / road networks
- Equipment replacement
- And of course the Internet

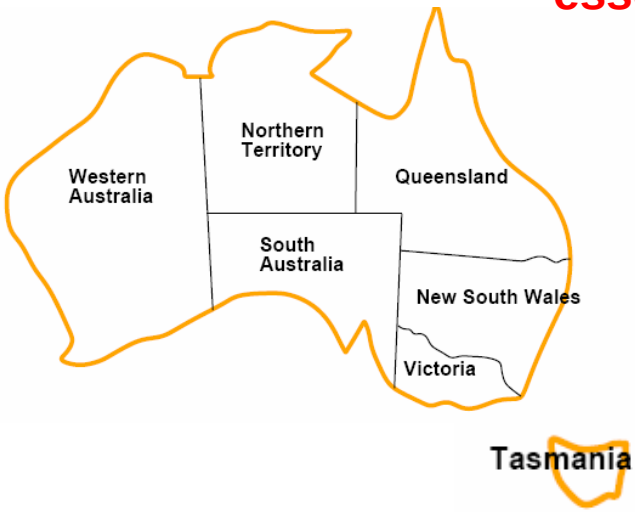
Aside: finding the right problem representation is one of the key issues.

Example: Coloring a Map

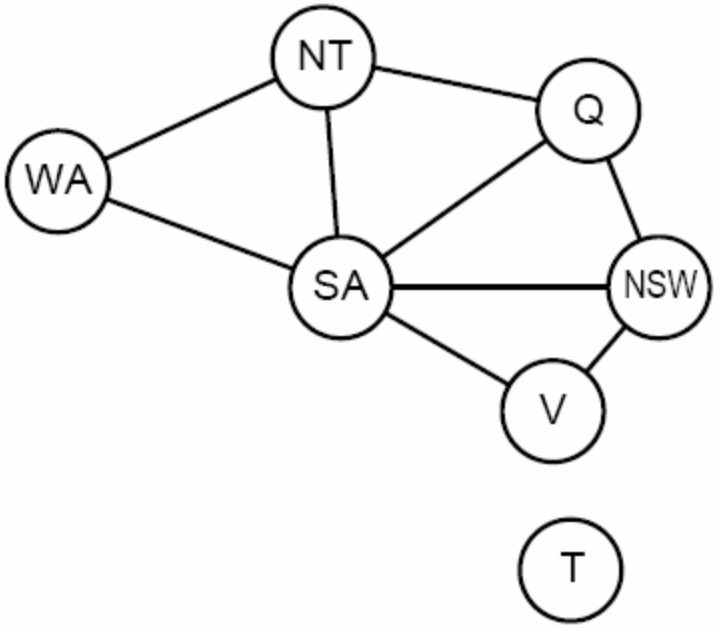


How to color this map so that no two adjacent regions have the same color?

Graph representation



Abstract the essential info:



Coloring the nodes of the graph:
What's the minimum number of colors such that any two nodes connected by an edge have different colors?

Introduction to logic

- What is logic?
- Why is it useful?
- Types of logic
  - Propositional logic
  - Predicate logic

What is Logic?

- **“Logic is the beginning of wisdom, not the end”**
- **Logic *n.1.* The branch of philosophy concerned with analysing the patterns of reasoning by which a conclusion is drawn from a set of premises, without reference to meaning or context**

(Collins English Dictionary)

Why study logic?

- Logic is concerned with two key skills, which any computer engineer or scientist should have:
  - Abstraction
  - Formalisation

Why is logic important?

- Logic is a **formalisation of reasoning**.
- Logic is a formal language for **deducing** knowledge from a small number of explicitly stated **premises** (or hypotheses, axioms, facts)
- Logic provides a formal framework for **representing knowledge**

Propositions

- A proposition is a statement that can be either true or false.
  - "Gopi is a Boy" (T)
  - "3 = 2 + 2" (F)
  - It is raining today. (T or F)

- Not propositions:
  - "Are you Bob?" (a question is not a proposition)
  - "x = 7" (since x is not specified, neither true nor false)
  - "She is heavy." (since she is not specified, neither true nor false)

Types of Propositions

Simple:

A proposition consisting of just one subject and one predicate is called simple statement.

Compound:

A proposition consisting of two or more simple proposition in the form of a single sentence is called a compound proposition.

Declarative sentence:

A sentence which cannot be further broken down or split into simple sentences is called declarative or atomic statements.

Propositional variables

- We use propositional variables to refer to propositions
  - Usually are lower case letters starting with p (i.e. *p*, *q*, *r*, *s*, etc.)
  - A propositional variable can have one of two values: true (T) or false (F)

- A proposition can be...
  - A single variable: p
  - An operation of multiple variables: $p \wedge (q \vee \neg r)$

Introduction to Logical Operators (or) Connectives

- More complex propositional statements can be build from elementary statements using **logical connectives.**

Logical connectives:

- Negation
- Conjunction
- Disjunction
- Exclusive or
- Implication
- Biconditional

- A **truth table** **displays the relationships between truth values (T or F) of propositions.**

Negation

- Switches (negates) the truth value
- Symbol: $\neg$ or ~
- $\neg p$ = “Today is not Friday”

p	$\neg p$
T	F
F	T

Conjunction

- Let p and q be propositions. The proposition "p and q" denoted by $p \wedge q$, is true then both p and q are true and is false otherwise. The proposition $p \wedge q$ is called the conjunction of p and q.

- $p \wedge q$ = "Today is Friday and today is my birthday"

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

Disjunction

- Let p and q be propositions. The proposition "p or q" denoted by $p \vee q$, is false when both p and q are false and is true otherwise. The proposition $p \vee q$ is called the disjunction of p and q.

- $p \vee q$ = "Today is Friday or today is my birthday (or possibly both)"

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

Exclusive or

- Let p and q be propositions. The proposition "p exclusive or q" denoted by $p \oplus q$, is true when exactly one of p and q is true and it is false otherwise.

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

Implication

- Let p and q be propositions. The proposition "p implies q" denoted by $p \rightarrow q$ is called implication. It is false when p is true and q is false and is true otherwise.
- A implication "if *p* then *q*"
- Symbol: $\rightarrow$
- $p \rightarrow q$ = "If today is Friday, then today is my birthday"
- $p \rightarrow q = \neg p \vee q$

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

the antecedent

the consequence

Implication

- Alternate ways of stating a conditional:
  - *p* implies *q*
  - If *p*, *q*
  - *p* only if *q*
  - *p* is sufficient for *q*
  - *q* if *p*
  - *q* whenever *p*
  - *q* is necessary for *p*

Implication

				Conditional	Inverse	Converse	Contrapositive
p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg p \rightarrow \neg q$	$q \rightarrow p$	$\neg q \rightarrow \neg p$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Bi-conditional

- A bi-conditional means "*p* if and only if *q*"
- Symbol: $\leftrightarrow$
- Alternatively, it means "(if *p* then *q*) and (if *q* then *p*)"
- Note that a bi-conditional has the opposite truth values of the exclusive or

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

Bi-conditional

- Let p = "You take this class" and q = "You get a grade"
- Then $p \leftrightarrow q$ means "You take this class if and only if you get a grade"
- Alternatively, it means "If you take this class, then you get a grade and if you get a grade then you take (took) this class"

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

Boolean operators summary

		not	not	and	or	xor	conditional	Bi-conditional
p	q	$\neg p$	$\neg q$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	F	F	T	T	F	T	T
T	F	F	T	F	T	T	F	F
F	T	T	F	F	T	T	T	F
F	F	T	T	F	F	F	T	T

- Learn what they mean, don't just memorize the table!

Translating English Sentences

- p = “It is below freezing”
- q = “It is snowing”

It is below freezing and it is snowing	$p \wedge q$
It is below freezing but not snowing	$p \wedge \neg q$
It is not below freezing and it is not snowing	$\neg p \wedge \neg q$
It is either snowing or below freezing (or both)	$p \vee q$
If it is below freezing, it is also snowing	$p \rightarrow q$
It is either below freezing or it is snowing, but it is not snowing if it is below freezing	$((p \vee q) \wedge \neg (p \wedge q)) \wedge (p \rightarrow \neg q)$
That it is below freezing is necessary and sufficient for it to be snowing	$p \leftrightarrow q$

Translation Example 3

- "I have neither given nor received help on this exam"
- Let p = "I have given help on this exam"
- Let q = "I have received help on this exam"

- $\neg p \wedge \neg q$

Translation Example 4

- You can access the Internet from campus only if you are a computer science major or you are not a freshman.
- $a \rightarrow (c \vee \neg f)$

- You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old.
- $(f \wedge \neg s) \rightarrow \neg r$
- $r \rightarrow (\neg f \vee s)$

WFF

The statement formula in which the order of finding the truth values are indicated by using parenthesis is called WFF.

Rules:

- A statement variable standing alone is a WFF.
- If A is a well formed formula, then $\neg A$ is a WFF.
- If A and B are WFF, then $(A \vee B)$, $(A \wedge B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$
- A string of symbols containg variables, connectives and parenthesis are WFF.

Precedence of operators

- Just as in algebra, operators have precedence
  - 4+3*2 = 4+(3*2), not (4+3)*2
- Precedence order (from highest to lowest):

  $\neg \ \wedge \ \vee \ \rightarrow \ \leftrightarrow$

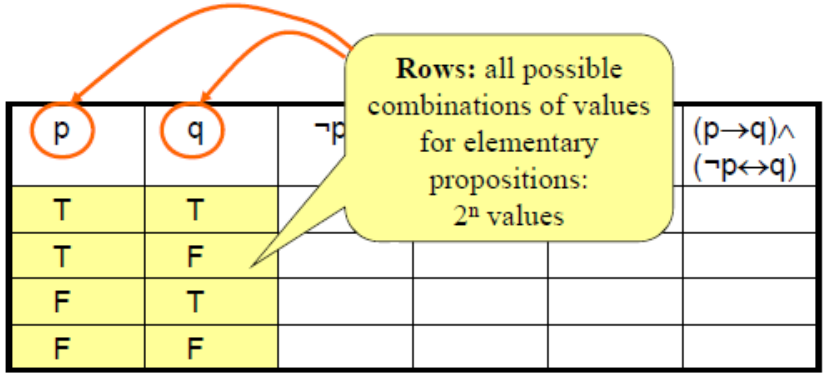
  - The first three are the most important
- This means that $p \vee q \wedge \neg r \rightarrow s \leftrightarrow t$ yields: $(p \vee (q \wedge (\neg r)) \rightarrow s) \leftrightarrow (t)$
- Not is *always* performed before any other operation

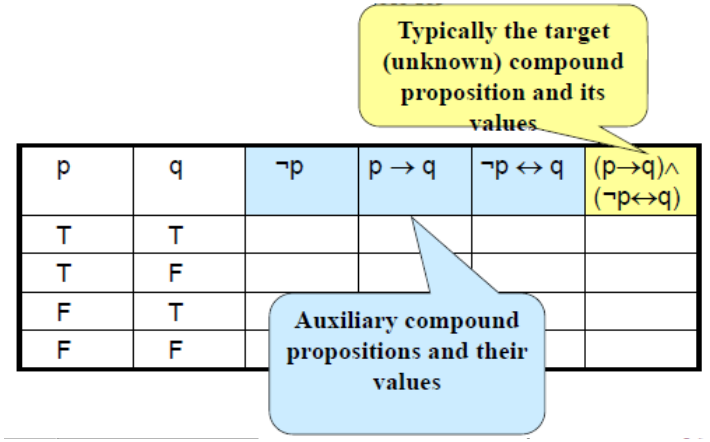
Constructing the truth table

- **Example: Construct a truth table for**
  $(p \rightarrow q) \wedge (\neg p \leftrightarrow q)$
- Simpler if we decompose the sentence to elementary and intermediate propositions

p	q	¬p	p → q	¬p ↔ q	(p→q)∧ (¬p↔q)
T	T				
T	F				
F	T				
F	F				

p	q	¬p	p → q	¬p ↔ q	(p→q)∧ (¬p↔q)
T	T	F	T	F	F
T	F	F	F	T	F
F	T	T	T	T	T
F	F	T	T	F	F





Evaluating the Truth of More General Compound Statements

Construct the truth table for the statement form $(p \vee q) \wedge \sim(p \wedge q)$.

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

Construct a truth table for the statement form $(p \wedge q) \vee \sim r$.

Evaluating the Truth of More General Compound Statements

Construct a truth table for the statement form $(p \wedge q) \vee \sim r$.

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

Logical Equivalence

- Two *statement forms* are called **logically equivalent** if, and only if, they have identical truth values for each possible substitution of statements for their statement variables.
- The logical equivalence of statement forms P and Q is denoted by writing P ≡ Q.

Example : $\sim(\sim p) \equiv$

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

p and $\sim(\sim p)$ always have the same truth values, so they are logically equivalent

Show that the statement forms $\sim(p \wedge q)$ and $\sim p \wedge \sim q$ are not logically equivalent.

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$		$\sim p \wedge \sim q$
T	T	F	F	T	F		F
T	F	F	T	F	T	$\neq$	F
F	T	T	F	F	T	$\neq$	F
F	F	T	T	F	T		T

$\sim(p \wedge q)$ and $\sim p \wedge \sim q$ have different truth values in rows 2 and 3, so they are not logically equivalent

Negations of And and Or: De Morgan's Laws

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

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

$\sim(p \wedge q)$ and $\sim p \vee \sim q$ always have the same truth values, so they are logically equivalent

Tautology and Contradiction

• Definition

A **tautology** is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a **tautological statement.**

A **contradication** is a statement form that is always false regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a contradication is a **contradictory statement.**

Show that the statement form $p \vee \sim p$ is a tautology and that the statement form $p \wedge \sim p$ is a contradiction.

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
T	F	T	F
F	T	T	F
		↑	↑
		all T's so $p \vee \sim p$ is a tautology	all F's so $p \wedge \sim p$ is a contradiction

Logical Equivalence (Theorems)

Given any statement variables p, q, and r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$, the following logical equivalences hold.

1. *Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2. *Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3. *Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. *Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5. *Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6. *Double negative law:*	$\sim(\sim p) \equiv p$	
7. *Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8. *Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9. *De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10. *Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11. *Negations of* $\mathbf{t}$ *and* $\mathbf{c}$*:*	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

TABLE 6 Logical Equivalences.

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

TABLE 7 Logical Equivalences Involving Conditional Statements.

$$p \to q \equiv \neg p \vee q$$

$$p \to q \equiv \neg q \to \neg p$$

$$p \vee q \equiv \neg p \to q$$

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

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

$$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$$

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

$$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$$

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

TABLE 8 Logical Equivalences Involving Biconditional Statements.

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

$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$

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

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

Show that $\neg(p \rightarrow q)$ and $p \wedge \neg q$ are logically equivalent.

$$\begin{aligned}
\neg(p \rightarrow q) &\equiv \neg(\neg p \vee q) && \text{by the conditional-disjunction equivalence} \\
&\equiv \neg(\neg p) \wedge \neg q && \text{by the second De Morgan law} \\
&\equiv p \wedge \neg q && \text{by the double negation law}
\end{aligned}$$

Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{by the second De Morgan law} \\
&\equiv \neg p \wedge [\neg(\neg p) \vee \neg q] && \text{by the first De Morgan law} \\
&\equiv \neg p \wedge (p \vee \neg q) && \text{by the double negation law} \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{by the second distributive law} \\
&\equiv \mathbf{F} \vee (\neg p \wedge \neg q) && \text{because } \neg p \wedge p \equiv \mathbf{F} \\
&\equiv (\neg p \wedge \neg q) \vee \mathbf{F} && \text{by the commutative law for disjunction} \\
&\equiv \neg p \wedge \neg q && \text{by the identity law for } \mathbf{F}
\end{aligned}$$

Consequently $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

$(p \wedge q) \rightarrow (p \vee q) \equiv \neg(p \wedge q) \vee (p \vee q)$ $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

$\equiv (\neg p \vee \neg q) \vee (p \vee q)$ by the first De Morgan law

$\equiv (\neg p \vee p) \vee (\neg q \vee q)$ by the associative and commutative laws for disjunction

$\equiv \mathbf{T} \vee \mathbf{T}$ Negation laws

$\equiv \mathbf{T}$ by the domination law

Satisfiability and validity