Chapter 1: The Foundations: Logic and Proofs

Dr. M Nouman Durrani

Department of Computer Science, FAST NUCES, KHI

Discrete Structures

- Discrete mathematics is the part of mathematics devoted to the study of discrete objects (Kenneth H. Rosen, 7th edition).
- **Discrete mathematics** is the mathematical study of properties, and relationships among discrete objects.
- **Discrete mathematics** is the study of mathematical **structures** that are fundamentally discrete rather than continuous.

  - Discrete objects are those which are separated from (distinct from) each other, such as integers, rational numbers, houses, people, etc.
  - Real numbers are not discrete.
  - Computers use discrete structures to represent and manipulate data.

Discrete Mathematics

Discrete Data: A set of data is said to be discrete if the values belonging to the set are distinct and separate. It is counted e.g., {1,2,3,4,5,6}

In this course:

- We'll be concerned with objects such as integers, propositions, sets, relations and functions, which are all discrete.
- We'll learn concepts associated with them, their properties, and relationships among them.
- We'll learn mathematical facts and their applications.

Discrete structures are:

– Theoretical basis of computer science

– A mathematical foundation that makes you think logically

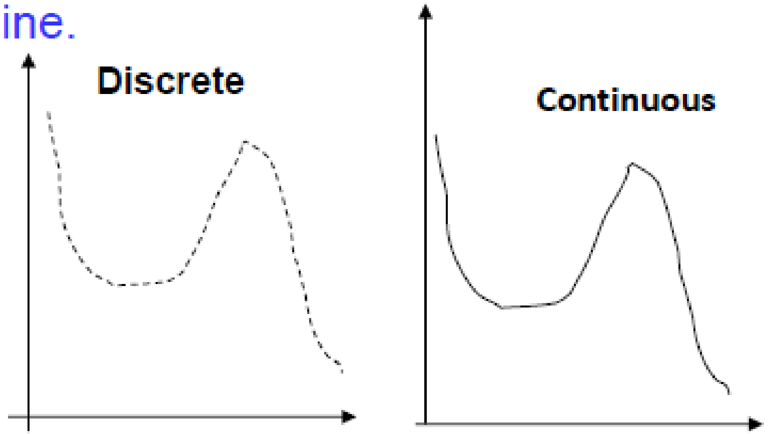
Discrete Vs Continuous

- Continuous Data: A set of data is said to be continuous if the values belonging to the set can take on any value within a finite or infinite interval.
- Continuous data is information that can be measured on a continuum or scale. , e.g., [0, 70].
- Continuous data can have almost any numeric value and can be meaningfully subdivided into finer and finer increments, depending upon the precision of the measurement system.

- Discrete Data: A set of data is said to be discrete if the values belonging to the set are distinct and separate. It is counted e.g., {1,2,3,4,5,6}

Discrete vs Continuous

- Examples of discrete Data
  - Number of boys in the class.
  - Number of candies in a packet.
  - Number of suitcases lost by an airline.



- Examples of continuous Data
  - Height of a person.
  - Time in a race.
  - Distance traveled by a car.

Why Discrete Structures -- Applications

- How many ways are there to choose a valid password on a computer system?
- What is the probability of winning a lottery?
- Is there a link between two computers in a network?
- How can I identify spam e-mail messages?
- How can I encrypt a message so that no unintended recipient can read it?
- What is the shortest path between two cities using a transportation system?
- How can a list of integers be sorted so that the integers are in increasing order?
- How many steps are required to do such a sorting?
- How many valid Internet addresses are there?

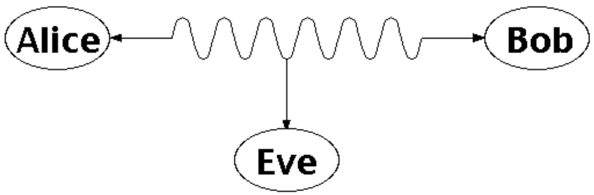
Why Discrete Structures -- Applications

- Digital computers are based on discrete "atoms" (bits).
  - Computers use discrete structures to represent and manipulate data.

- Therefore, both a computer's
  - structure (circuits) and
  - operations (execution of algorithms)

  can be described by discrete mathematics.

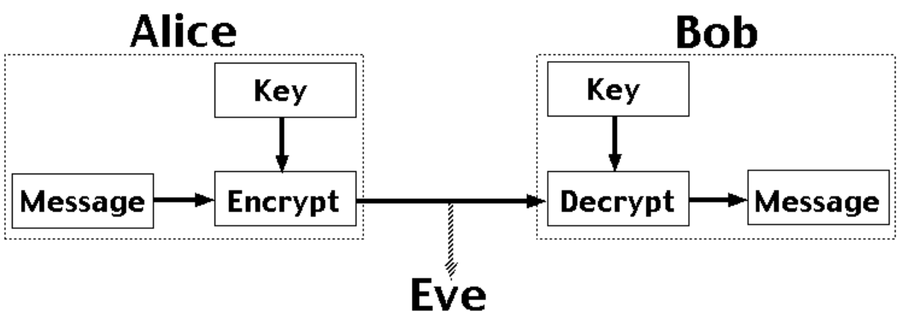
Applications: Number Theory
RSA and Public-key Cryptography



Alice and Bob have never met but they would like to exchange a message. Eve would like to eavesdrop.

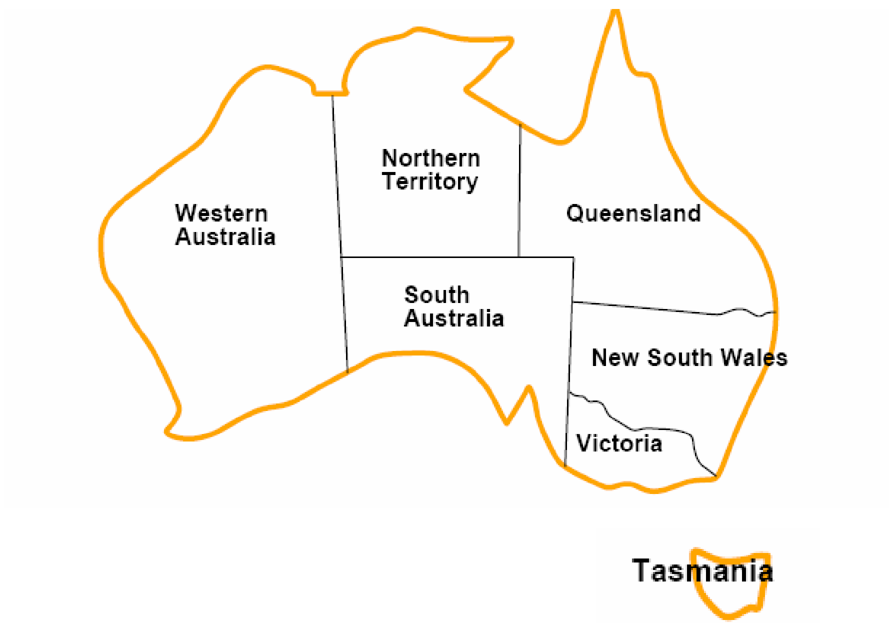
E.g. between you and the Bank of America.

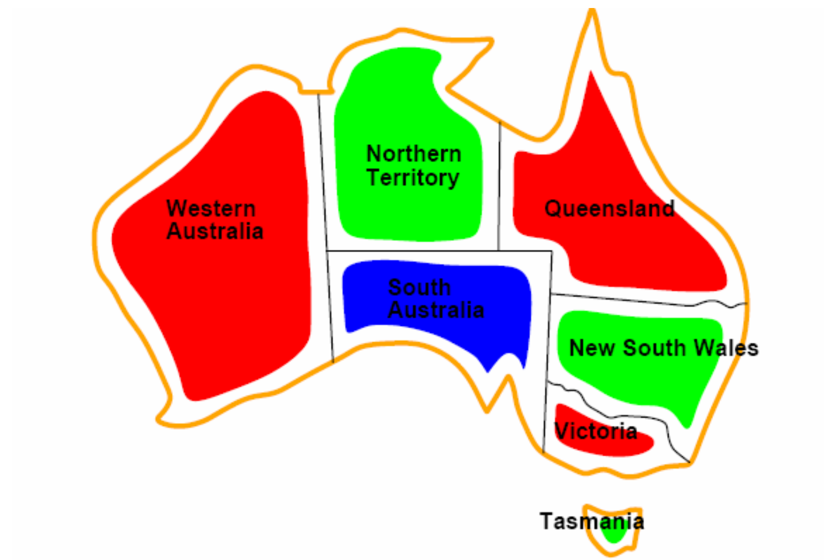
They could come up with a good encryption algorithm and exchange the encryption key – but how to do it without Eve getting it? (If Eve gets it, all security is lost.)



CS folks found the solution: *public key encryption*. Quite remarkable that is feasible.

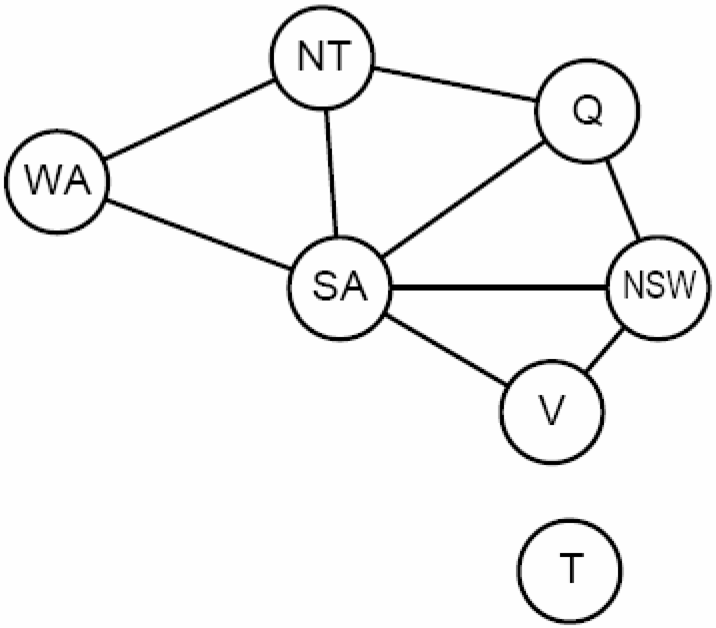
Applications: Coloring a Map

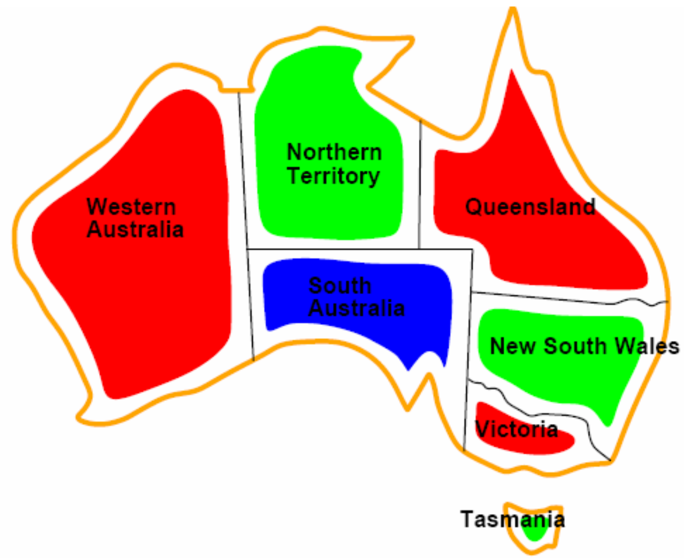




How to color this map so that no two adjacent regions have the same color?

Applications: Graph representation





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?

Applications: Scheduling of Final Exams

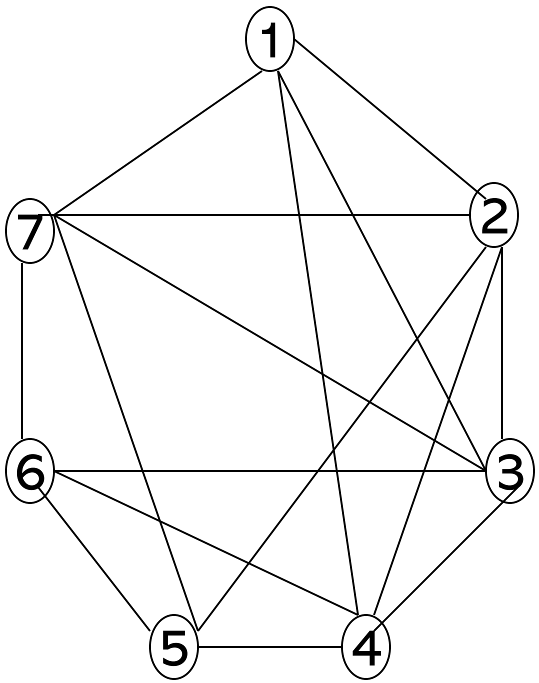
- How can the final exams at FAST be scheduled so that no student has two exams at the same time?

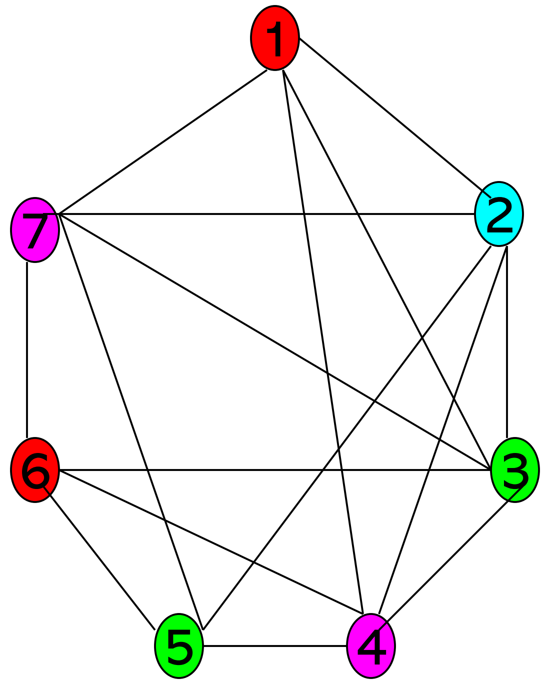
Graph:

A vertex correspond to a course.
An edge between two vertices denotes that there is at least one common student in the courses they represent.
Each time slot for a final exam is represented by a different color.

A coloring of the graph corresponds to a valid schedule of the exams.

Applications: Scheduling of Final Exams





Time Period	Courses
I	1,6
II	2
III	3,5
IV	4,7

What are the constraints between courses?

Find a valid coloring

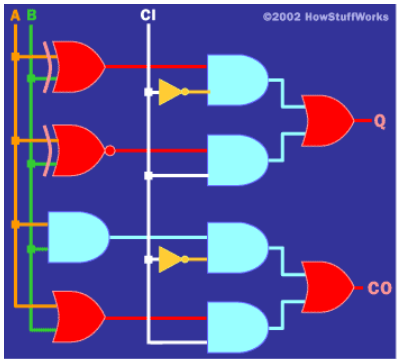
Applications: Index Registers

- The execution of loops can be speeded up by storing frequently used variables temporarily in registers in the central processing unit, instead in the regular memory. For a given loop, how many index registers are needed?

  - Each vertex corresponds to a variable in the loop.
  - An edge between two vertices denotes the fact that the corresponding variables must be stored in registers at the same time during the execution of the loop.
  - Chromatic number of the graph gives the number of index registers needed.

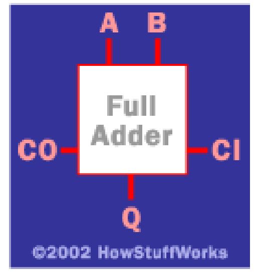
Applications: Logic

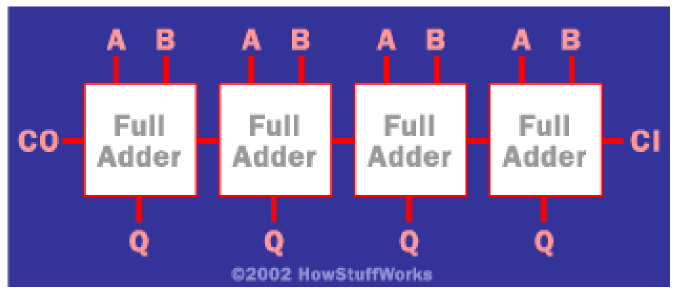
Hardware and software specifications



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**

Problem Solving requires mathematical rigor

- Your boss is not going to ask you to solve
  - an MST (Minimal Spanning Tree) or
  - a TSP (Travelling Salesperson Problem)
- Rarely will you encounter a problem in an abstract setting
- However, he/she may ask you to build a rotation of the company's delivery trucks to minimize fuel usage
- It is up to you to determine
  - a proper model for representing the problem and
  - a correct or efficient algorithm for solving it

Scenario I

- A limo company has hired you/your company to write a computer program to automate the following tasks for a large event
- **Task1**: In the first scenario, businesses request
  - limos and drivers
  - for a fixed period of time, specifying a start date/time and end date/time and
  - a flat charge rate
- The program must generate a schedule that accommodates the maximum number of customers

Scenario II

- **Task 2**: In the second scenario
  - the limo service allows customers to bid on a ride
  - so that the highest bidder get a limo when there aren't enough limos available
- The program should make a schedule that
  - Is feasible (no limo is assigned to two or more customers at the same time)
  - While maximizing the total profit

Scenario III

- Task 3: Here each customer
  - is allowed to specify a set of various times and
  - bid an amount for the entire event.
  - The limo service must choose to accept the entire set of times or reject it
- The program must again maximize the profit.

What's your job?

- Build a mathematical model for each scenario
- Develop an algorithm for solving each task
- Justify that your solutions work
  - Prove that your algorithms terminate. Termination
  - Prove that your algorithms find a solution when there is one. Completeness
  - Prove that the solution of your algorithms is correct Soundness
  - Prove that your algorithms find the best solution (i.e., maximize profit). Optimality (of the solution)
  - Prove that your algorithms finish before the end of life on earth. Efficiency, time & space complexity

The goal of this course

- Give you the foundations that you will use to eventually solve these problems.
  - Task1 is easily (i.e., efficiently) solved by a greedy algorithm
  - Task2 can also be (almost) easily solved, but requires a more involved technique, dynamic programming
  - Task3 is not efficiently solvable (it is NP-hard) by any known technique. It is believed today that to guarantee an optimal solution, one needs to look at all (exponentially many) possibilities

Course Description:

- This class teaches students
  - how to think logically and mathematically.
  - It stresses mathematical reasoning and different ways to solve problems.

  It enhance your ability to formulate and solve applied problems, to analyze and interpret algorithms and functions and to use them effectively.
  - It helps you form a logical basis to decompose a given problem into statements that make sense.

Course Outline

- Logic and Proofs
- Sets and Functions
- Relations
- Counting and Recurrence Relations
- Graphs
- Trees
- Number Theory
- Discrete Probability and Finite State Automata

TEXT Book:

- Discrete Mathematics & its Applications, 7th edition. By Kenneth H. Rosen.

References Book:

- Invitation to Discrete Maths, 2nd edition. By Matousek and Nesetril.
- Discrete Mathematics. By Lovasz, Pelikan and Vesztergombi.

Logic

Logic: Set of principles underlying the arrangements of elements (in a computer or electronic device) so as to perform a specified task.

- Logic is fundamental because it allows us to understand meaning of statements, deduce information about mathematical structures and uncover further structures.
- The rules of logic specify the meaning of mathematical statements.
- These rules are used to distinguish between valid and invalid arguments.

Logic: Understand meaning of statements, deduce information about mathematical structures and uncover further structures.

Nested Quantifiers: Example 3

- Translate the statement
  "If a person is female and is a parent, then this person is someone's mother"
  as a logical expression
- Let
  - F(x): x is female
  - P(x): x is a parent
  - M(x,y): x is y's mother

At least one y

$$(F(x) \wedge P(x)) \rightarrow M(x, y)$$

All x

- The domain is the set of all people

$$\forall x\ (\ (F(x) \wedge P(x)) \rightarrow \exists y\ M(x, y)\ ), \text{ or}$$

$$\forall x\ \exists y\ (\ (F(x) \wedge P(x)) \rightarrow M(x, y)\ )$$

Propositional Logic

- A **proposition** is a **declarative** sentence (a sentence that declares a fact) that is either **true or false**, but not both.
- Are the following sentences **propositions?**
  - Toronto is the capital of Canada. (Yes)
  - Read this carefully. (No)
  - 1+2=3 (Yes)
  - x+1=2 (No)
  - What time is it? (No)

Proposition

Definition

proposition (or statement):
a declarative sentence that is either true or false

- law of the excluded middle:
  a proposition cannot be partially true or partially false
- law of contradiction:
  a proposition cannot be both true and false

propositions

- The Moon revolves around the Earth.
- Elephants can fly.
- $3 + 8 = 11$

not propositions

- What time is it?
- Exterminate!
- $x < 43$

Examples: Propositions

Is the following sentence a proposition? If it is a proposition, determine whether it is true or false.

Islamabad is the capital of Pakistan.

This makes a declarative statement, and hence is a proposition. The proposition is TRUE (T).

Can Ali come with you?.

This is a question not the declarative sentence and hence not a proposition.

Take two aspirins.

This is an imperative sentence not the declarative sentence and therefore not a proposition.

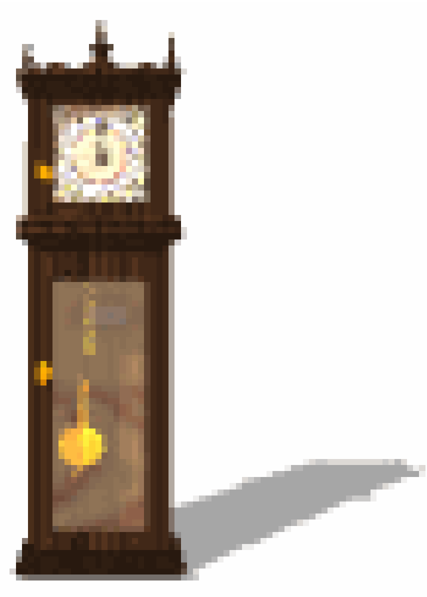
$x + 4 > 9$.

Because this is true for certain values of x (such as $x = 6$) and false for other values of x (such as $x = 5$), it is not a proposition.

He is a college student.

Because truth or falsity of this proposition depend on the reference for the pronoun *he*. it is not a proposition.

Activity 1



Write down at least 5 examples of propositions and Non-propositions.

Propositional Variable

- propositional variable:
  a name that represents the proposition

examples

- p_1: The Moon revolves around the Earth. (T)
- p_2: Elephants can fly. (F)
- p_3: $3 + 8 = 11$ (T)

Notations

- The small letters are commonly used to denote the propositional variables, that is, variables that represent propositions, such as, $p, q, r, s, \ldots$.
- The truth value of a proposition is true, denoted by T or 1, if it is a true proposition and false, denoted by F or 0, if it is a false proposition.

Compound Propositions

Logical operators are used to form new propositions also called compound propositions from two or more existing propositions.

- compound propositions are obtained by applying logical operators

  The logical operators are also called connectives.

- truth table:
  a table that lists the truth value of the compound proposition
  for all possible values of its variables

Propositional Logic – the area of logic that deals with propositions

1. Negation:

DEFINITION 1:

Let p be a proposition. The negation of p, denoted by $\neg p$, is the statement
"It is not the case that p."

The proposition $\neg p$ is read "not p." The truth value of the negation of p, $\neg p$ is the opposite of the truth value of p.

- Examples
  - Find the negation of the proposition "Today is Friday." and express this in simple English.

    Solution: The negation is "It is not the case that *today is Friday*."
    In simple English, "Today is not Friday." or "It is not Friday today."
  - Find the negation of the proposition "At least 10 mm of rain fell today in Karachi." and express this in simple English.

    Solution: The negation is "It is not the case that *at least 10 mm of rain fell today in Karachi*."
    In simple English, "Less than 10 mm of rain fell today in Karachi."

Negation:

- Note: Always assume fixed times, fixed places, and particular people unless otherwise noted.
- Truth table:

The Truth Table for the Negation of a Proposition.	
p	$\neg p$
T	F
F	T

examples

- $\neg p_1$: The Moon does not revolve around the Earth.
  $\neg T : F$
- $\neg p_2$: Elephants cannot fly.
  $\neg F : T$

2. Conjunction:

DEFINITION 2

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

- Examples
  - Find the conjunction of the propositions p and q where p is the proposition "Today is Friday." and q is the proposition "It is raining today.", and the truth value of the conjunction.

Solution: The conjunction is the proposition "Today is Friday and it is raining today." The proposition is true on rainy Fridays.

$p \wedge q$

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

examples

- $p_1 \wedge p_2$: The Moon revolves around the Earth and elephants can fly.
  $T \wedge F : F$
- $p_1 \wedge p_3$: The Moon revolves around the Earth and $3 + 8 = 11$.
  $T \wedge T : T$

3. Disjunction:

DEFINITION 3

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

- Note:

  inclusive or : The disjunction is true when at least one of the two propositions is true.

  - E.g. "Students who have taken calculus or computer science can take this class." – those who take one or both classes.

  exclusive or : The disjunction is true only when one of the proposition is true.

  - E.g. "Students who have taken calculus or computer science, but not both, can take this class." – only those who take one of them.

- Definition 3 uses of *inclusive or*.

Disjunction (OR)

$p \vee q$

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

example

- $p_1 \vee p_2$: The Moon revolves around the Earth or elephants can fly.
  $T \vee F : T$

4. Exclusive OR:

DEFINITION 4

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

The Truth Table for the Conjunction of Two Propositions.

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

The Truth Table for the Disjunction of Two Propositions.

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

The Truth Table for the Exclusive *Or* (*XOR*) of Two Propositions.

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

Examples

1. Find the *exclusive or* of the propositions p and q, where

p : Atif will pass the course CSC102.

q : Atif will fail the course CSC102.

The *exclusive or* is

$p \oplus q$: Atif will pass or fail the course CSC102.

The following proposition uses the (English) connective "or". Determine from the context whether "or" is intended to be used in the inclusive or exclusive sense.

1. "Nabeel has one or two brothers".

A person cannot have both one and two brothers. Therefore, "or" is used in the exclusive sense.

Examples (OR vs XOR)

2. To register for BSC you must have passed the qualifying exam or be listed as an Math major.

Presumably, if you have passed the qualifying exam and are also listed as an Math major, you can still register for BCS. Therefore, "or" is inclusive.

Example: "Soup or salad comes with this entrée" Meaning: do not expect to get both

The $\vee$ means "one or the other *or both*". **inclusive or.**
The "but not both" version is *exclusive or*.

EXAMPLE 1.7.1. *p: This book is interesting. q: I am staying at home.*

$p \oplus q$: Either this book is interesting, or I am staying at home, but not both.

5. Implication / Conditional Statements:

DEFINITION 5

Let p and q be propositions. The *conditional statement* $p \rightarrow q$, is the proposition "if p, then q." The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \rightarrow q$, p is called the *hypothesis* (or *antecedent* or *premise*) and q is called the *conclusion* (or *consequence*).

- A conditional statement is also called an implication.
- Example: "If I am elected, then I will lower taxes." $p \rightarrow q$

implication:

	p	q	$p \rightarrow q$
elected, lower taxes.	T	T	T
not elected, lower taxes.	F	T	T
not elected, not lower taxes.	F	F	T
elected, not lower taxes.	T	F	F

Examples: Implication

Examples of implications:

If you stand in the rain, then you'll get wet.
If you got an A in this class, I gave you \$5.

An implication $P \Longrightarrow Q$ is false only when P is true and Q is false. For example, the first statement would be false only if you stood in the rain but didn't get wet. The second statement above would be false only if you got an "A," yet I didn't give you \$5.

Here is the truth table for $P \Longrightarrow Q$:

P	Q	$P \Longrightarrow Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

[1] P is also called the *antecedent* and Q the *consequent*.

Examples: Implication

Note that $P \Longrightarrow Q$ is always true when P is false. This means that many statements that sound nonsensical in English are true, mathematically speaking. Examples are statements like: "If pigs can fly, then horses can read" or "If 14 is odd then $1+2=18$." When an implication is stupidly true because the hypothesis is false, we say that it is **vacuously true**. Note also that $P \Longrightarrow Q$ is logically equivalent to $\neg P \vee Q$, as can be seen in the above truth table.

$P \Longrightarrow Q$ is the most common form mathematical theorems take. Here are some of the different ways of saying it:

(1) If P, then Q.
(2) Q if P.
(3) P only if Q.
(4) P is sufficient for Q.
(5) Q is necessary for P.

Some other cases of implications:

"if p, then q"	"p implies q"
"if p, q"	"p only if q"
"p is sufficient for q"	"a sufficient condition for q is p"
"q if p"	"q whenever p"
"q when p"	"q is necessary for p"
"a necessary condition for p is q"	"q follows from p"
"q unless $\neg p$"	

Example: Conditional Statements

- Example:
  - Let p be the statement "Maria learns discrete mathematics." and q the statement "Maria will find a good job." Express the statement $p \longrightarrow q$ as a statement in English.

  Solution: Any of the following -

  "If Maria learns discrete mathematics, then she will find a good job. If p then q

  "Maria will find a good job when she learns discrete mathematics." q when p

  "For Maria to get a good job, it is sufficient for her to learn discrete mathematics." A sufficient condition for q is p

  "Maria will find a good job unless she does not learn discrete mathematics." q unless NOT(p)

Implication Example

- "If I weigh over 70 kg, then I will exercise."
- p: I weigh over 70 kg.
- q: I exercise.
- when is this claim false?

$p \rightarrow q$

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

- p_4: $3 < 8$, p_5: $3 < 14$, p_6: $3 < 2$, p_7: $8 < 6$

- $p_4 \rightarrow p_5$:
  if $3 < 8$, then $3 < 14$
  $T \rightarrow T : T$
- $p_4 \rightarrow p_6$:
  if $3 < 8$, then $3 < 2$
  $T \rightarrow F : F$
- $p_6 \rightarrow p_4$:
  if $3 < 2$, then $3 < 8$
  $F \rightarrow T : T$
- $p_6 \rightarrow p_7$:
  if $3 < 2$, then $8 < 6$
  $F \rightarrow F : T$

- **Other conditional statements:**
  - Converse of $p \longrightarrow q$: $q \longrightarrow p$
  - Contrapositive of $p \longrightarrow q$: $\neg q \longrightarrow \neg p$
  - Inverse of $p \longrightarrow q$: $\neg p \longrightarrow \neg q$

The contrapositive of "If you got an A in this class, I gave you \$5," is "If I did not give you \$5, you didn't get an A in this class." The converse is "If I gave you \$5 you must have received an A in this class." Does the contrapositive say the same thing as the original statement? Does the converse?

Let's look at the truth table:

P	Q	$\neg P$	$\neg Q$	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$\neg Q \Longrightarrow \neg P$	$P \Longleftrightarrow Q$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	F	F
F	T	T	F	T	F	T	F
F	F	T	T	T	T	T	T

Note that the contrapositive of $P \Longrightarrow Q$ has the same truth values, while the converse does not. Many students unreasonably assume that the converse is true, but the above truth table shows that it is not necessarily the case. When two propositional forms have the same truth values, they are said to be **logically equivalent** – they mean the same thing. We'll see next time how useful this can be for proving theorems.

Converse, Contrapositive, and Inverse

- From $p \to q$ we can form new conditional statements .
  - $q \to p$ is the **converse** of $p \to q$
  - $\neg q \to \neg p$ is the **contrapositive** of $p \to q$
  - $\neg p \to \neg q$ is the **inverse** of $p \to q$

Example: Find the converse, inverse, and contrapositive of "It is raining is a sufficient condition for my not going to town."

Assume: P: It will rain tomorrow

Q: I will not go to town

Solution:

converse: If I do not go to town, then it is raining.

inverse: If it is not raining, then I will go to town.

contrapositive: If I go to town, then it is not raining.

Contrapositive:

- Contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$
- Any proposition and its contrapositive are logically equivalent (have the same truth table values) – Check with the truth table.
- E.g. The contrapositive of "If you get 100% in this course, you will get an A+" is "If you do not get an A+ in this course, you did not get 100%".

Converse:

- Converse of $p \rightarrow q$ is $q \rightarrow p$
- Both are not logically equivalent.
- Ex 1: "If you get 100% in this course, you will get an A+" and "If you get an A+ in this course, you scored 100%"

are not equivalent.

- Ex 2: If you won the lottery, you are rich.

Inverse:

- Inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$
- Both are not logically equivalent.
- Ex1 : "If you get 100% in this course, you will get an A+" and "If you didn't 100%, then won't have an A+ in this course." are not equivalent.
- Ex2: You can not ride the roller coaster if you are under 4 feet. What is its inverse statement?

Example of converse (1/2)

- Find the converse of the following statement:
- R: 'Raining tomorrow is a sufficient condition for my not going to town.'
- Step 1: Assign propositional variables to
- component propositions
- P: It will rain tomorrow
- Q: I will not go to town

Example of converse (2/2)

- Step 2: Symbolize the assertion R: $P \to Q$
- Step 3: Symbolize the converse $Q \to P$
- Step 4: Convert the symbols back into words

  'If I don't go to town then it will rain tomorrow' or

  'Raining tomorrow is a necessary condition for my not going to town.' or

  'My not going to town is a sufficient condition for it raining tomorrow.'

6. Bi-implications:

DEFINITION 6

Let p and q be propositions. The *biconditional statement* $p \leftrightarrow q$ is the proposition "p if and only if q." The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise. Biconditional statements are also called *bi-implications*.

- $p \leftrightarrow q$ has the same truth value as $(p \rightarrow q) \land (q \rightarrow p)$
- "*if and only if*" can be expressed by "*iff*"
- Example:
  - Let p be the statement "You can take the flight" and let q be the statement "You buy a ticket." Then $p \leftrightarrow q$ is the statement "You can take the flight if and only if you buy a ticket."

Bi-implications:

The Truth Table for the Biconditional $p \boxed{\leftrightarrow} q$.		
p	q	$p \boxed{\leftrightarrow} q$
T	T	T
T	F	F
F	T	F
F	F	T

If p denotes "I am at home." and q denotes "It is raining." then $p \leftrightarrow q$ denotes "I am at home if and only if it is raining."

If both $P \implies Q$ and $Q \implies P$ are true, then we say "P if and only if Q" (abbreviated P iff Q). Formally, we write $P \iff Q$. P if and only if Q is true only when P and Q have the same truth values.

For example, if we let P be "3 is odd," Q be "4 is odd," and R be "6 is even," then $P \implies R$, $Q \implies P$ (vacuously), and $R \implies P$. Because $P \implies R$ and $R \implies P$, P if and only if R.

Expressing the Biconditional

- Some alternative ways "p if and only if q" is expressed in English:
  - **p is necessary and sufficient for q**
  - **if p then q , and conversely**
  - **p iff q**

Without changing their meanings, convert each of the following sentences into a sentence having the form "p iff q"

For a matrix to be invertible, it is necessary and sufficient that its determinant is not zero.

Answer: A matrix is invertible if and only if its determinant is not zero.

If $xy = 0$ then $x = 0$ or $y = 0$, and conversely.

Answer: $xy = 0$ if and only if $x = 0$ or $y = 0$

For an occurrence to become an adventure, it is necessary and sufficient for one to recount it.

Answer: An occurrence becomes an adventure if and only if one recounts it.

Truth Tables of Compound Propositions

- We can use connectives to build up complicated compound propositions involving any number of propositional variables, then use truth tables to determine the truth value of these compound propositions.
- Example: Construct the truth table of the compound proposition

$$(p \lor \neg q) \longrightarrow (p \land q).$$

The Truth Table of $(p \lor \neg q) \rightarrow (p \land q)$.

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

Example Truth Table

- Construct a truth table for

$$p \vee q \rightarrow \neg r$$

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

Problem:

- How many rows are there in a truth table with *n* propositional variables?

 Solution: 2^n We will see how to do this in Chapter 6.

- Note that this means that with n propositional variables, we can construct 2^n distinct (i.e., not equivalent) propositions.

Precedence of Logical Operators

- We can use parentheses to specify the order in which logical operators in a compound proposition are to be applied.
- To reduce the number of parentheses, the precedence order is defined for logical operators.

Precedence of Logical Operators.	
Operator	Precedence
$\neg$	1
$\wedge$ $\vee$	2 3
$\rightarrow$ $\boxed{\leftrightarrow}$	4 5

E.g. $\neg p \wedge q = (\neg p) \wedge q$

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

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

Translating English Sentences

(1) If P, then Q.
(2) Q if P.
(3) P only if Q.
(4) P is sufficient for Q.
(5) Q is necessary for P.

- English (and every other human language) is often ambiguous. Translating sentences into compound statements removes the ambiguity.
- Example: How can this English sentence be translated into a logical expression?

You cannot ride the coaster if You are under 4 feet tall and you are not older than 16 Years old.

Solution: Let q, r, and s represent "You can ride the roller coaster," "You are under 4 feet tall," and "You are older than 16 years old." The sentence can be translated into:

$$(r \wedge \neg s) \rightarrow \neg q.$$

Home Task: "You cannot ride the roller coaster **if** you are under 4 feet tall **unless** you are older than 16 years old."

Q unless NOT (P)

Translating English Sentences

- Steps to convert an English sentence to a statement in propositional logic
  - Identify atomic propositions and represent using propositional variables.
  - Determine appropriate logical connectives
- "If I go to Harry's or to the country, I will not go shopping."
  - *p*: I go to Harry's
  - q: I go to the country.
  - *r*: I will go shopping.

If *p* or *q* then not *r*.

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

Translating English Sentences

- Example: How can this English sentence be translated into a logical expression?

  "You can access the Internet from campus only if you are a computer science major or you are not a freshman."

Solution: Let a, c, and f represent "You can access the Internet from campus," "You are a computer science major," and "You are a freshman." The sentence can be translated into:

$$a \rightarrow (c \vee \neg f).$$

(1) If P, then Q.
(2) Q if P.
(3) P only if Q.
(4) P is sufficient for Q.
(5) Q is necessary for P.

System Specifications

- System and Software engineers take requirements in English and express them in a precise specification language based on logic.

Example: Express in propositional logic:

"The automated reply cannot be sent when the file system is full"

Solution: One possible solution: Let p denote "The automated reply can be sent" and q denote "The file system is full."

$$q \rightarrow \neg p$$

q when p

Logic and Bit Operations

- Computers represent information using bits.
- A **bit** is a symbol with two possible values, 0 and 1.
- By convention, 1 represents T (true) and 0 represents F (false).
- A variable is called a Boolean variable if its value is either true or false.
- Bit operation – replace true by 1 and false by 0 in logical operations.

Table for the Bit Operators *OR*, *AND*, and *XOR*.

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Logic and Bit Operations

> DEFINITION 7
>
> A *bit string* is a sequence of zero or more bits. The *length* of this string is the number of bits in the string.

- Example: Find the bitwise *OR*, bitwise *AND*, and bitwise *XOR* of the bit string 01 1011 0110 and 11 0001 1101.

Solution:

01 1011 0110

11 0001 1101

\-------------------

11 1011 1111 bitwise *OR*

01 0001 0100 bitwise *AND*

10 1010 1011 bitwise *XOR*

Propositional Equivalences

DEFINITION 1

A compound proposition that is always true, no matter what the truth values of the propositions that occurs in it, is called a *tautology*.

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

A compound proposition that is neither a tautology or a contradiction is called a *contingency*.

Examples of a Tautology and a Contradiction.

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

Tautologies and Contradictions

- Tautology is a statement that is always true regardless of the truth values of the individual logical variables
- Examples:
- $R \vee (\neg R)$
- $\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$

Tautologies and Contradictions

- A Contradiction is a statement that is always false regardless of the truth values of the individual logical variables

Examples

- $R \wedge (\neg R)$
- $\neg(\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q))$

- The negation of any tautology is a contradiction, and the negation of any contradiction is a tautology.

Propositional Equivalences

DEFINITION 2

The compound propositions p and q are called *logically equivalent* if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent.

- Compound propositions that have the same truth values in all possible cases are called logically equivalent.
- Example: Show that $\neg p \vee q$ and $p \rightarrow q$ are logically equivalent.

Truth Tables for $\neg p \vee q$ and $p \rightarrow q$.

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

Propositional Equivalences

- In general, 2^n rows are required if a compound proposition involves n propositional variables in order to get the combination of all truth values.

- Prove that $\neg(\neg p) \equiv p$

Solution

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

As you can see the corresponding truth values of p and $\neg(\neg p)$ are same, hence equivalence is justified.

Propositional Equivalences

Example

Show that the proposition forms $\neg(p \wedge q)$ and $\neg p \wedge \neg q$ are NOT logically equivalent.

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

Here the corresponding truth values differ and hence equivalence does not hold

Applications: Boolean Searches

- Logical connectives are used extensively in searches of large collections of information.
  - Example: indexes of Web pages.

- AND - used to match records that contain both of two search terms.
- OR - used to match one or both of two search terms.
- NOT - used to exclude a particular search term.

- Read about: Web Page Searching

Applications: Logic Puzzles

- Puzzles (important job interview question) that can be solved using logical reasoning

- [Sm78] Smullyan: An island that has two kinds of inhabitants.
  - knights, who always tell the truth.
  - knaves, who always lie.
- You encounter two people A and B.
- What are A and B if:
  - A says "B is a knight" and
  - B says "The two of us are opposite types?"

Example 1:

- p: A is a knight $\neg$p: A is a knave
- q: B is a knight $\neg$q: B is a knave

- Consider the possibility that A is a knight;
  - So, p is true. And he is telling truth.
  - So, q is true. So, A and B are the same type.

- However, if B is a knight, then B 's statement that A and B are of opposite types, the statement $(p \wedge \neg q) \vee (\neg p \wedge q)$, would have to be true, which it is not, because A and B are both knights. Consequently, we can conclude that A is not a knight, that is, that p is false.

Example 1: Solution (cont..)

- Consider the possibility that A is a knave,
  - everything a knave says is false; q is true, is a lie.
  - So, q is false. B is also a knave.
  - B 's statement that A and B are opposite types is a lie, which is consistent with both A and B being knaves.
- We can conclude that both A and B are knaves.

Example 2:

- A father tells his two children, a boy and a girl, to play in their backyard without getting dirty.
- However, while playing, both children get mud on their foreheads. When the children stop playing, the father says "At least one of you has a muddy forehead," and then asks the children to answer "Yes" or "No" to the question: "Do you know whether you have a muddy forehead?"
- The father asks this question twice. What will the children answer each time this question is asked, assuming that a child can see whether his or her sibling has a muddy forehead, but cannot see his or her own forehead?
- Assume that both children are honest and that the children answer each question simultaneously.

Example 2:

Solution: S denotes "Son has a muddy forehead" and D denotes " Daughter has a muddy forehead". The father states that $S \vee D$ is True. Boy can know D is True but can't know S. Girl can know D is True but can't know S. So no for the first time. After that they can conclude that both D and S are True. Since one of them will say yes for the first time if one of D and S is not True.

Example 3:

6. Determine whether these system specifications are consistent:
   "the diagnostic message is stored in the buffer or it is retransmitted"
   "the diagnostic message is not stored in the buffer"
   "if the diagnostic message is stored in the buffer, then it is retransmitted"

Solution: p denotes "the diagnostic message is stored in the buffer", q denotes "the diagnostic message is retransmitted". Then the specifications can be written as $p \vee q$, $\neg p$ and $p \rightarrow q$. $\neg p$ is True, so p is False. $p \vee q$ is True, so q is True. So $p \rightarrow q$ is True. They are consistent.

Propositional Satisfiability

- A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true.
- When no such assignments exists, that is, when the compound proposition is false for all assignments of truth values to its variables, the compound proposition is unsatisfiable.

- A truth table can be used to determine whether a compound proposition is satisfiable, or equivalently, whether its negation is a tautology.

De Morgan's laws

De Morgan's laws state that:

The negation of an **and** proposition is logically equivalent to the **or** proposition in which each component is negated.

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

The negation of an **or** proposition is logically equivalent to the **and** proposition in which each component is negated.

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

Propositional Equivalences

Constructing New Logical Equivalences

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

  Solution:

  $\neg(p \rightarrow q) \equiv \neg(\neg p \vee q)$ *by example discussed in slide 66*

  $\equiv \neg(\neg p) \wedge \neg q$ *by the second De Morgan law*

  $\equiv p \wedge \neg q$ *by the double negation law*

- *Example: Show that* $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

  Solution: To show that this statement is a tautology, we will use logical equivalences to demonstrate that it is logically equivalent to T.

  $(p \wedge q) \rightarrow (p \vee q) \equiv \neg(p \wedge q) \vee (p \vee q)$ *by example already discussed*

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

  $\equiv (\neg p \vee p) \vee (\neg q \vee q)$ *by the associative and communicative law for disjunction*

  $\equiv T \vee T$

  $\equiv T$

- *Note: The above examples can also be done using truth tables.*

Applying De-Morgan’s Law

Question: Negate the following compound Propositions

1. John is six feet tall and he weights at least 200 pounds.

2. The bus was late or Tom’s watch was slow.

Applying De-Morgan’s Law

Question: Negate the following compound Propositions

1. John is six feet tall and he weights at least 200 pounds.

2. The bus was late or Tom’s watch was slow.

Solution

a) John is not six feet tall or he weighs less than 200 pounds.

b) The bus was not late and Tom’s watch was not slow.

Inequalities and De Morgan's Laws

Question Use De Morgan's laws to write the negation of

$$-1 < x \leq 4$$

Solution: The given proposition is equivalent to

$$-1 < x \quad \text{and} \quad x \leq 4,$$

By De Morgan's laws, the negation is

$$-1 \geq x \quad \text{or} \quad x > 4.$$

Example

Show that the proposition form $p \vee \neg p$ is a tautology and the proposition form $p \wedge \neg p$ is a contradiction.

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

Exercise: If *t* is a tautology and *c* is contradiction, show that $p \vee t \equiv p$ and $p \wedge c \equiv c$?

Laws of Logic

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

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

Laws of Logic

4. Identity laws

   $p \wedge t \equiv p$; $p \vee c \equiv p$

5. Negation laws

   $p \vee \neg p \equiv t$; $p \wedge \neg p \equiv c$

6. Double negation law

   $\neg(\neg p) \equiv p$

7. Idempotent laws

   $p \wedge p \equiv p$; $p \vee p \equiv p$

Laws of Logic

8. Universal bound laws

$p \vee t \equiv t$; $p \wedge c \equiv c$

9. Absorption laws

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

10. Negation of *t* and *c*

$\neg t \equiv c$; $\neg c \equiv t$

Exercise

Using laws of logic, show that

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

Solution

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

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

$\equiv (p \vee \neg q) \wedge (p \vee q)$, (by double negative law)

$\equiv p \vee (\neg q \wedge q)$, (by distributive law)

$\equiv p \vee (q \wedge \neg q)$, (by the commutative law)

$\equiv p \vee c$, (by the negation law)

$\equiv p$, (by the identity law)

Skill in simplifying proposition forms is useful in constructing logically efficient computer programs and in designing digital circuits.

Exercise

Prove that $\neg[r \vee (q \wedge (\neg r \rightarrow \neg p))] \equiv \neg r \wedge (p \vee \neg q)$

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

$\equiv \neg r \wedge \neg(q \wedge (\neg r \rightarrow \neg p))$, De Morgan's law

$\equiv \neg r \wedge \neg(q \wedge (\neg\neg r \vee \neg p))$, Conditional rewritten as disjunction

$\equiv \neg r \wedge \neg(q \wedge (r \vee \neg p))$, Double negation law

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

$\equiv \neg r \wedge (\neg q \vee (\neg r \wedge p))$, De Morgan's law, double negation

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

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

$\equiv (\neg r \wedge \neg q) \vee (\neg r \wedge p)$, Idempotent law

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

$\equiv \neg r \wedge (p \vee \neg q)$, Commutative law