Mat2033 - Discrete Mathematics

Logic and Bit Operations

Computers represent information using bits. A bit has two possible values, namely, 0 and 1. This meaning of the word bit comes from binary digit, since zeros and ones are the digits used in binary representations of number

A bit can be used to represent a truth value, since there are two truth values, namely, true and false. We will use a 1 bit to represent true and a 0 bit to represent false. That is, 1 represents T (true), 0 represents F (false). A variable is called a Boolean Variable if its value is either true or false.

Consequently, a Boolean Variable can be represented using a bit.

Computer bit operations correspond to the logical connectives. By replacing true by ‹1› and false by a ‹0› in the truth tables for the operators $\wedge$, $\vee$, and $\oplus$, the tables shown in below Table for the corresponding bit operations are obtained. We will also use the notation OR, AND, and XOR for the operators $\vee$, $\wedge$, and $\oplus$, as is done in various programming languages.

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

TABLE 7: Tables for the bit operators OR, AND and XOR.

x	y
0	0
0	1
1	0
1	1

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

TABLE 7: Tables for the bit operators OR, AND and XOR.

x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

TABLE 7: Tables for the bit operators OR, AND and XOR.

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

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

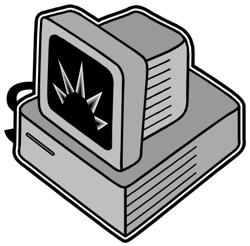
TABLE 7: Tables for the bit operators OR, AND and XOR.

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

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.

We can extend bit operations to bit strings. We define the bitwise OR, bitwise AND, and bitwise XOR of two strings of the same length to be the strings that have as their bits the OR, AND, and XOR of the corresponding bits in the two strings, respectively. We use the symbols $\vee$, $\wedge$, and $\oplus$ to represent the bitwise OR, bitwise AND, and bitwise XOR operations, respectively.

Bitwise operators



`a&b` AND $\wedge$

```
 1101 1001
 1110 0100
 ---------
 1100 0000
```

`a|b` OR $\vee$

```
 1101 1001
 1110 0100
 ---------
 1111 1101
```

`a^b` XOR $\oplus$

```
 1101 1001
 1110 0100
 ---------
 0011 1101
```

16

<u>Example:</u> Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 01 1011 0110 and 11 0001 1101.

<u>Solution:</u>

16

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

Solution:

$$\begin{array}{ccc} 01 & 1011 & 0110 \\ 11 & 0001 & 1101 \\ \hline \end{array}$$

16

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

Solution:

$$\begin{array}{rl} 01\ 1011\ 0110 & \\ 11\ 0001\ 1101 & \\ \hline 11\ 1011\ 1111 & \text{bitwise OR} \end{array}$$

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

Solution:

$$
\begin{array}{lll}
01 & 1011 & 0110 \\
11 & 0001 & 1101 \\
\hline
\end{array}
$$

01 0001 0100 bitwise AND

16

<u>Example:</u> Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 01 1011 0110 and 11 0001 1101.

<u>Solution:</u>

$$\begin{array}{r} 01\ 1011\ 0110 \\ 11\ 0001\ 1101 \\ \hline \end{array}$$

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 occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. Finally, a proposition that is neither a tautology nor a contradiction is called a contingency. The following exp. illustrates these types of propositions.

Table 1: Examples of Tautology and a Contradiction.

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

Tautology

Tautology - a compound proposition that is always true.

$(p \to q) \vee p$

p	q	$p \to q$	$(p \to q) \vee p$
T	T	T	T
T	F	F	T
F	T	T	T
F	F	T	T

Contradiction

Contradiction - a compound proposition that is always false.

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

Contingency

A contingency is neither a tautology nor a contradiction.

$p \rightarrow (p \wedge q)$

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

Logical Equivalances

Compound propositions that have the same truth values in all possible cases are called <u>logically equivalent</u>

<u>Definition 2</u>: The propositions p and q are called <u>logically equivalent</u> if $p \leftrightarrow q$ is a tautology. The notation $p \Leftrightarrow q$ denotes that p and q are logically equivalent.

Logical Equivalence

Compound propositions that always have the same truth value are called logically equivalent.

$$\Leftrightarrow$$

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

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

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$	
p	q
T	T
T	F
F	T
F	F

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

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

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

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

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

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

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

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

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

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

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

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

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

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$						
p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Example: Show that the propositions $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Example: Show that the propositions $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Solution:

p	q
T	T
T	F
F	T
F	F

Example: Show that the propositions $p \to q$ and $\neg p \vee q$ are logically equivalent.

Solution:

p	q	$\neg p$
T	T	F
T	F	F
F	T	T
F	F	T

<u>Example:</u> Show that the propositions $p \to q$ and $\neg p \vee q$ are logically equivalent.

<u>Solution:</u>

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

Example: Show that the propositions $p \to q$ and $\neg p \vee q$ are logically equivalent.

Solution:

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

- <u>Note:</u> If a compound proposition involves n propositions then 2^n
- rows are required.

- The following tables contains some important equivalances. In these equivalances, T denotes any proposition that is always true and F denotes any proposition that is always false

Logical Equivalences

$p \wedge \mathrm{T} \Leftrightarrow p$ $p \vee \mathrm{F} \Leftrightarrow p$	Identity laws	`x*1 = x` `x+0 = x`
$p \vee \mathrm{T} \Leftrightarrow \mathrm{T}$ $p \wedge \mathrm{F} \Leftrightarrow \mathrm{F}$	Domination laws	`x*0 = 0`
$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$	Idempotent laws	
$\neg(\neg p) \Leftrightarrow p$	Double negation law	`-(-x)= x`

Logical Equivalences

$p \vee q \Leftrightarrow q \vee p$ $p \wedge q \Leftrightarrow q \wedge p$	Commutative laws	`x+y = y+x` `x*y = y*x`
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	Associative laws	
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributive laws	
$\neg(q \wedge r) \Leftrightarrow \neg q \vee \neg r$ $\neg(q \vee r) \Leftrightarrow \neg q \wedge \neg r$	DeMorgan's laws	

Logical Equivalences

$$p \vee \neg p \Leftrightarrow \mathrm{T}$$

$$p \wedge \neg p \Leftrightarrow \mathrm{F}$$

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

Note: that De Morgan's laws extend to

$$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \Leftrightarrow (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n)$$

and

$$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Leftrightarrow (\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n)$$

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

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

Solution:

$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)$ 2. De Morgan's Law

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

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad \text{2. De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad \text{1. De Morgan's Law}$$

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

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad \text{2. De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad \text{1. De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double Negation Law}$$

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

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad \text{2. De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad \text{1. De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double Negation Law}$$

$$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{Distributive Law}$$

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

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad \text{2. De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad \text{1. De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double Negation Law}$$

$$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{Distributive Law}$$

$$\Leftrightarrow F \vee (\neg p \wedge \neg q) \quad \text{since } \neg p \wedge p \Leftrightarrow F$$

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

Solution:

$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)$ 2. De Morgan's Law

$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q]$ 1. De Morgan's Law

$\Leftrightarrow \neg p \wedge (p \vee \neg q)$ Double Negation Law

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

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

$\Leftrightarrow (\neg p \wedge \neg q) \vee F$ Law of disjunction

$\Leftrightarrow \neg p \wedge \neg q$ Identity Law

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

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

Solution:

$$(p \wedge q) \rightarrow (p \vee q) \Longleftrightarrow \neg(p \wedge q) \vee (p \vee q)$$

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

Solution:

$$(p \wedge q) \rightarrow (p \vee q) \Longleftrightarrow \neg(p \wedge q) \vee (p \vee q)$$

$$\Longleftrightarrow (\neg p \vee \neg q) \vee (p \vee q) \quad \text{1. De Morgan's law}$$

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

Solution:

$$(p \wedge q) \rightarrow (p \vee q) \Longleftrightarrow \neg(p \wedge q) \vee (p \vee q)$$

$$\Longleftrightarrow (\neg p \vee \neg q) \vee (p \vee q)$$ 1. De Morgan's law

$$\Longleftrightarrow (\neg p \vee p) \vee (\neg q \vee q)$$ associative and commutative laws for disjunction

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

Solution:

$$
\begin{aligned}
(p \wedge q) \rightarrow (p \vee q) &\Longleftrightarrow \neg(p \wedge q) \vee (p \vee q) \\
&\Longleftrightarrow (\neg p \vee \neg q) \vee (p \vee q) && \text{1. De Morgan's law} \\
&\Longleftrightarrow (\neg p \vee p) \vee (\neg q \vee q) && \text{associative and commutative laws for disjunction} \\
&\Longleftrightarrow T \vee T \\
&\Longleftrightarrow T && \text{Domination Law}
\end{aligned}
$$

Implication
$p \rightarrow q$

- "if p, then q"
- "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"
- "q when p"
- "a necessary condition for p is q"
- "a sufficient condition for q is p"
- "q follows from p"
- "q, it is sufficient that p"
- "q, it is sufficient to p"
- "p, it is necessary that q"
- "it is necessary to q, p"

Example

Express these system specifications using the propositions p "The message is scanned for viruses" and q "The message was sent from an unknown system" together with logical connectives.

a) "The message is scanned for viruses whenever the message was sent from an unknown system."

b) "The message was sent from an unknown system but it was not scanned for viruses."

c) "It is necessary to scan the message for viruses whenever it was sent from an unknown system."

d) "When a message is not sent from an unknown system it is not scanned for viruses."

Example

Express these system specifications using the propositions p "The message is scanned for viruses" and q "The message was sent from an unknown system" together with logical connectives.

a) "The message is scanned for viruses whenever the message was sent from an unknown system."

b) "The message was sent from an unknown system but it was not scanned for viruses."

c) "It is necessary to scan the message for viruses whenever it was sent from an unknown system."

d) "When a message is not sent from an unknown system it is not scanned for viruses."

a) $q \to p$

b) $q \wedge \neg p$

c) $q \to p$

d) $\neg q \to \neg p$