INFORMATION THEORY & CODING

NOTE:

MAKAUT course structure and syllabus of 6th semester has been changed from 2021. Previously **INFORMATION THEORY & CODING** was in 7th semester. This subject has been redesigned and shifted in 6th semester as per present curriculum. Subject organization has been changed slightly. Taking special care of this matter we are providing the relevant MAKAUT university solutions, so that students can get an idea about university questions patterns.

INFORMATION THEORY

Multiple Choice Type Questions

1. Which of the following expression is incorrect? [WBUT 2008, 2011, 2012, 2013]

a) $H(y/x) = H(x, y) - H(x)$ b) $I(x, y) = H(x) - H(y/x)$

c) $H(x, y) = H(x, y) + H(y)$ d) $I(x, y) = H(y) - H(y/x)$

Answer: (d)

2. Entropy represents [WBUT 2008, 2011, 2012, 2014, 2015]

a) amount of information b) rate of information

c) measure of uncertainty d) probability of message

Answer: (c)

3. The entropy of information source is maximum when symbol occurrences are [WBUT 2009, 2014]

a) equiprobable b) different probability

c) both (a) and (b) d) none of these

Answer: (a)

4. Measure of information (m_k) of a message m_k with probability p_k is given by

a) $\log_b(1/p_k)$ b) $\log_b(p_k)$ [WBUT 2009, 2014]

c) $\log_b(1-p_k)$ d) $\log_b(1/1-p_k)$

Answer: (a)

5. The ideal communication channel is defined for a system which has [WBUT 2009, 2011, 2012]

a) Finite *C* b) *BW* = 0 c) *S/N* = 0 d) Infinite *C*

Answer: (d)

6. The channel capacity is a measure of [WBUT 2011]

a) entropy rate

b) maximum rate of information a channel can handle

c) information contents of messages transmitted in a channel

d) none of these

Answer: (b)

7. The capacity of a communication channel with a bandwidth of 4 kHz and 15 SNR is approx [WBUT 2012]

a) 20 kbps b) 16 kbps c) 10 kbps d) 8 kbps

Answer: (b)

8 . Entropy means [WBUT 2013]

a) amount of information b) rate of information

c) measure of uncertainty d) probability of message

Answer: (a)

9. The ideal communication channel is defined for a system which has [WBUT 2013]

a) finite C b) BW = 0 c) S/N = 0 d) infinite C

Answer: (d)

10. Relation between message rate (r) and information rate (R) is [WBUT 2013, 2019]

a) $R = rH$ b) $r = RH$ c) $r = R^2H$ d) $R = r^2H$

Answer: (a)

11. Relation between channel capacity and bandwidth of channel is related as [WBUT 2013, 2017]

a) $C = B(\ln_2(S/N))$ b) $C = B(\ln_2(1+S/N))$

c) $C = B/N$ d) $C = B^2N$

Answer: (b)

12. A source delivers symbols m_1, m_2, m_3 and m_4 with probabilities 1/2, 1/4, 1/8 and 1/8 respectively. The entropy of the system is [WBUT 2013]

a) 1.75 bits/sec b) 1.75 bits/symbol

c) 1.75 symbols d) 1.75 symbol/bit

Answer: (b)

13. The mutual information of a channel with independent input and output is [WBUT 2015]

a) zero b) constant c) variable d) infinite

Answer: (a)

14. 1 decit equals [WBUT 2015]

a) 1 bit b) 3.32 bit c) 10 bits d) none of these

Answer: (b)

15. If a telephone channel has bandwidth 3000Hz and SNR = 20dB then channel capacity is [WBUT 2015]

a) 3 kbps b) 1.19 kbps c) 2.19 kbps d) 19.97 kbps

Answer: (d)

16. For a noiseless channel I(X; Y) is [WBUT 2015]

a) H(X)-H(Y) b) H(Y)-H(X) c) H(X) d) H(X)-H(Y/X)

Answer: (c)

[WBUT 2016]

17. The unit of information is
a) Bit b) Decit c) Nat d) all of these
Answer: (b)

18. For a Lossless channel, the number of non-zero elements in each column is [WBUT 2016]
a) 0 b) 1 c) 2 d) 3
Answer: (b)

[WBUT 2016]

19. Entropy is basically a measure of
a) rate of information b) average information
c) probability of information d) disorder of information
Answer: (a)

20. If $I(x_1)$ and $I(x_2)$ is the information carried by the symbols x_1 and x_2 respectively, then $I(x_1, x_2)$ is equal to [WBUT 2016]
a) $I(x_1)*I(x_2)$ b) $I(x_1)+I(x_2)$ c) $I(x_1)-I(x_2)$ d) $I(x_1)/I(x_2)$
Answer: (b)

21. If L is the average codeword length per symbol and $H(X)$ is the source entropy then which one is more appropriate? [WBUT 2016]
a) $L=H(X)$ b) $L\le H(X)$ c) $L\ge H(X)$ d) None of these
Answer: (c)

22. In the expression of Kraft Inequality, the value of K is given by [WBUT 2017]
a) $K=\sum_{j=1}^{m}2^{-nj}\ge 1$ b) $K=\sum_{j=1}^{m}2^{-nj}\le 1$
c) $K=\sum_{j=1}^{m}2^{-nj}=1$ d) none of these
Answer: (b)

23. The coding efficiency η is given by [WBUT 2017]
a) $\eta=H(X).L$ b) $\eta=H(X)/L$ c) $\eta=L/H(X)$ d) none of these
Answer: (b)

24. The capacity of a communication channel with a bandwidth of 4 kHz and 15 SNR is approx [WBUT 2017]
a) 20 kbps b) 16 kbps c) 10 kbps d) 8 kpbs.
Answer: (b)

25. The unit of information is
a) Bit b) Decit c) Nat [WBUT 2018]
Answer: (d) d) All of these

26. Entropy represents [WBUT 2018]
a) Rate of information
b) Average information
c) Probability of information
d) Disorder of information
Answer: (b)

27. The entropy of information source is maximum when symbol occurrences are
a) Equi-probable
b) Different probability [WBUT 2018]
c) Both (a) and (b)
d) None of these
Answer: (a)

28. The coding efficiency η is given by [WBUT 2018]
a) $\eta = H(X) \cdot \bar{L}$
b) $\eta = H(X) / \bar{L}$
c) $\eta = \bar{L} / H(X)$
d) $\eta =$ none of these
Answer: (b)

29. The capacity of a communication channel with a bandwidth of 4 kHz and 15 SNR is approx. [WBUT 2018]
a) 20 kbps
b) 16 kbps
c) 10 kbps
d) 8 kbps
Answer: (b)

30. A binary memory less source X with two symbols x_1, x_2. The Entropy of source $H(X)$ is maximum when [WBUT 2019]
a) both x_1 and x_2 are equiprobable
b) $x_1 \geq x_2$
c) $x_2 \geq x_1$
d) none of these
Answer: (a)

31. The relation between entropy and mutual information is [WBUT 2019]
a) $I(X; Y) = H(X) - H(X/Y)$
b) $I(X; Y) = H(X/Y) - H(Y/X)$
c) $I(X; Y) = H(X) - H(Y)$
d) $I(X; Y) = H(Y) - H(X)$
Answer: (a)

32. DMS X with two symbols x_1 and x_2 and $P(x_1) = 0.9$, $P(x_2) = 0.1$. Find efficiency and redundancy of this code. [WBUT 2019]
a) 45%, 55%
b) 40%, 80%
c) 46.9%, 53.1%
d) 90%, 90%
Answer: (c)

33. If the SNR of the signal is increased, then the channel capacity [WBUT 2019]
a) is increased
b) is decreased
c) remains constant
d) cannot be determined
Answer: (c)

Short Answer Type Questions

1. a) What is Entropy?
b) Consider a source *X* which produces five symbols with probabilities 1/2, 1/4, 1/8, 1/16 and 1/16. Find the source entropy. **[WBUT 2009]**

Answer:

a) The average information per message of a source is called source entropy or simply entropy. It is denoted by H and

$$H = -\sum_{i=1}^{m} p_i \log_2 p_i \qquad \text{bits} = \sum_{i=1}^{m} p_i \log_2 \frac{1}{p_i} \qquad \text{bits} = \sum_{i=1}^{m} p_i I_i \text{ bits}.$$

where m is the total number of messages in the source and p_i is the probability of occurrence of the i^{th} message. I_i is the information of the i^{th} message. Note that $\sum_{i=1}^{m} p_i = 1$.

b) Source entropy, $H(x)$ is given by

$$H(x) = \sum_{i=1}^{5} p(x_i) \log \left[\frac{1}{p(x_i)} \right]$$

Here, $p(x_1) = \frac{1}{2}, p(x_2) = \frac{1}{4}, p(x_3) = \frac{1}{8}, p(x_4) = p(x_5) = \frac{1}{16}$

So $H(x) = \frac{1}{2}\log_2 \frac{1}{1/2} + \frac{1}{4}\log_2 \frac{1}{1/4} + \frac{1}{8}\log_2 \frac{1}{1/8} + \frac{1}{16}\log_2 \frac{1}{1/16} + \frac{1}{16}\log_2 \frac{1}{1/16}$

$$= \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{1}{8}\log_2 8 + \frac{1}{16}\log_2 16 + \frac{1}{16}\log_2 16$$

$$= \frac{1}{2}\times 1 + \frac{1}{4}\times 2 + \frac{1}{8}\times 3 + \frac{1}{16}\times 4 + \frac{1}{16}\times 4$$

$$= \frac{1}{2} + \frac{1}{2} + \frac{3}{8} + \frac{1}{4} + \frac{1}{4}$$

$$= \frac{15}{8} = 1.875 \text{ bits/symbol}$$

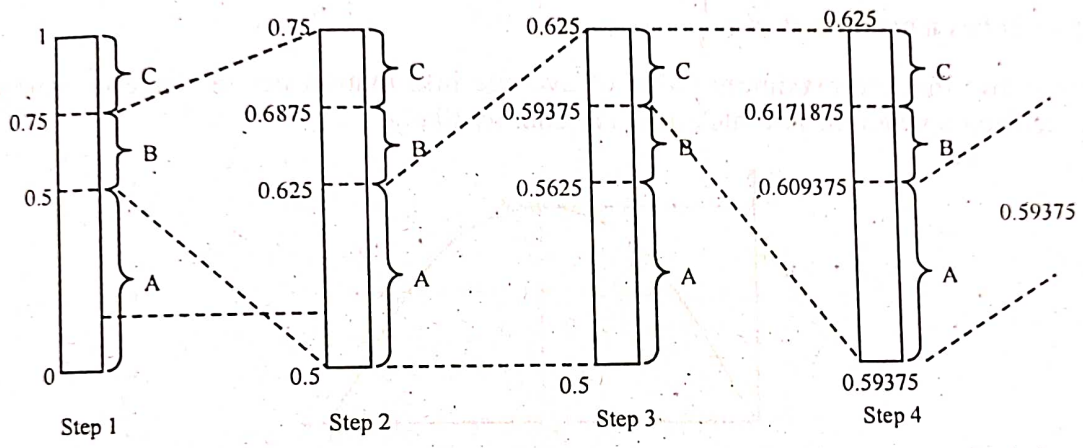
2. a) What are the drawbacks of Prefix coding that lead to the discovery of Arithmetic coding?
b) Let the alphabet consists of only three symbols *A*, *B* and *C* with probabilities of occurrence *P* (*A*) = 0.5, *P* (*B*) = 0.25 and *P* (*C*) = 0.25. Suppose the input symbol stream is *B A C A*, determine the arithmetic code for the stream. **[WBUT 2009]**

Answer:

a) The following drawbacks of prefix coding are observed.

1. In the case of prefix coding, the self-information of the symbols are matched. The codewords thus formed are having lengths as integers. Thus exact matching is not possible unless the self-information is in integral number of bits.
2. When prefix codes are generated using binary tree, each decision always takes one bit. But the average code length may not be exactly one bit.

b) The diagram below shows the steps for the generation of the arithmetic code.



Step 1 shows the probability of occurrence of A, B and C i.e., $P(A)=0.5, P(B)=0.25$ and $P(C)=0.25$. Now the first symbol of the input bit stream BACA is B. The second symbol is A. The variable A corresponds to $(0.5, 0.625)$ as shown in step 2. So the input to step 3 is $(0.59375, 0.625)$. The next symbol is A which corresponds to the interval $(0.59375, 0.625)$. After encoding the last symbol A, we have the interval $(0.59375, 0.609375)$. Hence the arithmetic code for the stream BACA is 0.59375.

3. Prove that the entropy is maximum when the messages are equally likely. **[WBUT 2013]**

Answer:

Since there are two messages this is a binary system and hence $m = 2$

Let one of the messages has probability p. Obviously the other message will have probability $(1-p)$.

The total entropy, $H = p\log\frac{1}{p} + (1-p)\log\frac{1}{(1-p)}$

Putting $\frac{dH}{dp} = 0$, we get

$$-\ell n\, 2 - \log p + \ell n\, 2 + \log(1-p) = 0$$

or, $\log p = \log(1-p)$

or, $p = 1-p$

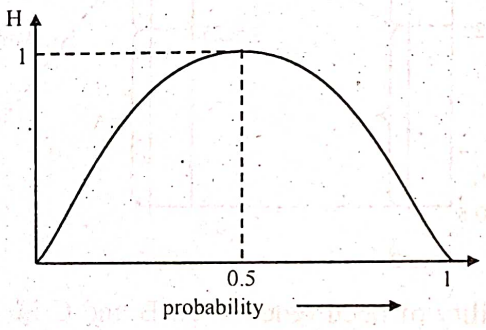
or, $p = \frac{1}{2}$

Thus, the messages are equally likely.

Also, $\frac{\partial^2 H}{\partial p^2} = -\frac{1}{p} - \frac{1}{1-p} < 0$

Hence H has a maxima at $p = \frac{1}{2}$

This shows that the maximum value of average information per message or entropy of source occurs when the two messages are equally likely.



$$H_{max} = \frac{1}{2}\log\frac{1}{(1/2)} + \frac{1}{2}\log\frac{1}{(1/2)} = \frac{1}{2}\log 2 + \frac{1}{2}\log 2 = \log_2 2 = 1 \text{ bit per message}$$

Thus the maximum value of entropy in such a case in 1 bit per message.

4. Consider a source X which produces five symbols with probabilities 1/2, 1/4, 1/8, 1/16 and 1/16. Calculate source entropy. **[WBUT 2013]**

Answer:

Information content of each message as given by

$$I(x_i) = \log_2 \frac{1}{p(x_i)} bit$$

Thus we can write

$$I(x_1) = \log_2 \frac{1}{p(x_1)} = \log_2 \frac{1}{\frac{1}{2}} = \log_2 2 = 1 \text{ bit}$$

$$I(x_2) = \log_2 \frac{1}{\frac{1}{4}} = \log_2 4 = 2 \text{ bits}$$

$$I(x_3) = \log_2 \frac{1}{1/8} = \log_2 8 = 3 \text{ bits}$$

$$I(x_4) = I(x_5) = \log_2 \frac{1}{1/16} = \log_2 16 = 4 \text{ bits}$$

5. Define the channel transition matrix and with suitable example show at least 3 channel transition matrix. **[WBUT 2015]**

Answer:

A DMC is described conveniently in terms of a matrix in which the various transition probabilities are arranged systematically as under. Such a matrix is called channel Matrix, P. Thus

$$P = \begin{bmatrix} P(y_1/x_1) & P(y_2/x_1) \ldots\ldots P(y_n/x_1) \\ P(y_1/x_2) & P(y_2/x_2) \ldots\ldots P(y_n/x_2) \\ \text{----------} & \text{----------} \\ \text{----------} & \text{----------} \\ P(y_1/x_m) & P(y_2/x_m) \ldots\ldots P(y_n/x_m) \end{bmatrix} = P(Y/X)$$

It is to be noted that each row of the channel matrix P corresponds to a fixed channel input and each column of the matrix corresponds to a fixed channel output.

An important property of the channel matrix P is that the sum of the elements along any row of the matrix is always equal to unity. Thus

$$\sum_{j=1}^{n} P(y_k/x_j) = 1 \text{ for all } k$$

These are special channels. A lossless channel is described by a channel matrix with only one non-zero element in each column. A lossless channel is shown below:

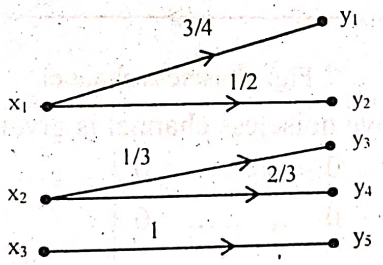


Fig: A lossless channel

The channel matrix of the above lossless channel is given by

$$[P(Y/X)] = \begin{bmatrix} \frac{3}{4} & \frac{1}{4} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & \frac{2}{3} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

In a lossless channel no source information in lost in transmission.

A channel described by a channel matrix with only one non–zero element in each row is called a deterministic channel.

A deterministic channel is shown below:

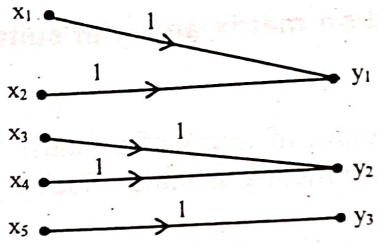


Fig: A deterministic channel

The channel matrix for the above deterministic channel is given by

$$[P(Y/X)] = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

A channel is called noiseless if it is both lossless and deterministic.

A noiseless channel is shown below:

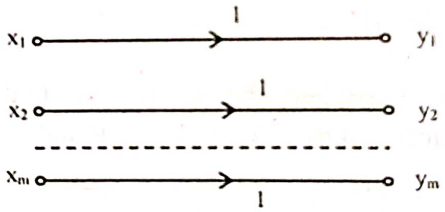


Fig: Noiseless channel

The channel matrix of the above noiseless channel is given by

$$[P(Y/X)] = \begin{bmatrix} 1 & 0 & 0 & \ldots\ldots & 0 \\ 0 & 1 & 0 & \ldots\ldots & 0 \\ \ldots & \ldots & \ldots & \ldots\ldots & \ldots \\ 0 & 0 & 0 & \ldots\ldots & 1 \end{bmatrix}$$

A binary symmetric channel (BSC) is defined by the channel diagram as shown below.

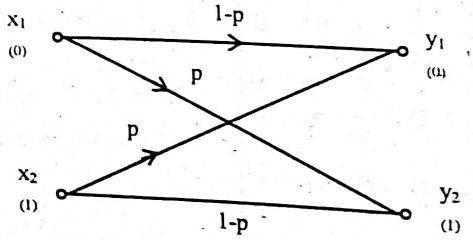


Fig: binary symmetric channel

The channel matrix of a binary symmetric channel is given by

$$[P(Y/X)]=\begin{bmatrix}1-p & p\\ p & 1-p\end{bmatrix}$$

6. $P(x_1)=0.4,\ P(x_2)=0.17,\ P(x_3)=0.18,\ P(x_4)=0.1$ **and** $P(x_5)=0.15$ **for 5 symbol** x_1, x_2, x_3, x_4 **and** x_5**. Construct a Shannon Fano code and find out its efficiency.** **[WBUT 2015]**

Answer:

$p(x_1)=0.4, p(x_2)=0.17, p(x_3)=0.18, p(x_4)=0.1$ and $p(x_5)=0.15$

Symbol	Probability	Encoded message		
x_1	0.4	0		
x_1	0.18	1	0	0
x_1	0.17	1	0	1
x_1	0.15	1	1	0
x_1	0.1	1	1	1

Hence, $c_1=0, c_2=101, c_3=100, c_4=111$ and $c_5=110$

Average word length $\bar{L}=1\times0.4+3\times0.17+3\times0.18+3\times0.1+3\times0.15$

$=2.2$ symbols/message

Entropy, $H(x)=-\left[\begin{array}{r}0.4\log_2 0.4+0.17\log_2 0.17+0.18\log_2 0.18\\ +0.1\log_2 0.1+0.15\log_2 0.15\end{array}\right]=2.1492$

≈ 2.15 bits/message

So, coding efficiency $=\eta=\dfrac{H(x)}{\bar{L}}=\dfrac{2.15}{2.2}=0.9772=97.7\%$

7. Explain Shannon Hartley law regarding channel capacity. **[WBUT 2015]**
What is mutual information? **[WBUT 2015]**

OR,

What is meant by mutual information? Prove that $I(X,Y)=H(X)-H(X/Y)$**, where notations have their usual meaning.** **[WBUT 2019]**

Answer:

1st Part:

Let S = Signal power in watts

N = Noise power in watts

Let us assume a load of 1 ohm.

Then Root mean square value of the received signal is $V_r=\sqrt{S+N}$ *volts*

RMS values of the noise voltage is $V_n=\sqrt{N}$ volts

The number of distinct levels that can be distinguished without errors is given by μ where

$$\mu = \frac{\sqrt{S+N}}{\sqrt{N}} = \sqrt{1+\frac{S}{N}}$$

Now let us consider a discrete channel having μ states and uniform signaling speed s where $s = \frac{1}{t_0}$ and t_0 is the duration per state.

A received message of length T will consist of $T/t_0 = sT$ symbols where each symbol is having one of the μ possible states.

The number of different messages = $N = \mu^{sT}$

Now channel capacity C is $C = \underset{T\to\infty}{Lt} \frac{1}{T}\log_2 N = \underset{T\to\infty}{Lt} \log_2 \mu^{sT}$

$$= \underset{T\to\infty}{Lt}\left(\frac{1}{T}\right)(sT)\log_2 \mu = s\log_2 \mu$$

A system with bandwidth B can transmit a maximum of 2B pulses per second. Thus

$s = 2B$

Hence $C = 2B\log_2\sqrt{1+\frac{S}{N}}$

or, $C = B\log\left(1+\frac{S}{N}\right)$

This is Hartley–Shannon's law.

2nd Part: ***Refer to Question No. 3(b) of Long Answer Type Questions.***

8. a) What do you mean by Information rate? Explain. **[WBUT 2016]**

Answer:

If a message source having entropy 'H' generates messages at the rate of 'r' messages per second, then the rate of information 'R' is defined as the average number of bits of information per second.

Then

$$R = \frac{\text{Average number of information}}{\text{Second}}$$

$$= \frac{\text{Average number information}}{\text{Number of messages}} \times \frac{\text{Number of messages}}{\text{Second}}$$

$$= H \times r$$

where H = Entropy

Thus $R = rH$ bits per second

b) What is a Discrete Memoryless Channel (DMC)? Explain. **[WBUT 2016]**

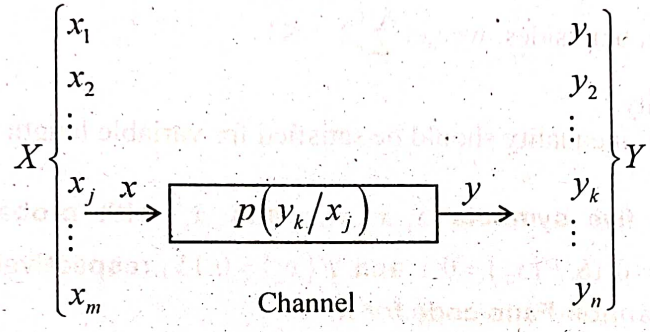
Answer:

Discrete Memoryless Channel (DMC)

A discrete memoryless channel is a channel in which both the source alphabet and receiver alphabet are of finite sizes and the current output symbol depends only on the current input symbol and not on the previous ones.

Let us consider a DMC channel which accepts an input signal xj from a source alphabet X and in response it emits a symbol yK from the receiver alphabet Y. We can form a statistical model of the channel in which X and Y are random variables. Y is a noisy version of X.

A DMC is shown in the diagram below:



Thus the input alphabet is $X = \{x_1, x_2, ...x_j ....x_m\}$ and the output alphabet is Y = $\{y_1 y_2 ....y_K ....y_n\}$. Each possible input-to-output path is characterized with a conditional probability P(yk / xj) where P(yk / xj) is the conditional probability of obtaining output Y= yK given that the channel input is X = xj. This conditional probability P(yk / xj) is called the channel transition probability.

9. What is Kraft inequality? Prove that Kraft inequality should be satisfied for variable length source coding. **[WBUT 2017]**

Answer:

1st part:

An instantaneous code satisfies the Kraft inequality. It states that we can construct an instantaneous binary code with word lengths $\ell_o, \ell_1, ...\ell_{m-1}$ in a discrete memoryless source (DMS) if and only if these lengths satisfy the condition

$$\sum_{i=0}^{m-1} 2^{-\ell_i} \leq 1$$

Thus Kraft inequality provides a necessary and sufficient condition for the existence of an instantaneous binary code.

Kraft inequality has the limitation that it does not show us how to obtain the code words. It also can not say if any code that satisfies the inequality is automatically uniquely decodable.

2nd part:

Let us consider a binary variable length code. The lengths of the code words are say $\ell_0, \ell_1, \cdots \ell_{m-1}$ where m is the number of code words. We may represent the code by a code tree. Let $\ell_{max} = \max\{\ell_0, \ell_1 \cdots \ell_{m-1}\}$. We expand the tree so that all branches have the depth ℓ_{max}. A code word at depth ℓ_i has $2^{\ell_{max}-\ell_i}$ leaves underneath itself at depth ℓ_{max}. The sets of leaves under code words are disjoint. Obviously, the total number of leaves under code words are less than or equal to $2^{\ell_{max}}$. Thus we have

$$\sum_{i=0}^{m-1} 2^{\ell_{max}-\ell_i} \le 2^{\ell_{max}}$$

By canceling $2^{\ell_{max}}$ on both sides, we get $\sum_{i=0}^{m-1} 2^{-\ell_i} \le 1$

This is Kraft inequality.

This proves that Kraft inequality should be satisfied for variable length source coding.

10. A DMS X has five symbols x_1, x_2, x_3, x_4 and x_5 with probability $P(x_1) = 0.4$, $P(x_2) = 0.17, P(x_3) = 0.18, P(x_4) = 0.1$ and $P(x_5) = 0.15$, respectively.

a) Construct the Shannon-Fano code for X.

b) Calculate the efficiency of the code. **[WBUT 2017]**

Answer:

$P(x_1) = 0.4, P(x_2) = 0.17, P(x_3) = 0.18, P(x_4) = 0.1$ and $P(x_5) = 0.15$

Symbol	Probability	Encoded message
x_1	0.4	0
x_3	0.18	1 0 0
x_2	0.17	1 0 1
x_5	0.15	1 1 0
x_4	0.1	1 1 1

Hence, $C_1 = 0$, $C_2 = 101$, $C_3 = 100$, $C_4 = 111$ and $C_5 = 110$

Average word length, $L = 1 \times 0.4 + 3 \times 0.17 + 3 \times 0.18 + 3 \times 0.1 + 3 \times 0.15$

$= 2.2$ symbols/message

Entropy,

$H(x) = -[0.4 \log_2 0.4 + 0.17 \log_2 0.17 + 0.18 \log_2 0.18 + 0.1 \log_2 0.1 + 0.15 \log_2 0.15]$

$= 2.1492$ bits/message

$\simeq 2.15$ bits/message

So, coding efficiency, $\eta = \frac{H(x)}{L} = \frac{2.15}{2.2} = 0.9772 = 97.72\%$

11. Give that AWGN channel with 4 kHz bandwidth and the noise power spectral density $\eta/2 = 10^{12}$ W/Hz. The signal power required at the receiver is 0.1 mW. Calculate the capacity of the channel. **[WBUT 2017, 2019]**

Answer:

The channel capacity, C, is given by $C = B\log_2\left(1+\frac{S}{N}\right)$

where B = Bandwidth

$\frac{S}{N}$ = Signal to noise ratio

Here, B = 4 kHz $= 4\times10^3$ Hz

S = signal power = 0.1 mw $= 10^{-4}$W

Noise power $= N = \frac{\eta}{2}\times 2B = 10^{-12}\times 2\times 4\times 10^3 - 8\times 10^{-9}$ W

So, $\frac{S}{N} = \frac{10^{-4}}{8\times10^{-9}} = 12,500$

Here $\log_2\left(1+\frac{S}{N}\right) = \log_2(1+12,500) = 3.32\log_{10}(12,501) = 3.32\times 4.0969 = 13.601$

So, $C = B\log_2\left(1+\frac{S}{N}\right) = 4\times10^3\times13.601 = 54.4$

12. Consider a binary memoryless source X with two symbols x_1 and x_2. Prove that $H(x)$ is maximum when both x_1 and x_2 are equiprobable. **[WBUT 2019]**

Answer:

Let, $P(x_1) = \alpha$, then $P(x_2 = 1-\alpha)$

$$H(X) = -\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha)$$

$$\frac{dH(X)}{d\alpha} = \frac{d}{d\alpha}[-\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha)]$$

Suing the relation

$$\frac{d}{d\alpha}\log_b y = \frac{1}{y}\log_b e\frac{dy}{dx}$$

We obtain

$$\frac{dH(X)}{d\alpha} = -\log_2\alpha + \log_2(1-\alpha) = \log_2\frac{1-\alpha}{\alpha}$$

The maximum value of $H(X)$ requires that

$$\frac{dH(X)}{d\alpha} = 0$$

That is $\frac{1-\alpha}{\alpha} = 1 \Rightarrow \alpha = \frac{1}{2}$

Thus, when $P(x_1) = P(x_2) = \frac{1}{2}$, $H(X)$ is maximum and is given by

$$H(X) = \frac{1}{2}\log_2 2 + \frac{1}{2}\log_2 2 = 1 \text{ b/symbol.}$$

13. What is the advantage of variable length coding over fixed length coding? **[WBUT 2019]**

Answer:

Variable-length codes (VLCs) are widely used in media transmission. Compared to fixed-length codes (FLCs), VLCs can represent the same message with a lower bit rate, thus having a better compression performance. But inevitably, VLCs are very sensitive to transmission errors. In this work, based on the trellis representation for VLCs and the BCJR algorithm, we present a variable-length soft-decision decoder utilizing bit-wise channel reliability information and achieving a better error robustness in contrast to hard-decision decoding. Given the application of VLCs in audio coding showing both source correlation and variable block lengths, a strong dependency of performance is observed for both. Therefore, we point out tradeoffs of (soft-decision) decoded FLCs and VLCs depending on quantization bit rate, source correlation, and block length. We find that VLCs over AWGN channels are only recommended for very low source correlation in combination with very short block lengths and soft-decision decoding.

14. Verify the following expression: **[WBUT 2019]**

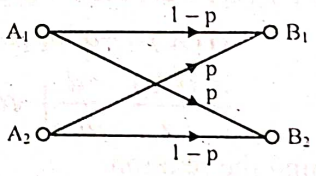
$$C_S = 1 + p\log_2 p + (1-p)\log_2(1-p),$$

where, C_S is the channel capacity of a BSC.

Answer:

The BSC is shown below where A_1 and A_2 are the inputs and B_1 and B_2 are the outputs.

The channel matrix is $P(B \mid A) = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$



Channel capacity, $C = \log_2 S - H$

where, S = No. of inputs

and H = Entropy

For BSC, $S = 2$ and $H = (1-p)\log_2 \frac{1}{(1-p)} + p\log_2 \frac{1}{p}$

So, $$C = \log_2 2 - (1-p)\log_2 \frac{1}{(1-p)} - p\log_2 \frac{1}{p}$$

$$= 1 + (1-p)\log_2(1-p) + p\log_2 p$$

$$= 1 + p\log_2 p + (1-p)\log_2(1-p)$$

Long Answer Type Questions

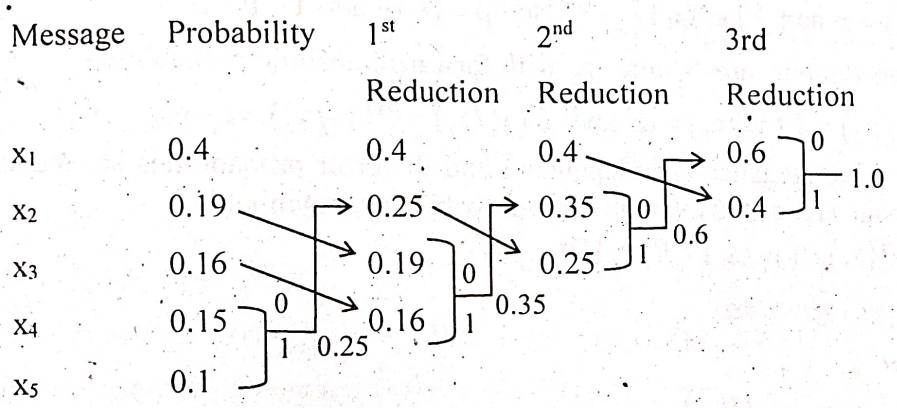
1. A discrete memoryless source has five symbols x_1, x_2, x_3, x_4 and x_5 with probabilities of occurrence

$P(x_1)=0.4,\ P(x_2)=0.19,\ P(x_3)=0.16,\ P(x_4)=0.15$ **and** $P(x_5)=0.1$

Construct the Huffman Code and determine **[WBUT 2008, 2014]**

a) entropy
b) average code length
c) code efficiency

Answer:



Thus the Huffman codes are formed and the code length are as follows:

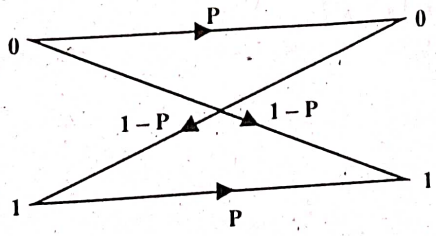
Code	Code length
$c_1 = 1$	1
$c_2 = 000$	3
$c_3 = 001$	3
$c_4 = 010$	3
$c_5 = 011$	3

Hence average code length $\bar{L} = 0.4\times1+0.19\times3+0.16\times3+0.15\times3+0.1\times3$
$= 2.2$ symbols / message.

Source entropy $H(X) = -[0.4\log0.4+0.19\log0.19+0.16\log0.16$
$+0.15\log0.15+0.1\log0.1]=2.15$ bits/message.

Thus, coding efficiency, $\eta = \frac{H(X)}{\bar{L}} = \frac{2.15}{2.2} = 0.977 = 97.7\%.$

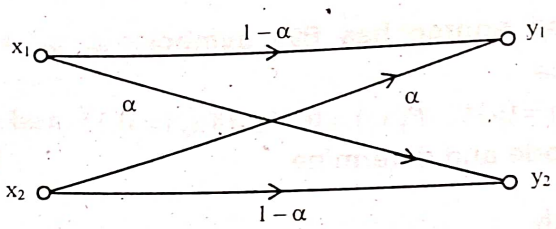
2. For a *BSC* shown below find the channel capacity of p = 0.9. Derive the formula that you have used.



[WBUT 2009, 2012, 2014]

Answer:

The figure below shows a binary symmetric channel (BSC)



The source symbols are x_1 and x_2 with probabilities

$P(x_1) = p$ and $P(x_2) = 1-p$. Also, $p = 1-\alpha$ and $1-p = \alpha$.

The destination symbols are y_1 and y_2 with forward transition probabilities

$$P(y_1/x_2) = P(y_2/x_1) = \alpha \text{ and } P(y_1/x_1) = P(y_2/x_2) = 1-\alpha.$$

Here the errors are statistically independent and the error probabilities are the same for both the symbols. Hence the average error probability per symbol is

$$\begin{aligned} P_e &= P(x_1)P(y_2/x_1) + P(x_2)P(y_1/x_2) \\ &= p\alpha + (1-p)\alpha \\ &= \alpha \end{aligned}$$

The destination entropy $H(Y)$ is

$$\begin{aligned} H(Y) &= P(y_1)\log\frac{1}{P(y_1)} + P(y_2)\log\frac{1}{P(y_2)} \\ &= P(y_1)\log\frac{1}{P(y_1)} + \left[1-P(y_1)\right]\log\frac{1}{1-P(y_1)} \\ &= \Omega\left[P(y_1)\right] \end{aligned}$$

where Ω is the horse-shoe function defined by

$$\Omega(x) = x\log\frac{1}{x} + (1-x)\log\frac{1}{1-x}.$$

The probability of the output symbol y is

$$\begin{aligned} P(y_1) &= \sum_x P(x_1, y_1) \\ &= P(y_1/x_1)P(x_1) + P(y_1/x_2)P(x_2) \\ &= (1-\alpha)p + \alpha(1-p) \\ &= \alpha + p - 2\alpha p \end{aligned}$$

Hence the noise entropy is

$$H(y/x)=\sum_{j=1}^{n}\sum_{k=1}^{m}P(x_k,y_j)\log\frac{1}{P(y_j/x_k)}$$

$$=\sum_{k=1}^{2}P(x_k)\left[\sum_{j=1}^{2}P(y_j/x_k)\log\frac{1}{P(y_j/x_k)}\right]$$

$$=P(x_1)P(y_1/x_1)\log\frac{1}{P(y_1/x_1)}+P(x_1)P(y_2/x_1)\log\frac{1}{P(y_2/x_1)}$$

$$+P(x_2)P(y_1/x_2)\log\frac{1}{P(y_1/x_2)}+P(x_2)P(y_2/x_2)\log\frac{1}{P(y_2/x_2)}$$

$$=p(1-\alpha)\log\frac{1}{1-\alpha}+p\alpha\log\frac{1}{\alpha}+(1-p)\alpha\log\frac{1}{\alpha}+(1-p)(1-\alpha)\log\frac{1}{1-\alpha}$$

$$=(1-\alpha)\log\frac{1}{1-\alpha}+\alpha\log\frac{1}{\alpha}$$

$$=\Omega(\alpha)$$

Thus the noise entropy, $H(Y/X)$, for a BSC is given by $H(Y/X)=\Omega(\alpha)$.

For a Binary symmetric channel, $P(y_1)=\alpha+p-2\alpha p$

and $H(Y)=\Omega[P(y_1)]$

So, $H(Y)=\Omega(\alpha+p-2\alpha p)=$ Destination entropy.

Also, $H(Y/X)=$ Noise entropy $=\Omega(\alpha)$

Hence, mutual information $I(X;Y)$ is given by

$$I(X;Y)=H(Y)-H(Y/X)$$

$$=\Omega(\alpha+p-2\alpha p)-\Omega(\alpha)$$

This shows that the information transfer over a BSC depends on both the error probability α and source probability p.

If the noise is small, then $\alpha<<1$ and $I(X;Y)\approx\Omega(p)=H(X)$ i.e. the mutual information is almost equal to the source entropy, $H(X)$.

If the noise is very large, $\alpha=\frac{1}{2}$ and $I(X;Y)=0$.

The term $\Omega(\alpha+p-2\alpha p)$ reaches a maximum value of 1 when $\alpha+p-2\alpha p=\frac{1}{2}$. This condition is satisfied by any α if $p=\frac{1}{2}$.

This means that equally likely binary input symbols maximize the information transfer. Hence the channel capacity of a BSC is

$$C = 1 - \Omega(\alpha).$$

$$\Omega(\alpha) = (1-\alpha)\log\frac{1}{1-\alpha} + \alpha\log\frac{1}{\alpha}$$

In the given problem, $1-\alpha = 0.9$

and $\alpha = 0.1$

So, $$\Omega(\alpha) = (1-0.1)\log\frac{1}{0.9} + 0.1\log\frac{1}{0.1}$$

$$= 0.9\log\frac{1}{0.9} + 0.1\log\frac{1}{0.1}$$

$$= 0.9\log_2 1.11 + 0.1\log_2 10$$

$$= 0.1355 + 0.3322 = 0.4677$$

Hence $C = 1 - \Omega(\alpha) = 1 - 0.4677 = 0.5323$ bits/symbol.

3. a) A code is composed of dots and dash. Assume that the dash is 3 times as long as the dot and has a one-third the probability of occurrence –

i) calculate the information in a dot and that in dash.

ii) calculate the average information in the dot-dash code.

iii) assume that dot lasts for 10ms and that this same time interval is allowed between symbols. Calculate the average rate of information transmission.

[WBUT 2010]

Answer:

Let the probabilities of a dot and a dash are p_1 and p_2 respectively.

Given, $p_1 = 3p_2$.

Thus if $p_2 = 0.25$ then $p_1 = 0.75$.

i) Information in a dot = $I_1 = -\log_2(p_1) = -\log_2(0.25) = 2$ bits.
Information in a dash = $I_2 = -\log_2(p_2) = -\log_2(0.75) = 0.414$ bit.

ii) Average information = $H(x) = -[p_1\log_2(p_1) + p_2\log_2(p_2)]$
$= (0.25)(2) + (0.75)(0.415)$
$= 0.811$ bit/message

iii) Duration of a dot = 10 ms, duration of a dash = 30 ms and time interval between symbols = 10 ms.

Hence, there are two symbols in every 40 ms i.e. 40 symbols per second.

Thus the average rate of information transmission = $R = 40 \times 0.811 = 32.44$ bits/sec.

b) What is mutual information?

[WBUT 2010]

Answer:

Let us study the transfer of information from a transmitter through a channel to a receiver.

Prior to the reception of a message, the state of knowledge at the receiver about a transmitted signal x_j is the a-priori probability $p(x_j)$.

After the reception and selection of the symbol y_k, the state of knowledge concerning x_j is the conditional probability $p(x_j/y_k)$. This is called a posteriori probability.

Thus before y_K is received, the uncertainty and hence information is $-\log\left[p(x_j)\right]$ and after y_k is received the uncertainty and hence information becomes $-\log\left[p(x_j/y_K)\right]$.

Obviously, the information gained about x_j by the reception of y_K is the net reduction of its uncertainty and is known as mutual information denoted by $I(x_j; y_k)$.

Thus $I(x_j; y_K) = -\log p(x_j) + \log p(x_j/y_k) = \log \dfrac{p(x_j/y_K)}{p(x_j)}$

Mutual information is also called transferred information or trans-information.

Mutual information is symmetrical in x_j and y_k. That is $I(x_j;y_k) = I(y_k ; x_j)$

Self information may be treated as a special case of mutual information where $y_k = x_j$.

Then $I(x_j;x_j) = \log \dfrac{p(x_j/x_j)}{p(x_j)} = \log \dfrac{1}{p(x_j)} = I(x_j)$.

The average of mutual information i.e. the entropy corresponding to mutual information is denoted by I(X;Y). It can be shown that

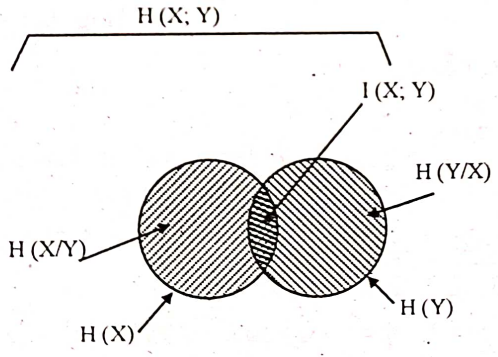
$I(X ; Y) \geq 0$

$I(X ; Y) = H(X) - H(X/Y)$

$= H(X) + H(Y) - H(X, Y) = H(Y) - H(Y/X)$

$I(X; Y) = I(Y ; X)$

The various entropies of a communication network can be represented diagrammatically by the following illustration.



Here H(X) = entropy of the channel input X. This is represented by the entire circle on the left.

H(Y) = Entropy of the channel output Y.

This is represented by the entire circle on the right.

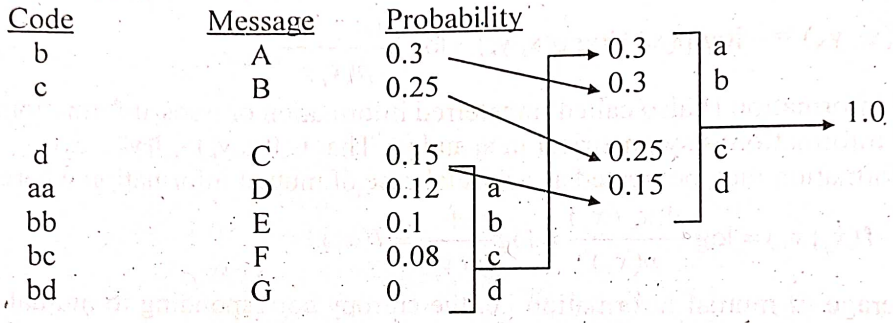
The mutual information I(X ; Y) is represented by the overlap between the two circles.

H(X ; Y) is the joint entropy of the channel.

4. a) A memoryless source emits six messages with probabilities 0.3, 0.25, 0.15, 0.12, 0.1, 0.008. Find the quaternary Huffman code. Determine its average word length, the efficiency and the redundancy. **[WBUT 2010]**

Answer:

As the sum of all probabilities should be equal to one, the probability of the sixth message is 0.08 and not 0.008. Since the number of symbols is 6, we need to add a dummy symbol of probability zero. Let the four symbols be denoted by a, b, c and d.



Thus the quaternary Huffman codes formed are:

b, c, d, aa, bb, bc and bd

Average word length $= \bar{L} = 1 \times 0.7 + 2 \times 0.3 = 0.7 + 0.6 = 1.3$ quaternary symbols.

Let $H(X)$ be the entropy of the source.

So, $H(X) = -[0.3\log_2 0.3 + 0.25\log_2 0.25 + 0.15\log_2 0.15 + 0.12\log_2 0.12 + 0.1\log_2 0.1 + 0.08\log_2 0.08]$

$= 2.42$ bits/message

Efficiency of the code, $\eta = \dfrac{H(X)}{\bar{L}\log_2 m}$

Here $m = 4$.

So, $\eta = \dfrac{H(X)}{\bar{L}\log_2 4} = \dfrac{2.42}{1.3 \times 2} = \dfrac{2.42}{2.6} = 93.07\%$

The redundancy of the code $= 1 - \eta = 1 - 0.9307 = 6.93\%$

b) Explain about Entropy of a source. Briefly discuss about channel capacity of a discrete memoryless channel. **[WBUT 2010]**

Answer:

Definition:

The average information per message of a source is called source entropy or simply entropy. It is denoted by H and

$$H = -\sum_{1}^{m} p_i \log p_i \text{ bits} = \sum_{i=1}^{m} p_i \log \frac{1}{p_i} \text{ bits} = \sum_{i=1}^{m} p_i I_i \text{ bits}$$

where m is the total number of messages in the source and p_i is the probability of occurrence of the i^{th} message. I_i is the information of the i^{th} message. Note that $\sum_{i=1}^{m} p_i = 1$.

Properties of entropy:

1. If all the probabilities of messages except one in a source are zero, the entropy $H(x) = 0$. This is the lower bound of the entropy.
2. If all the messages in a source are equiprobable, then the entropy $H(x) = \log_2 K$ where K is the radix or number of symbols of the alphabet of the source. This is the upper bound of the entropy.
3. The entropy of a source is bounded as $0 \le H(x) < \log_2 K$.
4. For a binary system, maximum entropy occurs when $p = \frac{1}{2}$.

Rate of Information:

If a message source having entropy 'H' generates messages at the rate of 'r' messages per second, then the rate of information 'R' is defined as the average number of bits of information per second.

Then

$$R = \frac{\text{Average number of information}}{\text{Second}}$$

$$= \frac{\text{Average number information}}{\text{Number of messages}} \times \frac{\text{Number of messages}}{\text{Second}}$$

$$= H \times r$$

where H = Entropy

Thus $R = rH$ bits per second.

Channel Capacity of a Discrete Memoriless Channel:

The channel capacity per symbol of a discrete memoriless channel (DMC) is defined as

$$C_S = \max_{\{p(x_i)\}} I(X;Y) \text{ bits / symbols}$$

where $p(x_i)$ denotes the source probabilities and $I(X;Y)$ is the average mutual information.

The quantity C_S denotes the maximum amount of information that can be transferred per channel symbol.

If r symbols are transmitted per second, then the maximum rate of transmission of information per second is given by

$C = rC_S$ bits / second where C is called the channel capacity per unit time.

c) What is conditional entropy? **[WBUT 2010]**

Answer:

In one-dimensional probability scheme there may be probability due to the transmitter or the receiver, say H(X) or H(Y).

A communication system has, however, a transmitter, a channel and a receiver. In such a case we have two-dimensional probability scheme and consequently there are joint probability and conditional probability.

Let there be two outcomes of an event, say x and y. The joint probability of first x and then y occurring is denoted by p(XY).

The conditional probability p(Y/X) is the relative frequency of occurrence of Y preceded by X.

Similarly p (X/Y) is the conditional probability of occurrence of X preceded by Y.

Accordingly we have joint entropy H(XY) corresponding to the joint probability p(X,Y) and conditional entropies H(Y/X) and H(X/Y) corresponding to the conditional probabilities p(Y/X) and p(X/Y) respectively.

$$H(XY) = -\sum_{j=1}^{m}\sum_{k=1}^{n} p(x_j, y_k)\log p(x_j; y_k)$$

$$H(X/Y) = -\sum_{j=1}^{m}\sum_{k=1}^{n} p(x_j, y_k)\log p(x_j / y_k)$$

$$H(Y/X) = -\sum_{j=1}^{m}\sum_{k=1}^{n} p(x_j, y_k)\log(y_k / x_j)\,.$$

5. a) State and prove the Shannon-Hartley law of channel capacity. **[WBUT 2011, 2017, 2018]**

Answer:

An additive white Gaussian noise (*AWGN*) channel is the most important example of continuous channel. An *AWGN* channel has the following properties:

1. The channel provides distortion-free transmission over some bandwidth B. Any transmission loss in the channel can be compensated by amplification.
2. The input from the source is constrained by the channel to be a band-limited signal $x(t)$ with fixed average power $S = \overline{x}^2$.
3. The signal received at the receiving end is contaminated by the addition of band-limited white Gaussian noise $n(t)$ with zero mean and average noise power $N = \overline{n}^2 = N_0 B$ where $\frac{N_0}{2}$ is the noise power spectral density.
4. The signal and noise are independent so that
   $y(t) = x(t) + n(t)$ and $\overline{y}^2 = \overline{x}^2 + \overline{n}^2 = S + N$.

To determine the channel capacity of an *AWGN* we note that $p_N(n)$ is a zero - mean Gaussian function with variance $\sigma^2 = N$.

Now

$$H(Y/X) = \int_{-\infty}^{\infty} p_N(n) \log_2 \frac{1}{P_N(n)} dn$$

$$= \int_{-\infty}^{\infty} p_N(n) \left[\frac{1}{2} \log_2 (2\pi N) + \frac{n^2}{2N} \log_2 e \right] dn$$

$$= \frac{1}{2} \log_2 (2\pi N) \int_{-\infty}^{\infty} p_N(n) dn + \frac{\log_2 e}{2N} \left\{ \int_{-\infty}^{\infty} n^2 p_N(n) dn \right\}$$

$$= \frac{1}{2} \log_2 (2\pi N) + \frac{\log_2 e}{2N} N$$

$$= \frac{1}{2} \log_2 (2\pi e N).$$

Also, $H(Y/X)$ does not depend on the source PDF. So,

$$C_S = \max_{p_X(x)} \left[H(Y/X) \right] - H(Y/X) = \left[\max_{p_X(x)} H(Y) \right] - \frac{1}{2} \log_2 (2\pi e N)$$

The signal $y(t)$ has fixed average power $\overline{y}^2 = S + N$. Hence

$$H(Y) \le \frac{1}{2} \log 2\pi e (S + N)$$

$p_X(x)$ is a zero-mean Gaussian function and $y = x + n$ has a Gaussian PDF. Thus $H(Y)$ is maximized.

Hence

$$C_S = \frac{1}{2} \log 2\pi e (S + N) - \frac{1}{2} \log_2 (2\pi e n) = \frac{1}{2} \log \left(\frac{S + N}{N} \right)$$

But we have $C = 2BC_S$

Hence we get $C = B \log_2 \left(1 + \frac{S}{N} \right)$

where $\frac{S}{N}$ is the signal-to-noise ratio at the destination.

This equation is known as the Hartley-Shannon law.

From Shannon's Channel Coding theorem it follows that $R \le B \log_2 \left(1 + \frac{S}{N} \right)$ bits/sec

This gives an upper limit for reliable information transmission over a band limited *AWGN* channel.

b) A Gaussian channel has a 1 MHz bandwidth. If the signal power-to-noise power spectral density $\frac{S}{\eta} = 10^5$ Hz, calculate the channel capacity C and the maximum information transfer rate. [WBUT 2011]

Answer:

From Hartley Shannon Law we know

$$C = B \log_2 \left(1 + \frac{S}{N}\right) = B \log_2 \left(1 + \frac{S}{N_o B}\right)$$

Here $B = 1$ MHz $= 10^6$ Hz.

$S/N_0 = 10^5$ Hz. So, $\frac{S}{N_o B} = \frac{10^5}{10^6} = 1/10$

So, $C = 10^6 \log_2 (1+0.1) = 13800$ bits / sec.

Maximum Information Rate, $R_{max} = 1.44 \frac{S}{N_o}$

or, $R_{max} = 1.44 \times 10^5 = 144000$ bits/sec.

c) Show that $H(X,Y) = H(X/Y) + H(Y)$ [WBUT 2011]

Answer:

We know,

$$P(x_i, y_i) = P(x_i / y_i) P(y_i)$$

$$and, \sum_{i=1}^{m} P(x_i, y_i) = P(y_i)$$

$$H(X,Y) = -\sum_{j=1}^{n} \sum_{i=1}^{m} P(x_i, y_j) \log_2 P(x_i, y_j)$$

$$= -\sum_{j=1}^{n} \sum_{i=1}^{m} P(x_i, y_j) \log_2 [P(x_i / y_j) P(y_j)]$$

$$= -\sum_{j=1}^{n} \sum_{i=1}^{m} P(x_i, y_j) \log_2 P(x_i / y_j)$$

$$-\sum_{j=1}^{n} [\sum_{i=1}^{m} P(x_i, y_j)] \log_2 P(y_j)$$

$$= H(X/Y) - \sum_{j=1}^{n} P(y_i) \log_2 P(y_j)$$

$$= H(X/Y) + H(Y)$$

6. a) Write down the advantages of Huffman coding over Shannon-Fano coding. [WBUT 2011]

Answer:

The following are the advantages of Huffman codes over Shannon-Fano codes

1. Huffman code always produce optional prefix codes whereas Shannon-Fano code is sub-optimal in the sense that the latter does not achieve the lowest possible expected codeword length.
2. Huffman codes are more efficient than Shannon-Fano codes.
3. Huffman coding will always at least equal the efficiency of the Shannon-Fano coding.
4. Shannon-Fano code does not guarantee that an optimal code is generated while Huffman code does it.

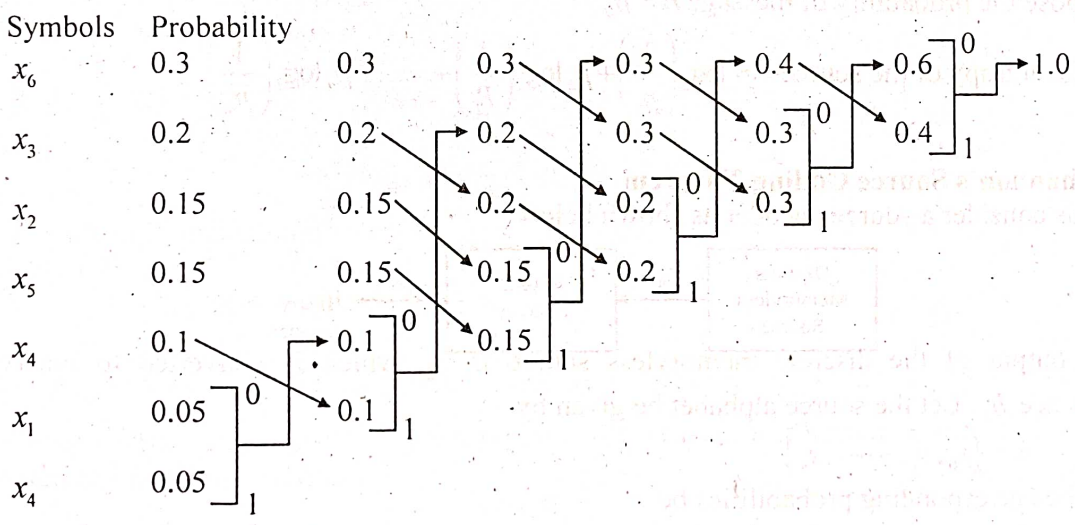
b) A discrete memoryless source has seven symbols $x_1, x_2, x_3, x_4, x_5, x_6$ and x_7 with probabilities of occurrence

$P(x_1)=0.05,\ P(x_2)=0.15,\ P(x_3)=0.2,\ P(x_4)=0.05, P(x_5)=0.15, P(x_6)=0.3$ and $P(x_7)=0.1$.

Construct the Huffman code and determine

i) Entropy
ii) Average code length
iii) Code efficiency. [WBUT 2011]

Answer:



Code word	Code	Code length
C_6	01	2
C_3	11	2
C_2	000	3
C_5	001	3
C_7	101	3
C_1	1000	4
C_4	1001	4

. Entropy, $H(x) = -[0.05\log_2 0.05 + 0.15\log_2 0.15 + 0.2\log_2 0.2 + 0.05\log_2 0.05$
$+0.15\log_2 0.15 + 0.3\log_2 0.3 + 0.1\log_2 0.1]$

$= 0.774 \times 3.32 = 2.57$ bits/message

Average code length,

$\bar{L} = [4\times0.05 + 3\times0.15 + 2\times0.2 + 4\times0.05 + 3\times0.15 + 2\times0.3 + 3\times0.1]$

$= 0.2 + 0.45 + 0.4 + 0.2 + 0.45 + 0.6 + 0.3 = 2.6$ symbols/message

Code efficiency $= \eta = \dfrac{H(x)}{\bar{L}} = \dfrac{2.57}{2.6} = 0.988 = 98.8\%$

7. a) Find the entropy of a source generating *n* number of messages having different probability of occurrence.
b) State and explain Source coding theorem.
c) An analog signal band limited to 10 kHz is quantized in 8 levels of a PCM system with probability ¼, 1/5, 1/5, 1/10, 1/10, 1/20, 1/20, 1/20 respectively. Calculate entropy and the rate of information **[WBUT 2012]**

Answer:

a) Suppose the probability of message $1 = p_1$

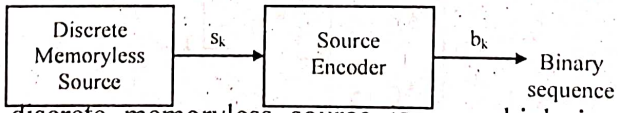
Suppose the probability of message $2 = p_2$

Suppose the probability of message $n = p_n$

So the entropy of the source $= p_1\log_2\left(\dfrac{1}{p_1}\right) + p_2\log_2\left(\dfrac{1}{P_2}\right) + \ldots\ldots + p_n\log_2\left(\dfrac{1}{p_n}\right)$.

b) Shannon's Source Coding Theorem

Let us consider a source encoder as shown below:



The output of the discrete memoryless source is s_k which is converted to binary sequence b_k. Let the source alphabet be given by

$$s = \{s_0, s_1, \ldots\ldots, s_k\}$$

Let the corresponding probabilities be

$\{p_0, p_1, \ldots\ldots, p_k\}$ and

Code length be

$\{\ell_0, \ell_1, \ldots\ldots, \ell_k\}$ respectively

Thus the average code length i.e., the average number of bits per symbol of the source is defined as

$$\bar{L} = \sum_{k=0}^{k-1} p_k \ell_k$$

Now the Shannon's Source Coding Theorem is stated as follows:
Given a discrete memoryless source of entropy $H(s)$, the average code-word length $\bar{L}$ for any distortionless source coding is bounded as

$$\bar{L} \geq H(s)$$

The source coding theorem is also known as the "noiseless coding theorem" and "Shannon's first theorem".
If $\bar{L}_{min}$ denotes the minimum possible value of $\bar{L}$, then we define the coding efficiency of the source encoder as

$$\eta = \frac{\bar{L}_{min}}{\bar{L}}$$

For an efficient code, η approaches unity
According to source coding theorem, the minimum value of $\bar{L}$ is $H(s)$. Hence,

$$\eta = \frac{H(s)}{\bar{L}}.$$

Shannon's source coding theorem provides the mathematical tool for assessing data compaction of data generated by a discrete memoryless source.

c) f_S = Sampling frequency = $2 \times f_m = 2 \times 10 = 20$ KHz. We consider each of the 8 quantised levels as a message.
Hence the Source Entropy

$$H(X) = \frac{1}{4}\log_2 4 + \frac{1}{5}\log_2 5 + \frac{1}{5}\log_2 5 + \frac{1}{10}\log_2 10 + \frac{1}{10}\log_2 10 + \frac{1}{20} + \frac{1}{20}\log_2 20 + \frac{1}{20}\log_2 20 = 2.84 \text{ bits/message.}$$

So, Rate of information, $R = r \times H$
Here, $r = 20{,}000$
So, $R = 20{,}000 \times 2.48 = 56800$ bits/sec.

8. A DMS has five symbols x_1, x_2, x_3, x_4, x_5 with $p(x_1) = 0.4$, $p(x_2) = 0.19$, $p(x_3) = 0.16$, $p(x_4) = 0.15$, $p(x_5) = 0.1$. Construct a Shanon Fano code and calculate the code efficiency. **[WBUT 2012]**

OR,

A source is generating five symbols (i.e., x_1, x_2, x_3, x_4, x_5) with probabilities 0.4, 0.19, 0.16, 0.15, 0.1. Determine the code word of the symbols using Huffman code. Calculate the efficiency of the above generated codes. **[WBUT 2019]**

Answer:

Message	Probability	Step 1	Step 2	Step 3	Code	Code Length
x_1	0.4	0	0		00	2
x_2	0.19	0	1		01	2
x_3	0.16	1	0		10	2
x_4	0.15	1	1	0	110	3
x_5	0.1	1	1	1	111	3

Thus the codes formed are $c_1 = 00$, $c_2 = 01$, $c_3 = 10$, $c_4 = 110$ and $c_5 = 111$

Average code length,

$$\bar{L} = (0.4\times2) + (0.19\times2) + (0.16\times2) + (0.15\times3) + (0.1\times3)$$
$$= 2.25 \text{ symbols/message}$$

Source Entropy, $H(X) = -[0.4 \log 0.4 + 0.19 \log 0.19 + 0.16 \log 0.16 + 0.15 \log 0.15 + 0.1 \log 0.1]$

$$= 2.15 \text{ bits/message.}$$

Hence efficiency $= \eta = \frac{H(X)}{\bar{L}} = \frac{2.15}{2.25} = 0.956 = 95.6\%$

9. a) Find the entropy of a source generating n number of messages having different probabilities of occurrence. [WBUT 2013]

b) State and explain source encoding theorem. [WBUT 2013, 2014]

c) An analog signal band limited to 10 kHz is quantized in 8 levels of a PCM system with probabilities 1/4, 1/5, 1/5, 1/10, 1/10, 1/20, 1/20, 1/20 respectively. Calculate entropy and the rate of information. [WBUT 2013]

Answer:

a) Let us consider a zero memory source, S. It delivers messages from its alphabet X such that $X = \{x_1, x_2 \ldots\ldots x_m\}$

Thus x_1 has the probability of occurrence p_1
x_2 has the probability of occurrence p_2
x_i has the probability of occurrence p_i
and so on.

Let N messages are delivered in a large span of time such that N tends to infinity. Obviously, the symbol x_i occurs Np_i times. Each occurrence of x_i conveys information of $(-\log_2 p_i)$ bits

Hence the total information due to Np_i messages $= -Np_i \log p_i$ bits

The total information due to all N messages $= -N\sum_{i=1}^{m} \log p_i$

Hence the average information per message or entropy

$$H = -\sum_{i-1}^{m} p_i \log p_i \quad where \sum p_i = 1.$$

b) ***Refer to Question No. 7(b) of Long Answer Type Questions.***

c) f_S = Sampling frequency = $2 \times f_m = 2 \times 10 = 20$ KHz. We consider each of the 8 quantised levels as a message.

Hence the Source Entropy

$$H(X) = \frac{1}{4}\log_2 4 + \frac{1}{5}\log_2 5 + \frac{1}{5}\log_2 5 + \frac{1}{10}\log_2 10 + \frac{1}{10}\log_2 10 + \frac{1}{20} + \frac{1}{20}\log_2 20 + \frac{1}{20}\log_2 20 = 2.84 \text{ bits/message.}$$

So, Rate of information, $R = r \times H$

Here, $r = 20{,}000$

So, $R = 20{,}000 \times 2.48 = 56800$ bits/sec.

10. Show that the channel capacity for a continuous channel is given by $C = B\log_2[1 + S/N]$ bit/sec. **[WBUT 2013, 2017]**

Answer:

Let S = Signal power in watts

N = Noise power in watts

Let us assume a load of 1 ohm.

Then Root mean square value of the received signal is $V_r = \sqrt{S+N}$ *volts*

RMS values of the noise voltage is $V_n = \sqrt{N}$ *volts*

The number of distinct levels that can be distinguished without errors is given by μ where

$$\mu = \frac{\sqrt{S+N}}{\sqrt{N}} = \sqrt{1 + \frac{S}{N}}$$

Now let us consider a discrete channel having μ states and uniform signaling speed s where $s = \frac{1}{t_0}$ and t_0 is the duration per state.

A received message of length T will consist of $T/t_0 = sT$ symbols where each symbol is having one of the μ possible states.

The number of different messages = $N = \mu^{sT}$

Now channel capacity C is $C = \underset{T\to\infty}{Lt}\frac{1}{T}\log_2 N = \underset{T\to\infty}{Lt}\log_2 \mu^{sT}$

$$= \underset{T\to\infty}{Lt}\left(\frac{1}{T}\right)(sT)\log_2 \mu = s\log_2 \mu$$

A system with bandwidth B can transmit a maximum of 2B pulses per second. Thus $s = 2B$

Hence $C = 2B\log_2\sqrt{1 + \frac{S}{N}}$

or, $C = B\log\left(1+\frac{S}{N}\right)$

This is Hartley–Shannon's law.

11. a) What do you mean by entropy of a source and mutual information of a communication channel? [WBUT 2015, 2018]

b) Consider a source X which produces five symbols with probabilities $\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{16}$ and $\frac{1}{16}$. Find the source entropy. [WBUT 2015]

c) Briefly discuss about the channel capacity of a discrete memoryless channel. Determine the channel capacity of a noiseless channel. [WBUT 2015]

OR,

Define (i) Lossless and (ii) Deterministic channel. [WBUT 2017]

Answer:

a) entropy of a source:

Refer to Question No. 4(b) (1st Part) of Long Answer Type Questions.

mutual information: ***Refer to Question No. 3(b) of Long Answer Type Questions.***

b) ***Refer to Question No. 1(b) of Short Answer Type Questions.***

c) The channel capacity per symbol of a discrete memoryless channel (DMC) is defined as $C_S = \max_{\{p(x_i)\}} I(X;Y)$ bits / symbols

where $p(x_i)$ denotes the source probabilities and $I(X;Y)$ is the average mutual information.

The quantity C_S denotes the maximum amount of information that can be transferred per channel symbol.

If r symbols are transmitted per second, then the maximum rate of transmission of information per second is given by

$C = rC_S$ bits / second

where C is called the channel capacity per unit time.

(i) Lossless channel

For a lossless channel $H(X/Y)=0$ *and* $I(X;Y)=H(X)$

Channel capacity $C = \max H(X) = \log_2 m$

where m is the number of symbols in X.

(ii) Deterministic channel

For a deterministic channel

$H(Y/X)=0$ for all input distributions $P(x_i)$ and

$$P(X;Y) = H(Y)$$

The channel capacity per symbol is $C = \max H(Y) = \log_2 n$
where n is the number of symbols in Y.

(iii) Noiseless channel

Since a noiseless channel is both lossless and deterministic, we may write,

$$I(X;Y) = H(X) = H(Y)$$

The channel capacity per symbol is $C = \log_2 m = \log_2 n$

(iv) Binary Symmetric channel

$$I(X;Y) = H(Y) + p\log_2 p + (1-p)\log_2(1-p)$$

Channel capacity per symbol is

$$C = 1 + p\log_2 p + (1-p)\log_2(1-p)$$

12. a) Explain the Shannon-Fano coding and Huffman coding with suitable example. **[WBUT 2016]**

Answer:

Refer to Question No. 17(b) & (c) of Long Answer Type Questions.

b) Show that the channel capacity of an ideal AWGN channel with infinite bandwidth is given by $C_\infty = 1.44S/\eta$ bit/sec, where S is the average signal power and $\eta/2$ is the power spectral density (psd) of white Gaussian noise. **[WBUT 2016, 2019]**

Answer:

For a noiseless channel S/N is infinity and thus from Hartley Shannon theorem, the channel capacity would be infinite. But actually channel capacity never becomes infinite because as bandwidth increases the noise power also increases. Now let us calculate the upper limit of channel capacity.

From Hartley Shannon theorem, we know channel capacity is given by

$$C = B\log_2\left(1 + \frac{S}{N}\right)$$

Since $N = \eta B$ where η is the two-sided noise power spectral density.

$$\text{So, } C = B\log_2\left(1 + \frac{S}{\eta B}\right) = \frac{S}{\eta} \times \frac{\eta B}{S}\log_2\left(1 + \frac{S}{\eta B}\right) = \frac{S}{\eta}\log_2\left(1 + \frac{S}{\eta B}\right)^{\frac{\eta B}{S}}$$

Since $\lim_{x\to 0}(1+x)^{\frac{1}{x}} = e$ we can write

$$C = \lim_{B\to\infty}\left(1 + \frac{S}{\eta B}\right)^{\frac{\eta B}{S}} = e$$

Hence $\lim_{B\to\infty} C = \frac{S}{\eta}\log e = 1.44\frac{S}{\eta}$

Thus $R_{max} = 1.44\frac{S}{\eta}$.

13. a) Verify the following expression: [WBUT 2016]

$$0 \le H(X) \le \log_2 m$$

where m is the size of the alphabet of X.

OR,

Verify the following expression:

$C_s = \log_2 m$

where C_s is the channel capacity of a lossless channel and m is the number of symbols in the channel. [WBUT 2017]

Answer:

The entropy $H(X)$ is always non-negative.

Since, $0 \le p(x) < 1$, $-\log p(x) \ge 0$

Hence $H(X) = -\sum p(x)\log p(x) \ge 0$

Hence $H(X) \ge 0$

Let $u(X) = \frac{1}{m}$ be the uniform probability mass function over X. Hence m is the size of the alphabet.

Then relative entropy, $D\left(\frac{p}{u}\right) = \sum p(x)\log\frac{p(x)}{u(x)} = \log_2 m - H(X)$

Since relative entropy $D\left(\frac{p}{u}\right) \ge 0$, we get $H(X) \le \log_2 m$

Hence $0 \le H(X) \le \log_2 m$

b) A DMS X has five symbols x_1, x_2, x_3, x_4 and x_5 with $P(x_1) = 0.4$, $P(x_2) = 0.19$, $P(x_3) = 0.16$, $P(x_4) = 0.15$ and $P(x_5) = 0.1$.

i) Construct a Shannon-Fano code for X, and calculate the efficiency of the code.

ii) Repeat for the Huffman code and compare the results. [WBUT 2016]

Answer:

i) $p(x_1) = 0.4$, $p(x_2) = 0.19$, $p(x_3) = 0.16$, $p(x_4) = 0.15$, $p(x_5) = 0.1$

We obtain Shannon-Fano code as under:

Symbol	Probability	Encoded message		
x_1	0.4	0		
x_2	0.19	1	0	0
x_3	0.16	1	0	1
x_4	0.15	1	1	0
x_5	0.1	1	1	1

So, the code words are: $c_1 = 0, c_2 = 100, c_3 = 101, c_4 = 110, c_5 = 111$

Average word length,

$$\bar{L} = 1\times 0.4 + 3\times 0.19 + 3\times 0.16 + 3\times 0.15 + 3\times 0.01 = 2.2 \text{ symbols/message}$$

Entropy $H(X) = -[0.4\times \log_2 0.4 + 0.19\log_2 0.19 + 0.16\log_2 0.16 + 0.15\log_2 0.15 + 0.1\log_2 0.1]$

$$= 0.4\times 1.32 + 0.19\times 2.39 + 0.16\times 2.64 + 2.73\times 0.15 + 0.1\times 3.32$$

$$= 2.146 \text{ bits/message}$$

$$\text{Coding efficiency} = \eta = \frac{H(X)}{\bar{L}} = \frac{2.146}{2.2} = 97.54\%$$

ii) We proceed to obtain Huffman codes as under:

Messages	Probabilities				
x_1	0.4	0.4	0.4	0.6	1.0
x_2	0.19	0.25	0.35	0.4	
x_3	0.16	0.19	0.25		
x_4	0.15	0.16			
x_5	0.1				

The Huffman codes are:

$$c_1 = 1, c_2 = 000, c_3 = 001, c_4 = 010, c_5 = 011$$

Average code length,

$$\bar{L} = 1\times 0.4 + 3\times 0.19 + 3\times 0.16 + 3\times 0.15 + 3\times 0.01 = 2.2 \text{ symbols/message}$$

Source entropy, $H(X) = 2.146$ bits/message

$$\text{Coding efficiency, } \eta = \frac{H(X)}{\bar{L}} = \frac{2.146}{2.2} = 97.54\%$$

Thus, the coding efficiency, η is same in both the cases.

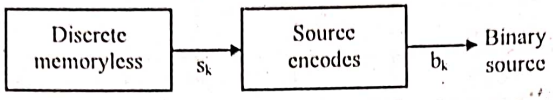
c) Write short notes on the following: [WBUT 2016]

i) **Codeword length**
ii) **Average codeword length**
iii) **Code efficiency**
iv) **Code redundancy.**

Answer:

The code word length is the number of bits in a code word. For example, in the code word 1011, the code word length is 4.

Let us consider a source encoder as shown below:



The output of the discrete memoryless source is s_k which is converted to binary sequence b_k. Let the source alphabet is given by

$$s = \{s_0, s_1, s_2, \ldots\ldots, s_m\}$$

Let the corresponding probabilities by

$\{p_0, p_1, p_2, \ldots\ldots, p_m\}$ and the corresponding code lengths be

$\{\ell_0, \ell_1, \ell_2, \ldots\ldots, \ell_m\}$ respectively

Then, the average code word length is

$$\bar{L} = \sum_{k=0}^{m} p_k \ell_k$$

If $H(s)$ is the source entropy, then coding efficiency,

$$\eta = \frac{H(s)}{\bar{L}}$$

The coding redundancy is equal to $1 - \eta = 1 - \frac{H(s)}{\bar{L}}$.

14. Explain the RSA algorithm with examples. **[WBUT 2017]**

Answer:

The RSA algorithm for public key cryptography is based on the inherent difficulty of determining the prime factors of large numbers. The algorithm is explained below with the help of an example.

Let us want to send an encrypted message consisting of letter 'x'. Its ASCII value is 88. First of all, we pick up two prime numbers, say p and q, and calculate their product 'n'. Thus $n = pq$. Both p and q are kept secret. Let $p = 13$ and $q = 17$. So $n = (13)(17) = 221$. Then we compute the Euler quotient function

$$\phi(n) = (p-1)(q-1) = 12 \times 16 = 192$$

Now we pick another prime number e such that the prime factor of $\phi(n)$ do not include e.

Let $e = 5$ and 5 is not a prime factor of 192.

Thus the public keys are $e = 5$ and $n = 221$.

The message is then encrypted using the public keys as

$$y = x^e \bmod n$$

i.e., $y = 88^5 \bmod 221$

$= \left[88^2 \bmod 221\right]\left[88^2 \bmod 221\right]\left[88^1 \bmod 221\right] \bmod 221$

$= (9 \times 9 \times 88) \bmod 221$

$= 56$

So the encrypted message is $y = 56$

Now to decrypt the message we consider the following function.

$x = y^d \bmod n$

where d is the private key.

We use the following algorithm for decryption

$de = 1 \bmod \left[\phi(n)\right]$ where d is less than $\phi(n)$.

We get d using Euclid's algorithm as below

$de = \phi(n).Q + 1$ where Q is an integer.

Now $\phi(n) = 192$ and $e = 5$

So, $5d = 192Q + 1$

If $Q = z$ we get $d = 77$.

Hence, $x = y^d \bmod n = 56^{77} \bmod 221$

$= \left\{\left[\left(56^4 \bmod 221\right)^{19} \bmod 221\right]\left(56 \bmod 221\right)\right\} \bmod 221 = 88$

Thus we have recovered our original message, $x = 88$.

15. A discrete source emits one of five symbols one every millisecond with probabilities $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$ and $\frac{1}{16}$ respectively. Find the source entropy and information rate. **[WBUT 2018]**

Answer:

$$H(s) = \sum_{i=1}^{5} p_i \log_2 \frac{1}{p_i}$$

$$= \frac{1}{2}\log_2(2) + \frac{1}{4}\log_2(4) + \frac{1}{8}\log_2(8) + \frac{1}{16}\log_2(16) + \frac{1}{16}\log_2(16)$$

$$= 0.5 + 0.5 + 0.375 + 0.25 + 0.25 = 1.875 \text{ bits/symbol}$$

Information rate, R

$R = r_s H(s)$ bits/sec $= 1000 \times 1.875$ bits/sec = 1875 bits/sec.

16. A DMS x has eight symbols $X_1, X_2, X_3, X_4, X_5, X_6, X_7$ and X_8 with $P(X_1) = \frac{1}{2}$, $P(X_2) = \frac{1}{8}$, $P(X_3) = \frac{1}{8}$, $P(X_4) = \frac{1}{16}$, $P(X_5) = \frac{1}{16}$, $P(X_6) = \frac{1}{16}$, $P(X_7) = \frac{1}{32}$ and $P(X_8) = \frac{1}{32}$. Construct a Shannon-Fano code for X and calculate the efficiency of code. **[WBUT 2018]**

Answer:

$$P(X_1)=\frac{1}{2},\ P(X_2)=\frac{1}{8},\ P(X_3)=\frac{1}{8},\ P(X_4)=\frac{1}{16},\ P(X_5)=\frac{1}{16},\ P(X_6)=\frac{1}{16},$$

$$P(X_7)=\frac{1}{32},\ P(X_8)=\frac{1}{32}$$

Symbols	Probabilities					
X_1	$\frac{1}{2}$	0				
X_2	$\frac{1}{8}$	1	0	0		
X_3	$\frac{1}{8}$	1	0	1		
X_4	$\frac{1}{16}$	1	1	0	0	
X_5	$\frac{1}{16}$	1	1	0	1	
X_6	$\frac{1}{16}$	1	1	1	0	
X_7	$\frac{1}{32}$	1	1	1	1	0
X_8	$\frac{1}{32}$	1	1	1	1	1

Thus the codes formed by Shanon Fano coding techniques are,

$C_1=0,\ C_2=100,\ C_3=101,\ C_4=1100,\ C_5=1101,\ C_6=1110,$

$C_7=11110,\ C_8=11111$

Entropy, $H=\sum_{i=1}^{8}P_i\log_2\frac{1}{P_i}=\frac{1}{2}\log_2 2+\frac{1}{8}\log_2 8+\frac{1}{8}\log_2 8+\frac{1}{16}\log_2 16+\frac{1}{16}\log_2 16$

$$+\frac{1}{16}\log_2 16+\frac{1}{32}\log_2 32+\frac{1}{32}\log_2 32$$

$$=\frac{1}{2}+\frac{3}{8}+\frac{3}{8}+\frac{4}{16}+\frac{4}{16}+\frac{4}{16}+\frac{5}{32}+\frac{5}{32}$$

$$=0.5+0.75+0.75+0.3125=2.3125 \text{ bits/message}$$

Average coding length,

$$\bar{L}=1\times\frac{1}{2}+3\times\frac{1}{8}+3\times\frac{1}{8}+4\times\frac{1}{16}+4\times\frac{1}{16}+4\times\frac{1}{16}+5\times\frac{1}{32}+5\times\frac{1}{32}$$

$$=2.3125 \text{ symbols/message}$$

Coding efficiency, $\%\eta=\frac{H}{\bar{L}}=\frac{2.3125}{2.3125}\times 100\%=100\%$

17. Write short notes on the following:
a) Shannon's theorems (three) in communication [WBUT 2008]
b) Shannon-Fano algorithm [WBUT 2009, 2011, 2014, 2018]
c) Huffman coding [WBUT 2010, 2014, 2015]
d) Source Coding [WBUT 2017, 2018]

Answer:

a) Shannon's theorems (three) in communication:

Three Shannon's theorems in communication are:

(i) Shannon's source coding theorem
(ii) Shannon's channel coding theorem and
(iii) Shannon's information capacity theorem.

Source coding theorem is stated as follows:

Given a discrete memoryless source of entropy H(S), the average code-word length $\overline{L}$ for any distortionless source coding scheme is bounded as

$$\overline{L} \geq H(S)$$

According to this theorem, the entropy of the source H(S) represents a fundamental limit on the average number of bits per source symbol necessary to represent a discrete memoryless source such that it can be made as small as H(S) but no smaller than H(S).

The channel coding theorem is stated as follows:

A DMS having source entropy H(S) produces symbols once every T_S seconds. A discrete memoryless channel having capacity C is used once every T_c seconds.

Thus if

$$\frac{H(S)}{T_S} \leq \frac{C}{T_C}$$

then there exists a coding scheme for which the source output can be transmitted over the channel and be reconstructed with an arbitrarily small probability or error.

If $\frac{H(S)}{T_S} > \frac{C}{T_C}$

then it is not possible to transmit information over the channel and reconstruct it with an arbitrarily small probability of error.

The information capacity theorem is stated as follows:

The information capacity of a continuous channel of bandwidth B Hz, perturbed by AWGN of power spectral density $\frac{N_0}{2}$ and limited in bandwidth to B is given by

$C = B\log_2\left(1+\frac{P}{N_0 B}\right)$ bits per second where P is the average transmitted power.

b) Shannon-Fano algorithm:

Shannon-Fano algorithm is an efficient source coding technique. The algorithm for constructing Shannon – Fano codes is as follows.

Step 1: The messages are first arranged in the order of decreasing probabilities.

Step 2: The message set is partitioned into two most equiprobable subsets $\{x_1\}$ and $\{x_2\}$.
Step 3: A '0' is assigned to each message in one subset say $\{x_1\}$ and a '1' is assigned to each message in the other subset say $\{x_2\}$.
Step 4: The above procedures are repeated for the subset $\{x_1\}$ and $\{x_2\}$. Thus $\{x_1\}$ will be partitioned into two subsets say $\{x_{11}\}$ and $\{x_{12}\}$ and $\{x_2\}$ set will be partitioned into two subsets say $\{x_{21}\}$ and $\{x_{22}\}$.
Step 5: The code words in subset $\{x_{11}\}$ will start with 00 and in $\{x_{12}\}$ with 01. Subset $\{x_{21}\}$ will start with 10 and $\{x_{22}\}$ will start with 11.
Step 6: The procedure is continued until each subset contains only one message.
Let $[X] = \{x_1, x_2, x_3, \ldots\ldots, x_8\}$ and probability

$$[P] = \left\{\frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{16}, \frac{1}{16}, \frac{1}{4}, \frac{1}{16}, \frac{1}{8}\right\}$$

Let us form the binary code words using Shannon Fano Coding.

First Step

Message	***Probability***
x_1	1/4 = 0.25
x_6	1/4 = 0.25
x_2	1/8 = 0.125
x_8	1/8 = 0.125
x_3	1/16 = 0.0625
x_4	1/16 = 0.0625
x_5	1/16 = 0.0625
x_7	1/16 = 0.0625

Second Step

$[X_1] = [x_1, x_6]$
$[X_2] = [x_2, x_8, x_3, x_4, x_5, x_7]$

Message	**Probability**	**Encoded Message**	**Subset**
x_1	0.25	0	subset$\{x_1\}$
x_6	0.25	0	
x_2	0.125	1	
x_8	0.125	1	subset$\{x_2\}$
x_3	0.0625	1	
x_4	0.0625	1	
x_5	0.0625	1	
x_7	0.0625	1	

Third Step

x_1	0.25	0 0	$\{x_{11}\}$
x_6	0.25	0 1	$\{x_{12}\}$

x_2	0.125	1 0	$\{x_{21}\}$
x_8	0.125	1 0	$\{x_{21}\}$
x_3	0.0625	1 1	$\{x_{22}\}$
x_4	0.0625	1 1	$\{x_{22}\}$
x_5	0.0625	1 1	$\{x_{22}\}$
x_7	0.0625	1 1	$\{x_{22}\}$

Fourth Step

x_2	1 0 0
x_8	1 0 1
x_3	1 1 0 0
x_4	1 1 0 1
x_5	1 1 1 0
x_7	1 1 1 1

Thus the codes formed by Shannon Fano Coding techniques are c_1= 00, c_2 =100, c_3 = 1100, c_4=1101, c_5=1110, c_6 = 01, c_7 = 1111 and c_8 = 101.

c) Huffman Coding:

The Huffman coding was invented by D.A. Huffman in 1962. It is a source code. Its average word length $\bar{L}$ approaches the fundamental limit set by the source coding theorem, i.e., $\bar{L} \rightarrow H(X)$ where H (X) is the entropy of the DMS.

Huffman code is said to be optimum because no other uniquely decodable set of code words has a similar average code-word length for a given DMS.

In the construction of Huffman code, a reduction process is followed in a step-by step manner.

The Huffman Encoding Algorithm:

Step 1: The source symbols are arranged in order of decreasing probability.

Step 2: The two source symbols of lowest probabilities are assigned a '0' and a '1'.

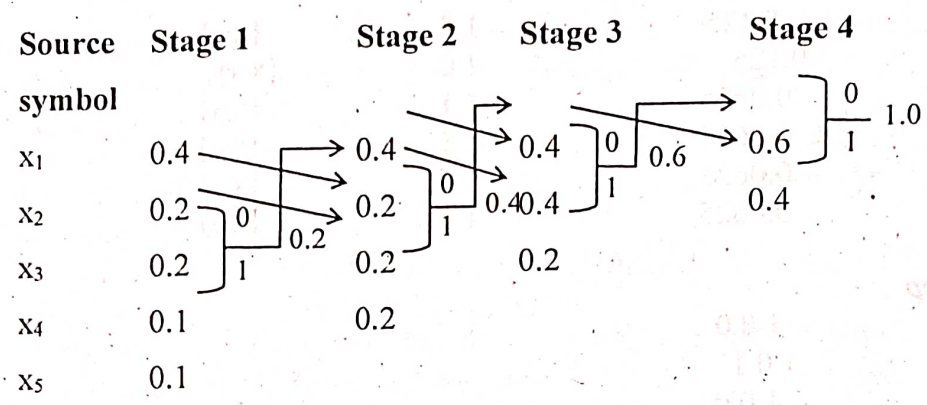
Step 3: The probability of the new symbol thus formed by summing the probabilities of the two symbols is placed in the list in accordance with its value.

Step 4: The procedure is repeated until we are left with a final list of source symbols of only two for which a '0' and a '1' are assigned.

Step 5: The code for each original source symbol is obtained by working backward and at the same time tracing the sequence of '0's and '1's assigned to that symbol and its successors.

Example

Let a DMS emits symbols x_1, x_2, x_3, x_4, and x_5 with corresponding probabilities 0.4, 0.2, 0.2, 0.1 and 0.1. We can find the Huffman codes as shown below.



1. First x_1, x_2, x_3, x_4 and x_5 are arranged in order of decreasing probabilities 0.4, 0.2, 0.2, 0.1 and 0.1 in stage 1.

2. x_4 is assigned a '0' and x_5 is assigned a '1'.

3. x_4 and x_5 are combined to form a new symbol with probability 0.1+ 0.1 = 0.2 and this new symbol is placed in the second position in the list in Stage 2 as indicated by the arrow ↱. x_2 comes in the 3rd position and x_3 comes in the 4th position in the list as indicated by the arrows ↘.

4. The symbols in the 3rd and 4th position having lowermost probabilities are combined to form a new symbol having probability 0.4 and it is placed at the top position in Stage 3. x_1 (prob = 0.4) and new symbol in 2nd position in Stage 2 (prob = 0 .2) are now placed in the 2nd and 3rd position respectively in stage 3.
Similarly 2nd and 3rd symbols in Stage 3 are combined to form a new symbol of probability 0.6 and placed at the top position in Stage 4. The 1st symbol in Stage 3 comes to the 2nd position in Stage 4.
Further 1st and 2nd symbols in Stage 4 are assigned '0' and'1' respectively.

5. Working backwards from State 4 we reach x_1 by assigning 00, x_2 by 10, x_3 by 11, x_4 by 010 and x_5 by 011.
Thus the Huffman codes are
$c_1 = 00$, $c_2 = 10$, $c_3 = 11$, $c_4 = 010$ and $c_5 = 011$ corresponding to the source symbols x_1, x_2, x_3, x_4 and x_5 respectively.

Disadvantage of Huffman Coding:
The Huffman encoding process is not unique. One reason is the arbitrariness in the way a '0' or a '1' is assigned to the last two source symbol. The upper one may be assigned 1 and the lower one may be assigned '0'. However in both the cases, the resulting differences are negligible.

There is another reason. We may place the probability of the new symbol after combining as high as possible or we may place it as lower as possible. However, whether the placement is made high or low it should consistently adhere to throughout the encoding process. Here noticeable differences will arise in the individual codes and their code lengths but average code-word length remains the same.

d) Source Coding:

Refer to Question No. 7(b) of Long Answer Type Questions.

CODING CHANNELS

Multiple Choice Type Questions

1. Gaussian channel is characterised by a distribution represented by [WBUT 2008]

a) $p(x)=\frac{l}{\sqrt{2\pi\sigma}}e^{-x^2/2\sigma^2}$

b) $p(x)=\frac{1}{\sqrt{2\pi\sigma}}e^{-x^2/2\sigma^2}$

c) $p(x)=\frac{\sqrt{2\pi}}{\sigma}e^{-x^2/2\sigma^2}$

d) $p(x)=\sqrt{2\pi\sigma}\,e^{-x^2/\sqrt{2\sigma^2}}$

Answer: (b)

Short Answer Type Questions

1. a) Draw the block diagram of a typical message information communication system. [WBUT 2008, 2014]

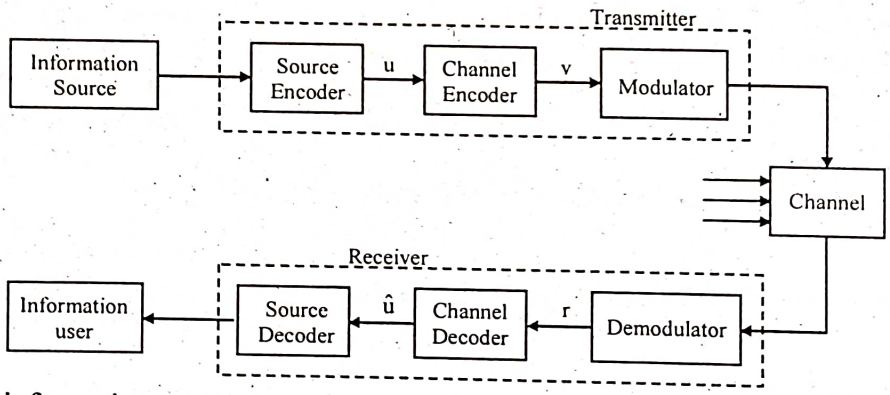
b) Define Forward Error Correction and Automatic Request for Retransmission. [WBUT 2008]

OR,

Draw the block diagram of a typical data transmission system and explain the function of each block. [WBUT 2013]

Answer:

a) The figure below shows a digital communication system consisting of a transmitter, communication channel and the receiver.

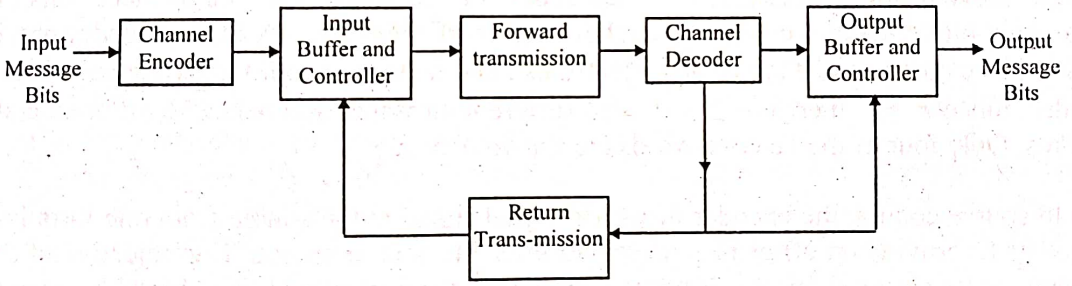


Here the information source is digital in nature. If the input signal is analog it has to be converted to digital signal by A to D conversion. The output of the digital source is converted into a sequence of binary digits for efficient representation and transmission of digital data over a particular channel. This is done in the source encoder which reduces the bandwidth requirement. After this, redundancy is introduced into the encoded data so as to reduce the effect of noise and interference during transmission through the channel. This is done in the channel encoder which carries out error-control coding. The source-

encoded and channel-encoded digital data are passed through a digital modulator for transmission through a physical medium such as free space, wire lines or optical fibers. The physical medium called channel introduces noise to the modulated signal.
The channel output is fed into the demodulator which carries out the inverse operation of the modulator to produce bit streams from the received signal. The channel decoder extracts the signal out of the noise. The source decoder performs the reverse operation of the source encoder to get the original digital signal. If original signal was analog then a D to A converter is used to obtain the original analog signal. The introduction of redundancy by the channel encoder, however, increases the transmission bandwidth.
In the case of a data storage system, such as compact disk system, the modulator, the channel and the demodulator can be regarded as the writing unit, the storage medium and the reading unit respectively.

b) Automatic Repeat Request

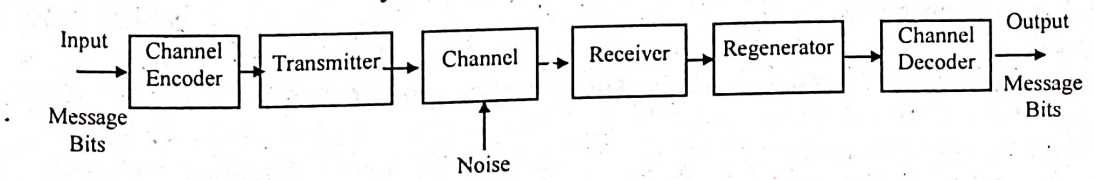
In this technique, the errors are detected only and no correction is possible. When error is detected, the receiver requests the transmitter for retransmission of the code word. This goes on till the received word does not have any error. ARQ is particularly suitable for data communication systems such as computer networks. A typical ARQ system is shown in the block diagram below.



The channel encoder adds the redundant bits to the message bits for error detection and the channel decoder looks for errors. If no errors are detected by the channel decoder it issues a positive acknowledgement called ACK. If errors are detected a negative acknowledgement called NAK is issued and sent to the input buffer and controller which then retransmits the code word stored in the buffer. A particular code word may be transmitted just once if no error is detected or it may be transmitted several times depending upon the occurrence of transmission errors.

Forward Error Correction (FEC) Systems

In FEC systems the channel coding is meant not only for detection of error but also for correction of error. An FEC system is shown in the block diagram below.



Here the input message bits are channel coded before transmission through the channel where noise is added to corrupt the code words. The channel decoder is used to detect errors in the codeword and also correct them.

2. a) What is systematic format of a code word. **[WBUT 2008]**
b) Explain 'Source Coding' and 'Channel Coding'. **[WBUT 2008]**

OR,

What is the difference between source coding and channel coding. **[WBUT 2019]**

Answer:

a) A code word whose message bits are kept together so that they can be identified readily is said to be in systematic form and such code words are called systematic codes. Otherwise, the code is called a non-systematic code. Systematic codes are normally preferred to non-systematic codes. A few binary block codes in systematic form with $n = 7$ and $k = 4$ are shown below.

Messages	Codewords
0000	0000000
1000	1101000
0100	0110100
1100	1011100

In the above example, it is seen that each codeword has $n = 7$ bits. Out of each 7-bits the last four bits are the message bits. The number of message bits in each codeword is $k = 4$. The message bits are clearly identifiable and hence the codes are systematic block codes. Since $k = 4$, there are $2^k = 2^4 = 16$ different messages and hence 16 different code words. Only four of the 16 code words are shown above.

b) In source coding, the encoder maps the digital signal at the source from one form into another to provide an efficient representation of the source output. The objective of the source coding is to eliminate or reduce redundancy and its benefit is reduced bandwidth requirement. In source coding, the mapping has one-to-one correspondence. The source decoder performs the inverse mapping. Typical source encoders are pulse code modulators, delta modulators, vector quantizers etc. In channel coding, the objective is to map the incoming digital signal into a channel input such that the effect of channel noise is minimized. A channel encoder adds redundant or extra bits to the input digital signal with some properly defined logic. The combination of channel encoder and channel decoder serves to achieve reliable communication over a noisy channel.

It may be noted that source coding removes redundancy whereas channel coding introduces controlled redundancy.

3. Draw the block diagram of a typical data transmission system and explain the function of each block. **[WBUT 2009]**

Answer:

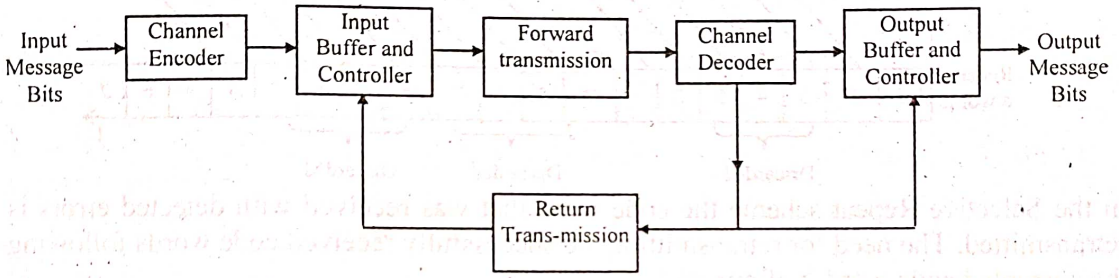
Refer to Question No. 1(a) of Short Answer Type Questions.

4. Compare ARQ & FEC schemes of Error control strategies. **[WBUT 2010]**

Answer:

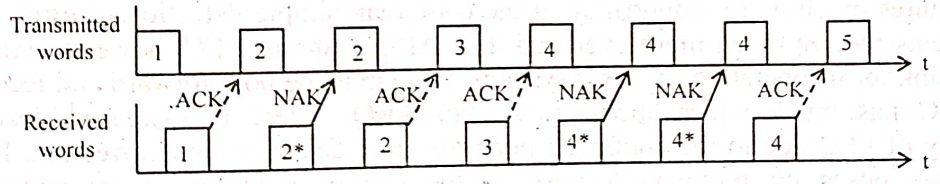
Automatic Repeat Request:

In this technique, the errors are detected only and no correction is possible. When error is detected, the receiver requests the transmitter for retransmission of the code word. This goes on till the received word does not have any error. ARQ is particularly suitable for data communication systems such as computer networks. A typical ARQ system is shown in the block diagram below.



The channel encoder adds the redundant bits to the message bits for error detection and the channel decoder looks for errors. If no errors are detected by the channel decoder it issues a positive acknowledgement called ACK. If errors are detected a negative acknowledgement called NAK is issued and sent to the input buffer and controller which then retransmits the code word stored in the buffer. A particular code word may be transmitted just once if no error is detected or it may be transmitted several times depending upon the occurrence of transmission errors.

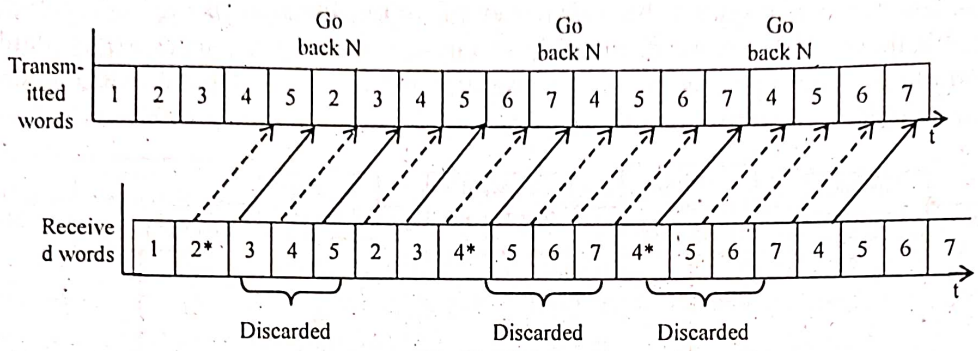
There are three basic types of ARQ schemes, viz. the Stop and Wait scheme, Go-back-N scheme and Selective Repeat scheme. The Stop and Wait scheme is the simplest ARQ scheme and used for half-duplex link. In half-duplex link, data transmissions over the link can be made in either direction but not simultaneously. Such a scheme is shown in the diagram below.



The received words marked with asterisks (*) have detected errors and these are retransmitted. In this scheme the transmitter has to stop after every word and wait for acknowledgement from the receiver. If the transmitter receives ACK it transmits the next word. If it receives NAK from the receiver the transmitter then retransmits the same code word. Though only one word is needed to be stored by the input buffer, there is idle time between words due to transmission time delay.

Idle time problem in Stop and Wait method is eliminated by the Go-back-N scheme (or sometimes called continuous ARQ with pull back scheme). In this scheme the code words are transmitted continuously until it receives a request from the receiver for a

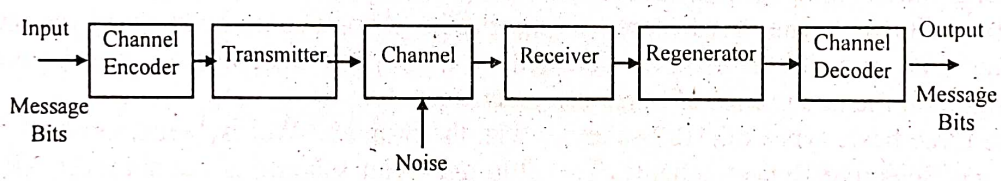
retransmission. When the receiver sends a NAK signal the transmitter goes back N words in the buffer and retransmits starting from that point. The receiver discards the N-1 intervening words in order to preserve proper sequence. The scheme is shown in the diagram below.



In the Selective Repeat scheme the code word that was received with detected errors is retransmitted. The need for retransmitting the successfully received code words following the corrupted code word is eliminated.

Forward Error Correction (FEC) Systems:

In FEC systems the channel coding is meant not only for detection of error but also for correction of error. An FEC system is shown in the block diagram below.



Here the input message bits are channel coded before transmission through the channel where noise is added to corrupt the code words. The channel decoder is used to detect errors in the codeword and also correct them.

This method is universally used for point-to-point digital communication. Correction of errors requires much more redundancy in the code than simple detection of error. Thus FEC systems require much more overhead than ARQ systems. FEC, however, requires only one link for its operation. In ARQ systems, there must be both forward and feedback links. FEC has much wider applications than ARQ. There is increased decoding complexity of FEC due to the combined need for error detection and correction. But at present this poses no problem because of the use of microprocessors and VLSI techniques.

5. Calculate the throughput efficiency of the stop and wait ARQ system.

[WBUT 2010]

Answer:

Let P_A = Probability that the receiver accepts the message on any particular transmission.

Then $1 - P_A$ = Probability that the first transmission is rejected.

So, $P_A(1-P_A)$ = Probability that two transmissions will be required. Thus the probability of requiring j transmissions $= P_A(1-P_A)^{j-1}$. Then the number of words transmitted for the acceptance of one word is

$$\bar{N} = 1\cdot P_A + 2\cdot P_A(1-P_A) + 3\cdot P_A(1-P_A)^2 + \cdots = \frac{1}{P_A}.$$

The average time required to transmit one word is

$$\bar{T} = \frac{T_w + T_t}{P_A}$$

where T_w = Time for transmission of one word

T_t = Time gap between two consecutive transmissions.

If no ARQ is used and no coding bits were added to the k information bits, the time needed to transmit the k-bits is

$$T_k = \frac{k}{n} T_w$$

where n = total number of bits in the code word.

Hence the throughput efficiency, $\eta = \frac{T_k}{\bar{T}} = \frac{k}{n}\frac{P_A \cdot T_w}{T_w + T_t}$ i.e. $\eta = \left(\frac{k}{n}\right)\frac{P_A}{1+\frac{T_t}{T_w}}$.

6. What is the systematic structure of a code word? **[WBUT 2011, 2014]**

Answer:

A code word whose message bits are kept together so that they can be identified readily is said to be in systematic form and such code words are called systematic codes. Otherwise, the code is called a non-systematic code. Systematic codes are normally preferred to non-systematic codes. The table 2 below shows a binary block code in systematic form with $n = 7$ and $k = 4$.

Messages	Codewords
0000	0000000
1000	1101000
0100	0110100
1100	1011100
0010	1110010
1010	0011010
0110	1000110
1110	0101110
0001	1010001
1001	0111001
1101	0001101
0011	0100011
1011	1001011
0111	0010111
1111	1111111

In the above table, it is seen that each codeword has $n=7$ bits. Out of each 7-bits the last four bits are the message bits. The number of message bits in each codeword is $k=4$. The message bits are clearly identifiable and hence the codes are systematic block codes. Since $k=4$, there are $2^k=2^4=16$ different messages and hence 16 different code words. has a memory order of m. Such a set of encoded sequences produced by a k-bit input, n-bit output of memory order m is called an (n,k,m) convolutional code. As in block code, the ratio $R=\frac{k}{n}$ is called the code rate. A convolutional code has memory and hence it is implemented with a sequential logic circuit.

7. a) What are the limitations of syndrome decoding methods for error corrections? **[WBUT 2019]**

Answer:
In syndrome decoding method for error correction, there is a need for a syndrome table. The decoding is done using the syndrome table. The requires the computation of the syndromes to prepare the syndrome table. This is a limitation of the syndrome decoding method. The hardware required for doing this are usually complicated and costly.

b) The generator matrix for $a(6,3)$ block code is shown below obtain codeword for the message bit 010 and 011.

$$G=\begin{bmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{bmatrix}$$

[WBUT 2019]

Answer:
The generator matrix is

$$G=\left|\begin{matrix}1&0&0\\0&1&0\\0&0&1\end{matrix}\right.\left.\begin{matrix}0&1&1\\1&0&1\\1&1&0\end{matrix}\right|=[I:P]$$

Let the message be $D_1=010$

So, the corresponding code word is $C_1=[D_1][G]$

$$=[0\ 1\ 0]\begin{bmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{bmatrix}=[0\ 1\ 0\ \ 1\ 0\ 1]$$

Now let the message be $D_2=011$

In this case, the corresponding code word $C_2=[D_2][G]$

$$=[0\ 1\ 1]\begin{bmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{bmatrix}=[0\ 1\ 1\ \ 0\ 1\ 1]$$

Long Answer Type Questions

1. Write short note on Error control strategies **[WBUT 2012, 2014]**

OR,

Error control strategy **[WBUT 2017]**

Answer:

Error-control strategies can be broadly classified into two types

1. Automatic repeat request (ARQ)
2. Forward Error Correction (FEC)

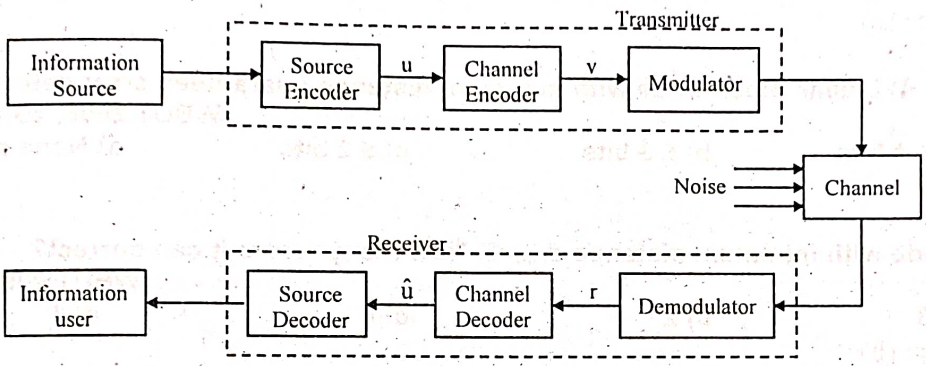


Fig: 1 Block diagram of a digital communication system

In figure 1 the block diagram shows a one-way system. That is, the transmission or recording is strictly in one direction from transmitter to receiver. In such a system, error correction is done by the FEC technique. In this technique error-correcting codes are employed that automatically correct at the receiver. Two well-known examples of FEC systems are:

1. Deep space communication systems
2. Magnetic tape storage systems.

In deep space communication systems, the relatively simple encoding equipment can be placed aboard the spacecraft. Much more complex decoding procedure is performed on earth. Thus FEC system is necessary in this case.

Similarly in magnetic tape storage systems, the information recorded on tape may be replayed after a long time of recording. In such a situation coding by FEC is the solution. Most of the coded systems in use today employ some form of FEC.

On the other hand, a transmission system can be two-way. It means information can be sent in both directions i.e. from transmitter to receiver and the receiver to the transmitter. Telephone channels and some satellite communication systems are examples of two-way systems. In such a 2-way system, ARQ system is used. Error control is achieved in Automatic repeat request strategy by error detection and retransmission. When errors are detected at the receiver, a request is sent from the receiver to the transmitter to repeat the message. This continues until the message is received correctly.

BLOCK CODES

Multiple Choice Type Questions

1. The binary Hamming Codes have the property that [WBUT 2008, 2010, 2014]

a) $(n, k) = (2^m + 1, 2^m - 1 - m)$ b) $(n, k) = (2^m - 1, 2^m - 1 + m)$

c) $(n, k) = (2^m - 1, 2^m - 1 - m)$ d) $(n, k) = (2^{m-1}, 2^{m-1} - m)$

Answer: (c)

2. A (7, 4) Linear Block Code with minimum distance guarantees error detection of [WBUT 2008, 2014, 2015]

a) ≤ 4 bits b) ≤ 3 bits c) ≤ 2 bits d) None of these

Answer: (c)

3. A code with minimum distance d_{min}=5. How many errors it can correct? [WBUT 2009, 2014]

a) 3 b) 2 c) 4 d) 1

Answer: (b)

4. The Hamming distance between *v* = 1001011 and *w* = 0100010 is [WBUT 2009, 2012]

a) 3 b) 4 c) 2 d) 1

Answer: (b)

5. The number of undetectable errors for a (*n*, *k*) linear code is [WBUT 2009, 2011, 2013, 2015]

a) 2^{n-k} b) 2^n c) $2^n - 2^k$ d) 2^k

Answer: (a)

6. A (8, 4) linear code has a code rate of [WBUT 2009, 2014, 2019]

a) 8 b) 4 c) 2 d) 0.5

Answer: (d)

7. Hamming codes are [WBUT 2010]

a) single error correcting codes b) double error correcting codes

c) Burst error correcting codes d) Triple error correcting codes

Answer: (a)

8. The condition of a dual code in case of linear block code is [WBUT 2010, 2014, 2015]

a) $GH^T = 0$ b) $(HG)^T = 0$ c) $H^T G^T = 0$ d) $GH^T = 1$

Answer: (a)

9. A $(7, 4)$ linear block code has a code rate of [WBUT 2011]

a) 7 b) 4 c) 1.75 d) 0.571

Answer: (d)

10. The Hamming distance between $V = 1100001011$ and $W = 1001101001$ is [WBUT 2011, 2014]

a) 1 b) 5 c) 3 d) 4

Answer: (d)

11. Consider the parity check matrix $H = \begin{vmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 101 \end{vmatrix}$ and the received vector $r = (001110)$. Then the syndrome is given by [WBUT 2011, 2014]

a) (110) b) (100) c) (111) d) (101)

Answer: (b)

12. A code with minimum distance $d_{mim} = 3$. How many errors it can correct? [WBUT 2012]

a) 3 b) 2 c) 1 d) 0

Answer: (c)

13. In block coding, if $k = 2$ and $n = 3$, then number of invalid code words is [WBUT 2015]

a) 8 b) 4 c) 2 d) 6

Answer: (b)

14. The efficiency of Huffman code is linearly proportional to [WBUT 2015]

a) average length of the code b) average entropy

c) maximum length of the code d) none of these

Answer: (b)

15. For (n, k) block code, the minimum distance d_{min} is [WBUT 2016]

a) $d_{min} \le n - k + 1$ b) $d_{min} \le n - k$ c) $d_{min} \le n + k + 1$ d) $d_{min} \le n + k - 1$

Answer: (a)

16. For Hamming Codes of (n, k) linear block codes, the block length (n) will be [WBUT 2016]

a) $2^q - 1$ b) 2^q c) $2^q + 1$ d) none of these

Answer: (a)

17. A code is with minimum distance 5. How many errors can it correct? [WBUT 2017]

a) 3 b) 2 c) 4 d) 1

Answer: (b)

18. The code rate for (15, 5) code is [WBUT 2017]

a) 3 b) 1/3 c) 5 d) 10

Answer: (b)

19. The efficiency of Huffman code is linearly proportional to [WBUT 2018]

a) average length of the code b) average entropy

c) maximum length of the code d) None of these

Answer: (b)

20. A code with minimum distance $d_{\min} = 5$. How many errors it can correct? [WBUT 2018]

a) 3 b) 4 c) 2 d) 1

Answer: (c)

21. The Hamming distance between $X = 1100001011$ and $Y = 1001101001$ is [WBUT 2018]

a) 1 b) 5 c) 3 d) 4

Answer: (d)

22. The condition of a dual code in case of a linear blods code is [WBUT 2018]

a) $GH^T = 0$ b) $(HG)^T = 0$ c) $H^T G^T = 0$ d) $GH^T = 1$

Answer: (a)

23. In block coding if $k = 2$ and $n = 3$, the number of invalid code word is [WBUT 2018]

a) 8 b) 4 c) 2 d) 6

Answer: (b)

24. Consider the parity check matrix [WBUT 2018]

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$ and the received vector $r = (001110)$. Then the syndrome is given by

a) (110) b) (100) c) (111) d) (101)

Answer: (b)

Short Answer Type Questions

1. The generator matrix for a $(7,4)$ block code is given: **[WBUT 2010]**

$$G=\begin{vmatrix}1000101\\0100111\\0010110\\0001011\end{vmatrix}$$

i) **Find the Parity check matrix of this code.**

ii) **If the received code word is $[0\ 0\ 0\ 1\ 1\ 1\ 0]$, then find the transmitted code word.**

Answer:

(i) Parity check Matrix,

$$H=\left[P^{T}_{k\times n}:I_{k\times k}\right]=\begin{bmatrix}1&1&1&1&0&1&0&0\\0&1&1&1&1&0&1&0\\1&1&1&0&1&0&0&1\end{bmatrix}$$

(ii) Let R = 0 0 0 1 1 1 0

$$S=RH^{T}=[0001110]\begin{bmatrix}101\\111\\110\\011\\100\\010\\001\end{bmatrix}=[101]$$

Since S is the first row of H^{T}, the error is in the first bit of received code. Thus transmitted code is 1 0 0 1 1 0.

2. What is syndrome and what is its significance? Draw the syndrome circuit for a $(7,4)$ linear block code with parity-check matrix $H=\begin{bmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{bmatrix}$

[WBUT 2011, 2014]

Answer:

1st Part:

Let us consider a linear (n, k) block code with a Generator Matrix $G=\left[I_K:P\right]$ and a Parity Check Matrix $H=\left[P^{T}:I_{n-k}\right]$.

Let C = transmitted code vectors and R = Received code vectors in a noisy communication system. E is the error vector.
Obviously, R = C + E
The function of the receiver is to decode C from R and the message block D from C. This is done by the receiver by determining an $(n-k)$ vector S. Vector S is known as the error syndrome of R. S is defined as $S = RH^T = (C+H)H^T = CH^T + EH^T$
Since $CH^T = 0$, we get $S = E H^T$
If any error occurs in transmission, the syndrome S of the received vector is non-zero. Error syndrome, S is related to the error vector E and the decoder uses S to detect and correct errors. S is zero if the received code word has no errors i.e. if R is a valid code word.

2nd Part:

Syndrome is given by; $S = rH^T$
where r is the received vector and H is the parity check matrix.
In the given problem,

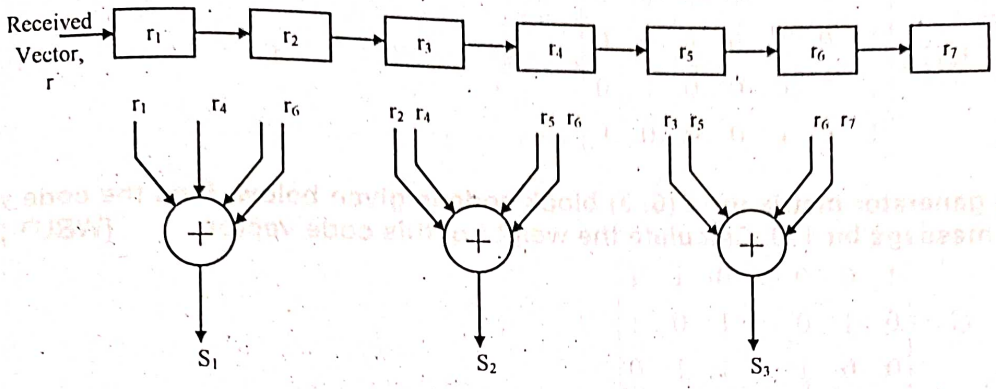
$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

So,
$$H^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Hence
$$S = \begin{bmatrix} r_1 & r_2 & r_3 & r_4 & r_5 & r_6 & r_7 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

i.e.,
$$S_1 = r_1 + r_4 + r_6 + r_7$$
$$S_2 = r_2 + r_4 + r_5 + r_6$$
$$S_3 = r_3 + r_5 + r_6 + r_7$$

Thus the syndrome circuit for the $(7,4)$ block is as shown below.



3. Design a generator matrix for a (7, 4) linear binary code (LBC). [WBUT 2013]

Answer:

In a $(7,4)$ Hamming code there are four date bits, $[d]$, which are transformed into a seven bit Hamming code. To achieve this we need to use a (4×7) generator matrix, $[G]$. To design the generator matrix, let $[d]$ be the (1×4) vector $[d_1, d_2, d_3, d_4]$. We can create a (4×7) generator matrix $[G]$ such that the product modulo 2 of $[d]$ and $[G]$ is the desired (1×7) Hamming code word.

Let each data bit be represented by a column vector.

$$d_1 = \begin{bmatrix}1\\0\\0\\0\end{bmatrix},\ d_2 = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ d_3 = \begin{bmatrix}0\\0\\1\\0\end{bmatrix},\ d_4 = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.$$

Let the parity bits are:

$$p_1 = \begin{bmatrix}0\\1\\1\\1\end{bmatrix},\ p_2 = \begin{bmatrix}1\\0\\1\\1\end{bmatrix},\ p_3 = \begin{bmatrix}1\\1\\0\\1\end{bmatrix}.$$

Now to create a generator matrix $[G]$ we have to arrange the column vectors into a (4×7) matrix such that the columns are ordered to match their corresponding bits in a code word.

The code words are $p_1\ \ p_2\ \ p_3\ \ d_1\ \ d_2\ \ d_3\ \ d_4$.

So, we use the vector above and arrange them into the following columns $[p_1\ \ p_2\ \ p_3\ \ d_1\ \ d_2\ \ d_3\ \ d_4]$

This results into the following (4×7) generator matrix, $[G]$

$$[G]=\begin{bmatrix}0&1&1&1&0&0&0\\1&0&1&0&1&0&0\\1&1&0&0&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}.$$

4. The generator matrix for a (6, 3) block code is given below. Find the code vector of the message bit 110. Calculate the weight of this code vector. **[WBUT 2016]**

$$G=\begin{Bmatrix}1&0&0&:&0&1&1\\0&1&0&:&1&0&1\\0&0&1&:&1&1&0\end{Bmatrix}.$$

Answer:

The message length $= k = 3$

The code word length $= n = 6$

Generator matrix, $G=[I \;:\; P]=\begin{bmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{bmatrix}$

Message bits, $d = 110$

The code word, $c=[D][G]=[1\;\;1\;\;0]\begin{bmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{bmatrix}=[1\;\;1\;\;0\;\;1\;\;1\;\;0]$

There are four 1s in the code vector. So its weight is 4.

5. Define Linear Block Codes. What are the properties of Linear Block Code? **[WBUT 2019]**

Answer:

1st Part:

If blocks of data bits are encoded to a particular format then that kind of coding is called Block code.

A code is called as linear if any two code words in the code can be added in modulo 2 arithmetic to generate a third code word in the code.

Block codes in which the message bits are transmitted in unaltered form are called systematic codes.

Linear block codes have the property of linearity, i.e. the sum of any two codeword is also a code word, and they are applied to the source bits in blocks, hence the name linear blocks codes. There are block codes that are not linear, but it is difficult to prove that a code is a good one without this property.

Linear block codes are summarized by their symbol alphabets (e.g. binary or ternary) and parameters (n, m, d_{min}) where

1. n is the length of the codeword, in symbols,
2. m is the number of source symbols that will be used for encoding at once,
3. d_{min} is the minimum hamming distance for the code

There are many types of linear block codes, such as

1. Cyclic codes
2. Repetition codes
3. Parity codes
4. Polynomial codes
5. Reed Solomon codes
6. Algebraic geometric codes

Hamming code is a subset of cyclic codes and BCH codes are a subset of the polynomial codes.

2nd Part:

The codewords in a linear block code are blocks of symbols that are encoded using more symbols than the original value to be sent. A linear code of length n transmits blocks containing n symbols. For example, the [7, 4, 3] Hamming code is a linear binary code which represents 4-bit messages using 7-bit codewords.

Long Answer Type Questions

1. Consider a systematic (8, 4) code whose parity-check equations are[WBUT 2008]

$$v_0 = u_1 + u_2 + u_3$$
$$v_1 = u_0 + u_1 + u_2$$
$$v_2 = u_0 + u_1 + u_3$$
$$v_3 = u_0 + u_2 + u_3$$

where v_0, v_1, v_2 and v_3 are message digits and v_0, v_1, v_2, v_3 are parity-check digits.
Find the generator and parity-check matrix for the code.
Show that minimum distance of the code is 4.

Answer:

$$v_0 = u_1 + u_2 + u_3$$
$$v_1 = u_0 + u_1 + u_2$$
$$v_2 = u_0 + u_1 + u_3$$
$$v_3 = u_0 + u_2 + u_3$$

Obviously, $v_4 = u_0$, $v_5 = u_1$, $v_6 = u_2$ and $v_7 = u_3$

We can write,

$$v=(u_0,u_1,u_2,u_3)\begin{bmatrix}0&1&1&1&1&0&0&0\\1&1&1&0&0&1&0&0\\1&1&0&1&0&0&1&0\\1&0&1&1&0&0&0&1\end{bmatrix}$$

We know $v=u\cdot G$

where G is the Generator matrix. Thus, we have

$$G=\begin{bmatrix}0&1&1&1&1&0&0&0\\1&1&1&0&0&1&0&0\\1&1&0&1&0&0&1&0\\1&0&1&1&0&0&0&1\end{bmatrix}=[P:I]$$

The parity-check matrix is denoted by H which is given by

$$H=\left[I_{n-k}:P^T\right]$$

Hence $$H=\begin{bmatrix}1&0&0&0&0&1&1&1\\0&1&0&0&1&1&1&0\\0&0&1&0&1&1&0&1\\0&0&0&1&1&0&1&1\end{bmatrix}$$

It may be noted that all columns of H are non-zero and no two columns are alike. Therefore, no two or fewer columns sum to zero. Hence the minimum weight or minimum distance of this code is at least 4. However, the zeroth, fifth, sixth and seventh columns sum to zero. Thus the minimum weight of the code is 4.

2. The parity check bits of a (8, 4) block code are generated by

$C_5=d_1\oplus d_2\oplus d_4$, $C_6=d_1\oplus d_2\oplus d_3$

$C_7=d_1\oplus d_3\oplus d_4$, $C_8=d_2\oplus d_3\oplus d_4$ **[WBUT 2009, 2012, 2014]**

a) Find the generator matrix and the parity check matrix for this code.
b) Find the minimum weight of this code.
c) Find the error detecting and the error correcting capability of this code.
d) Show through an example that this code can detect three errors/code word.

Answer:

a) $C_5=d_1\oplus d_2\oplus d_4$, $C_6=d_1\oplus d_2\oplus d_3$, $C_7=d_1\oplus d_3\oplus d_4$, $C_8=d_2\oplus d_3\oplus d_4$

Obviously, $C_1=d_1$, $C_2=d_2$, $C_3=d_3$ and $c_4=d_4$.

So, we may write

$$C=(d_1,d_2,d_3,d_4)\begin{bmatrix}1&0&0&0&1&1&1&0\\0&1&0&0&1&1&0&1\\0&0&1&0&0&1&1&1\\0&0&0&1&1&0&1&1\end{bmatrix}$$

But $C=d\,G$ where G is the generator matrix

Hence $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$

We know, $G = [I : P]$ where P is the coefficient matrix.

The parity check matrix is $H = [P^T : I_{n-k}]$

Here $P = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$

Hence $P^T = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$

So, the parity check matrix, $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

b) The code vectors and their weights are computed below.

Message	Code word	Weight of the code word
0000	00000000	0
0001	00011011	4
0010	00100111	4
0011	00111100	4
0100	01001101	4
0101	01010110	4
0110	01101010	4
0111	01110001	4
1000	10001110	4
1001	10010101	4
1010	10101001	4
1011	10110010	4
1100	11000011	4
1101	11011000	4
1110	11100100	4
1111	11111111	7

Hence the minimum weight of the code is 4.

c) We know, $t \leq \frac{1}{2}(d_{min} - 1)$
where t is the number of errors that can be corrected.
Here minimum distance, $d_{min} = 4$.

So, $t \leq \frac{1}{2}(4-1)$

or, $t \leq \frac{3}{2}$

So, $t = 1$

Thus the code is a single error-correcting code.
If ℓ is the error-detecting capability of the code i.e., the number of errors that the code can detect, then

$$\ell \leq d_{min} - 1$$

or, $\ell \leq 4 - 1$

or, $\ell \leq 3$.

Thus the code can detect three or fewer errors.

d) From the above parity check matrix H we find that the maximum number of 1's in columns of H is 3. Hence this code can detect 3 errors per code word.

3. a) What is standard array? Explain how the standard array can be used to make a correct decoding. **[WBUT 2010, 2014]**

Answer:

Standard Array:

A standard array for an (n, k) code C is an array of all vectors in which the first row consists of the code C with 0 on the extreme left and the other rows are the cosets each arranged in corresponding order with the coset leader on the left.
If c is an (n, k) code and a is any vector of length n, then the set a + c is called a coset of c. Mathematically, $a + c = \{a + x \mid x \in c\}$
The vector having the minimum weight in a coset is called a coset leader. In case there is more than one vector with the minimum weight, then one of them is chosen at random and this randomly chosen vector is called the coset leader.

Syndrome Decoding with Standard Array:

Let H be a parity check matrix of an (n, k) code. For any vector r, the vector $S = rH^T$ is called the syndrome of r where H^T is the transpose of the matrix H. A syndrome gives the symptoms of the error and thus helps us to diagnose the error. Each member of a coset has the same syndrome. The syndrome for each coset is different from that of any other coset in the code.

Decoding is possible using syndromes. The technique is known as syndrome decoding. The following steps are followed in syndrome decoding.

Step 1: First determine the syndrome $S = rH^T$ of the received word, r.
Step 2: Locate the syndrome in the 'syndrome column' of a standard array.
Step 3: Determine the corresponding coset leader which is the error vector, e.
Step 4: Subtract the error vector from the received word, r, to get the code word $C = r - e$.
Let us take the following example to explain the above algorithm.

b) Consider the $(7, 4)$ linear block code whose decoding table is given below:

Syndrome	Coset leader
100	1000000
010	0100000
001	0010000
110	0001000
011	0000100
111	0000010
101	0000001

Show with an example that this code can correct any single error but makes a decoding error when two or more errors occur. **[WBUT 2010, 2014]**

Answer:

Let the transmitted code word be $v = 1\ 0\ 0\ 1\ 1\ 1\ 1$ and the received vector is $r = 1\ 0\ 0\ 1\ 1\ 1\ 1$. Thus there is a single error in the received vector.

Now let us compute the syndrome of r which is given by

$$s = rH^T = (1\ 0\ 0\ 1\ 1\ 1\ 1) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = (0\ 1\ 1)$$

From the given decoding table it is found that the syndrome $(0\ 1\ 1)$ corresponds to the coset leader $e = (0\ 0\ 0\ 0\ 1\ 0\ 0)$.

Thus $(0\ 0\ 0\ 0\ 1\ 0\ 0)$ is assumed to be the error pattern caused by the channel.

Hence r is decoded into

$$v^* = r + e = (1\ 0\ 0\ 1\ 1\ 1\ 1) + (0\ 0\ 0\ 0\ 1\ 0\ 0) = (1\ 0\ 0\ 1\ 0\ 1\ 1)$$

This is the actual code vector transmitted.

Now let the transmitted code vector be $v = (0\ 0\ 0\ 0\ 0\ 0\ 0)$ and the received vector be $r = (1\ 0\ 0\ 0\ 1\ 0\ 0)$. This indicates that two errors have occurred during the transmission of v.

When r is received, the receiver computes the syndrome

$$s = rH^T = (1\ 0\ 0\ 0\ 1\ 0\ 0)\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = (1\ 1\ 1)$$

From the decoding table we find that the coset leader $e = (0\ 0\ 0\ 0\ 0\ 1\ 0)$ corresponding to the syndrome $s = (1\ 1\ 1)$. Hence r is decoded into the code vector

$$v^* = r + e = (1\ 0\ 0\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 0\ 0\ 1\ 0) = (1\ 0\ 0\ 0\ 1\ 1\ 0)$$

We find that v^* is not the actual code vector transmitted and a decoding error is committed.

c) Show that if the minimum distance of a t-error correcting code is d_{min}, then $t \le (d_{min} - 1)/2$. **[WBUT 2010, 2014]**

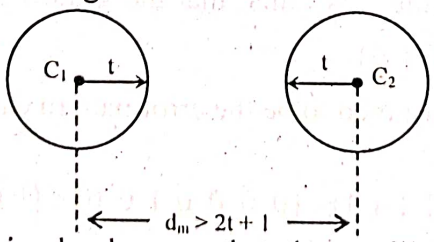
OR,

Prove that $d_{min} \ge 2t + 1$, where t = Number of error. **[WBUT 2018]**

Answer:

Let us consider an (n, k) linear block code. It is required to detect and correct all error patterns over a binary symmetric channel. In the above code, the Hamming weight is less than or equal to t. We assume that the 2^k vectors in the code are transmitted with equal probability.

Any received word can be represented by a q–ary vector of length n. Every q–ary vector can be represented as a point in space containing all q–ary n–tuples. All words at a Hamming distance of t or less would lie within the sphere centered at the codeword and with a radius of t. This sphere is called the Decoding sphere of the corresponding codeword. This is shown in the diagram below:



From the above diagram it is clearly seen that there will be errors in decoding if the spheres centered around different code words overlap. If the two spheres touch, then there will be ambiguity in the detection of codeword. Therefore, if the Hamming distance of the code, $d(x_i, x_j)$, is such that

$$d(x_i, x_j) > 2t + 1$$

then no two decoding spheres of the code intersect or touch. Thus we see that an (n, k) linear block code has the power to correct all error patterns of weight t or less if and only if $d(x_i, x_j) \le 2t + 1$ for all x_i and x_j

However, the smallest distance between any pair of code vectors in a code is the minimum distance of the code, d_{min}.

Hence $d_{min} \le 2t + 1$

or, $t \le \left[\frac{1}{2}(d_{min} - 1)\right]$.

Thus we can say that an (n, k) linear block code of minimum distance d_{min} can correct up to t errors if and only if $t \le \left[\frac{1}{2}(d_{min} - 1)\right]$,

where [. .] denotes the largest integer no greater than the enclosed number.

4. Consider a systematic $(8, 4)$ code with parity check equations **[WBUT 2011]**

$$V_0 = U_0 + U_1 + U_2$$
$$V_1 = U_1 + U_2 + U_3$$
$$V_2 = U_0 + U_1 + U_3$$
$$V_3 = U_0 + U_2 + U_3$$

where U_0, U_1, U_2 and U_3 are message, V_0, V_1, V_2 and V_3 are parity check digit

i) **Find the generator matrix and the parity check matrix for this code.**
ii) **Find the minimum weight for this code.**
iii) **Find the error detecting and the error correcting capability of this code.**
iv) **Show through an example that the code can detect three errors in code word.**

Answer:

i) Given,

$$V_0 = U_0 + U_1 + U_2$$
$$V_1 = U_1 + U_2 + U_3$$
$$V_2 = U_0 + U_1 + U_3$$
$$V_3 = U_0 + U_2 + U_3$$

Obviously,

$$V_4 = U_0$$
$$V_5 = U_1$$
$$V_6 = U_2$$
$$V_7 = U_3$$

If G is the generator matrix then, [G] [U] = [V].

Hence, the generator matrix is,

$$[G] = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We know, $G = [P \vdots I_k]$ and the parity check matrix is $H = [I_k : P^T]$.

$$P^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

So, $H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$

ii) It is found that all columns of H are non-zero and no two columns are alike. Therefore, no two or fewer columns sum to zero. Hence minimum weight or minimum distance of this code is at least 4. However, zeroeth, fourth, fifth and sixth columns sum to zero. Hence the minimum weight of the code is 4.

iii) $t \le \frac{1}{2}(d_{min} - 1)$ where t is the number of errors that can be corrected.

Here, minimum distance = 4.

So, $t \le \frac{1}{2}(4-1)$

or, $t \le \frac{3}{2}$

or, $t = 1$.

Thus the code can correct single error.

If k is the number of errors that the code can detect, then

$k \le d_{min} - 1$

or, $k \le 4 - 1$

or, $k \le 3$

Thus the code can detect three or fewer errors.

iv) From the above parity check matrix, H, we find that the maximum number of 1's in columns of H is 3. Hence the code can detect 3 errors per code word.

5. a) Show that $C=(0000,1100,0011,1111)$ is a linear code. What is its minimum distance? **[WBUT 2011]**

Answer:

Let $C_1 = 0000$, $C_2 = 1100$, $C_3 = 0011$, $C_4 = 1111$

Now, $C_3 + C_2 = 1111 = C_4$

$C_2 + C_4 = 0011 = C_3$

$C_3 + C_4 = 1100 = C_2$

Hence, C is a linear code.

The minimum distance is 2.

b) A $(7,3)$ linear code has the following generator matrix: **[WBUT 2011]**

$$G=\begin{bmatrix}1 & 1 & 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 1 & 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 1 & 0 & 0 & 1\end{bmatrix}$$

Determine a systematic form of *G*. Hence find the parity-check matrix *H* for the code.

Answer:

$$G=\begin{bmatrix}1 & 1 & 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 1 & 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 1 & 0 & 0 & 1\end{bmatrix}$$

Adding second row to first row, we get

$$G=\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 1 & 0\\ 0 & 1 & 1 & 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 1 & 0 & 0 & 1\end{bmatrix}$$

Adding first row to third row, we get

$$G=\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 1 & 0\\ 0 & 1 & 1 & 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 1 & 1 & 1\end{bmatrix}$$

Adding second row to third row, we get

$$G=\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 1 & 0\\ 0 & 1 & 1 & 1 & 0 & 1 & 0\\ 0 & 0 & 1 & 1 & 1 & 0 & 1\end{bmatrix}$$

Adding third row to second row, we get

$$G=\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 1 & 1 & 1\\ 0 & 0 & 1 & 1 & 1 & 0 & 1\end{bmatrix}$$

This is in systematic form

$$P \text{ in } G = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

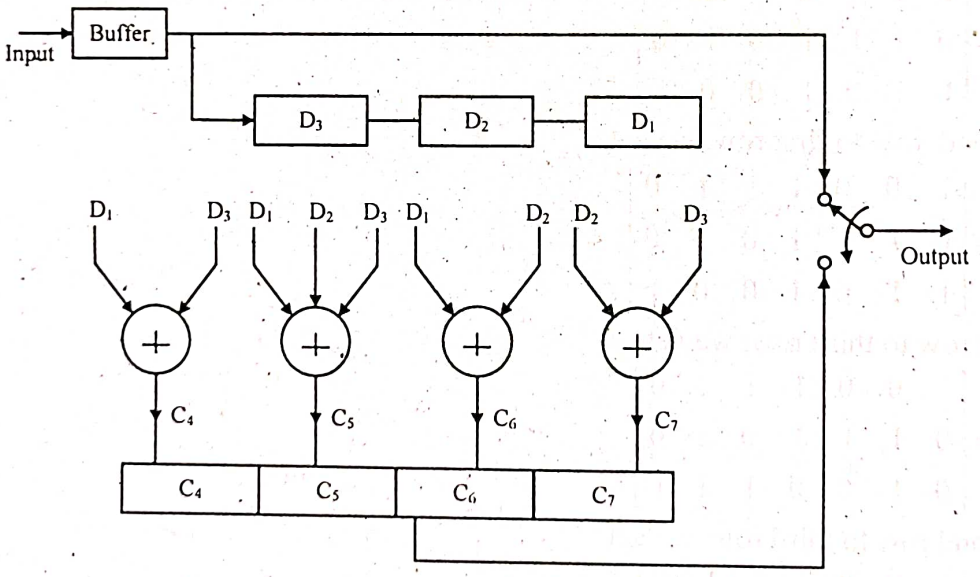
So, $$P^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Hence, H = Parity check matrix $= \left[\begin{array}{ccc|cccc} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$

c) Design the encoder circuit for the above code. **[WBUT 2011]**

Answer:

The encoder circuit for the above code is as shown below.



6. One parity check code has parity check matrix as: **[WBUT 2013]**

$$H = \left[\begin{array}{ccc:ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

i) Determine generator matrix

ii) Find the code word that begins with [101]

iii) If received word is [110110], then decode this word.

Answer:

i) H is a 6×3 matrix and $n = 6$ and $k = 3$.

$$H = [P^T : I_{n-k}]$$

So, $$P^T = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Hence, $$P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

So, $$G = [I : P] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

ii) $$C = DG = [1\ 0\ 1] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [1\ 0\ 1\ 0\ 1\ 1]$$

iii) $R = [1\ 1\ 0\ 1\ 1\ 0]$

So $$S = RH^T = [1\ 1\ 0\ 1\ 1\ 0] \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0\ 1\ 1]$$

Since S is equal to the second row of H^T, an error is at the second bit. The correct code word is 1 0 0 1 1 0 and the data bits are 1 0 0.

7. a) A (7, 1) repetition code used to encode information sent through a channel with a bit error probability of 0.01. Find the probability that an information bit is erroneous after coding. **[WBUT 2013]**

Answer:

Let P_e be the probability that an information bit is erroneous after decoding then,

$$P_e = {}^7C_4 P^4 (1-p)^3 + {}^7C_5 P^5 (1-p)^2 + {}^7C_6 P^6 (1-p) + {}^7C_7 P^7$$

Here, $p = 0.01$

$${}^7C_4 = 35,\ {}^7C_5 = 21,\ {}^7C_6 = 7 \text{ and } {}^7C_7 = 1$$

So, $$P_e = 35(0.01)^4 (1-0.01)^3 + 21(0.01)^5 (1-0.01)^2 + 7(0.01)^6 (1-0.01) + 1(0.01)^7$$

$$\simeq 3.4 \times 10^{-7}.$$

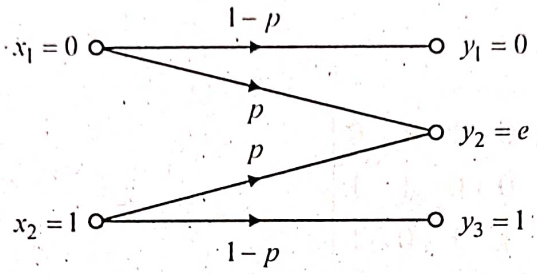
b) A channel has the following channel matrix: **[WBUT 2013]**

$$[P(Y/X)]\begin{bmatrix} 1-P & P & 0 \\ 0 & P & 1-P \end{bmatrix}$$

Draw the channel diagram. If the source has equally likely outputs, compute the probability associated with the channel outputs for $p = 0.2s$.

Answer:

The channel diagram is shown below:



$$[P(Y)] = (0.5 \quad 0.5)\begin{bmatrix} 0.8 & 0.2 & 0 \\ 0 & 0.2 & 0.8 \end{bmatrix} = [0.4 \quad 0.2 \quad 0.4]$$

Then, $P(Y_1) = 0.4$, $P(Y_2) = 0.2$ and $P(Y_3) = 0.4$

8. What is Hamming distance? Give relation between minimum distance and error detecting and correcting capability. Describe a Hamming code. Also define Hamming sphere and Hamming bound. **[WBUT 2013]**

OR,

What is Hamming distance? Give relation between minimum distance and error correcting capability. Define Hamming bound. **[WBUT 2017]**

Answer:

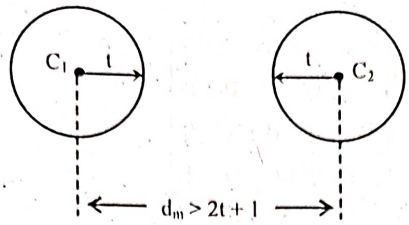
1st Part:

The Hamming distance between two code words is defined as the number of places in which the code words differ. For example, let two code words be 1010 and 0111. The two code words differ at three places and hence the Hamming distance between these two code words is 3.

2nd Part:

Let us consider an (n, k) linear block code. It is required to detect and correct all error patterns over a binary symmetric channel. In the above code, the Hamming weight is less than or equal to t. We assume that the 2^k vectors in the code are transmitted with equal probability.

Any received word can be represented by a q–ary vector of length n. Every q–ary vector can be represented as a point in space containing all q–ary n–tuples. All words at a Hamming distance of t or less would lie within the sphere centered at the codeword and with a radius of t. This sphere is called the Decoding sphere of the corresponding codeword. This is shown in the diagram below:



From the above diagram it is clearly seen that there will be errors in decoding if the spheres centered around different code words overlap. If the two spheres touch, then there will be ambiguity in the detection of codeword. Therefore, if the Hamming distance of the code, $d(x_i, x_j)$, is such that then no two decoding spheres of the code intersect or touch. Thus we see that an (n, k) linear block code has the power to correct all error patterns of weight t or less if and only if

$$d(x_i, x_j) \leq 2t + 1 \quad \text{for all } x_i \text{ and } x_j$$

However, the smallest distance between any pair of code vectors in a code is the minimum distance of the code, d_{min}.

Hence

$$d_{min} \leq 2t + 1$$

$$\text{or,} \quad t \leq \left[\tfrac{1}{2}(d_{min} - 1)\right]$$

Thus we can say that an (n, k) linear block code of minimum distance d_{min} can correct up to t errors if and only if

$$t \leq \left[\tfrac{1}{2}(d_{min} - 1)\right],$$

where [. .] denotes the largest integer no greater than the enclosed number.

3rd Part:

Hamming code is a family of (n, k) linear block codes that have the following parameters:

Block length, $n = 2^m - 1$

Number of message bits, $k = 2^m - m - 1$

Number of parity bits = $m = n - k$

Error correcting capability = $t = 1$ ($d_{min} = 3$)

For example, (7, 4) Hamming code is a family of linear block codes with n = 7 and k = 4 corresponding to m = 3.

Hamming codes were invented by R.W. Hamming in 1950. There are both binary and non-binary Hamming codes. Hamming codes are the first class of linear codes devised for error correction. These codes and their variations have been widely used for error control in digital communication and data storage systems.

The generator matrix of a linear block code is a $k \times n$ matrix. For a (7, 4) Hamming code an appropriate generator matrix may be given by

$$G = \left[\begin{array}{cccc:cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

P $\qquad$ I_K

where P is $k \times (n-k)$ coefficient matrix and I is the $k \times k$ Identity matrix

From the above generator matrix we may find the parity check matrix, H, given by $H = \left[I_{n-k} : P^T\right]$.

$$\text{So, } H = \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

I_{n-k} $\qquad$ P^T

Since k = 4, there are $2^k = 2^4 = 16$ distinct message words.

From the generator matrix we can form all the 16 code words corresponding to sixteen distinct message words. From the code words we can find the weight of each code word. The complete list of sixteen code wards of the above (7, 4) Hamming code is given below.

Message Word	Code Word	Weight of Code Word
0 0 0 0	0 0 0 0 0 0 0	0
0 0 0 1	1 0 1 0 0 0 1	3
0 0 1 0	1 1 1 0 0 1 0	4
0 0 1 1	0 1 0 0 0 1 1	3
0 1 0 0	0 1 1 0 1 0 0	3
0 1 0 1	1 1 0 0 1 0 1	4
0 1 1 0	1 0 0 0 1 1 0	3
0 1 1 1	0 0 1 0 1 1 1	4
1 0 0 0	1 1 0 1 0 0 0	3
1 0 0 1	0 1 1 1 0 0 1	4
1 0 1 0	0 0 1 1 0 1 0	3
1 0 1 1	1 0 0 1 0 1 1	4
1 1 0 0	1 0 1 1 1 0 0	4
1 1 0 1	0 0 0 1 1 0 1	3
1 1 1 0	0 1 0 1 1 1 0	4
1 1 1 1	1 1 1 1 1 1 1	7

From the above list of codewords it is seen that the smallest of the Hamming weights for the non-zero codewords is 3. Thus the minimum distance of the code is 3. In fact, Hamming codes have the property that the minimum distance, d_{min} of the code is equal to 3. This is independent of the value assigned to m.

An important property of Hamming codes is that they satisfy the condition for Hamming bound with equality sign with $t = 1$. Hamming bound is given by

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i}$$

For (7, 4) Hamming code, the Hamming condition becomes

$$2^{7-4} \geq \sum_{i=0}^{1} \binom{7}{i}$$

This shows that Hamming codes are single error correcting binary perfect codes.
Moreover, from the condition

$$t \leq \left[\tfrac{1}{2}(d_{\min} - 1)\right]$$

Putting $d_{\min} = 3$ we get $t \leq 1$. With the equality sign $t = 1$.
For Hamming's single error correcting codes the syndrome of a received vector is equal to the $j\ th$ row of H^T. There is no ambiguity in associating a unique error vector with each of the first k rows of H^T. Each row in H^T has (n – k) entries and all zero entry is not possible in H^T. Hence we can have $2^{n-k} - 1$ distinct rows of H^T. The condition for all of these rows in H^T to be distinct is

$$2^{n-k} - 1 \geq n$$

i.e. $(n-k) \geq \log_2(n+1)$

i.e. $n \geq k + \log_2(n+1)$

This relation is useful in designing block code since the minimum size of the codeword i.e. n can be determined from this relation.

Now $$H^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Let the message vector is 1 1 0 1. Then the corresponding code vector D is 0 0 0 1 1 0 1.
Let the third bit in the code word D is in error at the receiving end.

r = Received Word = [0 0 1 1 1 0 1]

↑
error

The syndrome of r is $S = r H^T$.

$$\text{So, } S=[0001101]\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\\1&1&0\\0&1&1\\1&1&1\\1&0&1\end{bmatrix}=[001]=eH^T$$

Note that the third row of H^T is same as that of the syndrome. This has happened because the third bit of the code word was in error. Thus the transmitted word is [0 0 0 1 1 0 1].

4th Part:

An (n, k) linear block code can correct up to t errors per code word provided it satisfies the relation

$$2^{n-k}\geq\sum_{i=0}^{t}\binom{n}{i}\text{ where }\binom{n}{i}=\frac{n!}{(n-i)!\,i!}$$

This relation is known as Hamming bound. Hamming bound is also called the Sphere Packing Bound. This bound holds good for non-linear codes as well.

9. a) Define code rate and block length. **[WBUT 2015]**

b) Give diagrammatic representation of block encoder.

c) The generator matrix of a (7, 4) block code is given by

$$G=\begin{bmatrix}1&1&1&1&0&0&0\\1&0&1&0&1&0&0\\0&1&1&0&0&1&0\\1&1&0&0&0&0&1\end{bmatrix}$$

i) Find H, the parity check matrix of the code.

ii) Find the syndrome for the received vector 1101101. Is this a valid code vector?

iii) Find all code words of the code.

iv) What is error correcting capability of the code?

v) What is error detecting capability of the code?

Answer:

a) The code rate of an (n, k) code is defined as the ratio k/n. It denotes the fraction of the codeword that consists of the information symbols. Code rate is also called rate efficiency of the code.

Let the codeword with n bits be transmitted in more time than is required for the transmission of the k information bits.

Let T_b = bit duration of the uncoded word

T_c = bit duration of the coded word.

Obviously, $n\,T_c = k\,T_b$.

Also $T_c = \frac{1}{f_c}$ and $T_b = \frac{1}{f_b}$

So, $\frac{f_c}{f_b} = \frac{T_b}{T_c} = \frac{n}{k}$

or, Code Rate, $R_c = \frac{k}{n} = \frac{T_c}{T_b} = \frac{f_b}{f_c}$

It may be noted that the smaller the code rate, the greater the redundancy. In other words, smaller code rate means more of redundant symbols are present per information symbol in a code word. A code with smaller code rate has the potential to detect and correct more of symbols in error. But it reduces the actual rate of transmission of information. Code rate is always less than unity.

A block code is a set of fixed length code words. The fixed length of these code words is called the block length. It is typically denoted by the symbol n.

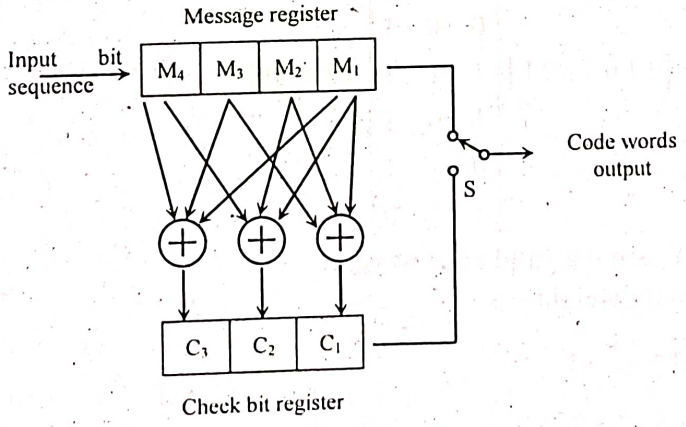
b) Let us consider $a(7,4)$ block code. The encoder for this code is implemented by the generator matrix. Let the generator matrix be:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The parity check bits are obtained from the message bits by mod-2 additions, according to the following equations.

$$c_1 = m_1 \oplus m_2 \oplus m_3$$
$$c_2 = m_1 \oplus m_2 \oplus m_4$$
$$c_3 = m_1 \oplus m_3 \oplus m_4$$

These are implemented by four message register M_1, M_2, M_3 and M_4 and three EXOR gates as shown below.



The switch 'S' is connected to message register first and all message bits are transmitted. The switch is then connected to the check bit register and check bits are transmitted. This forms a block of 7 bits. The input bits are then taken for next block.

c) (i) Here, $G = [P : I_k]$

Now, C = DG,

Hence,

Messages	Code Vectors
0 0 0 0	0 0 0 0 0 0 0
0 0 0 1	1 1 0 0 0 0 1
0 0 1 0	0 1 1 0 0 1 0
0 1 1 1	1 0 1 0 0 1 1
0 1 0 0	1 0 1 0 1 0 0
0 1 0 1	0 1 1 0 1 0 1
0 1 1 0	1 1 0 0 1 1 0
0 1 1 1	0 0 0 0 1 1 1
1 0 0 0	1 1 1 1 0 0 0
1 0 0 1	0 0 1 1 0 0 1
1 0 1 0	1 0 0 1 0 1 0
1 0 1 1	0 1 0 1 0 1 1
1 1 0 0	0 1 0 1 1 0 0
1 1 0 1	1 0 0 1 1 0 1
1 1 1 0	0 0 1 1 1 1 0
1 1 1 1	1 1 1 1 1 1 1

(ii) $H = \left[I_{n-k} \vdots P^T \right] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$

(iii) $S = r H^T = [1\,1\,0\,1\,1\,0\,1] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} = [0\,1\,0]$

Thus 1 1 0 1 1 0 1 is not a valid code word.

(iv) d_{min} = minimum weight = 3

So, $t = \dfrac{d_{min} - 1}{2} = 1$

(v) $m = d_{min} - 1 = 3 - 1 = 2$

10. One parity check code has parity check matrix as

$H = 110:100$
$\quad 101:010$
$\quad 100:001$

i) Determine generator matrix
ii) Find the code word that begins with [100]
iii) If received word is [110011], then decode this word **[WBUT 2017]**

Answer:

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \left[P^T : I_{n-k} \right]$$

So, $P^T = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ Hence, $P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

$$G = [I : P] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$C = DG = [1 \quad 0 \quad 0] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} = [1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1]$$

$R = [1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1]$ and $H^T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

So, $S = RH^T = [1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0 \quad 0 \quad 1]$

$= 6^{th}$ row of H^T

Thus, 6^{th} bit is in error.

Correct code word is $[1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0]$.

11. a) Prove that for (n, k) Linear block code $2^{n-k} \geq \sum_{i=0}^{t} nCi$, $t =$ number of error.

[WBUT 2018]

Answer:

We know that in an (n, k) block code, there are a total of 2^{n-k} syndromes, including the all-zero syndrome. It is known that each syndrome corresponds to a specific error pattern.

For an n-bit code word, the number of error patterns $= \binom{n}{i}$ where i is the number of error locations in the n-by-1 error pattern, e.

Hence, the total number of all possible error patterns

$$= \text{Sum of } \binom{n}{i} \text{ for } i = 0, 1, \cdots\cdots, t = \sum_{i=0}^{t} \binom{n}{i}$$

where t is the maximum number of error location in e.

It is seen that if an (n, k) linear block code is to be able to correct up to t errors, the total number of syndromes must not be less than the total number of all possible error patterns.

Thus the block length n and the number of message bits k must satisfy the Hamming bound i.e.

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i}$$

b) Consider a systematic (8, 4) code whose parity check equations are

$$V_0 = U_1 + U_2 + U_3$$
$$V_1 = U_0 + U_1 + U_2$$
$$V_2 = U_0 + U_1 + U_3$$
$$V_3 = U_0 + U_2 = U_3$$

where U_0, U_1, U_2 and U_3 are message digits and V_0, V_1, V_2 and V_3 are parity check digits. Find the generator and parity check matrices for this code. Show analytically that the minimum distance of this code is 4. **[WBUT 2018]**

Answer:

Refer to Question No. 1 of Long Answer Type Questions.

12. Consider a (6, 3) linear block code define by the generator matrix.

$$G = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{vmatrix}$$

a) Determine if the code is a Hamming-code. Find the parity check matrix H of the code is symmetrical form.

b) Find is the encoding table for the linear block code.

c) What is the minimum distance d_{min} of the code?

d) For a particular code word transmitted, the received code word is 111110. Find the corresponding data word transmitted. **[WBUT 2018]**

Answer:

We consider a (6, 3) linear code defined by the generator matrix G given by

$$G = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{vmatrix}$$

(a) For a Hamming code, the following conditions should be satisfied.

Block length, $n = 2^m - 1$

Number of message bits $= k = 2^m - m - 1$

Number of parity bits $= m = n - k$

In the given case, $n = 6$, $k = 3$

So, $m = n - k = 6 - 3 = 3$

But it does not satisfying the conditions of block length, n and number of message bits k.

$n = 2^m - 1 = 2^3 - 1 = 8 - 1 = 7$.

But here $n = 6$

Also $k = 2^m - m - 1 = 2^3 - 3 - 1 = 8 - 3 - 1 = 4$

But in our case $k = 3$.

So, the given (6, 3) code is not a Hamming code.

$$G = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{vmatrix} = [P \ : \ I]$$

where $P = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{vmatrix}$

So, $P^T = \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix}$

$$H = |I \ : \ P^T| = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{vmatrix}$$

(b) Now the codes are the following:

$$c_1 = [0\ 0\ 0]\begin{bmatrix}1&0&0&1&0&1\\0&1&0&1&1&0\\0&0&1&0&1&1\end{bmatrix} = [0\ 0\ 0\ 0\ 0\ 0]$$

$$c_2 = [0\ 0\ 1]\begin{bmatrix}1&0&0&1&0&1\\0&1&0&1&1&0\\0&0&1&0&1&1\end{bmatrix} = [1\ 0\ 1\ 0\ 0\ 1]$$

$$c_3 = [0\ 1\ 0]\begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix} = [0\ 1\ 1\ 0\ 1\ 0]$$

$$c_4 = [0\ 1\ 1]\begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix} = [1\ 1\ 0\ 0\ 1\ 1]$$

$$c_5 = [1\ 0\ 0]\begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix} = [1\ 1\ 0\ 1\ 0\ 0]$$

$$c_6 = [1\ 0\ 1]\begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix} = [0\ 1\ 1\ 1\ 0\ 1]$$

$$c_7 = [1\ 1\ 0]\begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix} = [1\ 0\ 1\ 1\ 1\ 0]$$

$$c_8 = [1\ 1\ 1]\begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix} = [0\ 0\ 0\ 1\ 1\ 1]$$

Thus the encoding table is an under

Transmitted word	Code word
000	000000
001	101001
010	011010
011	110011
100	110100
101	011101
110	101110
111	000111

(c) To find the minimum distance, d_{min}, let us find the Hamming weight of each codeword as under

Code word	Hamming weight, w
$c_1 = 000000$	0
$c_2 = 101001$	3
$c_3 = 011010$	3
$c_4 = 110011$	4
$c_5 = 110100$	3
$c_6 = 011101$	4
$c_7 = 101110$	4
$c_8 = 000111$	3

(d) We observe that the minimum weight of non-zero code word is 3. Hence, $d_{min} = 3$.

The received code word, $R = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0]$

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

So, $$H^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Thus, the syndrome,

$$S = RH^T = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = [0 \quad 1 \quad 0]$$

S is equal to the second row of H^T. So, an error is in the second bit of the received word.

Hence, the correct code word is $[1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0]$ which corresponds to the code word c_7.

Thus, the transmitted word is $[1 \quad 1 \quad 0]$.

13. Write short notes on the following:
a) Hamming code [WBUT 2010, 2011, 2014, 2017]
b) Standard array [WBUT 2012]
c) Standard array decoding [WBUT 2013, 2015, 2016]

Answer:

a) Hamming code:

Hamming code is a family of (n, k) linear block codes that have the following parameters:

Block length, $n = 2^m - 1$

Number of message bits, $k = 2^m - m - 1$

Number of parity bits = m = n – k

Error correcting capability = $t = 1$ ($d_{min} = 3$)

For example, (7, 4) Hamming code is a family of linear block codes with n = 7 and k = 4 corresponding to m = 3.

Hamming codes were invented by R.W. Hamming in 1950. There are both binary and non-binary Hamming codes. Hamming codes are the first class of linear codes devised for error correction. These codes and their variations have been widely used for error control in digital communication and data storage systems.

The generator matrix of a linear block code is a $k \times n$ matrix. For a (7, 4) Hamming code an appropriate generator matrix may be given by

$$G = \left[\begin{array}{cccc:cccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\underbrace{\qquad\qquad}_{P} \qquad\qquad \underbrace{\qquad\qquad}_{I_K}$$

where P is $k \times (n-k)$ coefficient matrix and I is the $k \times k$ Identity matrix

From the above generator matrix we may find the parity check matrix, H, given by $H = \left[I_{n-k} : P^T\right]$

$$\text{So, } H = \left[\begin{array}{cccc:cccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

$$\underbrace{\qquad\qquad}_{I_{n-k}} \qquad\qquad \underbrace{\qquad\qquad}_{P^T}$$

The smallest of the Hamming weights for the non-zero codewords is 3. Thus the minimum distance of the code is 3. In fact, Hamming codes have the property that the minimum distance, d_{min} of the code is equal to 3. This is independent of the value assigned to m.

b) Standard array:

A standard array for an (n, k) code C is an array of all vectors in which the first row consists of the code C with 0 on the extreme left and the other rows are the cosets each arranged in corresponding order with the coset leader on the left.

Coset and Coset Leader: If c is an (n, k) code and a is any vector of length n, then the set $a + c$ is called a coset of c. Mathematically, $a + c = \{a + x \mid x \in c\}$

A coset is also called a translate. It is the short form of "a set of numbers having a common feature".

The vector having the minimum weight in a coset is called a coset leader. In case there is more than one vector with the minimum weight, then one of them is chosen at random and this randomly chosen vector is called the coset leader.

c) Standard array decoding:

Decoding means obtaining the information symbols from the received code words. The standard array comprises all possible code words. Hence the received code word can always be identified with one of the elements of the standard array.

If the received code word is a valid codeword no errors have occurred. In the case the received word 'v' does not belong to the set of valid code words, we feel that an error has occurred. From the decoder we find the coset leader is the error vector e. The decoder decodes the codeword as v – e. This codeword is found at the top of the column containing v. Thus we can decode the codeword as the one on the top of the column containing the received word.

The above decoding process can be explained with the example considered above. Let the code c = {0 0 0 0, 1 0 1 1, 0 1 0 1, 1 1 1 0}. Let the received word $r = 1101$. Since this is not a valid codeword it is inferred that an error has occurred. Now let us find out which one of the four possible code words was actually transmitted. The standard array is shown below.

$r - e$ ↓

	0 0 0 0	1 0 1 1	0 1 0 1	1 1 1 0
$e \rightarrow$	1 0 0 0	0 0 1 1	1 1 0 1	0 1 1 0
	0 1 0 0	1 1 1 1	0 0 0 1	1 0 1 0
	0 0 1 0	1 0 0 1	0 1 1 1	1 1 0 0

r

We find that $r = 1101$ lies in the third column. The topmost entry of this column is 0 1 0 1. Hence the estimated codeword is 0 1 0 1. The error vector e is the coset leader and e = 1000.

CYCLIC CODES

Multiple Choice Type Questions

1. The generator polynomial of a cyclic code is a factor of [WBUT 2008, 2009, 2011, 2012]

a) X^n+1 b) $X^{(n+1)}+1$ c) $X^{(n+2)}+1$ d) none of these

Answer: (a)

2. A polynomial is called monic if [WBUT 2008, 2011]

a) odd terms are unity b) even terms are unity

c) leading coefficient is unity d) leading coefficient is zero

Answer: (c)

3. A (7, 4) cyclic code is generated by a generator polynomial of degree [WBUT 2009, 2012, 2013]

a) 3 b) 2 c) 4 d) 5

Answer: (a)

4. Cyclic Redundancy Check is a type of [WBUT 2010]

a) Convolution code b) Cyclic code

c) Parity check code d) None of these

Answer: (b)

5. For a (7, 4) cyclic code generated by $g(x)=1+x+x^3$ the syndrome for the error pattern $e(x)=x^3$ is [WBUT 2011, 2014, 2019]

a) 101 b) 111 c) 110 d) 011

Answer: (c)

6. The syndrome polynomial in a cyclic code solely depends on [WBUT 2013]

a) generator polynomial b) parity polynomial

c) error polynomial d) code word

Answer: (c)

7. Cyclic redundancy check is a type of [WBUT 2014]

a) Convolution code b) Cyclic code

c) Parity check code d) none of these

Answer: (b)

8. The properties of Cyclic code is / are [WBUT 2016]

a) Linearity b) Cyclic

c) Both (a) and (b) d) None of these

Answer: (c)

9. For $a(7,4)$ cyclic code generated by $g(x)=x^3+x+1$. The syndrome for error pattern $e(x)=x^3$ is [WBUT 2017]

a) 101 b) 111 c) 110 d) 011

Answer: (c)

10. Which among the below stated logical circuits are present in encoder and decoder used for the implementation of cyclic codes? [WBUT 2017]

A) Shift register
B) Modulo-2 adders
C) Counters
D) Multiplexers

a) A and B b) C and D c) A and C d) B and D

Answer: (a)

11. The generator polynomial of a cyclic code is factor of [WBUT 2017]

a) X^n+1 b) $X^{(n+1)}+1$ c) $X^{(n+2)}+1$ d) $X^{(n-1)}+1$

Answer: (a)

12. Cycle redundancy check is a type of [WBUT 2018]

a) Convolution code b) Cyclic code
c) Parity check code d) None of these

Answer: (b)

Short Answer Type Questions

1. What do you mean by Cyclic Burst? [WBUT 2010]

Answer:

A cyclic burst of length B is a vector whose non-zero components are among B successive components, the first and last of which are non-zero.

2. A $(8,4)$ cyclic code is generated by $g(X)=1+X+X^4$. Find the generator and parity-check matrix in systematic form. [WBUT 2011, 2014]

Answer:

It is known that if g(x) is a polynomial of degree (n-K) and it is also a factor of x^n+1, then g(x) is the generator polynomial of an (n, k) cyclic code. Also, if h(x) is the parity check polynomial of the cyclic code, then $g(x)h(x) = x^n+1$

In the given problem, $n = 8$ and $k = 4$. Hence $n-k=4$.

$g(x)=1+x+x^4$

is a polynomial of degree 4.

But, $1+x+x^4$ is not a factor of x^n+1. Hence, though $1+x+x^4$ is a polynomial of degree (n-k) =4, it is not a generator polynomial of x^n+1.

So, h(x) can not be determined.

3. What is irreducible polynomial? What do you mean by polynomial over $GF(2)$. Prove that $f(X)=1+X+X^3$ is a irreducible polynomial over $GF(2)$. [WBUT 2017]

Answer:

A polynomial of the form

$f(x)=f_0+f_1x+f_2x^2+\cdots+f_nx^n$ is defined as a polynomial over GF(2).

Here $f_0, f_1, \cdots f_n$ are the coefficients of the polynomial and they are either 0 or 1.

A polynomial $p(x)$ defined over GF(2) of degree m is said to be irreducible if $p(x)$ has no factor polynomial of degree higher than zero and lower than m.

An irreducible polynomial over the binary field GF(2) of degree m is a factor of the polynomial $\left(x^{2^m-1}+1\right)$

In this case, $f(x)=1+x+x^3$

Here $m=3$ and $x^{2^m-1}+1=x^7+1$

Let us divide $\left(x^7+1\right)$ by $\left(x^3+x+1\right)$

$$
\begin{array}{r|l}
 & x^4+x^2+x+1 \\
\hline
x^3+x+1 & x^7+1 \\
 & x^7+x^5+x^4 \\
\hline
 & x^5+x^4+1 \\
 & x^5+x^3+x^2 \\
\hline
 & x^4+x^3+x^2+1 \\
 & x^4+x^2+x \\
\hline
 & x^3+x+1 \\
 & x^3+x+1 \\
\hline
\end{array}
$$

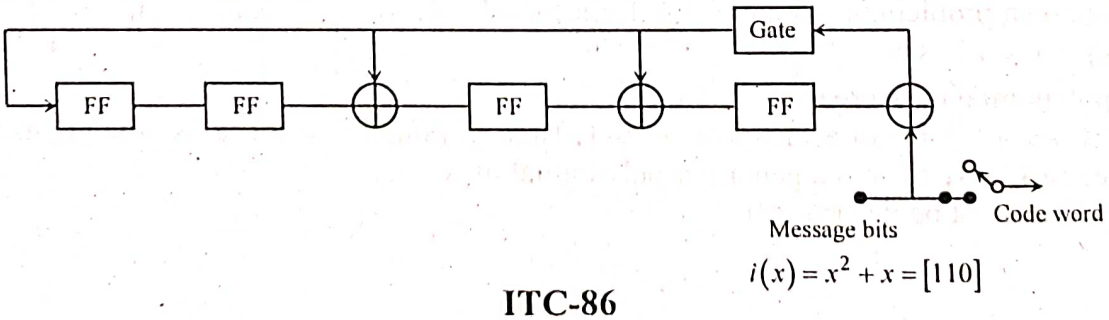
Thus x^3+x+1 is a factor of x^7+1 and hence $f(x)=x^3+x+1$ is an irreducible polynomial over GF(2) of degree 3.

4. Construct the encoder circuit for the (7, 3) code with $g(x)=x^4+x^3+x^2+1$ and input $i(x)=x^2+x$. [WBUT 2017]

Answer:

$g(x)=x^4+x^3+x^2+1$

So, the encoder circuit is as under



$i(x)=x^2+x=[110]$

Initially the register contents are 0 0 0 0. Then 0 will come from the message bits [110]. The register contents subsequently will be as under.

Shift	Input	Register contents
0	–	0 0 0 0
1	0	0 0 0 0
2	1	1 0 1 1
3	1	0 1 0 1

Thus, the message bits are 0 1 1
Parity bits are 0 1 0 1
Hence code word is 0 1 0 1 0 1 1.

5. Given that (7,3) Cyclic code with $g(x)=x^4+x^3+x^2+1$. Construct its dual code.

[WBUT 2017]

Answer:

The parity check polynomial is given by $h(x)$

where $h(x)=\dfrac{x^7+1}{9(x)}=\dfrac{x^7+1}{x^4+x^3+x^2+1}$

let us divide (x^7+1) by (x^4+x^3+x+1)

$$
\begin{array}{l|l}
x^4+x^3+x^2+1 & x^7+1 \quad \Big| \; x^3+x^2+1 \\
& \underline{x^7+x^6+x^5+x^3} \\
& x^6+x^5+x^3+1 \\
& \underline{x^6+x^5+x^3+x^2} \\
& x^4+x^3+x^2+1 \\
& \underline{x^4+x^3+x^2+1} \\
&
\end{array}
$$

Hence, $h(x)=x^3+x^2+1$

The reciprocal polynomial, $h^*(x)=x^3\left(\dfrac{1}{x^3}+\dfrac{1}{x^2}+1\right)=1+x+x^3$

The generator polynomial of the dual code

$=g_p(x)=x^3+x+1$

The block length of the dual code is 7.

The degree of $g(x)$ is 3.

So, the information length is 4.

Therefore, the dual code to the (7, 3) cyclic code is the (7, 4) code with generator matrix given by $g_D(x)=x^3+x+1$

Long Answer Type Questions

1. Let the polynomial $g(X) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ be the generator polynomial of cyclic code over $GF(2)$ with block length 15.

a) Find the parity-check matrix H.
b) How many errors can this code detect?
c) How many errors can this code correct?
d) Write the generator matrix in the systematic form.
e) Find the generator polynomial of its dual code. [WBUT 2010]

Answer:

a) $g(X) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$

$n = 15, n - k = 10$ and $k = 5$

$$h(X) = \frac{X^n + 1}{g(X)} = \frac{X^5 + 1}{X^{10}X^8 + X^5 + X^4 + X^2 + X + 1}$$

$$X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1 \,\big|\, X^5 + 1 \,\big|\, X^5 + X^3 + X + 1$$

$$\frac{X^{15} + X^{13} + X^{10} + X^9 + X^7 + X^6 + X^5}{X^{13} + X^{10} + X^9 + X^7 + X^6 + X^5 + 1}$$

$$\frac{X^{13} + X^{11} + X^8 + X^7 + X^5 + X^4 + X^3}{X^{11} + X^{10} + X^9 + X^8 + X^6 + X^4 + X^3 + 1}$$

$$\frac{X^{11} + X^9 + X^6 + X^5 + X^3 + X^2 + X}{X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1}$$

$$X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$$

So, parity check polynomial, $h(X)$ is

$$h(X) = X^5 + X^3 + X + 1$$

$$h(0) = 1, h(1) = 1, h(2) = 0, h(3) = 1, h(4) = 0, h(5) = 1$$

Hence, the parity check matrix, H is

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

b) $d_{min} \le 1+n-k$

$n=15, k=5$

So, $d_{min} \le 1+15-5$

i.e., $d_{min} \le 11$

e = No. of errors that can be detected

$= d_{min} - 1 = 11-1 = 10$

c) No. of errors that can be corrected $= t$

$$t = \frac{1}{2}(d_{min}-1) = \frac{1}{2}(11-1) = 5.$$

d) To find the generator matrix in its systematic form we add fifth row to the third row, fourth row to the second row and third row to the first row. Thus the generator matrix in its systematic form, G', is given by

$$G' = \left[\begin{array}{ccccc|ccccccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

e) $g(X) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$

Let $h^*(X)$ be the generator polynomial of dual code

$h(X) = X^5 + X^3 + X + 1$

$h^*(X) = X^r h\left(\frac{1}{X}\right)$ where r = degree of $h(X) = 5$

So, $h^*(X) = X^5\left[\left(\frac{1}{X}\right)^5 + \left(\frac{1}{X}\right)^3 + \left(\frac{1}{X}\right) + 1\right] = X^5\left[\frac{1}{X^5} + \frac{1}{X^3} + \frac{1}{X} + 1\right]$

$= 1 + X^2 + X^4 + X^5$

Thus the generator polynomial of dual code is

$g(X) = h^*(X) = X^5 + X^4 + X^2 + 1$

2. a) For a systematic (7, 4) cyclic code determine the generator matrix and parity check matrix if $g(x) = 1 + x + x^3$. **[WBUT 2013, 2015, 2017]**

b) A codeword polynomial $c(x)$, belonging to the (7, 4) code with $g(x) = x^3 + x + 1$, incurs error so giving the received polynomial $v(x)$. Find $c(x)$ when

i) $v(x) = x^5 + x^2 + 1$

ii) $v(x) = x^6 + x^3 + 1$ **[WBUT 2013, 2017]**

Answer:

a) We can express $g(X)$ in the following way.

$$g(X) = (1)\,1 + (1)\,X + (0)\,X^2 + (1)X^3 + (0)X^4 + (0)X^5 + (0)X^6$$

Thus the generator matrix, G is given by

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

However, this G is in non-systematic form. We can convert this into systematic form with row operations. To do this the first row is added to the third row and the sum of the first two rows is added to the fourth row. If we do these operations we get the generator matrix in the systematic form and this may be denoted as G'. Thus G' is given by.

$$G' = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This matrix G' will also generate the same code as the matrix G.

Now let us proceed to obtain the parity check matrix, H. Since generator polynomial $g(X)$ is a factor of $X^n + 1$ we may write

$$X^n + 1 = g(X)h(X)$$

The polynomial $h(X)$ is called the parity-check polynomial and it has the degree k. It can be expressed as

$$h(X) = h_0 + h_1 X + \ldots\ldots + h_k X^k$$

where $h_0 = h_k = 1$.

$v = (v_0, v_1, v_2 \ldots v_{n-1})$ is a code vector in c.

$v(X) = a(X)g(X)$.

We multiply $v(X)$ by $h(X)$ and we obtain

$$\begin{aligned} v(X)\,h(X) &= a(X)g(X)h(X) \\ &= a(X)(X^n + 1) \qquad [\because g(X)\,h(X) = X^n + 1] \ldots. (1) \\ &= a(X) + X^n a(X) \end{aligned}$$

The degree of $a(X)$ is k – 1 or less. Hence the powers $X^k, X^{k+1}, \ldots\ldots, X^{n-1}$ do not appear in $a(X) + X^n a(X)$. We expand the product $v(X)\,h(X)$ on the left-hand side of the equation (1). We find that the coefficients of X^k, $X^{k+1}, \ldots X^{n-1}$ must be equal to zero. Hence we get the following n – k equalities

$$\sum_{j=0}^{k} h_i\, v_{n-i-j} = 0 \quad \text{for } 1 \le j \le n-k \qquad \ldots. (2)$$

Now let us denote reciprocal of $h(X)$ as $h(X^{-1})$ such that

$X^k h(X^{-1}) = h_k + h_{k-1} X + h_{k-2} X^2 + \ldots\ldots + h_0 X^k$ .... (3)

Equation (3) shows that $X^k h(X^{-1})$ is also a factor of $(n, n-k)$ cyclic code with the following (n – k) × n matrix as a generator matrix:

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \ldots\ldots & h_0 & 0 & 0\ldots. & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \ldots\ldots & h_0 & 0\ldots. & 0 \\ 0 & 0 & h_k & h_{k-1} & \ldots\ldots & & h_0\ldots. & 0 \\ \vdots & & & & & & & \\ \vdots & & & & & & & \\ 0 & 0 & 0\ldots\ldots & 0 & 0 & h_k & h_{k-1}\ldots. & h_0 \end{bmatrix}$$

From equation (2) it follows that any code vector v in c is orthogonal to every row of H. This matrix H is called the parity-check matrix of the cyclic code c. The polynomial $h(X)$ is called the parity polynomial of c. Thus we can say that a cyclic code is also uniquely specified by its parity polynomial. It may be noted that the row space of H is the dual code of c.

Thus we can state another important property of cyclic code as below:

Let c be an (n, k) cyclic code with generator polynomial $g(X)$. The dual code of c is also cyclic and is generated by the polynomial $X^k h(X^{-1})$ where $h(X) = (X^n + 1)/g(X)$.

b) The generator polynomial is $g(x) = x^3 + x + 1$

i) Let $v(x) = x^5 + x^2 + 1$

To get the syndrome $s(x)$, we will have to divide $v(x)$ by $g(x)$.

$$\begin{array}{r|l} x^3 + x + 1 \;\big|\; x^5 + x^2 + 1 & x^2 + 1 \\ \underline{x^5 + x^3 + x^2\;\big|} & \\ x^3 + 1 & \\ \underline{x^3 + x + 1} & \\ x & \end{array}$$

So, $s(x) = x$

We know for a $(7, 4)$ code, the error polynomial for $s(x) = x$ is $c(x) = x$.

Now, $c(x)$ is the code polynomial which is given by

$$c(x) = v(x) + e(x) = (x^5 + x^2 + 1) + x = x^5 + x^2 + x + 1$$

ii) In this case, $v(x) = x^6 + x^3 + 1$

Let us divide $v(x)$ by $g(x)$, the remainder is the syndrome, $s(x)$

$$x^3+x+1 \;\Big|\; x^6+x^3+1 \;\Big|\; x^3+x$$
$$\underline{\;\;x^6+x^4+x^3\;\;}$$
$$x^4+1$$
$$\underline{\;\;x^4+x^2+x\;\;}$$
$$x^2+x+1$$

So, $s(x)=x^2+x+1$

The corresponding error polynomial is $e(x)=x^5$

Since, $c(x)=v(x)+e(x)$,

we get, $c(x)=(x^6+x^3+1)+x^5=x^6+x^5+x^3+1$

3. a) A (15, 5) linear cyclic code has a generator polynomial has $g(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$

Draw the block diagram of the encoder for this code. **[WBUT 2014]**

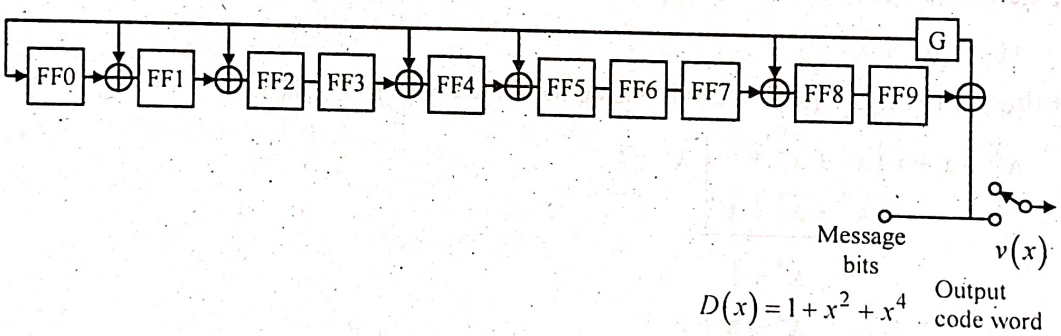
Answer:

We consider a $(15,5)$ linear cyclic code. The generator polynomial is

$$g(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$$

Here, $n=15$ and $k=5$

Thus, the block diagram of the encoder for this code is as under.



In the above block diagram, there are ten flip-flops, $FF0, FF1, \ldots\ldots, FF9$ and six EXOR gates. G also denotes a gate. The message bits are represented by the message polynomial $D(x)=1+x^2+x^4$. The output of the encoder is $v(x)$.

b) Find the code polynomial $d(x)=1+x^2+x^4$ for the message polynomial (in a systematic form).

Answer: **[WBUT 2014]**

We know, $\dfrac{x^{10}\cdot D(x)}{g(x)}=q(x)+p(x)$

where $q(x)$ is the quotient and $p(x)$ is the remainder.

$x^{10} \cdot D(x) = x^{10}(x^4 + x^2 + 1) = x^{14} + x^{12} + x^{10}$.

Let us divide

$x^{14} + x^{12} + x^{10}$ by $g(x)$

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 & x^{14} + x^{12} + x^{10} \\
 & x^{14} + x^{12} + x^9 + x^8 + x^6 + x^5 + x^4 \\
\hline
 & x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 \\
 & x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 \\
\hline
 & x^9 + x^6 + x^2 + x + 1
\end{array}
$$

Thus, $p(x) = x^9 + x^6 + x^2 + x + 1 = \{1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\}$

In systematic form,

$v(x) = \{p_0\ p_1\ p_2\ p_3\ p_4\ p_5\ p_6\ p_7\ p_8\ p_9\ d_0\ d_1\ d_2\ d_3\ d_4\}$

$= \{1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\}$

Hence, the code polynomial is $v(x) = 1 + x + x^2 + x^6 + x^9 + x^{10} + x^{12} + x^{14}$.

c) Is $v(x) = 1 + x^4 + x^6 + x^8 + x^{14}$ a code polynomial? If not, find the syndrome of $v(x)$. **[WBUT 2014]**

Answer:

$v(x)$ is given by $v(x) = 1 + x^4 + x^6 + x^8 + x^{14}$

Let us divide $v(x)$ by $g(x)$

$$
\begin{array}{r|l}
 & x^4 + x^2 + 1 \\
\hline
x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 & x^{14} + x^8 + x^6 + x^4 + 1 \\
 & x^{14} + x^{12} + x^9 + x^8 + x^6 + x^5 + x^4 \\
\hline
 & x^{12} + x^9 + x^5 + 1 \\
 & x^{12} + x^{10} + x^7 + x^6 + x^4 + x^3 + x^2 \\
\hline
 & x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 \\
 & x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 \\
\hline
 & x^9 + x^8 + x^7 + x^6 + x^3 + x
\end{array}
$$

Since $x^4 + x^2 + 1$ is not exactly divisible by $g(x)$, the $v(x)$ is not a code polynomial.

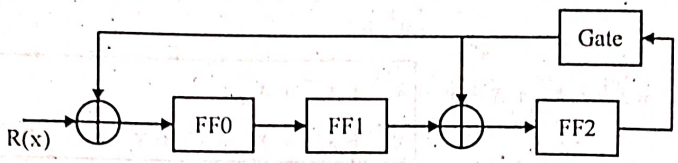
The remainder is the syndrome polynomial, $s(x)$.

Thus, $s(x) = x^9 + x^8 + x^7 + x^6 + x^3 + x$.

d) A (7, 4) linear cyclic code has a generator polynomial $g(x)=1+x^2+x^3$. Draw the syndrome circuit and find out the syndrome showing all the contents of the resister in al the required shifts for $r=0010110$. **[WBUT 2014, 2018]**

Answer:

The syndrome circuit is as shown below:



$g(x)=1+x^2+x^3$

$R(x)=0\ 0\ 1\ 0\ 1\ 1\ 0$

Shift	Initial bit	Contents of shift register
—	—	0 00
1	0	0 00
2	1	100
3	1	1 10
4	0	0 11
5	1	0 00
6	0	0 0 0
7	0	0 00

Thus, the syndrome is 0 00. Since the syndrome is zero, the received word $R(x)$ is error-free.

4. a) What are cyclic codes? Why are they called subclass of block code?
b) Write the advantages and disadvantages of cyclic code.
c) Prove that the generator polynomial $f(x)$ of an (n,k) cyclic code is a factor of $1+x^n$. **[WBUT 2015]**

Answer:

a) 1st Part:

An (n, k) linear code c is called a cyclic code if every cyclic shift of a code vector c is also a code vector c.

Properties

The two basic properties of cyclic codes are, namely, (a) linearity property and (b) cyclic property.

The linearity property means that the sum of two code words in the code is also a code word.

The cyclic property implies that any cyclic shift of a code word in the code is also a code word.

2nd Part:

Cyclic codes are a type of block codes. Like block codes they use a block of input data for coding. As they are a kind of block codes, they are called a sub-class of block codes.

b) Advantages:

1. The error correcting and decoding methods of cyclic codes are simpler and easy to implement.
2. These methods eliminate the storage needed for look-up table decoding
3. Cyclic codes are powerful and efficient.
4. The encoders and decoders of cyclic codes are simpler compared to non-cyclic codes.
5. Cyclic codes can detect error burst
6. Cyclic codes have well-defined mathematical structure. Hence very efficient decoding techniques are possible.

Disadvantage

1. The error detection in cyclic codes is simpler but error correction is little complicated
2. The combinational logic circuits in error detector for cyclic codes are complex.

c) Property

Statement

The generator polynomial $g(X)$ of an (n, k) cyclic code is a factor of X^n+1.

Proof

$$g(X)=1+g_1X+g_2X^2+.....+g_{n-k-1}X^{n-k-1}+X^{n-k}$$

Let us multiply $g(X)$ by X^k. We obtain

$$X^k g(X)=\left(X^n+1\right)+g^{(k)}(X) \qquad \text{.... (1)}$$

where $g^{(k)}(X)$ is the remainder.

From equation (1) we know that $g^{(k)}(X)$ is the code polynomial which is obtained by cyclically shifting $g(X)$ to the right k times. Therefore, $g^{(k)}(X)$ is a multiple of $g(X)$.

So we can write $g^{(k)}(X)=a(X)g(X)$ .... (2)

Substituting (4.9) in (4.8) we obtain $X^n+1=\left[X^k+a(X)g(X)\right]$ .... (3)

This proves that $g(X)$ is a factor of X^n+1.

5. Write short note on the following:

a) Golay codes [WBUT 2009, 2014, 2015, 2018]
b) Shortened cyclic code [WBUT 2012]
c) Spanning of generator matrix in cyclic code [WBUT 2012]
d) Dual codes [WBUT 2013, 2016, 2019]
e) Cyclic burst [WBUT 2015]
f) Shortened & Extended Code [WBUT 2019]

Answer:

a) Golay codes:

Golay code is a (23, 12) cyclic code capable of correcting any combination of three or fewer random errors in a block of 23 bits. The code has 12 redundant bits. It is the only known three error-correcting binary perfect cyclic code. It is a perfect code since it satisfies the Hamming bound for $t = 3$ i.e. $t = \left[\frac{1}{2}(d_{min} - 1)\right]$

The code has minimum distance of 7.

The generator polynomial of a Golay code is given by

$$g_1(X) = X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1$$

Golay code is also generated by the generating polynomial

$$g_2(X) = X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1$$

Both $g_1(X)$ and $g_2(X)$ are factors of $X^{23} + 1$.

Thus $1 + X^{23} = (1 + X)g_1(X)g_2(X)$

The Golay code can detect 8 errors or correct 3 errors. The extended Golay code is a (24, 12) cyclic code. It is formed by appending an overall parity bit to original (23, 12) Golay code. For the extended Golay code, the minimum distance $d_{min} = 8$. Extended Golay code has code rate $R_c = \frac{k}{n} = \frac{1}{2}$. Rate one-half coding is easier to implement than other rates. The 2 : 1 ratio between the code bits and the message bits simplifies clock synchronization between the input data stream and the output coded stream. The extended Golay code i.e. (24, 12) cyclic code can detect all patterns of 7-bit errors and correct all patterns of 3-bit errors.

b) Shortened Cyclic Codes:

If a code of suitable natural length or suitable number of information digits cannot be found, then it may be desirable to shorten a code to meet the requirements. Such a code is called a shortened cyclic code.

Let us consider an (n, k) cyclic code c. Let these be 2^{k-l} code vectors for which the ℓ leading high-order information digits are zero. The 2^{k-l} code vectors form a linear subcode of c. If we delete the ℓ zero information digits from each of these code vectors, we obtain a set of $2^{k-\ell}$ vectors of length $n - \ell$. These 2^{k-l} shortened vectors form an $(n - \ell,\ k - \ell)$ linear code. This code is called a shortened cyclic code or polynomial code. Such a code is not cyclic. A shortened cyclic code has at least the same error-correcting capability as the code from which it is derived.

The encoding and decoding for a shortened cyclic code can be done by the same circuits as those used for the original cyclic code since the deleted ℓ leading-zero information digits do not affect the parity check and syndrome calculations. However, in decoding the shortened cyclic code after the entire received vector has been shifted into the syndrome register, the syndrome register must be cyclically shifted ℓ times to generate the proper syndrome for decoding the first received digit $r_{n-\ell-1}$. For large value of ℓ, this may lead

to undesirable decoding delay which can, however, be eliminated by modifying either the connections of the syndrome register or the error-pattern detection circuit.

c) Spanning of generator matrix in cyclic code:

Let us consider an (n, k) cyclic code c with generator polynomial $g(X) = g_0 + g_1X + ...g_{n-k}X^{n-k}$. From the generator polynomial $g(X)$ we may construct the generator matrix G of the code by noting that the k polynomials $g(X), Xg(X), ...X^{k-1}g(X)$ span the code c. Hence the n-tuples corresponding to these polynomials may be used as rows of the $k \times n$ generator matrix G. Thus the generator matrix G for the code c will be as under.

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & & 0 \\ 0 & 0 & g_0 & \cdots & & g_{n-k} & \cdots & & 0 \\ \vdots & & & & & & & & \\ \vdots & & & & & & & & \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{bmatrix}$$

If we put n – k = r we may express G in the following form also

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & & 0 \\ 0 & 0 & g_0 & \cdots & & g_r & \cdots & & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & 0 & \cdots & 0 & \cdots & & & g_r \end{bmatrix}$$

This matrix has k rows and n columns. The k = n – r rows of the matrix are obviously linearly independent as the matrix is expressed in echelon form. These k rows represent the code words $g(X)$, $Xg(X)$, $X^2g(X)$,....., $X^{k-1}g(X)$. It may be noted that $g_0 = g_{n-k} = 1$. However, G is not in a systematic form.

d) Dual Cyclic Codes:

Let $h(x)$ is the parity check polynomial of a cyclic code. The reciprocal polynomial $h^*(x)$ of $h(x)$ is given by $h^*(x) = x^r h\left(\frac{1}{x}\right)$

where r is the degree of $h(x)$

The reciprocal polynomial is the generator polynomial of the dual code.

Thus, $g(x) = h^*(x)$

For example, $h(x) = h_3x^3 + h_2x^2 + h_1x + h_0$

The reciprocal polynomial is obtained by replacing x with $\frac{1}{x}$ and multiplying it by x^3.

Thus reciprocal polynomial $h^*(x)$ is given by

$$h^*(x)=x^3\left(\frac{h_3}{x^3}+\frac{h_2}{x^2}+\frac{h_1}{x}+h_0\right)=h_3+h_2x+h_1x^2+h_0x^3=h_0x^3+h_1x^2+h_2x+h_3$$

It is obvious that the coefficients of $h^*(x)$ are in the reverse order to those of $h(x)$.

e) Cyclic burst:

During transmission of data from one machine to another, data may become corrupted on its way. Some of the bits may be altered, damaged or lost during transmission and error is said to have occurred. The error may occur because of noise on line, attenuation and delay distortion. For reliable communication it is necessary to detect and correct the errors. There are mainly two types of errors, namely, random errors and burst errors. In random errors, the errors are distributed at random. When errors occur at a stretch, the errors are termed as burst errors. Burst errors occur in a mobile communication channel when fading takes place. It can also occur when there is a stroke of lightning or a man-made electrical interference. Scratches on compact discs also create burst errors.

An error burst of length B is an n-bit received word is defined as a contiguous sequence of B bits in which the first and last bits or any number of intermediate bits received are in error. A cyclic burst is a vector whose non-zero components are among B successive components, the first and last of which are non-zero. Cyclic codes are particularly suitable for burst error detection. A cyclic code with generator polynomial of degree r can detect all burst of length $\leq r$. The Reed Solomon codes can correct a corrupted symbol with a single bit error and also it can correct a symbol with all bits corrupted. This makes the RS codes very suitable for correcting burst errors. The most common application of RS codes is for correction of burst errors in compact discs. Fire codes are cyclic codes which are also constructed systematically for correcting burst errors.

f) Shortened & Extended Code:

If a code of suitable number of information digits cannot be found, then it may be desirable to shorten and extend a code to meet the requirements. Such a code is called a shortened or extended code respectively.

An (n,k) linear code can be shortened to an $(n-i,\ k-i)$ shortened linear code by setting the first left hand side i information bits to zero. Encoding and decoding can be carried out in the same way as for (n,k) code. Thus the same generator and parity check matrices G and H respectively of the (n,k) code can be used for the shortened code. However, the generator matrix of the shortened code is obtained by omitting the first i rows and columns of G. The parity check matrix is obtained by omitting the first i columns of H. The code words have $(n-i)$ bits but the number of parity bits remain the same as $(n-i)-(k-i)=(n-k)$. The minimum distance of the shortened $(n-i,\ k-i)$

code is greater than or equal to the minimum distance of the (n, k) code from which it is derived. In other words, shortening of a code does not reduce the error control capability. Another way of modifying an (n, k) code is by adding an overall parity check bit to produce an extended $(n+1, k)$ code. such a code is a extended code. The parity check bit is added so as to give even parity code words. This preserves the linearity of the code. For example, a Hamming code $(2^r - 1, 2^r - 1 - r)$ single error correcting Hamming code for $r \geq 3$, are often extended in this way. The inclusion of an overall parity check bit gives $(2^r, 2^r - 1 - r)$ extended Hamming code with minimum distance code which are single error correcting and double error detecting codes.

BCH CODES

Multiple Choice Type Questions

1. If $m = 4$, then what will be the length of the BCH Code? [WBUT 2008, 2010, 2014, 2016]

a) 16 b) 15 c) 17 d) none of these

Answer: (b)

2. For GF(2^3), the elements in the set are [WBUT 2008, 2010, 2013, 2014, 2016]

a) $(1, 2, 3, 4, 5, 6, 7)$ b) $(0, 1, 2, 3, 4, 5, 6)$ c) $(0, 1, 2, 3)$ d) $(0, 1, 2, 3, 4, 5, 6, 7)$

Answer: (d)

3. Chein search is used for decoding [WBUT 2010]

a) Linear Block codes b) BCH codes

c) Convolution codes d) None of these

Answer: (b)

4. A code is with minimum distance $d_{\min} = 5$. How many errors can it correct? [WBUT 2013]

a) 3 b) 2 c) 4 d) 1

Answer: (b)

5. A (63, 15) BCH code over $GF(2^6)$ can produce the code maximum error capability of [WBUT 2013]

a) 6 b) 8 c) 10 d) 12

Answer: (b)

6. Relation between Syndrome Vector (S) and error vector (E) is [WBUT 2016]

a) $S = H^T E$ b) $S = EH^T$

c) Both (a) and (b) d) None of these

Answer: (b)

7. For $GF(2^2)$ the elements in the set are [WBUT 2017]

a) $\{1\ 2\ 3\ 4\ 5\ 6\ 7\}$ b) $\{0\ 1\ 2\ 3\ 4\ 5\ 6\}$

c) $\{0\ 1\ 2\ 3\}$ d) $\{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\}$

Answer: (d)

8. For a Reed-Solomon code, the minimum distance is [WBUT 2017]

a) $n-k-1$ b) $n-k+1$ c) $k-n-1$ d) $k-n+1$

Answer: (b)

9. If $m=4$, then what will be the length of the BCH code? [WBUT 2018]
a) 16 b) 17 c) 15 d) None of these
Answer: (c)

10. For a Reed-Solomon code, the minimum distance is [WBUT 2018]
a) $n+k-1$ b) $n-k+1$ c) $k-n-1$ d) $k-n+1$
Answer: (b)

11. In $GF(2^3)$, α^7 equal to [WBUT 2019]
a) 1 b) α^{14} c) α^{21} d) all of these
Answer: (a)

Short Answer Type Questions

1. Determine the generator polynomial of a double error correcting BCH code of block length, $n=15$. [WBUT 2011, 2014, 2019]
Answer:
Here t = 2 and n = 15.
Let α be a primitive element of Galois field, GF (2^4). Then from the table of the Galois field, $1+\alpha+\alpha^4=0$. The minimal polynomial of α, α^3 and α^5 are respectively.

$$\phi_1(X)=1+X+X^4$$
$$\phi_3(x)=1+X+X^2+X^3+X^4$$
$$\phi_5(X)=1+X+X^2$$

Here $n=2^m-1=2^4-1=15$. So $m=4$.
The generator polynomial is

$$g(X)=LCM\{\phi_1(X),\phi_3(X)\}=(1+X+X^4)(1+X+X^2+X^3+X^4)$$
$$=1+X^4+X^6+X^7+X^8$$

The degree of $g(X)$ is 8. Thus $n-k=8$.
i.e. $15-k=8$ or, $k=7$
Thus we have got a (15, 7) double-error correcting BCH code with minimum distance, $d_{min}\geq 2t+1$ i.e. $d_{min}\geq 5$. Since, the generator polynomial is of weight 5, $d_{min}=5$.

2. Find the generator polynomial $g(x)$ for a double error correcting ternary BCH code of block length 8. What is the code rate of the code? [WBUT 2016]
Answer:
$n=8$, $q=3$,

$$n=q^m-1$$

So, $m=2$ and $t=2$

The generator polynomial for the $t=2$ error correcting BCH code is given by

$$g(x)=\text{LCM}\left[f_1(x), f_2(x), \cdots\cdots, f_{2t}(x)\right]$$
$$=\text{LCM}\left[\left(x^4+x+1\right)\left(x^4+x+1\right)\left(x^4+x^3+x^2+x+1\right)\left(x^4+x+1\right)\right]$$

3. What are Hamming Code and Hamming Bound? **[WBUT 2016]**

Answer:

Hamming code is a family of (n,k) linear block codes that have the following parameters:

Block length, $n=2^m-1$

Number of message bits, $k=2^m-m-1$

Number of parity bits $=m=n-k$

Error correcting capability $=t=1$ $(d_{\min}=3)$

An (n,k) linear block code can correct up to t errors per code word provided it satisfies the relation

$$2^{n-k}\geq\sum_{i=0}^{t}\binom{n}{i} \text{ where } \binom{n}{i}=\frac{n!}{(n-i)!\,i!}$$

This relation is known as Hamming bound. Hamming bound is also called the Sphere Packing Bound. This bound holds good for non-linear codes as well.

4. Construct a table $GF(2^3)$ based on the primitive polynomial $P(X)=1+X+X^3$. **[WBUT 2018]**

Answer:

Let α be an element of $GF(2^3)$.

Then $\alpha^3+\alpha+1=0$

Hence $\alpha^3=\alpha+1$ since $\alpha=-\alpha$

Now, $\alpha^4=\alpha\cdot\alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha$

$$\alpha^5=\alpha\cdot\alpha^4=\alpha\left(\alpha^2+\alpha\right)=\alpha^3+\alpha^2=(\alpha+1)+\alpha^2=\alpha^2+\alpha+1$$

$$\alpha^6=\alpha\cdot\alpha^5=\alpha\left(\alpha^2+\alpha+1\right)=\alpha^3+\alpha^2+\alpha=(\alpha+1)+\alpha^2+\alpha$$
$$=(\alpha+\alpha)+\alpha^2+1=0+\alpha^2+1=\alpha^2+1$$

Thus the field elements of $GF(2^3)$ with primitive polynomial $p(X)=X^3+X+1=0$ are the following:

0

1

α

α^2

$\alpha^3 = \alpha + 1$

$\alpha^4 = \alpha^2 + \alpha$

$\alpha^5 = \alpha^2 + \alpha + 1$

$\alpha^6 = \alpha^2 + 1$

The Galois field $GF(2^3)$ generated by $p_i(X) = 1 + X + X^3$ is shown in the table below.

ield elements	Polynomial representation	Vector representation
0	0	0 0 0
1	1	1 0 0
α	α	0 1 0
α^2	α^2	0 0 1
α^3	$1+\alpha$	1 1 0
α^4	$+\alpha+\alpha^2$	0 1 1
α^5	$1+\alpha+\alpha^2$	1 1 1
α^6	$1 \quad +\alpha^2$	1 0 1

Long Answer Type Questions

1. a) Find the generator polynomial of a triple-error correcting BCH code with block length $n = 31$ over $GF(2^5)$. **[WBUT 2010]**

Answer:

Since it is a triple-error-correcting code, $t = 3$. Let α be the primitive element of GF(2^5).

$n = 2^m - 1 = 2^5 - 1 = 31$. Hence $m = 5$

The generator polynomial $g(x)$ is given by

$$g(X) = LCM\{\phi_1(X)\phi_3(X)\phi_5(X)\}$$
$$= (X^5 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1)(X^5 + X^4 + X^2 + X + 1)$$
$$= X^{15} + X^{11} + 10 + X^9 + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1).$$

b) Given that the codewords $c_1(x)$ and $c_2(x)$, belonging to the double-error correcting $(15, 7)$ code constructed over $GF(2^4)$, incur 2 and 1 errors so giving

i) $v_1(x) = x^{11} + x^9 + x^8 + x^6 + x^5 + x + 1$

ii) $v_2(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x$

respectively, determine $c_1(x)$ and $c_2(x)$. **[WBUT 2010]**

Answer:

i) The error syndromes are given by

$S_1 = v_1(\alpha) = \alpha^3$

$S_2 = v_1(\alpha^3) = \alpha^{13}$ over $GF(2^4)$

We know, $x^2 + S_1 x + (S_1^3 + S_3) / S_1 = 0$
Substituting in this equation, we get
$x^2 + \alpha^3 x + \alpha^7 = 0.$
Also, $\alpha^{10} + \alpha^{12} = \alpha^3$ and $\alpha^{10}\,\alpha^{12} = \alpha^7$ over $GF(2^4)$
Hence, $x^2 + \alpha^3 x + \alpha^7 = (x + \alpha^{10})(x + \alpha^{12}) = 0.$
So, the error location numbers are the roots of the equation i.e. $X_1 = \alpha^{10}$ and $X_2 = \alpha^{12}$.
Thus, $e = x^{10} + x^{12}$ and $c_1(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x + 1.$
ii) $S_1 = \alpha^4$
$S_3 = \alpha^{12}$ over $GF(2^4)$
We know, $x^2 + S_1 x + (S_1^3 + S_3) / S_1 = 0$
Substituting in this equation, we get $x + \alpha^4 = 0.$
The error location number is $\mathbf{X_1 = \alpha^4}$ and $\mathbf{e = x^4}$
So, $C_2(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x.$

2. What is Galois Field? **[WBUT 2013]**

Answer:

In linear algebra, a field F is defined as a set of elements with two operations addition and multiplication. A field F satisfies the following properties:

1. **Closure property:** It states that F is closed under the addition (+) and multiplication (*) operations. It means if the elements a and b are in F, then $(a + b)$ and $(a * b)$ are in F.
2. **Commutative property:** If a and b are two elements of a field, then $a + b = b + a$ and $a * b = b * a$
3. **Distributive property:** If a, b and c are three elements of a field, then $a * (b + c) = a * b + a * c$
4. **Associative property:** If a, b and c are three elements of a field, then $(a + b) + c = a + (b + c)$ and $a * (b * c) = (a * b) * c$
5. **Identity elements:** Identity elements 0 and 1 must exist in the field F such that
   $a + 0 = a$
   $a * 1 = a$
6. **Additive inverse:** For any element a in the field F, there exists an additive inverse (– a) such that $a + (-a) = 0$.
7. **Multiplicative inverse:** For any element a in the field F, there exists a multiplicative inverse a^{-1} such that $a * a^{-1} = a^{-1} * a = 1$

If the field F has finite number of elements, then it is called a Galois field.

3. a) Find the generator polynomial of a triple error correcting BCH code with block length $n = 31$ over $GF(2^3)$.

b) What are the advantages of turbo code? Discuss how it is implemented? **[WBUT 2015]**

Answer:

a) Since it is a triple-error-correcting code, $t = 3$. Let α be the primitive element of GF(2^5). $n = 2^m - 1 = 2^5 - 1 = 31$. Hence m = 5

The generator polynomial $g(x)$ is given by

$$g(X) = LCM\{\phi_1(X)\ \phi_3(X)\ \phi_5(X)\}$$

$$= (X^5 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1)\ (X^5 + X^4 + X^2 + X + 1)$$

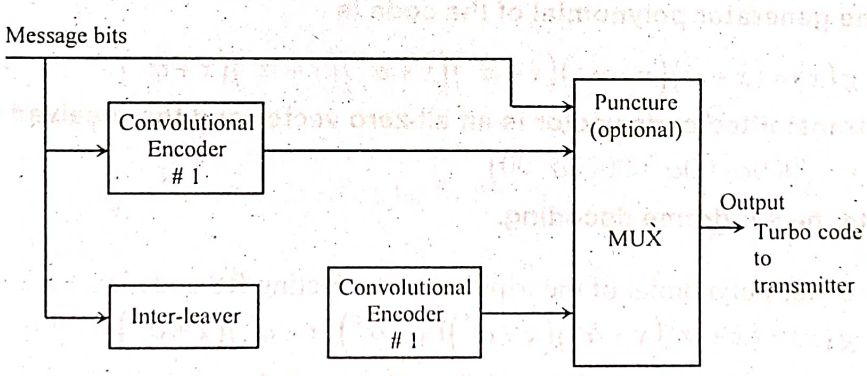
$$= X^{15} + X^{11} + 10 + X^9 + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1)$$

b) Advantages of turbo codes:

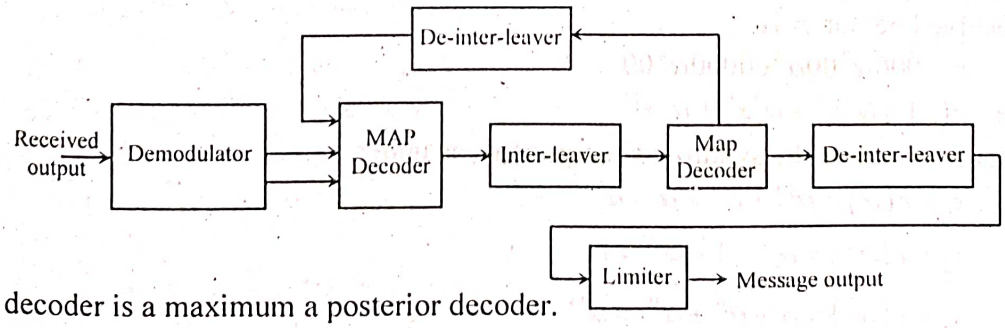
1. Turbo codes significantly outperform conventional codes. They use interleaves which reduce burst errors.
2. Turbo codes give more than 2.7 dB better coding gain than conventional Viterbi / Reed Solomon codes.
3. Turbo codes can come closer to achieve the Shannon limit of information transfer rate over a noisy channel.
4. Turbo codes make it possible to increase data rate without increasing the power of a transmission.

Implementation of Turbo codes

Turbo codes are parallel concatenated convolutional codes with interleaving. A turbo encoder is shown below



A typical turbo decoder is shown below.



MAP decoder is a maximum a posterior decoder.

4. a) Let α be a primitive element of the Galois field GF (2^4), such that $1+\alpha+\alpha^4=0$. Generate the triple-error correcting BCH code of length 15. [WBUT 2016]

Answer:

$$n=2^m-1=z^4-1=15$$

Hence $m=4$

The generator polynomial $g(x)$ is given by

$$g(x)=\text{LCM}\{\phi_1(X)\phi_3(X)\phi_5(X)\}$$
$$=(1+X+X^4)(1+X+X^2+X^3+X^4)(1+X+X^2)$$
$$=1+X+X^2+X^4+X^5+X^8+X^{10}$$

The degree of $g(x)$ is 10 i.e., $n-k=10$.

Hence $k=5$.

$$d_{\min}\geq 2t+1$$

i.e., $d_{\min}\geq 7$.

The generator polynomial is of weight 7. So it generates a BCH code of minimum Hamming distance $d_{\min}=7$. We get a (15, 5) BCH code.

b) Consider a triple-error correcting Reed-Solomon code with symbols from GF (2^4). The generator polynomial of the code is

$$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6).$$

Let the transmitted code vector is an all-zero vector and the received vector is

$$r=(000\alpha^7 00\alpha^3 00000\alpha^4 00)$$

Compute the syndrome decoding. [WBUT 2016]

Answer:

The Generator polynomial of the triple-error correcting RS code is

$$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$$
$$=\alpha^6+\alpha^9x+\alpha^6x^2+\alpha^4x^3+\alpha^{14}x^4+\alpha^{10}x^5+x^6$$

Let the transmitted code vector is an all-zero vector.

The received vector r is

$$r=000\alpha^7 00\alpha^3 00000\alpha^4 00$$

Hence $r(x)=\alpha^7x^3+\alpha^3x^6+\alpha^4x^{12}$

Now let us compute the syndrome components as under.

$$s_1=r(\alpha)=\alpha^{10}+\alpha^9+\alpha=\alpha^{12}$$

$$s_2=r(\alpha^2)=\alpha^{13}+1+\alpha^{13}=1$$

$$s_3=r(\alpha^3)=\alpha+\alpha^6+\alpha^{10}=\alpha^{14}$$

$$s_4 = r(\alpha^4) = \alpha^4 + \alpha^{12} + \alpha^7 = \alpha^{10}$$
$$s_5 = r(\alpha^5) = \alpha^7 + \alpha^3 + \alpha^4 = 0$$
$$s_6 = r(\alpha^6) = \alpha^{10} + \alpha^9 + \alpha = \alpha^{12}$$

Using Berlekamp's iterative procedure, we can find the error-location polynomial $\sigma(x)$.

Thus, $\sigma(x) = 1 + \alpha^7 x + \alpha^4 x^2 + \alpha^6 x^3$

By substituting $1, \alpha, \alpha^2, \ldots\ldots, \alpha^{14}$ into $\sigma(x)$, we observe that α^3, α^9 and α^{12} are roots of $\sigma(x)$.

The reciprocals of these roots are α^{12}, α^6 and α^3. These are the error-location numbers of the error pattern $e(x)$.

Thus errors occur at positions x^3, x^6 and x^{12}.

5. a) Find the generator polynomial $g(x)$ for single error correcting binary BCH code of blocklength 31.

b) Use the primitive polynomial $p(x) = x^5 + x^2 + 1$ to construct GF (32).

[WBUT 2017]

Answer:

a) *Refer to Question No. 3 of Long Answer Type Questions.*

b) Here $p(x) = x^5 + x^2 + 1$

So, $\alpha^5 + \alpha^2 + 1 = 0$ i.e., $\alpha^5 = \alpha^2 + 1$

Now let us construct GF(32). The first two elements of GF(32) are 0 and 1. The third element is α. The fourth element is α^2. The fifth element is α^3 and the sixth element is α^4.

The seventh element $= \alpha^5 = \alpha^2 + 1$. The subsequent elements are as follows.

$$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha$$
$$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^3 + \alpha) = \alpha^4 + \alpha^2$$
$$\alpha^8 = \alpha.\alpha^7 = \alpha(\alpha^2 + \alpha^2) = \alpha^5 + \alpha^3$$
$$= \alpha^2 + 1 + \alpha^3 = \alpha^3 + \alpha^2 + 1$$
$$\alpha^9 = \alpha.\alpha^8 = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha$$
$$\alpha^{10} = \alpha.\alpha^9 = \alpha(\alpha^4 + \alpha^3 + \alpha) = \alpha^5 + \alpha^4 + \alpha^2$$
$$= \alpha^2 + 1 + \alpha^4 + \alpha^2 = \alpha^4 + 1$$
$$\alpha^{11} = \alpha.\alpha^{10} = \alpha(\alpha^4 + 1) = \alpha^5 + \alpha$$

$$= \alpha^2 + 1 + \alpha = \alpha^2 + \alpha + 1$$

$$\alpha^{12} = \alpha.\alpha^{11} = \alpha\left(\alpha^2 + \alpha + 1\right) = \alpha^3 + \alpha^2 + \alpha$$

$$\alpha^{13} = \alpha.\alpha^{12} = \alpha\left(\alpha^3 + \alpha^2 + \alpha\right) = \alpha^4 + \alpha^3 + \alpha^2$$

$$\alpha^{14} = \alpha.\alpha^{13} = \alpha\left(\alpha^4 + \alpha^3 + \alpha^2\right) = \alpha^5 + \alpha^4 + \alpha^3$$

$$= \alpha^2 + 1 + \alpha^4 + \alpha^3 = \alpha^4 + \alpha^3 + \alpha^2 + 1$$

$$\alpha^{15} = \alpha.\alpha^{14} = \alpha\left(\alpha^4 + \alpha^3 + \alpha^2 + 1\right)$$

$$= \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^2 + 1 + \alpha^4 + \alpha^3 + \alpha$$

$$= \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$$

$$\alpha^{16} = \alpha.\alpha^{15} = \alpha\left(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1\right)$$

$$= \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$

$$= \alpha^4 + \alpha^3 + \alpha + 1$$

$$\alpha^{17} = \alpha.\alpha^{16} = \alpha\left(\alpha^4 + \alpha^3 + \alpha + 1\right) = \alpha^5 + \alpha^4 + \alpha^2 + \alpha$$

$$= \alpha^2 + 1 + \alpha^4 + \alpha^2 + \alpha = \alpha^4 + \alpha + 1$$

$$\alpha^{18} = \alpha.\alpha^{17} = \alpha\left(\alpha^4 + \alpha + 1\right) = \alpha^5 + \alpha^2 + \alpha$$

$$= 1 + \alpha^2 + \alpha^2 + \alpha = 1 + \alpha$$

$$\alpha^{19} = \alpha.\alpha^{18} = \alpha\left(1 + \alpha\right) = \alpha + \alpha^2 = \alpha^2 + \alpha$$

$$\alpha^{20} = \alpha.\alpha^{19} = \alpha\left(\alpha^2 + \alpha\right) = \alpha^3 + \alpha^2$$

$$\alpha^{21} = \alpha.\alpha^{20} = \alpha\left(\alpha^3 + \alpha^2\right) = \alpha^4 + \alpha^3$$

$$\alpha^{22} = \alpha.\alpha^{21} = \alpha\left(\alpha^4 + \alpha^3\right) = \alpha^5 + \alpha^4$$

$$= 1 + \alpha^2 + \alpha^4 = \alpha^4 + \alpha^2 + 1$$

$$\alpha^{23} = \alpha.\alpha^{22} = \alpha\left(\alpha^4 + \alpha^2 + 1\right) = \alpha^5 + \alpha^3 + \alpha$$

$$= 1 + \alpha^2 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$$

$$\alpha^{24} = \alpha.\alpha^{23} = \alpha\left(\alpha^3 + \alpha^2 + \alpha + 1\right) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$

$$\alpha^{25} = \alpha.\alpha^{24} = \alpha\left(\alpha^4 + \alpha^3 + \alpha^2 + \alpha\right) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$$

$$= 1 + \alpha^2 + \alpha^4 + \alpha^3 + \alpha^2 = \alpha^4 + \alpha^3 + 1$$

$$\alpha^{26} = \alpha.\alpha^{25} = \alpha\left(\alpha^4 + \alpha^3 + 1\right) = \alpha^5 + \alpha^4 + \alpha$$

$$= 1 + \alpha^2 + \alpha^4 + \alpha = \alpha^4 + \alpha^2 + \alpha + 1$$

$$\alpha^{27} = \alpha.\alpha^{26} = \alpha\left(\alpha^4 + \alpha^2 + \alpha + 1\right) = \alpha^5 + \alpha^3 + \alpha^2 + \alpha$$

$$= 1 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha + 1$$

$$\alpha^{28} = \alpha.\alpha^{27} = \alpha\left(\alpha^3 + \alpha + 1\right) = \alpha^4 + \alpha^2 + \alpha$$

$$\alpha^{29} = \alpha.\alpha^{28} = \alpha\left(\alpha^4 + \alpha^2 + \alpha\right) = \alpha^5 + \alpha^3 + \alpha^2$$
$$= 1 + \alpha^2 + \alpha^3 + \alpha^2 = \alpha^3 + 1$$
$$\alpha^{30} = \alpha.\alpha^{29} = \alpha\left(\alpha^3 + 1\right) = \alpha^4 + \alpha$$

Thus, GF(32) Galois field is formed with the 32 elements i.e.,

$$GF(32) = \left\{0, 1, \alpha, \alpha^2 \ldots\ldots \alpha^{29}, \alpha^{30}\right\}$$

6. a) Prove that $f(X) = 1 + X + X^3$ is a primitive polynomial over $GF(2)$.

[WBUT 2019]

Answer:

A polynomial $p(X)$ defined over $GF(2)$ of degree m is said to be irreducible if $p(X)$ has no factor polynomials of degree higher than zero and lower than m.

A property of irreducible polynomials over binary field $GM(2)$ of degree m is that they are factor of the polynomial $\left(X^{2^m-1} + 1\right)$.

The polynomial $\left(1 + X + X^3\right)$ is a factor of $X^{2^3-1} + 1 = x^7 + 1$.

Hence, $1 + X + X^3$ is an irreducible polynomial.

An irreducible polynomial $p_i(X)$ of degree m is a primitive polynomial if the smallest integer number for which $p_i(X)$ is a factor of $X^n + 1$ where $n = 2^m - 1$

Since $1 + X + X^3$ satisfies this condition if proves that $1 + X + X^3$ is a primitive polynomial over $GF(2)$.

b) What do you mean by minimal polynomial? Find out the minimal polynomials over the field $GF(2^3)$. Given $P(X) = 1 + X + X^3$.

[WBUT 2019]

Answer:

Minimal polynomial of αi denoted by $\phi(X)$ is defined as the smallest degree polynomial in $GF(2i)$ that has αi as a root.

Let the primitive polynomial be $p(X) = 1 + X + X^3$

Based on this, the field elements of $GF\left(2^3\right)$ are $0, 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$ and $\alpha^6 = \alpha^2 + 1$

The conjugates of $GF\left(2^3\right)$ are

0

1

$\alpha, \alpha^2, \alpha^4$

$\alpha^3, \alpha^5, \alpha^6$

The minimal polynomial of α^5 is

$$\phi_5(X)=(X+\alpha^5)(X+\alpha^3)(X+\alpha^6)=X^3+X^2+1$$

This is also the minimal polynomial of α^3 and α^6.

The minimal polynomial of α^2 is

$$\phi_2(X)=(X+\alpha)(X+\alpha^2)(X+\alpha^4)=X^3+X+1$$

For 0, the minimal polynomial is $\phi_0(X)=X+0=X$

For 1, the minimal polynomial is $\phi_1(X)=X+1$

Hence the minimal polynomials are:

$$X,\ X+1,\ X^3+X+1 \text{ and } X^3+X^2+1$$

c) Determine the generator sequence of double error correcting (n, k) BCH code over the field $GF(2^3)$. Evaluate n and k. Where, symbols have their usual meanings. **[WBUT 2019]**

Answer:

Here $t=2$

So, the generator polynomial is

$$g(X)=\text{LCM}\{\phi_1(X),\ \phi_3(X)\}$$

where, $\phi_1(X)$ and $\phi_3(X)$ are the minimal polynomials of α and α^3 respectively over $GF(2^3)$.

$$\phi_1(X)=X^3+X+1$$

$$\phi_3(X)=X^3+X^2+1$$

So, $$g(X)=(X^3+X+1)(X^3+X^2+1)=X^6+X^5+X^4+X^3+X^2+X+1$$

The degree of $g(X)$ is $6=n-k=r$

Here, $n=2^m-1=2^3-1=8-1=7$

So, $k=n-r=7-6=1$

So, the defined BCH code is $a(7,1)$ code.

7. Write short notes on the following:

a) Triple error correcting codes **[WBUT 2009]**

b) BCH code **[WBUT 2010, 2013, 2016]**

c) Reed-Solomon code **[WBUT 2019]**

Answer:

a) Triple error correcting codes:

A triple error correcting code can correct three or fewer errors. Thus for such a code $t\le 3$. For a Hamming code, $t=1$ i.e., a Hamming code can correct a single error. Triple error correcting codes are usually BCH codes.

The generator polynomial of a $(31,16)$ triple error correcting BCH code over $GF(2^5)$ is

$g(x)=x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1$ ◁

Here $t=3$ and let α be a primitive element of $GF(2^5)$. Hence the generator polynomial is

$$g(x)=LCM\{\phi_1(x),\phi_2(x),\phi_3(x),\phi_4(x),\phi_5(x),\phi_6(x)\}.$$

In $GF(2^5)$, the minimal polynomials are given by:

$$\phi_1(x)=x^5+x^2+1$$
$$\phi_2(x)=\phi_1(x)$$
$$\phi_3(x)=x^5+x^4+x^3+x^2+1$$
$$\phi_4(x)=x_2(x)$$
$$\phi_5(x)=x^5+x^4+x^2+x+1$$
$$\phi_6(x)=\phi_3(x).$$

So, $g(x)=\phi_1(x)\phi_3(x)\phi_5(x)=(x^5+x^2+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^2+x+1)$

$$=x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1.$$

The block length is $n=2^5-1=31$. The message length is $k=31-15=16$.

Thus we can form a triple error correcting $(31,16)$ binary BCH code.

b) BCH code:

For any positive integers m $(m\geq 3)$ and $t(t<2^{m-1})$, there exists a binary BCH code with the following parameters:

Block length : $n=2^m-1$

Number of parity check digits : $n-k\leq mt$

Number of errors that can be corrected = t where $t<2^{m-1}$.

Minimum distance : $d_{min}\geq 2t+1$

This code is capable of correcting any combination of t or fewer errors in a block of $n=2^{m-1}$ digits. Thus each BCH code is a t-error correcting code. At block lengths n of a few hundred or less, the BDH codes are the best known codes of the same block length and code rate. For example, a (1023, 923) BCH code has t = 10 and $d_{min}\geq 21$. This code requires the transmission of 100 parity-check bits for every 923 data bits giving a code rate of 923/1023.

As in cyclic codes, BCH codes are generated by generator polynomial. The generator polynomial of this code is specified in terms of its roots from the Galois field GF(2^m). If the field element is primitive, then the codes are known as primitive BCH codes. For such t-error correcting BCH code of block length n = 2^m-1 the generator polynomial $g(X)$ is the lowest-degree polynomial over GF(2). The polynomial has 2t roots which

are denoted by $\alpha, \alpha^2, \alpha^3, ...\alpha^{2t}$ such that $g(\alpha^i)=0$ for $1 \le i \le 2t$. Thus $g(X)$ has $\alpha, \alpha^2, ...\alpha^{2t}$ and their conjugates as all its roots.

Let $\phi_i(X)$ be the minimal polynomial of α^i. Then $g(X)$ must be the least common multiple (LCM) of $\phi_1(X)$, $\phi_2(X)$...., $\phi_{2t}(X)$.

Thus, $g(X) = LCM\{\phi_1(X), \phi_2(X), ..., \phi_{2t}(X)\}$ .... (1)

If we consider i as an even integer, then we can write, $i = i' 2^{\ell}$

where i' is an odd number and $\ell \ge 1$.

Then $\alpha^i = (\alpha^{i'})2^{\ell}$ is a conjugate of $\alpha^{i'}$

So, α^i and $\alpha^{i'}$ have the same minimal polynomial.

Thus $\phi_i(X) = \phi_{i'}(X)$.

Hence every even power of α in the sequence $\alpha, \alpha^2, ..., \alpha^{2t}$ has the same minimal polynomial as some preceding odd power of α in the sequence. Thus the generator polynomial $g(X)$ is reduced to

$$g(X) = LCM\{\phi_1(X), \phi_3(X), ..., \phi_{2t-1}(X)\} \quad .... (2)$$

As the degree of each minimal polynomial is m or less, the degree of $g(X)$ is at most mt.

Thus the number of parity-check bits, $n-k$, of the code is at most equal to mt.

If t is small, then $n-k = m\,t$

From the equation (2) we find that the generator polynomial of the single-error correcting BCH code of length $2^m - 1$ is $g(X) = \phi_1(X)$

α is a primitive element of GF(2^m). Hence $\phi_1(X)$ is a primitive polynomial of degree m. This shows that the single error-correcting BCH code of length $2^m - 1$ is a Hamming code.

c) Reed-Solomon code:

Reed Solomon code, commonly called RS code, is a subset of the BCH odes. It is a non-binary or m-ary BCH code. In this code, symbols are used instead of bits in forming the codes. (n, k) RS codes are described by the following parameters.

Block length = Total number of symbols in the code

$= n = 2^m - 1$

k = Number of information symbols

Number of parity check digits $= n - k = 2t$

where, t = Number of errors it can correct

Minimum distance, $D_{min} = n - k + 1$

Thus RS codes are guaranteed to correct up to t or fewer symbol errors with

$$t = \frac{d_{min} - 1}{2} = \frac{n-k}{2}$$

RS codes have good distance properties. It is possible to implement RS codes of relatively long lengths in many practical applications. RS codes perform well under burst error conditions and can be used with m-ary modulation systems. RS codes are extensively used in CDs, DVDs, Blu-ray discs, QR codes, DSL, WiMAX and satellite and space communications.

Reed Solomon codes were developed in 1960 by I.S. Reed and G. Solomon in MIT Lincoln laboratory. (255, 223) is a typical RS code in which $n = 255$ and $k - 223$.

Here $m = 8$ so that $n = 2^8 - 1 = 255$ symbols. It is a $t = 16$ correcting RS code. Then $r = n - k = 2t = 32$.

So, $k = n - r = 255 - 32 = 223$ information symbols per code word. The code rate of this RS code is $R_c = \frac{k}{n} = \frac{223}{255} = \frac{7}{8}$. The total number of bits in the code word $= 255 \times 8 = 2040$ bits per code word. Thus this code can correct $t = 16$ symbol and it can correct a burst of $16 \times 8 = 128$ consecutive bit errors. RS code is not an efficient code for correcting random errors. It is an efficient code for correcting burst errors.

In decoding a Reed Solomon code the same steps used for decoding a binary BCH code are required. In addition to these another step involving calculation of the error values is required.

CONVOLUTIONAL CODES

Multiple Choice Type Questions

1. Which of the following techniques is used for Viterbi algorithm for decoding?
   a) Code tree b) Trellis [WBUT 2009, 2011]
   c) State diagram d) Parity generator

Answer: (b)

2. An encoder for a (4, 3, 2) convolution code has a memory order of
   a) 4 b) 3 c) 2 d) 1 [WBUT 2009, 2010, 2012]

Answer: (c)

3. The no. of shift registers in a $(2, 1, 2)$ convolution encoder is [WBUT 2010]
   a) 2 b) 1 c) 3 d) 0

Answer: (a)

4. An encoder for a $(4, 3, 5)$ convolution code has a memory order of
   a) 4 b) 2 c) 3 d) 5 [WBUT 2011, 2016]

Answer: (c)

5. In any linear feed forward path of a (4, 3, 2) convolution encoder, we need maximum [WBUT 2013]
   a) 4 shift registers b) 3 shift registers
   c) 2 shift registers d) none of these

Answer: (c)

6. An encoder for a (4, 3, 5) convolution code has a memory of order [WBUT 2019]
   a) 4 b) 2 c) 3 d) 5

Answer: (d)

7. The code in convolution coding is generated using [WBUT 2019]
   a) EX-OR logic b) AND logic c) OR logic d) None of these

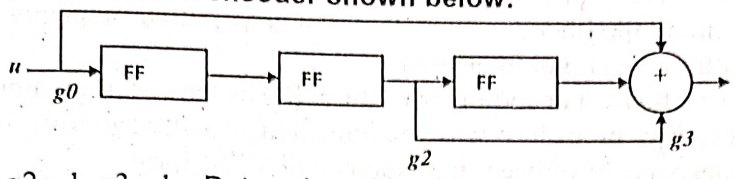
Answer: (a)

8. For decoding in convolution coding, in a code tree [WBUT 2019]
   a) diverge upward when a bit is 0 and diverge downward when the bit is 1
   b) diverge downward when a bit is 0 and diverge upward when the bit is 1
   c) diverge left when a bit is 0 and diverge right when the bit is 1
   d) diverge right when a bit is 0 and diverge left when the bit is 1

Answer: (a)

Short Answer Type Questions

1. Consider the convolution encoder shown below:



$g0 = 1, g1 = 0, g2 = 1, g3 = 1$, **Determine the output sequence given for the given input sequence** $u = (1001)$ **using impulse domain method.** **[WBUT 2010]**

Answer:

Let us write, $u = (u_0\, u_1\, u_2\, u_3)$.

Using impulse domain method, we can write

$v_0 = u_0\, g_0 = u_0$

$v_1 = u_1 g_0 + u_0 g_1 = u_1$

$v_2 = u_2 g_0 + u_1 g_1 + u_0 g_2 = u_2 + u_0$

$v_3 = u_3 g_0 + u_2 g_1 + u_1 g_2 + u_0 g_3 = u_3 + u_1 + u_0$.

Here, $u_0 = 1$, $u_1 = 0$, $u_2 = 0$ and $u_3 = 1$.

Hence, $v_0 = 1$, $v_1 = 0$, $v_2 = 1$ and $v_3 = 0$.

The other three inputs are u_4, u_5 and u_6. To return the register to its zero state, these inputs are equal to zero.

Thus, $v_4 = u_4 g_0 + u_3 g_1 + u_2 g_2 + u_1 g_3 = 0$

$v_5 = u_5 g_0 + u_4 g_1 + u_3 g_2 + u_2 g_3 = 1$

$v_6 = u_6 g_0 + u_5 g_1 + u_4 g_2 + u_3 g_3 = 1$

Hence the output sequence is $v = (v_0\, v_1\, v_2\, v_3\, v_4 v_5\, v_6) = (1\ 0\ 1\ 0\ 0\ 1\ 1)$.

2. Discuss the advantages and disadvantages of convolutional codes. **[WBUT 2012,2013]**

Answer:

Advantages

1. As convolutional codes operate on smaller blocks of data, the decoding delay is small.
2. There is no synchronization problem in convolution code.
3. The storage hardware required is less in convolutional codes.

Disadvantages

1. The analysis of convolutional codes is relatively difficult.
2. The convolutional codes are less developed as compared to block codes.

3. Explain the concept of Maximum likelihood decoding. **[WBUT 2012, 2013]**

Answer:

In 1967, Viterbi introduced a decoding algorithm for convolutional codes which ha become known as Viterbi algorithm. Later Omura showed that the Viterbi algorithm wa equivalent to a dynamic programming solution to the problem of finding the shortest pa through a weighted graph. Forney later recognized that Viterbi algorithm was in fac

maximum likelihood decoding algorithm for convolutional codes. This means that the decoder output selected is always the codeword that gives the largest value of the log-likelihood function. Forney also pointed out that the Viterbi algorithm could be used to produce the maximum likelihood estimate of the transmitted sequence over a band-limited channel with inter symbol interference.

Viterbi algorithm is actually a decoding procedure. It was termed as an algorithm because historically the decoding procedure was implemented in software form on a computer. Recently, Viterbi decoders have been implemented in VLSI form.

Now we proceed to show that for a binary symmetric channel, the maximum-likelihood decoder reduces to a maximum Hamming distance decoder.

Let u denote a message vector and c denote the corresponding code vector. The code vector is applied to the input of a discrete memoryless channel
(D M C) as shown in the fig. below.

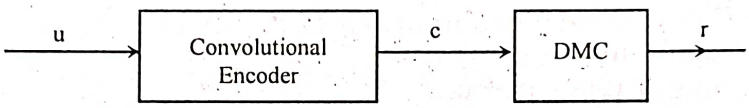


Fig: 1 Maximum likelihood decoding

Let, r = received vector.

r is different form c due to channel noise.

Let $\hat{u}$ is the estimate of the message vector and $\hat{c}$ is the estimate of the code vector. Since there is a one-to-one correspondence between u and c we can write

$$\hat{u} = u \text{ if and only if } \hat{c} = c$$

Otherwise a decoding error will occur in the receiver. The decoding rule is optimum when the probability of decoding error is minimized. From the theory of maximum likelihood estimation we know that for equiprobable messages, the probability of decoding error is minimized if the estimate $\hat{c}$ is chosen to maximize the log-likelihood function.

Let $p(r/c)$ = the conditional probability of receiving r, given that c was sent.

The log-likelihood function $= \ell n(r/c)$

Thus the maximum likelihood decoder or decision rule is stated as:

Choose the estimate $\hat{c}$ if $\ell n(r/c)$ is maximum.

Now let us consider a binary symmetric channel (B S C) where both c and r represent binary sequences of length, say N. Because of channel noise, these two sequences may differ from each other in some locations.

Let $c_i = i\ th$ element of c and

$r_i = i\ th$ element of r.

Then, $p(r/c) = \prod_{i=1}^{N} p(r_i/c_i)$

Also, $\ell n\, p(r/c) = \sum_{i=1}^{N} \ell n\, p(r_i/c_i)$

Let the transition probability $p(r_i/c_i) = \begin{cases} p & \text{if } r_i \neq c_i \\ 1-p & \text{if } r_i = c_i \end{cases}$

Let the received vector r differs from the transmitted code vector c in exactly d positions. d is the Hamming distance between vectors c and r. Thus

$$\ell n\, p(r/c) = d\ \ell n\ p + (N-d)\ell n(1-p) = d\,\ell n\left(\frac{p}{1-p}\right) + N\ \ell n(1-p)$$

The probability of an error occurring is generally low and hence we may write $p < \frac{1}{2}$. Also $N\,\ell n(1-p)$ is a constant for all c. This gives us the maximum – likelihood decoding rule for the binary symmetric channel as follows:

Choose the estimate $\hat{c}$ that maximizes the Hamming distance between the two vectors r and c.

In other words, the maximum-likelihood decoder reduces to a minimum distance decoder for a binary symmetric channel. Thus in a maximum – likelihood decoder, the received vector r is compared with each possible transmitted code vector c and the particular one closest to r is chosen as the correct transmitted code vector.

4. Draw the state diagram for (2, 1, 2) convolution code and explain.

[WBUT 2015, 2016]

Answer:

As a convolutional encoder is a sequential circuit, its operation can be described by a state diagram. The state of a register is defined as the contents of the stages at a given point during encoding. The state diagrams provide information about the structure and encoding of convolutional codes.

Let us consider a (2, 1, 2) convolutional encoder shown in the figure 1.

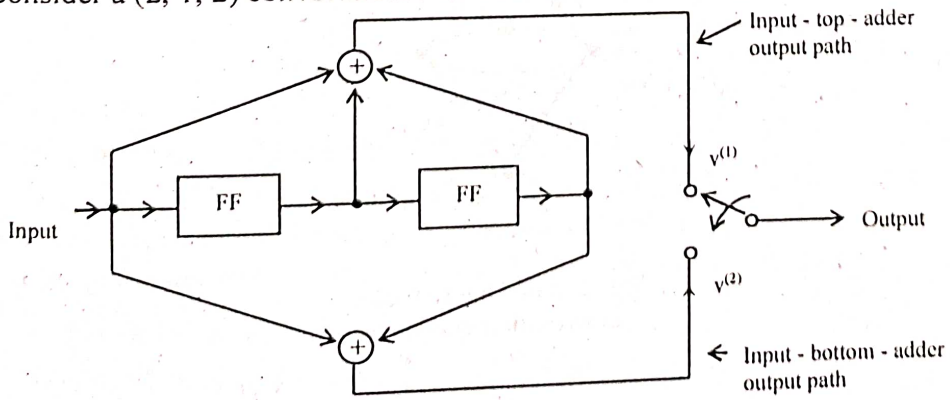


Fig: 1 A convolutional encoder

At any point during encoding, the encoder can be in any one of the 4 states 00, 01, 10 and 11. Let us define the four states as

$S_0 = 00$

$S_1 = 01$

$S_2 = 10$

$S_3 = 11$

The states are shown as nodes connected together by branches (solid or dashed lines). Each node has two incoming branches and two outgoing branches. A transition from one state to another on receiving an input 1 is a solid line while that on receiving on input 0 is a dashed line. The output occurring with each transition is shown next to relevant branch. For a given input, the output and the next state of the encoder can be determined from the state diagram. However, to arrive at the state diagram it is necessary to consider the operation of the encoder taking into account all possible transitions.

The figure (2) shows the state diagram for the (2, 1, 2) convolutional encoder.

Let us assume that encoding starts at S_0. This is the zero state with the stages at 00. When the input stays at 0, the transitions occur to the same state S_0 and the output is 00. This forms a loop at S_0. When the first non-zero input comes transition takes place from S_0 to S_2. The stage contents change to 10 giving on output of 11. If the next input is also a 1, then transition takes place from S_2 to S_3. The state contents change to 11 giving an output 01. If, however a 0 comes, transition takes places from S_2 to S_1. The contents change to 01 and the output is 10. Thus if an arbitrary input $u = (u_0, u_1 u_2 ..)$ is given, the output can be determined by following the transitions through the state diagram.

Now let us consider the input sequence $u = (110100)$ and find the output using the state diagram.

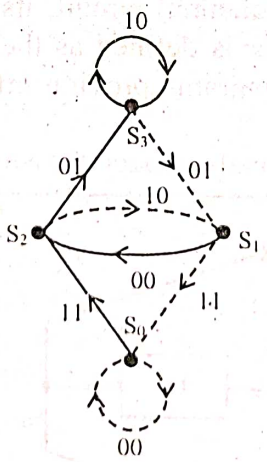


Fig: 2 State Diagram of a convolution encoder

First we start from the state S_0:

Input	Transition	Output
1	S_0 to S_2	1 1
1	S_2 to S_3	0 1
0	S_3 to S_1	0 1
1	S_1 to S_2	0 0
0	S_2 to S_1	1 0
0	S_1 to S_0	1 1

Therefore, the output sequence $v = (11, 01, 01, 00, 10, 11)$

Long Answer Type Questions

1. a) Analyse with proper diagram the encoding of a convolutional code.

[WBUT 2019]

Answer:

A convolutional code is generated by combining the outputs of a k-stage shift register with a number of EXOR summers. A typical encoder for generating convolutional codes is shown in the Fig. 1.

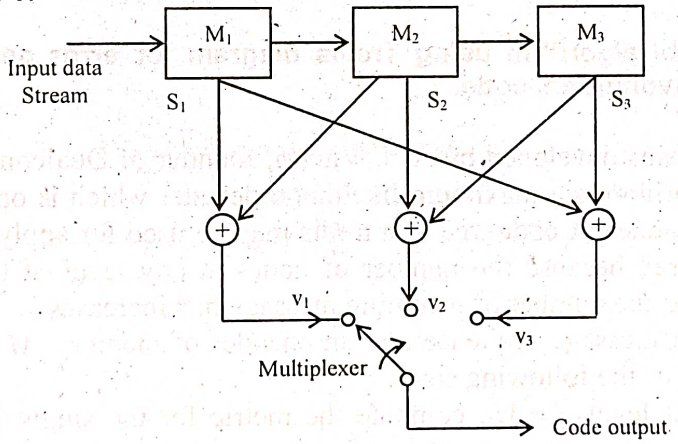


Fig: 1 A convolutional encoder

$M_1 M_2 M_3$ constitutes a three stage shift register. So, $k = 3$. There are three modulo - 2 adders (or EXOR gates). So, v = No. of bits in the code block = 3. The output is obtained from a multiplexer. Let L = Length of input data stream = 4.

The outputs of the adders are, say, v_1, v_2 and v_3 and they are given by

$$v_1 = S_1 \oplus S_2$$
$$v_2 = S_2 \oplus S_3$$
$$v_3 = S_1 \oplus S_3$$

Let initially all the shift registers be (0 0 0). Let the input data stream u be (1 1 0 1) entered in the shift register from left most end i.e. from MSB.

At the end of the first bit interval, $S_1 = 1$, $S_2 = 0$, $S_3 = 0$ and so $v_1 = 1 \oplus 0 = 1$, $v_2 = 0 \oplus 0 = 0$ and $v_3 = 1 \oplus 0 = 1$. Hence the output at the end of the first bit internal is 1 0 1.

Similarly at the end of the second bit internal, $S_1 = 1$, $S_2 = 1$ and $S_3 = 0$ and $v_1 = 1 \oplus 1 = 0$, $v_2 = 1 \oplus 0 = 1$ and $v_3 = 1 \oplus 0 = 1$. Hence the output at the end of the second bit interval is 0 1 1. Proceeding in this way, we obtain the coded output bit stream as follows.

Input data stream	Coded output bit stream						
	1	2	3	4	5	6	7
1 1 0 1	1 0 1	0 1 1	1 0 1	1 1 0	1 1 0	0 1 1	0 0 0

Since $L = 4$, $K = 3$, the register resets at 7^{th} bit interval. Thus for each message, there are $v \times (L + K)$ bits in the output code word. In the above case, $v = 3$, $L + K = 4 + 3 = 7$ and so the number of code words corresponding to the message is $3 \times 7 = 21$ bits.

It is to be noted that each message bit remains in the shift register for K bit intervals. In the above code, the bit remains in the shift register for $K = 3$ bit intervals. Hence each input bit has an influence on the K groups of output bits i.e. on $v \times K$ output bits.

b) Analyse Viterbi algorithm using Trellis diagram for error detection and error correction of convolutional code. **[WBUT 2019]**

Answer:

Viterbi algorithm was developed by A. J. Viterbi, founder of Qualcomm Corporation, in 1967. Viterbi algorithm is a maximum-likelihood decoder which is optimum for a white Gaussian noise channel. A code tree or a trellis may be used for applying this algorithm. A trellis is preferred because the number of nodes at any level of the trellis does not continue to grow as the number of incoming message bits increases.

Consider an L-bit message sequence and an encoder of memory M. Then the Viterbi algorithm consists of the following steps.

Step 1: Starting at level $j = M$, compute the metric for the single path entering each state of the encoder. Store the path of the survivor and its metric for each state.

Step 2: Increment the level j by 1. Compute the metric for all the paths entering each state by adding the metric of the incoming branches to the metric of the connecting survivor from the previous level. For each state, identify the path with the lowest metric as the survivor of step 2. Store the survivor and its metric.

Step 3: If level $j < L + M$, repeat Step 2. Otherwise stop.

Metric is the Hamming distance between the branch output and the corresponding decoder input. The branch and the path with the lower metric are referred to as the survivor branch and path respectively.

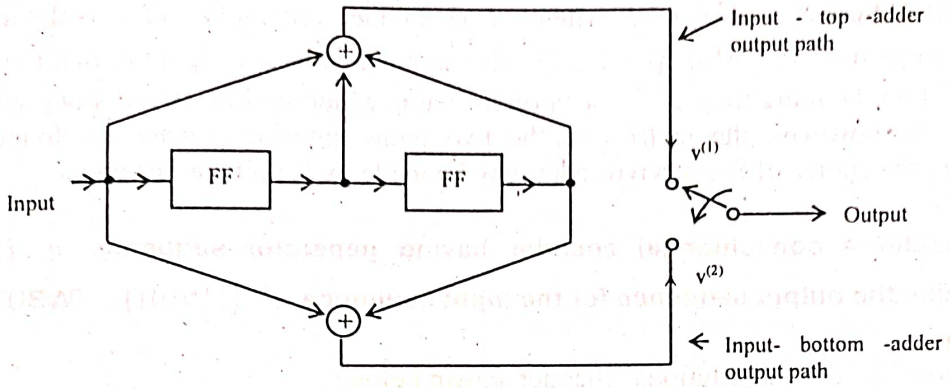


Fig: 1 A convolutional encoder

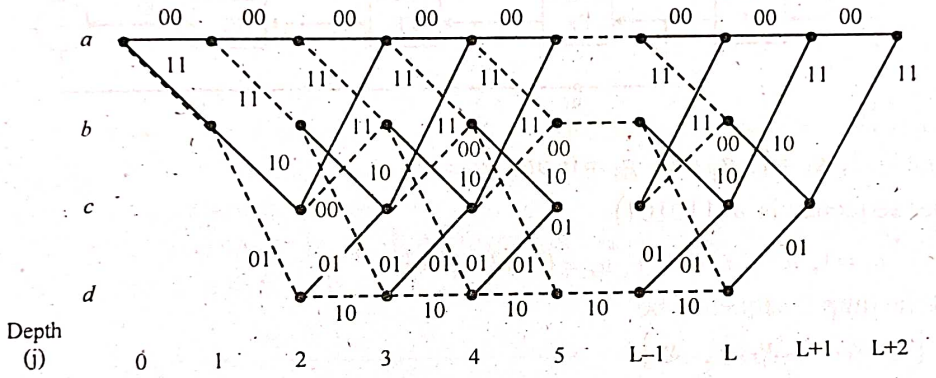


Fig: 2 Trellis diagram for the encoder of Fig 1

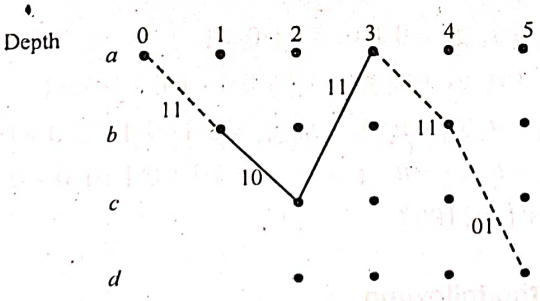


Fig: 3 Trellis for the encoding u = (10011)

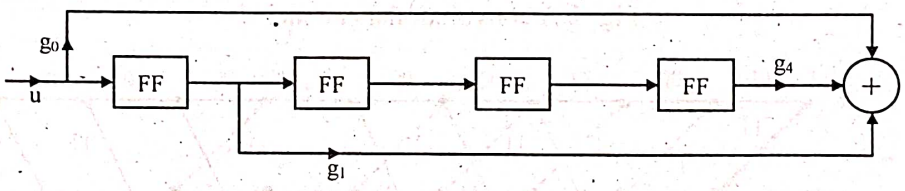
Consider the trellis diagram of Fig. 2. It corresponds to a convolutional encoder with rate $r = \frac{1}{2}$ and constraint length $K = 3$ as shown in Fig. 1. It is observed that at level (i.e. time unit) $j = 3$, there are two paths entering any of the four nodes in the trellis. Those two paths are identical onward from that point. For each node or state in the trellis, the algorithm compares the two paths entering the node. The path with the lower metric is retained and the other path is discarded. This computation is repeated for every level j of

the trellis in the range $M \le j \le L$ where M is encoder's memory and L is the length of the incoming message. Also $M = K - 1$. The retained paths are the survivors. For $K = 3$, there will not be more than $2^{K-1} = 4$ survivor paths which will be stored along with their metrics. If, however, the metrics of the two paths entering a state are found to be identical, the choice of the survivor path may be made by flipping a fair coin.

c) Consider a convolutional encoder having generator sequence $g = (11001)$. Determine the output sequence for the input sequence $u = (110101)$. **[WBUT 2019]**

Answer:

Let us consider the convolutional encoder shown below:



Here $g_0 = 1,\ g_1 = 1,\ g_2 = 0,\ g_3 = 0$ and $g_4 = 1$

The input sequence is $u(110101)$

So, $u_0 = 1,\ u_1 = 1,\ u_2 = 0,\ u_3 = 1,\ u_4 = 0$ and $u_5 = 1$

Now let the output sequence be

$$[v_0,\ v_1,\ v_2,\ v_3,\ v_4,\ v_5]$$

$$v_0 = u_0\ g_0 = 1 \cdot 1 = 1$$

$$v_1 = u_1\ g_0 + u_0\ g_1 = 1 \cdot 1 + 1 \cdot 1 = 1 + 1 = 0$$

$$v_2 = u_2\ g_0 + u_1\ g_1 + u_0\ g_2 = 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 1$$

$$v_3 = u_3\ g_0 + u_2\ g_1 + u_1\ g_2 + u_0\ g_3 = 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 = 1$$

$$v_4 = u_4\ g_0 + u_3\ g_1 + u_2\ g_2 + u_1\ g_3 + u_0\ g_4 = 0 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 = 1 + 1 = 0$$

$$v_5 = u_5\ g_0 + u_4\ g_1 + u_3\ g_2 + u_2\ g_3 + u_1\ g_4 = 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1 + 1 = 0$$

So, the output sequence is (101100)

2. Write short notes on the following:

a) Viterbi decoding **[WBUT 2011, 2013, 2015, 2016, 2017, 2018]**

b) Turbo codes **[WBUT 2013, 2016, 2018, 2019]**

c) Trellis diagram **[WBUT 2017, 2018]**

d) Code Tree **[WBUT 2019]**

Answer:

a) Viterbi algorithm:

Viterbi algorithm was developed by A. J. Viterbi, founder of Qualcomm Corporation, in 1967. Viterbi algorithm is a maximum-likelihood decoder which is optimum for a white Gaussian noise channel. A code tree or a trellis may be used for applying this algorithm.

A trellis is preferred because the number of nodes at any level of the trellis does not continue to grow as the number of incoming message bits increases.
Consider an L-bit message sequence and an encoder of memory M. Then the Viterbi algorithm consists of the following steps.

Step 1

Starting at level j = M,. compute the metric for the single path entering each state of the encoder. Store the path of the survivor and its metric for each state.

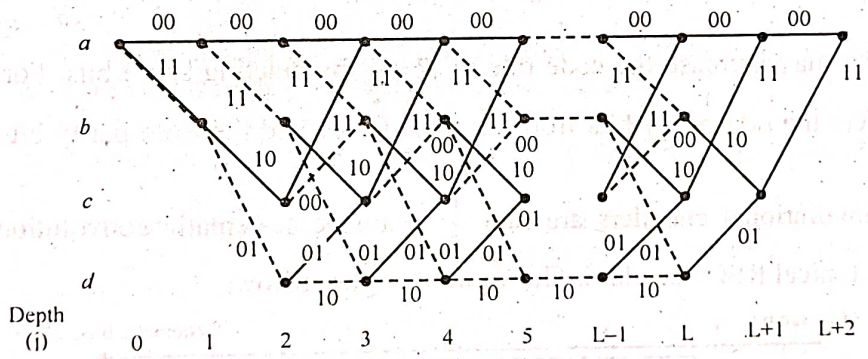
Step 2

Increment the level j by 1. Compute the metric for all the paths entering each state by adding the metric of the incoming branches to the metric of the connecting survivor from the previous level. For each state, identify the path with the lowest metric as the survivor of step 2. Store the survivor and its metric.

Step 3

If level $j < L + M$, repeat Step 2. Otherwise stop.

Metric is the Hamming distance between the branch output and the corresponding decoder input. The branch and the path with the lower metric are referred to as the survivor branch and path respectively.
Consider the trellis diagram of fig. 1 It corresponds to a convolutional encoder with rate $r = \frac{1}{2}$ and constraint length K = 3.

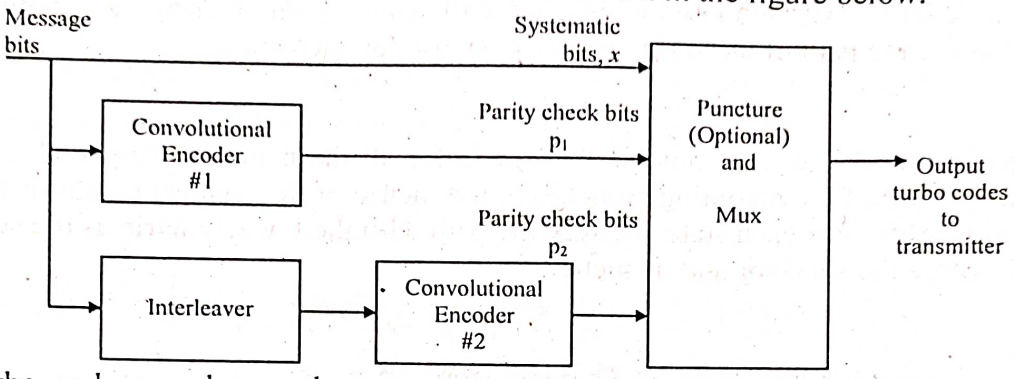


Trellis diagram for the encoder

It is observed that at level (i.e. time unit) j = 3, there are two paths entering any of the four nodes in the trellis. Those two paths are identical onward from that point. For each node or state in the trellis, the algorithm compares the two paths entering the node. The path with the lower metric is retained and the other path is discarded. This computation is repeated for every level j of the trellis in the range $M \leq j \leq L$ where M is encoder's memory and L is the length of the incoming message. Also $M = K - 1$. The retained paths are the survivors. For $K = 3$, there will not be more than $2^{K-1} = 4$ survivor paths which will be stored along with their metrics. If, however, the metrics of the two paths entering a state are found to be identical, the choice of the survivor path may be made by flipping a fair coin.

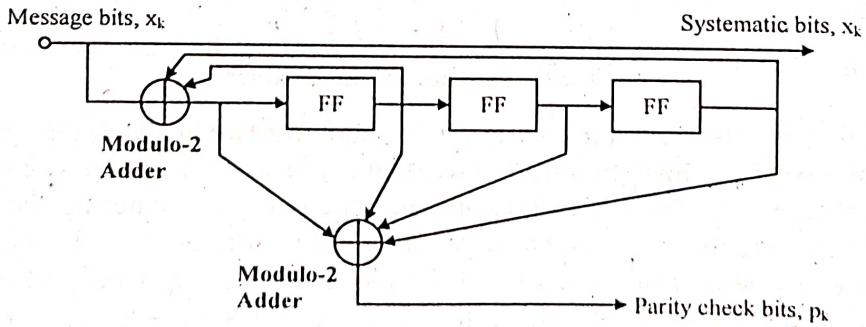
b) Turbo codes:

Turbo codes were first introduced in 1993 by Berrou, Glavieux and Thitimajshima. Turbo codes are parallel concatenated convolutional codes with interleaving. Turbo codes are very powerful codes. They have made it possible to achieve channel capacities to nearly reach the Shannon limit. A turbo code encoder is shown in the figure below.



The turbo code encoder employs two convolutional encoders in parallel. The second encoder is preceded by a pseudorandom block interleaver. The interleaver permutes the bits in the information sequence before feeding them to the second encoder. Higher code rate is achieved optionally by using puncturing. Both encoders produce the parity check bits. These parity check bits and the original bit stream called the systematic bits are multiplexed and then transmitted without puncturing the code rate is $R=\frac{1}{3}$. The process of puncturing may increase the code rate to $R=\frac{1}{2}$ by deleting some bits. For example, we may delete the odd parity bits from the encoder #1 and the even parity bits from the encoder #2.

The two convolutional encoders are rate $\frac{1}{2}$ recursive systematic convolutional (RSC) encoders. A typical RSC encoder is shown in the figure below.

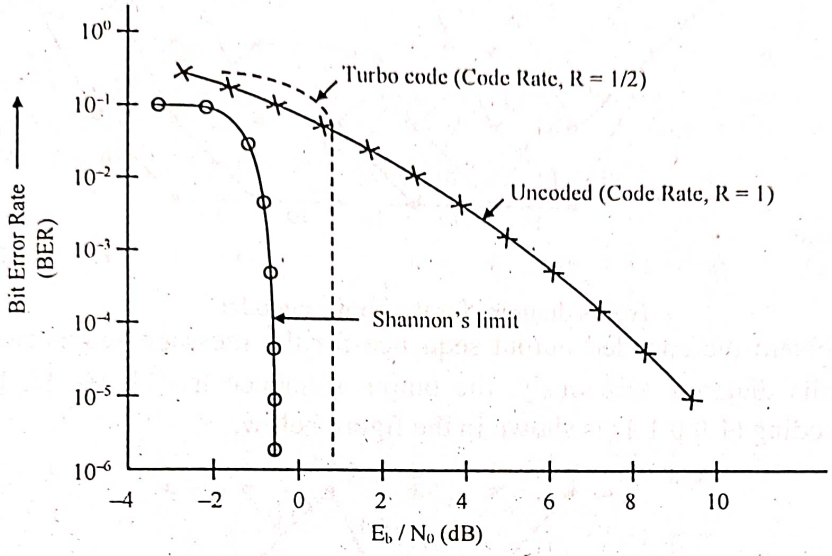


Here three flip flops (FF) and two modulo-2 address are used. Feedback is provided as shown in the figure. The output the RSC encoder gives the parity check bits, p_k.

Turbo codes are extensively used in 3G mobile communications and deep-space satellite communications.

Performance of Turbo Codes

The performance of the turbo code may be compared with that of an uncoded signal. A typical performance comparison is shown below.



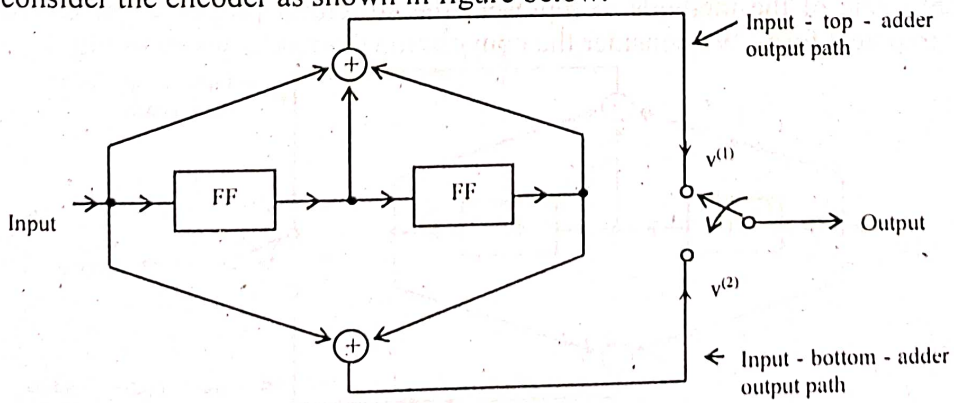
From the above graph, it is seen that the bit error rate (BER) for the turbo code falls very sharply after a critical value of E_b/N_0 . At a BER of 10^{-5} or so, the turbo code is about 0.5 dB from Shannon's limit.

c) Trellis diagram:

There are a lot of redundancies in the tree diagram. To reduce the redundancy we consider a structure called trellis. A trellis is a collapsed code tree. It is so-called since a trellis is a tree-like structure with remerging branches. The term trellis was first introduced by Forney in 1973. The convention used in drawing a code trellis is as follows:

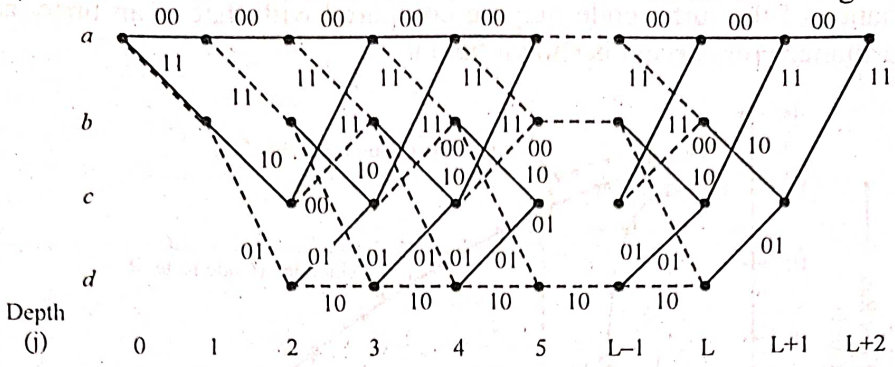
A code branch produced by an input 0 is drawn as a solid line. A code branch produced by an input 1 is drawn as a dashed line. An input message sequence corresponds to a specific path through the trellis.

Let us consider the encoder as shown in figure below:



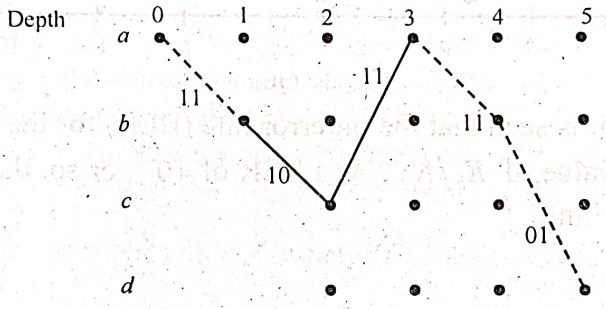
A convolutional encoder

We draw the trellis structure for the above encoder. This is shown in the figure below.



Trellis diagram for the above encoder

Now let us obtain the encoded output sequence for the message sequence $u = (10011)$ from the trellis diagram. Obviously, the output sequence is (11, 10, 11, 11, 01). The trellis for encoding (1 0 0 1 1) is shown in the figure below.



Trellis for the encoding u = (10011)

The trellis follows the path $a_0 - b_1 - c_2 - a_3 - b_4 - d_5$. The path $a_0 - b_1$ is shown dotted and the output is 11. The paths $b_1 - c_2$ and $c_2 - a_3$ are solid lines. Their outputs are 10 and 11 respectively. The paths $a_3 - b_4$ and $b_4 - d_5$ are dotted lines with outputs 11 and 01 respectively.

d) Code tree:

Code tree is one of the methods to represent the structural properties of convolutional codes in graphical form. We consider the convolutional encoder given in Fig. 1.

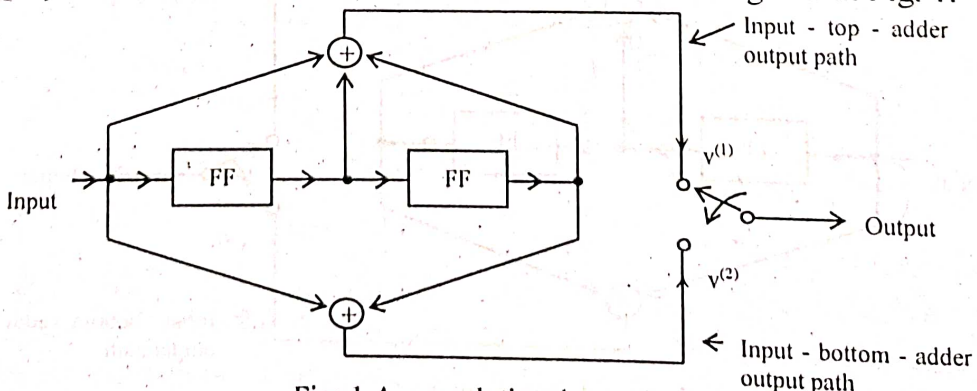


Fig: 1 A convolutional encoder

In constructing a code tree, each branch of the tree represents an input symbol. The corresponding pair of output binary symbols is indicated on the branch. An input 0 specifies the upper branch of a bifurcation while an input 1 specifies the lower branch. A specific path in the tree is traced from left to right in accordance with the input message sequence. The corresponding coded symbols on the branches of that path constitutes the output of the convolutional encoder. The code tree is shown in Fig. 2 below.

Now let us consider the message sequence u = 1 0 0 1 1. Following the convention outlined above we obtain the corresponding encoded sequence as (11, 10, 11, 11, 01).

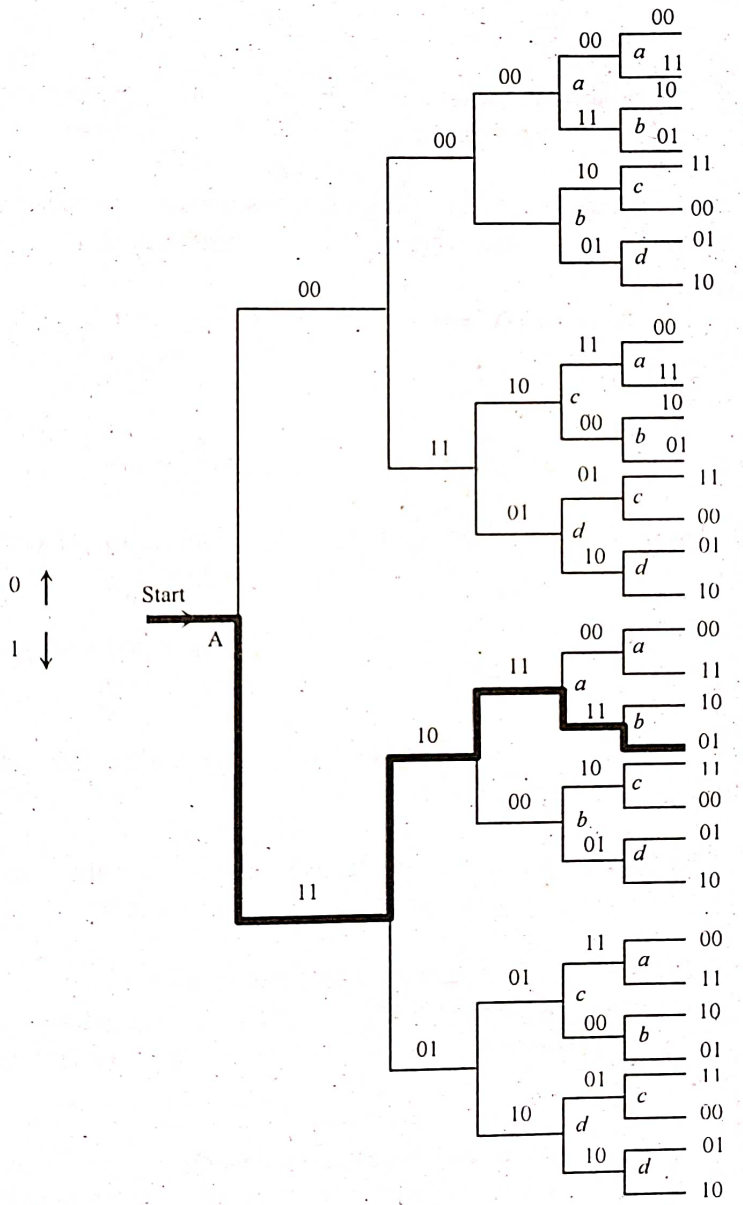


Fig: 2 A code tree

We start from the point A. As the first input bit is 1, we move downwards generating the symbols 11. Next input bit is 0. So we move upwards so that the output symbol is 10. Then input bit is once again 0. So we move upward again to generate 11. The next input bit is 1 and we move downward generating 11. Finally the last input bit is 1. We move downward and generate 01. Therefore the output sequence is (11, 10, 11, 11, 01). The entire path starting form A is shown by thick lines.

QUESTION 2015

GROUP – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any ten of the following:

i) The number of undetectable errors for a (n,k) linear code is

✓a) 2^{n-k} b) 2^n c) $2^n - 2^k$ d) 2^k

ii) Entropy represents

a) amount of information b) rate of information

✓c) measure of uncertainty d) probability of message

iii) The mutual information of a channel with independent input and output is

✓a) zero b) constant c) variable d) infinite

iv) In block coding, if $k = 2$ and $n = 3$, then number of invalid code words is

a) 8 ✓b) 4 c) 2 d) 6

v) 1 decit equals

a) 1 bit ✓b) 3.32 bits c) 10 bits d) none of these

vi) If a telephone channel has bandwidth 3000Hz and SNR = 20dB then channel capacity is

a) 3 kbps b) 1.19 kbps c) 2.19 kbps ✓d) 19.97 kbps

vii) For a noiseless channel I(X; Y) is

a) H(X)-H(Y) b) H(Y)-H(X) ✓c) H(X) d) H(X)-H(Y/X)

viii) The condition of a dual code in case of linear block code is

✓a) $GH^T = 0$ b) $(GH)^T = 0$ c) $G^TH^T = 0$ d) $HG^T = 0$

ix) A (7, 4) linear block code with minimum distance guarantees error detection of

a) ≤ 4 bits ✓b) ≤ 3 bits c) ≤ 2 bits d) ≤ 6 bits

x) The efficiency of Huffman code is linearly proportional to

a) average length of the code ✓b) average entropy

c) maximum length of the code d) none of these

GROUP – B
(Short Answer Type Questions)

2. Draw the state diagram for (2, 1, 2) convolution code and explain.

See Topic: CONVOLUTIONAL CODES, Short Answer Type Question No. 4.

3. Define the channel transition matrix and with suitable example show at least 3 channel transition matrix.

See Topic: INFORMATION THEORY, Short Answer Type Question No. 5.

4. $P(x_1) = 0.4$, $P(x_2) = 0.17$, $P(x_3) = 0.18$, $P(x_4) = 0.1$ and $P(x_5) = 0.15$ for 5 symbol x_1, x_2, x_3, x_4 and x_5. Construct a Shannon Fano code and find out its efficiency.

See Topic: INFORMATION THEORY, Short Answer Type Question No. 6.

5. Explain Shannon Hartley law regarding channel capacity. What is mutual information?

See Topic: INFORMATION THEORY, Short Answer Type Question No. 7.

6. Consider $g(x) = 1 + x + x^3$ for a (7, 4) cyclic code. Find the generator matrix of systematic form.

See Topic: CYCLIC CODES, Long Answer Type Question No. 2(a).

GROUP – C
(Long Answer Type Questions)

7. a) Define code rate and block length.

b) Give diagrammatic representation of block encoder.

c) The generator matrix of a (7, 4) block code is given by

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

i) Find H, the parity check matrix of the code.

ii) Find the syndrome for the received vector 1101101. Is this a valid code vector?

iii) Find all code words of the code.

iv) What is error correcting capability of the code?

v) What is error detecting capability of the code?

See Topic: BLOCK CODES, Long Answer Type Question No. 9(a), (b) & (c).

8. a) What are cyclic codes? Why are they called subclass of block code?

b) Write the advantages and disadvantages of cyclic code.

c) Prove that the generator polynomial $f(x)$ of an (n, k) cyclic code is a factor of $1 + x^n$.

See Topic: CYCLIC CODES, Long Answer Type Question No. 4(a), (b) & (c).

9. a) Find the generator polynomial of a triple error correcting BCH code with block length $n = 31$ over $GF(2^3)$.

b) What are the advantages of turbo code? Discuss how it is implemented?

See Topic: BCH CODES, Long Answer Type Question No. 3(a) & (b).

10. a) What do you mean by entropy of a source and mutual information of a communication channel?

b) Consider a source X which produces five symbols with probabilities $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$ and $\frac{1}{16}$. Find the source entropy.

c) Briefly discuss about the channel capacity of a discrete memoryless channel. Determine the channel capacity of a noiseless channel.

See Topic: INFORMATION THEORY, Long Answer Type Question No. 11(a), (b) & (c).

11. Write short notes on any three of the following:
   a) Standard array decoding
   b) Golay code
   c) Huffman coding
   d) Cyclic burst
   e) Viterbi decoding.

a) See Topic: BLOCK CODES, Long Answer Type Question No. 13(c).
b) See Topic: CYCLIC CODES, Long Answer Type Question No. 5(a).
c) See Topic: INFORMATION THEORY, Long Answer Type Question No. 17(c).
d) See Topic: CYCLIC CODES, Long Answer Type Question No. 5(e).
e) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(a).

QUESTION 2016

GROUP – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any *ten* of the following:

i) The unit of information is
   a) Bit ✓b) Decit c) Nat d) all of these

ii) For a Lossless channel, the number of non-zero elements in each column is
   a) 0 ✓b) 1 c) 2 d) 3

iii) Entropy is basically a measure of
   ✓a) rate of information b) average information
   c) probability of information d) disorder of information

iv) An encoder for a (4, 3, 5) convolution code has a memory order of
   a) 4 b) 2 ✓c) 3 d) 5

v) If $I(x_1)$ and $I(x_2)$ is the information carried by the symbols x_1 and x_2 respectively, then $I(x_1, x_2)$ is equal to

a) $I(x_1) * I(x_2)$ ✓b) $I(x_1) + I(x_2)$ c) $I(x_1) - I(x_2)$ d) $I(x_1) / I(x_2)$

vi) If L is the average codeword length per symbol and $H(X)$ is the source entropy then which one is more appropriate?

a) $L = H(X)$ b) $L \le H(X)$ ✓c) $L \ge H(X)$ d) None of these

vii) For (n, k) block code, the minimum distance d_{min} is

✓a) $d_{min} \le n - k + 1$ b) $d_{min} \le n - k$

c) $d_{min} \le n + k + 1$ d) $d_{min} \le n + k - 1$

viii) The properties of Cyclic code is / are

a) Linearity b) Cyclic ✓c) Both (a) and (b) d) None of these

ix) If $m = 4$ then what will be the length of BCH code?

a) 16 ✓b) 15 c) 17 d) None of these

x) For Hamming Codes of (n, k) linear block codes, the block length (n) will be

✓a) $2^q - 1$ b) 2^q c) $2^q + 1$ d) none of these

xi) Relation between Syndrome Vector (S) and error vector (E) is

a) $S = H^T E$ ✓b) $S = EH^T$ c) Both (a) and (b) d) None of these

xii) For GF (2^3) the elements in the set are

a) {1, 2, 3, 4, 5, 6, 7} b) {0, 1, 2, 3, 4, 5, 6}

c) {0, 1, 2, 3} ✓d) {0, 1, 2, 3, 4, 5, 6, 7}

GROUP – B

(Short Answer Type Questions)

2. The generator matrix for a (6, 3) block code is given below. Find the code vector of the message bit 110. Calculate the weight of this code vector.

$$G = \begin{Bmatrix} 1 & 0 & 0 & : & 0 & 1 & 1 \\ 0 & 1 & 0 & : & 1 & 0 & 1 \\ 0 & 0 & 1 & : & 1 & 1 & 0 \end{Bmatrix}$$

See Topic: BLOCK CODES, Short Answer Type Question No. 4.

3. Draw the state diagram for (2, 1, 2) convolutional code and explain.
See Topic: CONVOLUTIONAL CODES, Short Answer type Question No. 4.

4. a) What do you mean by Information rate? Explain.
b) What is a Discrete Memoryless Channel (DMC)? Explain.
See Topic: INFORMATION THEORY, Short Answer Type Question No. 8(a) & (b).

5. Find the generator polynomial $g(x)$ for a double error correcting ternary BCH code of block length 8. What is the code rate of the code?
See Topic: BCH CODES, Short Answer Type Question No. 2.

6. What are Hamming Code and Hamming Bound?
See Topic: BCH CODES, Short Answer Type Question No. 3.

GROUP – C
(Long Answer Type Questions)

7. a) Explain the Shannon-Fano coding and Huffman coding with suitable example.
b) Show that the channel capacity of an ideal AWGN channel with infinite bandwidth is given by

$$C_\infty = 1.44S/\eta \text{ bit/sec,}$$

where S is the average signal power and $\eta/2$ is the power spectral density (psd) of white Gaussian noise.
See Topic: INFORMATION THEORY Long Answer Type Question No. 12(a) & (b).

8. a) Verify the following expression:

$$0 \le H(X) \le \log_2 m$$

where m is the size of the alphabet of X.

b) A DMS X has five symbols x_1, x_2, x_3, x_4 and x_5 with $P(x_1) = 0.4$, $P(x_2) = 0.19$, $P(x_3) = 0.16$, $P(x_4) = 0.15$ and $P(x_5) = 0.1$.

i) Construct a Shannon-Fano code for X, and calculate the efficiency of the code.
ii) Repeat for the Huffman code and compare the results.

c) Write short notes on the following:
i) Codeword length
ii) Average codeword length
iii) Code efficiency
iv) Code redundancy.
See Topic: INFORMATION THEORY, Long Answer Type Question No. 13(a), (b) & (c).

9. Design a (12, 3) systematic convolutional encoder with a constraint length $\nu = 3$ and $d^* >= 3$.
i) Construct the trellis diagram for this encoder.
ii) What is the d_{free} for the code?

There is a mistake in Question No. 9. (12, 3) encoder is meaningless. Hence it cannot be worked out.

10. a) Let α be a primitive element of the Galois field GF (2^4), such that $1+\alpha+\alpha^4=0$. Generate the triple-error correcting BCH code of length 15.

b) Consider a triple-error correcting Reed-Solomon code with symbols from GF (2^4). The generator polynomial of the code is

$$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6).$$

Let the transmitted code vector is an all-zero vector and the received vector is

$$r=(000\alpha^7 00\alpha^3 00000\alpha^4 00)$$

Compute the syndrome decoding.

See Topic: BCH CODES, Long Answer Type Question No. 4(a) & (b).

11. Write short notes on any *three* of the following.

a) Viterbi decoding
b) Turbo codes
c) Dual codes
d) Standard array decoding
e) BCH codes.

a) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(a).
b) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(b).
c) See Topic: CYCLIC CODES, Long Answer Type Question No. 5(d).
d) See Topic: BLOCK CODES, Long Answer Type Question No. 13(c).
e) See Topic: BCH CODES, Long Answer Type Question No. 7(b).

QUESTION 2017

GROUP – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any *ten* of the following:

i) Relation between channel capacity and bandwidth of channel is related as

a) $C=B(\ln 2(S/N))$ ✓b) $C=B(\ln 2(1+S/N))$

c) $C=B/N$ d) $C=B*N$

ii) A code is with minimum distance 5. How many errors can it correct?

a) 3 ✓b) 2 c) 4 d) 1

iii) In the expression of Kraft Inequality, the value of K is given by

a) $K=\sum_{j=1}^{m}2^{-nj}\geq 1$ ✓b) $K=\sum_{j=1}^{m}2^{-nj}\leq 1$

c) $K=\sum_{j=1}^{m}2^{-nj}=1$ d) none of these

iv) The coding efficiency η is given by

a) $\eta = H(X).L$ ✓b) $\eta = H(X)/L$ c) $\eta = L/H(X)$ d) none of these

v) For $GF(2^2)$ the elements in the set are

a) $\{1\ 2\ 3\ 4\ 5\ 6\ 7\}$ b) $\{0\ 1\ 2\ 3\ 4\ 5\ 6\}$

c) $\{0\ 1\ 2\ 3\}$ ✓d) $\{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\}$

vi) For a Reed-Solomon code, the minimum distance is

a) $n+k-1$ ✓b) $n-k+1$ c) $k-n-1$ d) $k-n+1$

vii) The code rate for (15, 5) code is

a) 3 ✓b) 1/3 c) 5 d) 10.

viii) For $a(7,4)$ cyclic code generated by $g(x) = x^3 + x + 1$. The syndrome for error pattern $e(x) = x^3$ is

a) 101 b) 111 ✓c) 110 d) 011

ix) Which among the below stated logical circuits are present in encoder and decoder used for the implementation of cyclic codes?

A) Shift register
B) Modulo-2 adders
C) Counters
D) Multiplexers

✓a) A and B b) C and D c) A and C d) B and D

x) The generator polynomial of a cyclic code is factor of

✓a) $X^n + 1$ b) $X^{(n+1)} + 1$ c) $X^{(n+2)} + 1$ d) $X^{(n-1)} + 1$

xi) The capacity of a communication channel with a bandwidth of 4 kHz and 15 SNR is approx

a) 20 kbps ✓b) 16 kbps c) 10 kbps d) 8 kpbs.

GROUP – B

(Short Answer Type Questions)

2. What is Hamming distance? Give relation between minimum distance and error correcting capability. Define Hamming bound.

See Topic: BLOCK CODES, Long Answer Type Question No. 8.

. Show that the channel capacity for a continuous channel is given by $C = B\log_2^{\left(1+\frac{S}{N}\right)}$ bit/sec.

See Topic: INFORMATION THEORY, Long Answer Type Question No. 10.

4. What is Kraft inequality? Prove that Kraft inequality should be satisfied for variable length source coding.

See Topic: INFORMATION THEORY, Short Answer Type Question No. 9.

5. A DMS X has five symbols x_1, x_2, x_3, x_4 and x_5 with probability $P(x_1) = 0.4$, $P(x_2) = 0.17$, $P(x_3) = 0.18$, $P(x_4) = 0.1$ and $P(x_5) = 0.15$, respectively.

a) Construct the Shannon-Fano code for X.

b) Calculate the efficiency of the code.

See Topic: INFORMATION THEORY, Short Answer Type Question No. 10.

6. What is irreducible polynomial? What do you mean by polynomial over $GF(2)$. Prove that $f(X) = 1 + X + X^3$ is a irreducible polynomial over $GF(2)$.

See Topic: CYCLIC CODES, Short Answer Type Question No. 3.

GROUP – C
(Long Answer Type Questions)

7. a) Verify the following expression:

$$C_s = \log_2 m$$

where C_s is the channel capacity of a lossless channel and m is the number of symbols in the channel.

b) Give that AWGN channel with 4 kHz bandwidth and the noise power spectral density $\eta/2 = 10^{12}$ W/Hz. The signal power required at the receiver is 0.1 mW. Calculate the capacity of the channel.

c) Define (i) Lossless and (ii) Deterministic channel.

d) State and prove the Shannon-Hartley law of channel capacity.

a) See Topic: INFORMATION THEORY, Long Answer Type Question No. 13(a).

b) See Topic: INFORMATION THEORY, Short Answer Type Question No. 11.

c) See Topic: INFORMATION THEORY, Long Answer Type Question No. 11(c).

d) See Topic: INFORMATION THEORY, Long Answer Type Question No. 5(a).

8. a) For a systematic (7, 4) cyclic code determine the generator matrix and parity check matrix if $g(x) = x^3 + x + 1$

b) A codeword polynomial $c(x)$, belonging to the (7, 4) code with $g(x) = x^3 + x + 1$, incurs error so giving the received polynomial $v(x)$. Find $c(x)$ when

i) $v(x) = x^5 + x^2 + 1$

ii) $v(x) = x^6 + x^3 + 1$

c) Construct the encoder circuit for the (7, 3) code with $g(x) = x^4 + x^3 + x^2 + 1$ and input $i(x) = x^2 + x$.

a) See Topic: CYCLIC CODES, Long Answer Type Question No. 2(a).
b) See Topic: CYCLIC CODES, Long Answer Type Question No. 2(b).
c) See Topic: CYCLIC CODES, Short Answer Type Question No. 4.

9. a) One parity check code has parity check matrix as

$$H = 110:100$$
$$101:010$$
$$100:001$$

i) Determine generator matrix
ii) Find the code word that begins with [100]
iii) If received word is [110011], then decode this word
b) Explain the RSA algorithm with examples.

a) See Topic: BLOCK CODES, Long Answer Type Question No. 6.
b) See Topic: INFORMATION THEORY, Long Answer Type Question No. 14.

10. a) Given that (7,3) Cyclic code with $g(x) = x^4 + x^3 + x^2 + 1$. Construct its dual code.

b) Find the generator polynomial $g(x)$ for single error correcting binary BCH code of blocklength 31.

c) Use the primitive polynomial $p(x) = x^5 + x^2 + 1$ to construct GF (32).

a) See Topic: CYCLIC CODES, Short Answer Type Question No. 5.
b) & c) See Topic: BCH CODES, Long Answer Type Question No. 5.

11. Write short notes on any three of the following:
    a) Source Coding
    b) Hamming Code
    c) Trellis diagram
    d) Error control strategy
    e) Viterbi decoding

a) See Topic: INFORMATION THEORY, Long Answer Type Question No. 17(d).
b) See Topic: BLOCK CODES, Long Answer Type Question No. 13(a).
c) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(c).
d) See Topic: CODING CHANNELS, Long Answer Type Question No. 1.
e) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(a).

QUESTION 2018

GROUP – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for the followings (*any ten*):

i) The unit of information is
a) Bit b) Decit c) Nat ✓d) All of these

ii) Entropy represents
a) Rate of information ✓b) Average information
c) Probability of information d) Disorder of information

iii) The efficiency of Huffman code is linearly proportional to
a) average length of the code ✓b) average entropy
c) maximum length of the code d) None of these

iv) A code with minimum distance $d_{min} = 5$. How many errors it can correct?
a) 3 b) 4 ✓c) 2 d) 1

v) The Hamming distance between $X = 1100001011$ and $Y = 1001101001$ is
a) 1 b) 5 c) 3 ✓d) 4

vi) The entropy of information source is maximum when symbol occurrences are
✓a) Equi-probable b) Different probability c) Both (a) and (b) d) None of these

vii) The coding efficiency η is given by
a) $\eta = H(X) \cdot \overline{L}$ ✓b) $\eta = H(X)/\overline{L}$ c) $\eta = \overline{L}/H(X)$ d) $\eta =$ none of these

viii) The capacity of a communication channel with a bandwidth of 4 kHz and 15 SNR is approx.
a) 20 kbps ✓b) 16 kbps c) 10 kbps d) 8 kbps

ix) Cycle redundancy check is a type of
a) Convolution code ✓b) Cyclic code c) Parity check code d) None of these

x) The condition of a dual code in case of a linear blods code is
✓a) $GH^T = 0$ b) $(HG)^T = 0$ c) $H^T G^T = 0$ d) $GH^T = 1$

xi) In block coding if $k = 2$ and $n = 3$, the number of invalid code word is
a) 8 ✓b) 4 c) 2 d) 6

xii) If $m = 4$, then what will be the length of the BCH code?

a) 16 b) 17 ✓c) 15 d) None of these

xiii) Consider the parity check matrix

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$ and the received vector $r = (001110)$. Then the syndrome is given by

a) (110) ✓b) (100) c) (111) d) (101)

xiv) For a Reed-Solomon code, the minimum distance is

a) $n+k-1$ ✓b) $n-k+1$ c) $k-n-1$ d) $k-n+1$

GROUP – B
(Short Answer Type Questions)

2. State and prove the Shannon-Hartley law of channel capacity.

See Topic: INFORMATION THEORY, Long Answer Type Question No. 5(a).

3. A DMS X had five symbols with probability $P(X_1) = 0.1$, $P(X_2) = 0.2$, $P(X_3) = 0.5$, $P(X_4) = 0.3$ and $P(X_5) = 0.25$ respectively.

(a) Construct the Binary Huffman code for X.

(b) Calculate the efficiency of the code.

Data inaccurate cannot be solved.

4. Prove that $d_{min} \geq 2t + 1$, where t = Number of error.

See Topic: BLOCK CODES, Long Answer Type Question No. 3.c).

5. Construct a table $GF(2^3)$ based on the primitive polynomial $P(X) = 1 + X + X^3$.

See Topic: BCH CODES, Short Answer Type Question No. 4.

6. A (7, 4) cyclic code has a generator polynomial $g(x) = 1 + x^2 + x^3$. Draw the syndrome circuit and find out the syndrome showing all the contents of the registers in all the required shift for $r = 0010110$.

See Topic: CYCLIC CODES, Long Answer Type Question No. 3(d).

GROUP – C
(Long Answer Type Questions)

7. a) What do you mean by entropy of a source and mutual information of a communication channel?.

See Topic: INFORMATION THEORY, Long Answer Type Question No. 11(a).

b) A discrete source emits one of five symbols one every millisecond with probabilities $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$ and $\frac{1}{16}$ respectively. Find the source entropy and information rate.

See Topic: INFORMATION THEORY, Long Answer Type Question No. 15.

8. a) Explain the Shannon-Fano coding.

See Topic: INFORMATION THEORY, Long Answer Type Question No. 17(b).

b) A DMS x has eight symbols $X_1, X_2, X_3, X_4, X_5, X_6, X_7$ and X_8 with $P(X_1)=\frac{1}{2}$, $P(X_2)=\frac{1}{8}, P(X_3)=\frac{1}{8}, P(X_4)=\frac{1}{16}, P(X_5)=\frac{1}{16}, P(X_6)=\frac{1}{16}, P(X_7)=\frac{1}{32}$ and $P(X_8)=\frac{1}{32}$. Construct a Shannon-Fano code for X and calculate the efficiency of code.

See Topic: INFORMATION THEORY, Long Answer Type Question No. 16.

9. a) Prove that for (n, k) Linear block code $2^{n-k} \geq \sum_{i=0}^{t} nCi$, t = number of error.

See Topic: BLOCK CODES, Long Answer Type Question No. 11(a).

b) Consider a systematic (8, 4) code whose parity check equations are

$$V_0 = U_1 + U_2 + U_3$$
$$V_1 = U_0 + U_1 + U_2$$
$$V_2 = U_0 + U_1 + U_3$$
$$V_3 = U_0 + U_2 = U_3$$

where U_0, U_1, U_2 and U_3 are message digits and V_0, V_1, V_2 and V_3 are parity check digits. Find the generator and parity check matrices for this code. Show analytically that the minimum distance of this code is 4.

See Topic: BLOCK CODES, Long Answer Type Question No. 11(b).

10. Consider a (6, 3) linear block code define by the generator matrix.

$$G = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{vmatrix}$$

a) Determine if the code is a Hamming-code. Find the parity check matrix H of the code is symmetrical form.
b) Find is the encoding table for the linear block code.
c) What is the minimum distance d_{min} of the code?
d) For a particular code word transmitted, the received code word is 111110. Find the corresponding data word transmitted.

See Topic: BLOCK CODES, Long Answer Type Question No. 12.

11. Write short notes on any *three* of the following:
a) Viterbi decoding
b) Golay code
c) Trellis diagram
d) Source coding
e) Turbo codes

a) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(a).
b) See Topic: CYCLIC CODES, Long Answer Type Question No. 5(a).
c) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(c).
d) See Topic: INFORMATION THEORY, Long Answer Type Question No. 17(d).
e) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(b).

QUESTION 2019

GROUP – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for the followings (*any ten*):

i) A binary memory less source X with two symbols x_1, x_2. The Entropy of source $H(X)$ is maximum when

✓a) both x_1 and x_2 are equiprobable
b) $x_1 \geq x_2$
c) $x_2 \geq x_1$
d) none of these

ii) The relation between entropy and mutual information is

✓a) $I(X;\ Y) = H(X) - H(X/Y)$
b) $I(X;\ Y) = H(X/Y) - H(Y/X)$
c) $I(X;\ Y) = H(X) - H(Y)$
d) $I(X;\ Y) = H(Y) - H(X)$

iii) An encoder for a (4, 3, 5) convolution code has a memory of order

a) 4
b) 2
c) 3
✓d) 5

iv) DMS X with two symbols x_1 and x_2 and $P(x_1) = 0.9$, $P(x_2) = 0.1$. Find efficiency and redundancy of this code.

a) 45%, 55%
b) 40%, 80%
✓c) 46.9%, 53.1%
d) 90%, 90%

v) If the SNR of the signal is increased, then the channel capacity
a) is increased
b) is decreased
✓c) remains constant
d) cannot be determined

vi) $A(8, 4)$ linear code has code rate of
a) 8
b) 4
✓c) 0.5
d) 2

vii) For $a(7, 4)$ cyclic code generated by $g(x) = 1 + x + x^3$ the syndrome for the error pattern $e(x) = x^3$ is
a) 101
b) 111
✓c) 110
d) 011

viii) In $GF(2^3)$, α^7 equal to
✓a) 1
b) α^{14}
c) α^{21}
d) all of these

ix) Relation between message rate(r) and information rate(R) is
✓a) $R = rH$
b) $r = RH$
c) $r = R^2H$
d) $R = r^2H$

x) The code in convolution coding is generated using
✓a) EX-OR logic
b) AND logic
c) OR logic
d) None of these

xi) For decoding in convolution coding, in a code tree
✓a) diverge upward when a bit is 0 and diverge downward when the bit is 1
b) diverge downward when a bit is 0 and diverge upward when the bit is 1
c) diverge left when a bit is 0 and diverge right when the bit is 1
d) diverge right when a bit is 0 and diverge left when the bit is 1

GROUP – B
(Short Answer Type Questions)

2. Define Linear Block Codes. What are the properties of Linear Block Code?
See Topic: BLOCK CODES, Short Answer Type Question No. 5.

3. Consider a binary memoryless source X with two symbols x_1 and x_2. Prove that $H(x)$ is maximum when both x_1 and x_2 are equiprobable.
See Topic: INFORMATION THEORY, Short Answer Type Question No. 12.

4. Determine the generation polynomial for double error correcting BCH code for code length $n = 15$.
See Topic: BCH CODES, Short Answer Type Question No. 1.

5. What is meant by mutual information? Prove that $I(X, Y) = H(X) - H(X/Y)$, where notations have their usual meaning.

See Topic: INFORMATION THEORY, Short Answer Type Question No. 7(OR).

6. a) What are the limitations of syndrome decoding methods for error corrections?

b) The generator matrix for $a(6, 3)$ block code is shown below obtain codeword for the message bit 010 and 011.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

See Topic: CODING CHANNELS, Short Answer Type Question No. 7.

GROUP – C
(Long Answer Type Questions)

7. a) What is the difference between source coding and channel coding?

b) What is the advantage of variable length coding over fixed length coding?

c) A source is generating five symbols (i.e., x_1, x_2, x_3, x_4, x_5) with probabilities 0.4, 0.19, 0.16, 0.15, 0.1. Determine the code word of the symbols using Huffman code. Calculate the efficiency of the above generated codes.

a) See Topic: CODING CHANNELS, Short Answer Type Question No. 2(b).
b) See Topic: INFORMATION THEORY, Short Answer Type Question No. 13.
c) See Topic: INFORMATION THEORY, Long Answer Type Question No. 8.

8. a) Verify the following expression:

$$C_S = 1 + p \log_2 p + (1 - p) \log_2 (1 - p),$$

where, C_S is the channel capacity of a BSC.

b) Show that the channel capacity of an ideal AWGN channel with infinite bandwidth is given by $C_{\text{infinite}} = \frac{1}{\ln 2} \frac{S}{\eta} = \frac{1.44S}{\eta} \frac{b}{s}$ where S is the average signal power and $\frac{\eta}{2}$ is the power spectral density of white Gaussian noise.

c) Given an AWGN channel with 4 kHz bandwidth and the noise power spectral density $\frac{\eta}{2} = 10^{-12}$ W/Hz. The signal power required at the receiver is $\upsilon 0.1$ mW. Calculate the capacity of this channel.

a) See Topic: INFORMATION THEORY, Short Answer Type Question No. 14.
b) See Topic: INFORMATION THEORY, Long Answer Type Question No. 12(b).
c) See Topic: INFORMATION THEORY, Short Answer Type Question No. 11.

9. a) Prove that $f(X) = 1 + X + X^3$ is a primitive polynomial over $GF(2)$.

b) What do you mean by minimal polynomial? Find out the minimal polynomials over the field $GF(2^3)$. Given $P(X) = 1 + X + X^3$.

c) Determine the generator sequence of double error correcting $(n,,k)$ BCH code over the field $GF(2^3)$. Evaluate n and k. Where, symbols have their usual meanings.

See Topic: BCH CODES, Long Answer Type Question No. 6.

10. a) Analyse with proper diagram the encoding of a convolutional code.

b) Analyse Viterbi algorithm using Trellis diagram for error detection and error correction of convolutional code.

c) Consider a convolutional encoder having generator sequence $g = (11001)$. Determine the output sequence for the input sequence $u = (110101)$.

See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 1.

11. Write short notes on any *three* of the following:
    a) Shortened & Extended Code
    b) Dual code
    c) Code Tree
    d) Turbo Codes
    e) Reed-Solomon code

a) See Topic: CYCLIC CODES, Long Answer Type Question No. 5(f).
b) See Topic: CYCLIC CODES, Long Answer Type Question No. 5(d).
c) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(d).
d) See Topic: CONVOLUTIONAL CODES, Long Answer Type Question No. 2(b).
e) See Topic: BCH CODES, Long Answer Type Question No. 7(c).