# Chapter One

# Review of Probability Theory

## 1.1 Probability of an event X

If an experiment has $x_1$, $x_2$, ……$x_n$ outcomes, then

$$P(x_i) = \lim_{N \to \infty} \frac{n(x_i)}{N}$$

where

$n(x_i)$ = Number of times event (outcome) $x_i$ occurs

N = total number of trails

Notes:

$$1 \le P(x_i) \ge 0$$

$$\sum_{i=1}^{n} P(x_i) = 1$$

If $P(x_i) = 1$, then $x_i$ is certain event

## 1.2 Joint Probability

If we have two experiments X & Y

Experiment X has $x_1$, $x_2$, ……$x_n$ outcomes

Experiment Y has $y_1$, $y_2$, ……$y_n$ outcomes, then

$P(x_i,y_j)$ = Joint probability that event $x_i$ occurs from experiment X and event $y_j$ from experiment Y

Note:

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

$P(x_i,y_j)$ is written in matrix form.

① chapters:1, 2, 3

$$P(X,Y) = \begin{array}{c} \\ x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{array} \begin{array}{c} \begin{array}{cccccc} y_1 & y_2 & . & . & . & y_m \end{array} \\ \left[\begin{array}{cccccc} . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \end{array}\right] \end{array}$$

Note

$$\sum_{i=1}^{n} P(x_i, y_j) = P(y_j) = \text{ sum of the jth column}$$

$$\sum_{j=1}^{m} P(x_i, y_j) = P(x_i) = \text{ sum of the ith row}$$

**Example1.1**

Given that $$P(X,Y) = \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \begin{bmatrix} 0.2 & 0.1 \\ 0.15 & 0.25 \\ 0.1 & 0.2 \end{bmatrix}$$

then $$P(x_1) = \sum_{j=1}^{2} P(x_1, y_j) = 0.2 + 0.1 = 0.3$$

$$P(y_2) = \sum_{i=1}^{3} P(x_i, y_2) = 0.1 + 0.25 + 0.2 = 0.55$$

$$\sum_{j=1}^{m} \sum_{i=1}^{n} P(x_i, y_j) = 0.2 + 0.1 + 0.15 + 0.25 + 0.1 + 0.2 = 1$$

## 1.3 Conditional Probability

Two experiments X&Y with their outcomes affect on each other

$P(x_i/y_j)$ = conditional probability of xi given that yj has already occurred in experiment Y. $y_j$

$P(y_j/x_i)$ = conditional probability of yi given that $x_i$ has already occurred in experiment X.

Note:

$P(x_i,y_j) = P(x_i).P(y_j/x_i) = P(y_j).P(x_i/y_j)$

$P(x_i,y_j) = P(y_j,x_i)$

i.e. the joint probability is symmetric and is related with conditional probability

Both P(X/Y) and P(Y/X) can be written in matrix form

$$P(X/Y) = \begin{array}{c|cccccc|} & y_1 & y_2 & \cdots & & & y_m \\ \hline x_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_n & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array} \qquad P(Y/X) = \begin{array}{c|cccccc|} & y_1 & y_2 & \cdots & & & y_m \\ \hline x_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_n & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}$$

Note:

$\sum_{i=1}^{n} P(x_i / y_j) = 1$ the sum of each column equals 1

$\sum_{j=1}^{m} P(y_j / x_i) = 1$ the sum of each row equals 1

**Example1.2**

$$P(X/Y) = \begin{array}{c}x1\\x2\\x3\end{array}\begin{bmatrix} 2/7 & 5/13 \\ 0 & 4/13 \\ 5/7 & 4/13 \end{bmatrix} \qquad P(Y/X) = \begin{array}{c}x1\\x2\\x3\end{array}\begin{bmatrix} 2/7 & 5/7 \\ 0 & 1 \\ 5/9 & 4/9 \end{bmatrix} \begin{array}{c}\sum=1\\\sum=1\\\sum=1\end{array}$$

$$\sum=1 \quad \sum=1$$

$$P(X,Y) = \begin{array}{c}x_1\\x_2\\x_3\end{array}\begin{bmatrix} 0.1 & 0.25 \\ 0 & 0.2 \\ 0.25 & 0.2 \end{bmatrix} \quad \sum=1$$

**Example1.3**

The two experiments X & Y have the joint probability matrix

$P(X,Y)=\begin{bmatrix} 0.1 & 0.25 \\ 0 & 0.2 \\ 0.25 & 0.2 \end{bmatrix}$ find (a) P(X), (b) P(Y), (c) P(X/Y), (d) P(Y/X)

**Solution:**

(a) $P(x_1) = 0.1 + 0.25 = 0.35$

$P(x_2) = 0 + 0.2 = 0.2$

$P(x_3) = 0.25 + 0.2 = 0.45 = 1 - P(x_1) - P(x_2)$

Hence $P(X) = [0.35 \quad 0.2 \quad 0.45]$

(b) $P(y_1) = 0.1 + 0 + 0.25 = 0.35$

$P(y_2) = 0.25 + 0.2 + 0.2 = 0.65 = 1- P(y_1)$

Hence $P(Y) = [0.35 \quad 0.65]$

(c) P(X/Y) = P(X,Y) / P(Y)

$$P(X/Y)=\begin{bmatrix} 0.1/0.35 & 0.25/0.65 \\ 0/0.35 & 0.2/0.65 \\ 0.25/0.35 & 0.2/0.65 \end{bmatrix}=\begin{bmatrix} 2/7 & 5/13 \\ 0 & 4/13 \\ 5/7 & 4/13 \end{bmatrix}$$

(d) P(Y/X) = P(X,Y) / P(X)

$$P(X/Y)=\begin{bmatrix} 0.1/0.35 & 0.25/0.35 \\ 0/0.2 & 0.2/0.2 \\ 0.25/0.45 & 0.2/0.45 \end{bmatrix}=\begin{bmatrix} 2/7 & 5/7 \\ 0 & 1 \\ 5/9 & 4/9 \end{bmatrix}$$

**H.W 1.1**

If $P(X/Y)=\begin{bmatrix} 0.1 & 0.25 & 0.32 \\ 0.65 & 0.2 & 0.32 \\ 0.25 & 0.55 & 0.34 \end{bmatrix}$, $P(y_1) = 0.2$ and $P(y_2)=0.3$

Find (a) P(X) (b) P(Y/X)

## 1.4 Statistical Independence

If $x_i$ has no effect on the probability of $y_j$, they are called independent, and

$$P(x_i/y_j) = P(x_i)$$

$$P(y_j/x_i) = P(y_j)$$

hence $P(x_i,y_j) = P(x_i).P(y_j)$

## 1.5 Random Variable

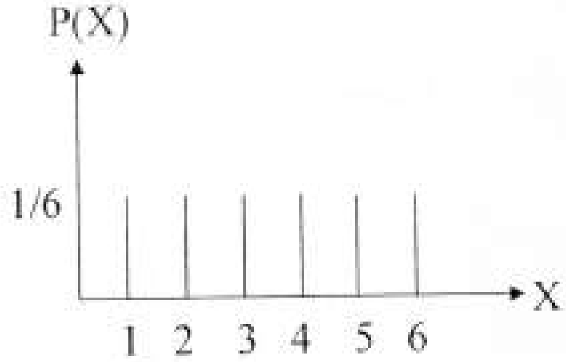
- **Discrete random variable**

Recall the case of a die, each face is numbered as 1,2, ….,6. If the die is fair, then P(1) = P(2) = ………= P(6) = 1/6

$$\overline{X} = \sum_{i=1}^{n} x_i P(x_i) \quad \text{mean value}$$

$$\overline{X^2} = \sum_{i=1}^{n} x_i^2 P(x_i) \quad \text{mean square value}$$

$$\sigma_X^2 = \overline{X^2} - (\overline{X})^2 \quad \text{variance of } X$$



### H.W 1.2

Find $\overline{X}$, $\overline{X^2}$ and $\sigma_X^2$ for (a) one fair die (b) two fair dice

- **Continuous random variable**

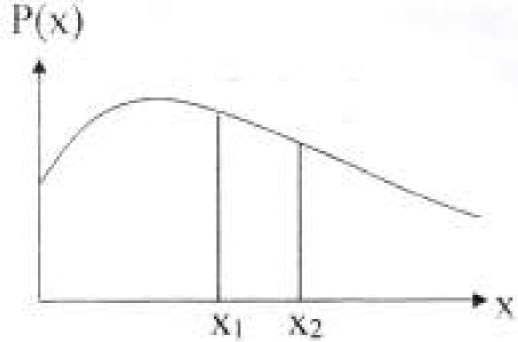
Here x have all real values (not discrete) then, we call

P(x)=PDF (Probability Density Function)

That gives the probability that x lies between any two values $x_1$ & $x_2$

$$P(x_2 > x > x_1) = \int_{x_1}^{x_2} P(x)dx$$

$$\int_{-\infty}^{\infty} P(x)dx = 1$$



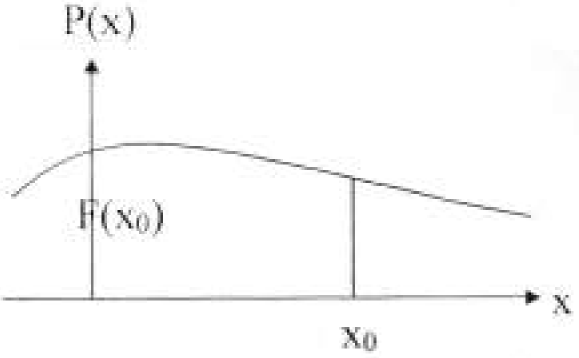
$$\overline{X} = \int_{-\infty}^{\infty} xP(x)dx$$ mean value

$$\overline{X}^2 = \int_{-\infty}^{\infty} x^2 P(x)dx$$ mean square value

$$\sigma_X^2 = \overline{X}^2 - (\overline{X})^2$$ variance of X

Also F(x) = CDF of x (Cumulative Distribution of x)

$$F(x) = \int_{-\infty}^{x} P(x)dx$$



$$F(x_0) = \int_{-\infty}^{x_0} P(x)dx$$

$$P(x) = \frac{d}{dx}F(x) \qquad F(x) = \int_{-\infty}^{x} P(x')dx'$$

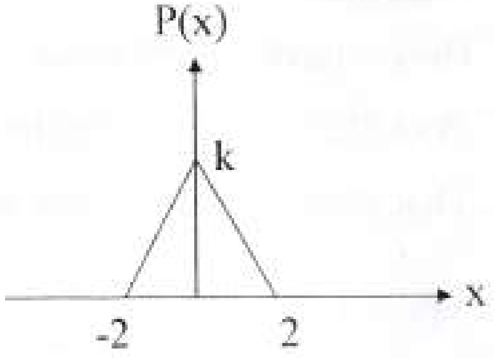
F(∞)=1 F(-∞)=0

**Example1.4**

If x is a continuous random variable having PDF shown, Find:

(a) the constant k, (b) P(x>1), (c) $\overline{X}$, $\overline{X}^2$ and $\sigma_x^2$

**Solution:**



(a) $\int_{-\infty}^{\infty} P(x)dx = Area = \int_{-2}^{2} P(x)dx = 1$

Area = (1/2)(4)(k)=1 then k=1

(b) $P(x>1) = \int_{1}^{2} P(x)dx = \int_{1}^{2} (\frac{1}{2} - \frac{1}{4}x)dx = \left[\frac{x}{2} - \frac{x^2}{8}\right]_1^2$

= (1/2)-(3/8) = 1/8

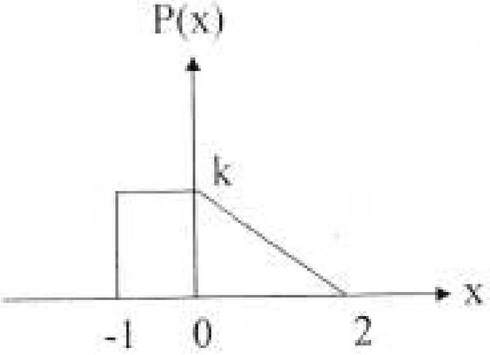
(c) $\overline{X}=\int_{-2}^{0}x(\frac{1}{2}+\frac{1}{4}x)dx+\int_{0}^{2}x(\frac{1}{2}-\frac{1}{4}x)dx=0$ (symmetrical around x=0)

$$\overline{X^2}=2\int_{0}^{2}x^2(\frac{1}{2}-\frac{1}{4}x)dx=2\left[\frac{x^3}{6}-\frac{x^4}{16}\right]_0^2=\frac{2}{3}$$

$$\sigma_X^2=\overline{X^2}-(\overline{X})^2=\frac{2}{3}-(0)^2=\frac{2}{3}$$

**H.W 1.3**

Repeat the previous example if P(x) is as shown in Fig. below



# Chapter Two

# Measuring of Information

## 2.1 Information Theory

Information theory is a subject that deals with information and data transmission from one point to another. The block diagram of any digital communication system is shown below:

| | | |
|---|---|---|
| Audio | modulation | speaker |
| Video | ciphering | TV |
| Telex | error correction | computer |
| Computer | data compression | typewriter |
| : | : | : |
| : | : | : |

The concept of information is related to probability. Any signal that conveys information must be unpredictable (random), but not visa versa, i.e. not any random signal conveys information.(noise is a random signal conveying no information).

## 2.2 Self Information:

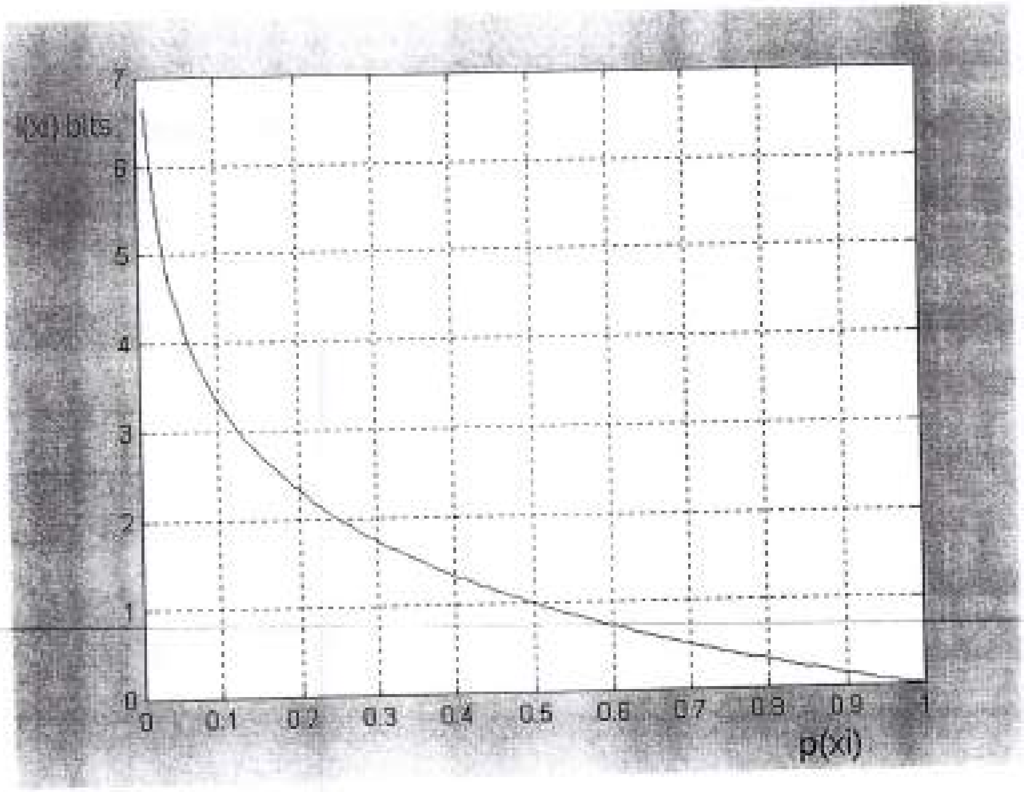
Suppose that the source of information produces finite set of messages $x_1$, $x_2$, $x_3$,...., $x_n$ with probabilities $p(x_1)$, $p(x_2)$, $p(x_3)$,.:......,$p(x_n)$ and such that $\sum_{i=1}^{n} p(x_i)=1$. The amount of information gained by knowing that the source produces the message $x_i$ is related with $p(x_i)$ as follows:

1-information is zero if $p(x_i)=1$ (certain event)

2-information increases as $p(x_i)$ decreases to zero.

3-information is a +ve quantity.

The function that relates $p(x_i)$ with information of $x_i$ is denoted by **$I(x_i)$** and is called **self information of $x_i$.** The **log** function shown satisfies all previous three points hence:



$$\boxed{I(x_i) = -\log_a \mathrm{p(xi)}}$$

1-if "a"=2 (this is mostly used in digital communication) then $I(x_i)$ has the units of **bits.**

2-if "a"=e=2.71828, then $I(x_i)$ has the units of **nats.**

3- if "a"=10 , then $I(x_i)$ has the units of **Hartly.**

Recall that $\log_a x = \frac{\ln x}{\ln a}$

### Example 2.1:

A fair die is thrown, find the amount of information gained if you are tolled that 4 will appear.

**Solution:**

Since fair, die then, p(1) = p(2) =……= p(6) =1/6, then:

$I(4) = -\log_2 p(4) = -\log_2(1/6) = \ln6/\ln2 = 2.5849$ bits.

(note that if "a" is not given then a = 2)

### Example 2.2

A biased coin has P(Head) = 0.3. Find the amount of information gained if you are tolled that a tail will appear.

**Solution:**

P(tail) = 1- P(Head) = 1-0.3 = 0.7, then

$I(\text{tail}) = -\log_2(0.7) = -\ln0.7/\ln2 = 0.5145$ bits.

### Example 2.3

Find the amount of information contained in a black & white (B/W) TV picture if we assume that each picture has $2*10^5$ dots (pixels or picture elements) and each pixel has 8 equiprobable and distinguishable levels of brightness.

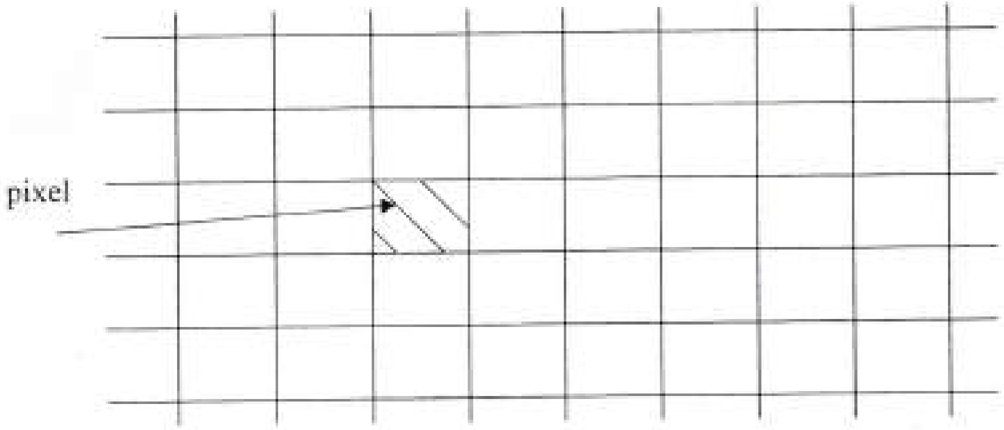
**Solution:**

P(each level) = 1/8 since equiprobable levels

Information/pixel = $-\log_2(1/8) = 3$ bits

Information/picture = Information/pixel * no. of pixels

$= 3 * 2 * 10^5 = 600$ kbits.



**H.W 1:**

Repeat previous example for color TV with 16 equiprobable colors and 8 equiprobable levels of brightness.

## 2.3 Source Entropy

If the source produces not equiprobable messages then $I(x_i)$ , $i=1,2,\ldots,n$, are different. Then the **statistical average** of $I(x_i)$ over i will give the **average amount of uncertainty** associated with the source X. This average is called source entropy and is denoted by H(X). This H(X) is given by:

$$\boxed{H(X)=\sum_{i=1}^{n} p(x_i)\, I(x_i)}$$

or

$$\boxed{H(X)=-\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)}$$

Bits/symbol

**Example 2.4**

Find the entropy of the source producing the following messages:

$$p(X) = \begin{matrix} x1 & x2 & x3 & x4 \\ 0.25 & 0.1 & 0.15 & 0.5 \end{matrix}$$

**Solution:**

$$H(X) = -\sum_{i=1}^{4} p(xi)\log_2 p(xi)$$

H(X) = -[0.25ln0.25+ 0.1ln0.1+ 0.15ln0.15+0.5ln0.5]/ln2

H(X) = 1.7427 bits/symbol

Note:

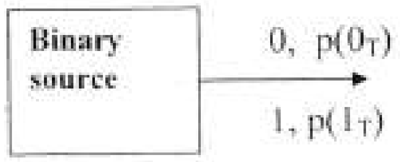
Usually and according to our previous study in logic and digital electronic we are not familiar with fractions of bits. Here in communication, these fractions occur due to averaging., i.e., for the previous example the 1.7427 is the average, i.e, if the source produces say 100000 message, then the amount of information produced is 174270 bits.

**Example 2.5**

Find and plot the entropy of a binary source.

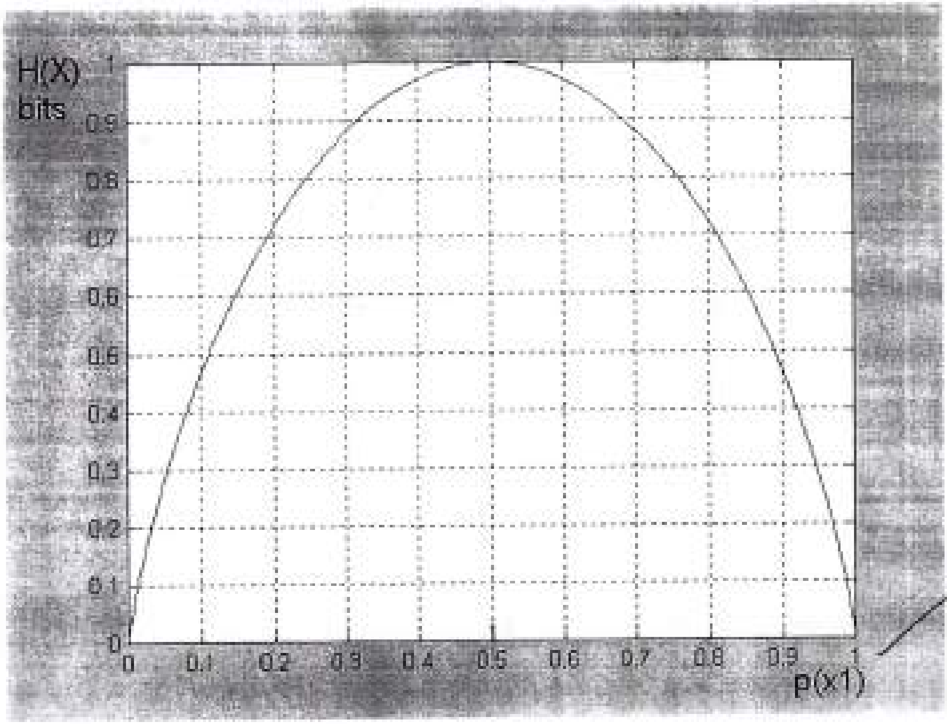
**Solution:**

$P(0_T) + P(1_T) = 1$, hence:



$H(X) = -[\, P(0_T)\log_2 P(0_T) + (1 - P(0_T))\log_2(1 - P(0_T))]$ bits/symbol

Note that H(X) has maximum equals 1 bit if $P(0_T) = P(1_T) = 0.5$



Notes:

1- In general $\boxed{H(X) = H(X)|_{max} = \log_2 n}$ bits/symbol

if all messages are **equiprobable**, i.e, **$p(x_i)=1/n$**, then :

$$H(X)=H(X)|_{max}=-[(\frac{1}{n}\log_2(\frac{1}{n})*n]=\log_2 n \quad \text{bits/symbol}$$

2- H(X) = 0 if one of the messages has the probability of a certain event.

## 2.4 Source Entropy Rate

This is the average rate of amount of information produced per second. It is denoted by R(X) and is given by:

$$\boxed{R(X)=r*H(X)} \quad \text{bits/sec}$$

where r is the rate of producing the symbols

The units of R(X) is **bits/sec (bps)** if H(X) is in **bits/symbol** and r in **symbols/sec.**

Sometimes R(X) is also given as:

$$\boxed{R(X) = \frac{H(X)}{\bar{\tau}}} \quad \text{bps}$$

where :

$\bar{\tau} = \sum_{i=1}^{n} \tau_i \, p(xi)$ = average time duration of symbols.

$\tau_i$ is the time duration of the symbol $x_i$.

**Example 2.6:**

A source produces dots "." and dashes "—" with P(dot)=0.65. If the time duration of a dot is 200ms and that for a dash is 800ms. Find the average source entropy rate.

**Solution:**

P(dot) = 0.65, then P(dash)=1 - P(dot)=1-0.65=0.35.

H(X) = - [0.65 $\log_2$ 0.65 + 0.35 $\log_2$ 0.35] = 0.934 bits/symbol

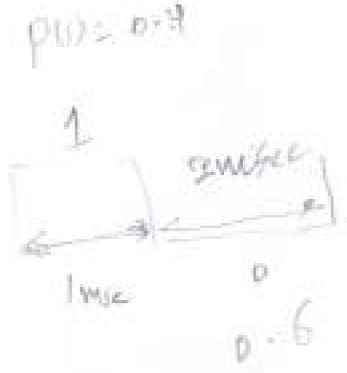
$\tau_{dot}$ = 0.2 sec, $\tau_{dash}$ = 0.8 sec, then

$$\bar{\tau} = 0.2 * 0.65 + 0.8 * 0.35 = 0.41 \ \text{sec}$$

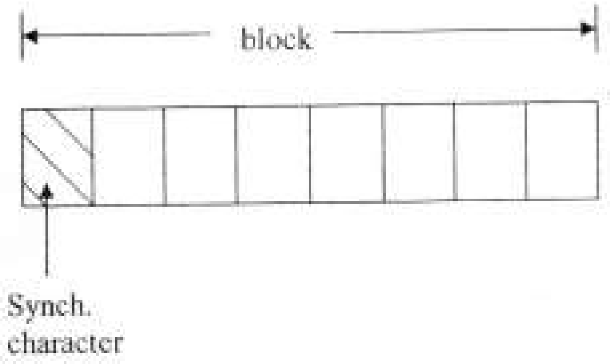
$$then \quad R(X) = \frac{H(X)}{\bar{\tau}} = \frac{0.934}{0.41} = 2.278 \ bps$$

**Example 2.7:**

In a telex link, information is arranged in blocks of 8 characters. The 1st position (character) in each block is always kept the same for synchronization purposes. The remaining 7 places are filled randomly from the English alphabets with equal prob. If the system produces 400 blocks/sec, find the average source entropy rate.



**Solution:**



Each of the 7 positions behaves as a source that may produce randomly one of the English alphabets with prob. of 1/26, hence:

Information/position = - $\log_2(1/26) = \log_2 26 = 4.7$ bits

Information/block = $7 * 4.7 = 32.9$ bits

we exclude the 1st character since it has no information having the prob. of certain event (contains synch only), then:

R(X) = Information/blocks * rate of producing blocks/sec

$= 32.9 * 400 = 13160$ bits/sec

## 2.5 Source Efficiency and Redundancy:

- **Source efficiency ($\eta_{source}$)**

  Source efficiency is the ratio of the average information generated from the source to the maximum possible average information can be generated from the same source, i.e.

$$\boxed{\eta_{source} = \frac{H(x)}{H(x)_{\max}} = \frac{H(x)}{\log_2 n}}$$

- **Source redundancy ($R_{source}$)**

  Source redundancy is the complementary part of the source efficiency, i.e.

$$\boxed{R_{source} = 1 - \eta_{source} = 1 - \frac{H(x)}{\log_2 n}}$$

Above relations can also be given as percentages.

**Example 2.8**

Suppose that a Discrete Memoryless Source (DMS) is defined over the range of $X = \{x_1, x_2, x_3, x_4\}$, and the corresponding probability values for each symbol are $P(x_1) = 1/2$, $P(x_2) = P(x_3) = 1/8$ and $P(x_4) = 1/4$. Calculate (a) Source entropy, (b) Source efficiency and redundancy.

**Solution:**

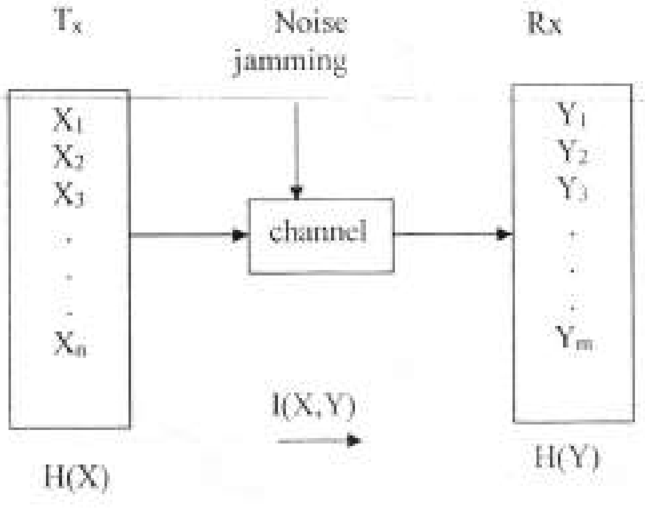
(a) $H(x) = -[(1/2)\log_2(1/2) + 2^*(1/8)\log_2(1/8) + (1/4)\log_2(1/4)]$

$= 1.75$ bits/symbol

(b) $\eta_{source} = \frac{H(x)}{\log_2 n} = \frac{1.75}{\log_2 4} = \frac{1.75}{2} = 87.5\%$

$R_{source} = 1 - \eta_{source} = 12.5\%$

## 2.6 Mutual Information



Consider the set of symbols $x_1, x_2, \ldots, x_n$, the transmitter $T_x$ may produce. The receiver $R_x$ may receive $y_1, y_2, \ldots, y_m$. Theoretically, if the noise and jamming is zero, then set X = setY and n=m. However, and **due to noise and jamming, there will be a conditional probability $p(y_j/x_i)$:**

Define:

1- $P(x_i)$ to be what is called the **apriori prob** of the symbol $x_i$ , which is the prob of selecting $x_i$ for transmission.

2- $P(x_i/y_j)$ to be what is called the **aposteriori prob** of the symbol $x_i$ after the reception of $y_j$.

The amount of information that $y_j$ provides about $x_i$ is called the mutual information between $x_i$ and $y_j$. This is given by:

$$\boxed{I(xi, yj) = \log_2 \frac{aposterori\ prob}{apriori\ prob} = \log_2 \frac{P(xi/yj)}{P(xi)}}$$

Note that also and since $P(x_i)\,P(y_j/x_i) = P(y_j)\,P(x_i/y_j) = P(x_i, y_j)$, then:

$$\boxed{I(xi, yj) = \log_2 \frac{p(yj/xi)}{p(yj)} = I(yj, xi)}$$

i.e. the mutual information is symmetric.

Note:

$P(x_i/y_j) \neq P(y_j/x_i)$ in general. In fact, $P(y_j/x_i)$ gives the prob of $y_j$ given that $x_i$ is transmitted, as if we are at the $T_x$ and we transmit $x_i$ and we ask about the prob of receiving $y_j$ instead. The prob $p(x_i/y_j)$ is the prob of $x_i$ given we receive $y_j$ as if we are at the $R_x$ and we receive $y_j$ and we ask about if it was coming from $x_i$.

Properties of $I(x_i,y_j)$:

1- It is symmetric, i.e. $I(x_i,y_j) = I(y_j,x_i)$

2- $I(x_i,y_j)>0$ if aposteriori prob> apriori prob, $y_j$ provides **+ve information about $x_i$.**

3- $I(x_i,y_j)=0$, if aposteriori prob =apriori prob, which is the case of statistical independence when $y_j$ provides **no information** about $x_i$.

4- $I(x_i,y_j)<0$ if aposteriori prob< apriori prob, $y_j$ provides -ve information about $x_i$, i.e., $y_j$ **adds ambiguity**.

## 2.7 Transinformation (average mutual information):

This is the statistical averaging of all the pair $I(x_i,y_j)$, $i=1,2,\ldots n$, $j=1,2,3\ldots m$. This is denoted by $I(X,Y)$ and is given by:

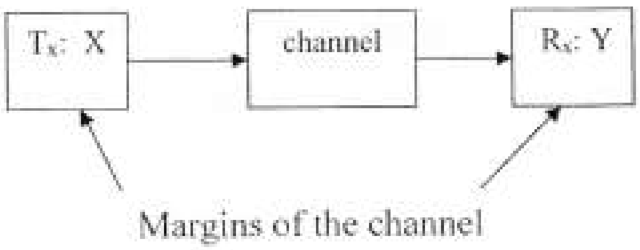
$$\boxed{I(X,Y)=\sum_{i=1}^{n}\sum_{j=1}^{m} I(x_i,y_j)p(x_i,y_j)} \quad \text{bits/symbol}$$

$$\boxed{I(X,Y)=\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i,y_j)\log_2\frac{p(x_i/y_j)}{p(x_i)}} \quad \text{bits/symbol}$$

or

$$\boxed{I(X,Y)=\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i,y_j)\log_2\frac{p(y_j/x_i)}{p(y_j)}} \quad \text{bits/symbol}$$

## 2.8 Marginal Entropies



Marginal entropies is a term usually used to denote both source entropy H(X) defined as before and the receiver entropy H(Y) is given by:

$$\boxed{H(Y) = -\sum_{j=1}^{m} P(y_j)\log_2 P(y_j)} \quad \text{bits/symbol}$$

## 2.9 Joint and conditional entropies:

The average amount of information associated with the pair $(x_i,y_j)$ is called joint or system entropy H(X,Y):

$$\boxed{H(X,Y) = H(XY) = -\sum_{j=1}^{m}\sum_{i=1}^{n} P(x_i,y_j)\log_2 P(x_i,y_j)} \quad \text{bits/symbol}$$

The average amount of information associated with the pairs $(y_j/x_i)$ & $(x_i/y_j)$ are called conditional entropies H(Y/X) & H(X/Y), they are given by:

$$\boxed{H(Y/X) = -\sum_{j=1}^{m}\sum_{i=1}^{n} P(x_i,y_j)\log_2 P(y_j/x_i)} \quad \text{bits/symbol}$$

$$\boxed{H(X/Y) = -\sum_{j=1}^{m}\sum_{i=1}^{n} P(x_i,y_j)\log_2 P(x_i/y_j)} \quad \text{bits/symbol}$$

**Example 2.9:**

Show that H(X,Y) = H(X) + H(Y/X)

**Solution:**

This is a very useful identity to ease calculations in problem solving.

To prove it, then we know that:

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

But $P(x_i,y_j) = P(x_i)\,P(y_j/x_i)$, putting this inside the log term only, then:

$$H(X,Y) = -\sum_{j=1}^{m}\sum_{i=1}^{n} p(xi,yj)\log_2 p(xi) - \sum_{j=1}^{m}\sum_{i=1}^{n} p(xi,yj)\log_2 p(yj/xi)$$

After reversing the order of summation, then $\sum_{j=1}^{m} p(xi,yj) = p(xi)$

Substituting in the previous equation, we get:

$$H(X,Y) = -\sum_{i=1}^{n} p(xi)\log_2 p(xi) - \sum_{i=1}^{n}\sum_{j=1}^{m} p(xi,yj)\log_2 p(yj/xi)$$

In the above equation, the 1st term is in fact H(X) and the 2nd term with -ve sign is H(Y/X), then:

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

**H.W 2:**

Show that H(X,Y) = H(Y) + H(X/Y)

**Example 2.10:**

Show that I(X,Y)=H(X)-H(X/Y)

**Solution:**

we know that: $$I(X,Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} p(xi,yj)\log_2 \frac{p(xi/yj)}{p(xi)}$$

$$I(X,Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} p(xi,yj)\log_2 p(xi/yj) - \sum_{i=1}^{n}\sum_{j=1}^{m} p(xi,yj)\log_2 p(xi)$$

As before, we reverse the order of summation of the 2nd term, then

$\sum_{j=1}^{m} p(xi,yj) = p(xi)$ and:

$$I(X,Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} p(xi,yj)\log_2 p(xi/yj) - \sum_{i=1}^{n} p(xi)\log_2 p(xi)$$

or $I(X,Y) = H(X) - H(X/Y)$

Note:

Above identity indicates that the transinformation I(X,Y) is in fact the net average information obtained at the receiver coming from the difference between the original information produced by the source H(X) and that information lost at the channel H(X/Y)(losses entropy) due to noise and jamming.

**H.W 3:**

Show that $I(X,Y) = H(Y) - H(Y/X)$

**Example 2.11:**

Show that I(X,Y) is zero for extremely noisy channel.

**Solution:**

For extremely noisy channel, then $y_j$ gives no information about $x_i$ (the receiver can not decide anything about $x_i$ as if we transmit a deterministic signal $x_i$ but.the receiver receives noise like signal $y_j$ that is completely has no correlation with $x_i$). Then $x_i$ and $y_j$ are statistically independent and

$P(x_i/y_j) = P(x_i)$ and $P(y_j/x_i) = P(y_j)$ for all i and j , then:

$I(x_i,y_j)=\log_2 1=0$ for all i & j, then $I(X,Y)=0$

**Example 2.12:**

The joint prob of a system is given by:

$$p(X,Y)=\begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array}\begin{bmatrix} 0.5 & 0.25 \\ 0 & 0.125 \\ 0.0625 & 0.0625 \end{bmatrix}, \text{ find:}$$

(a) marginal entropies.

(b) joint entropy.

(c) conditional entropies.

(d) the mutual information between $x_1$ and $y_2$.

(e) the transinformation.

(f) draw the channel model.

**Solution:**

(a) First we find p(X) & p(Y) from p(X,Y) by summing the rows and columns:

$$p(X)=\begin{bmatrix} x1 & x2 & x3 \\ 0.75 & 0.125 & 0.125 \end{bmatrix} \quad p(Y)=\begin{bmatrix} y1 & y2 \\ 0.5625 & 0.4375 \end{bmatrix}, \text{ then:}$$

H(X) = - [0.75 $\log_2$0.75 ) +2*0.125 $\log_2$0.125] = 1.06127 bits/symbol

H(Y) = - [0.5625 $\log_2$0.5625 + 0.4375 $\log_2$0.4375] = 0.9887 bits/symbol

(b) $H(X,Y)=-\sum_{j=1}^{m}\sum_{i=1}^{n} p(xi,yj)\log_2 p(xi,yj)$

H(X,Y) = -[0.5$\log_2$0.5 +0.25$\log_2$0.25 +0.125$\log_2$0.125+ 2*0.0625$\log_2$0.0625]

H(X,Y) = 1.875 bits/symbol

(c) H(Y/X) = H(X,Y) - H(X) = 1.875-1.06127 = 0.813 bits/symbol

H(X/Y) = H(X,Y) - H(Y) = 1.875-0.9887 = 0.886 bits/symbol

(d) $I(x1,y2)=\log_2\dfrac{p(x1/y2)}{p(x1)}$ but $p(x1/y2)=\dfrac{p(x1,y2)}{p(y2)}$ then:

$$I(x1,y2)=\log_2\frac{p(x1,y2)}{p(x1)p(y2)}=\log_2\frac{0.25}{0.75*0.4375}=-0.3923 \text{ bits}$$

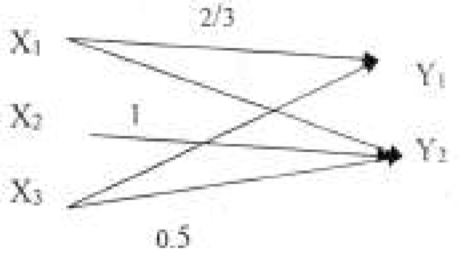
That means $y_2$ gives ambiguity about $x_1$

(e) I(X,Y)=H(X)-H(X/Y)=1.06127-0.8863=0.17497 bits/symbol

(f) To draw the channel model, we find p(Y/X) matrix from p(X,Y) matrix by dividing its rows by the corresponding $p(x_i)$:

$$P(Y/X)=\begin{array}{c}\\ x_1\\ x_2\\ x_3\end{array}\left[\begin{array}{cc} y_1 & y_2\\ 0.5/0.75 & 0.25/0.75\\ 0/0.125 & 0.125/0.125\\ 0.0625/0.125 & 0.0625/0.125\end{array}\right]=\begin{array}{c}\\ x_1\\ x_2\\ x_3\end{array}\left[\begin{array}{cc} y_1 & y_2\\ 2/3 & 1/3\\ 0 & 1\\ 0.5 & 0.5\end{array}\right]$$

note that the sum of each row in P(Y/X) matrix is unity.

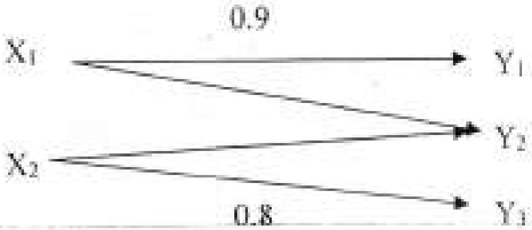


## H.W 4:

For the channel model shown, find:

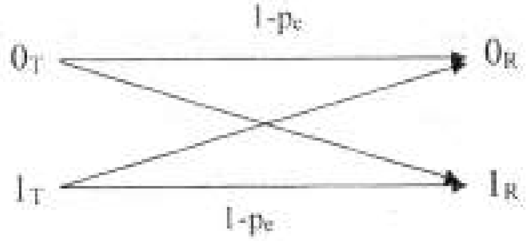
(a) source entropy rate if $\tau_{x1}$ = 1ms and $\tau_{x2}$ = 2 ms, $I(x_1)$=2 bits.

(b) the transinformation.



## Example 2.13:

Find and plot the transinformation for a binary symmetric channel (BSC) shown if $p(0_T) = p(1_T) = 0.5$



**Solution:**

This BSC is a very well known channel with practical values of $p_e$<<1.

If we denote $0_T = x_1$, $1_T = x_2$, $0_R = y_1$, $1_R = y_2$, then:

$$p(Y/X) = \begin{array}{c|cc} & y1 & y2 \\ x1 & 1-pe & pe \\ x2 & pe & 1-pe \end{array} \qquad p(X,Y) = \begin{array}{c|cc} & y1 & y2 \\ x1 & 0.5(1-pe) & 0.5pe \\ x2 & 0.5pe & 0.5(1-pe) \end{array}$$

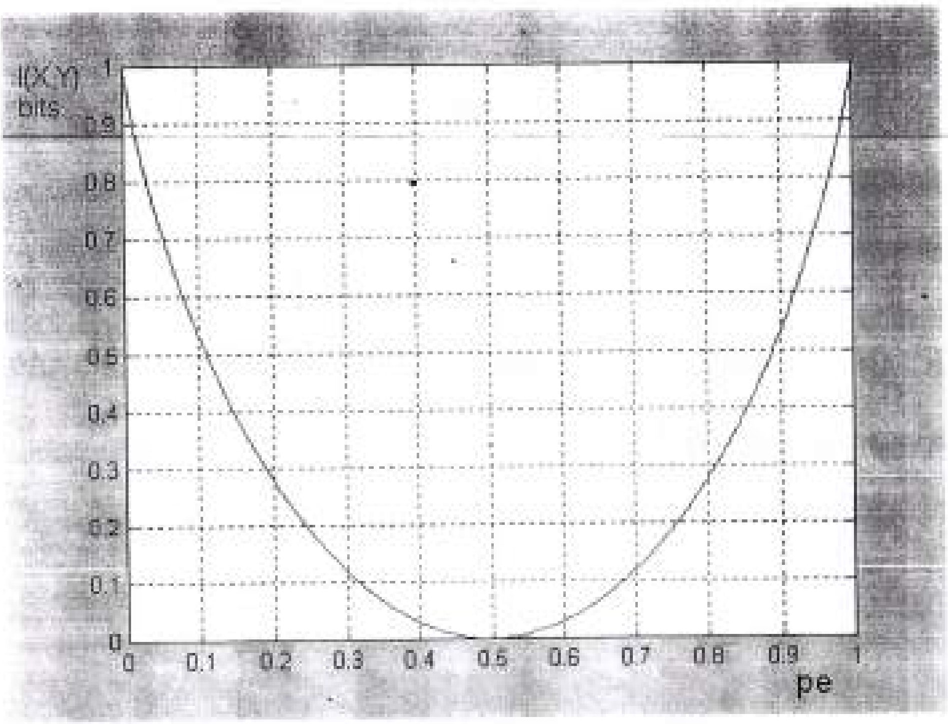
Then $p(Y) = [0.5 \quad 0.5]$ and $H(Y)=H(Y)|_{max}=1$ bit.

Next, we find H(Y/X), as:

$$H(Y/X) = -[\{0.5(1-pe)\log_2(1-pe)\}*2 + \{0.5pe\log_2 pe\}*2]$$

$$H(Y/X) = -[(1-pe)\log_2(1-pe) + pe\log_2 pe]$$

Then $I(X,Y) = H(Y) - H(Y/X) = 1 + (1-p_e)\log_2(1-p_e) + p_e\log_2 p_e$



## H.W 5:

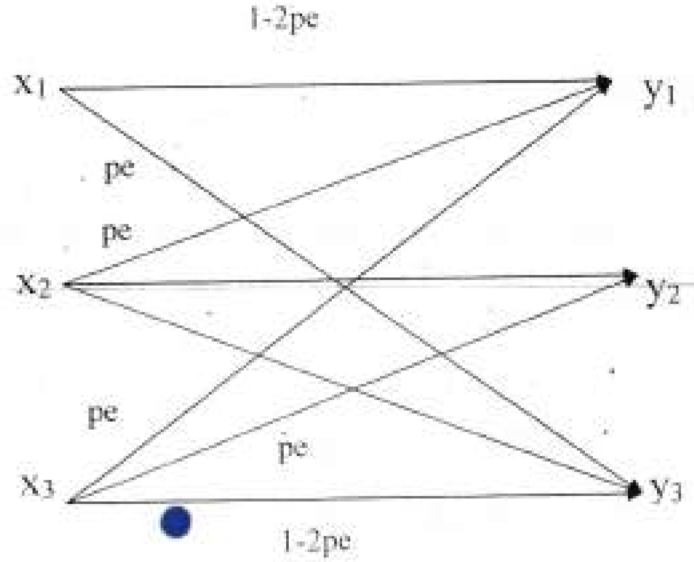
A BSC has $p(Y/X)=\begin{bmatrix}0.8 & 0.2\\0.2 & 0.8\end{bmatrix}$ , if $I(0_T)$ = 3bits, find system and losses entropies.

## 2.10 Ternary symmetric channel TSC:

This has the transitional probability:

$$p(Y/X)=\begin{array}{c|ccc|} & y_1 & y_2 & y_3 \\ x_1 & 1-2\,pe & pe & pe \\ x_2 & pe & 1-2\,pe & pe \\ x_3 & pe & pe & 1-2\,pe \end{array}$$

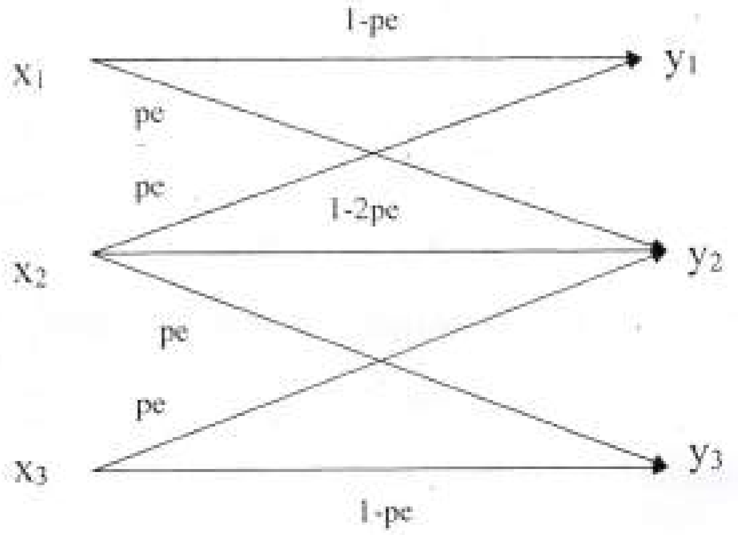
This TSC is symmetric but not very practical since practically $x_1$ and $x_3$ do not affected so much as $x_2$. In fact the interference between $x_1$ and $x_3$ is much less than the interference between $x_1$ & $x_2$ or $x_2$ & $x_3$.



Hence, the more practical but nonsymmetric channel has the trans prob:

$$p(Y/X) = \begin{array}{c|ccc|} & y_1 & y_2 & y_3 \\ x_1 & 1-p_e & p_e & 0 \\ x_2 & p_e & 1-2p_e & p_e \\ x_3 & 0 & p_e & 1-p_e \end{array}$$

where $x_1$ interfere with $x_2$ exactly the same as interference between $x_2$ and $x_3$, but $x_1$ and $x_3$ are not interfered.



## 2.11 Other special channels:

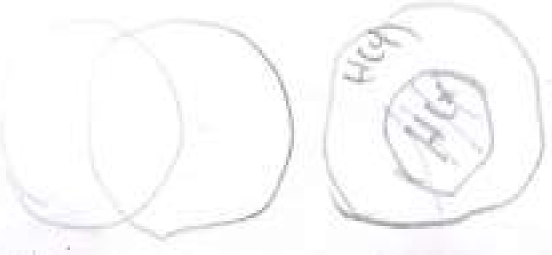
- **lossless channel:**

  This has only one nonzero element in each column of the transitional matrix p(Y/X). As an example:

$$p(Y/X) = \begin{array}{c}  \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{bmatrix} y_1 & y_2 & y_3 & y_4 & y_5 \\ 3/4 & 1/4 & 0 & 0 & 0 \\ 0 & 0 & 1/3 & 2/3 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This channel has **H(X/Y) = 0** and **I(X,Y) = H(X)** with **zero losses entropy**.

**H.W 6**



Draw the model of this channel.

- **Deterministic channel:**

This has only one nonzero element in each row of the transitional matrix p(Y/X). As an example:

$$p(Y/X)=\begin{array}{c}\\x_1\\x_2\\x_3\\x_4\\x_5\end{array}\begin{bmatrix}y_1 & y_2 & y_3\\1 & 0 & 0\\1 & 0 & 0\\0 & 1 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

This has **H(Y/X)=0** and **I(X,Y) = H(Y)** with **zero noise entropy**.

**H.W 7**

Draw the model of this channel.

- **Noiseless channel:**

This has only one nonzero element in each row and column of the transitional matrix p(Y/X), i.e. it is an identity matrix. As an example:

$$p(Y/X)=\begin{array}{c}\\x1\\x2\\x3\end{array}\begin{bmatrix}y1 & y2 & y3\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

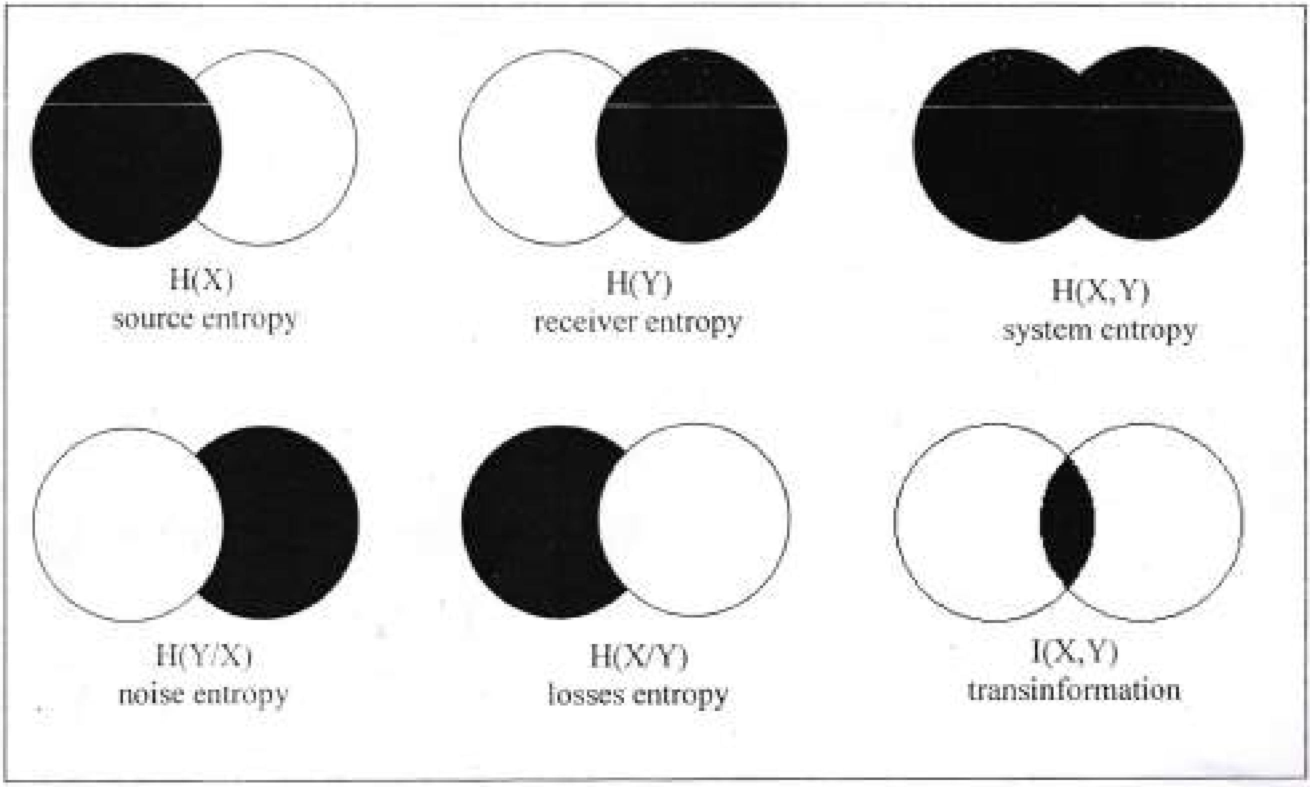
This has **H(X/Y) = H(Y/X) = 0**, and **I(X,Y) = H(X) = H(Y)**.

**H.W 8**

Draw the model of this channel.

## 2.12 Venn Diagram Representations of Entropies:

X = Transmitter ($T_x$ ),    Y = Receiver ( $R_x$ )



H(X)
source entropy

H(Y)
receiver entropy

H(X,Y)
system entropy

H(Y/X)
noise entropy

H(X/Y)
losses entropy

I(X,Y)
transinformation

**H.W 9**

Write mathematical expression to calculate I(X,Y) using H(X,Y), H(X) and H(Y).

# Chapter 2 Tutorial Problems

<u>Q1</u>. In Facsimile transmission, $2.25*10^6$ square picture elements are needed to provide proper picture resolution. Find the maximum information content if 12 brightness levels are required for good reproduction
(Ans : 8 Mbits/picture)

**Solution:**

$p(\text{level}) = \frac{1}{12}$

information/element $= -\log_2 \frac{1}{12} = \log_2 12 = 3.585$ bits

information/picture $= H(x) = 3.585 * 2.25 * 10^8 = 8 \text{ M}\frac{\text{bits}}{\text{picture}}$

<u>Q2</u>: (a) Find the capacity in bit per second that would be required to transmit TV picture signals if 500,000 picture elements were required for good resolution and 10 different brightness levels were specified for proper contrast. Thirty pictures per second are to be transmitted. All picture elements are assumed to vary independently with equal likelihood of occurance.

(b) In addition to the above requirements for a monochrome system, a particular colour TV system must provide 30 different colours. Show that the transmission in this colour system requires almost 2.5 times as much capacity as the monochrome system
(Ans : (a) $R_1(x) = 49.8$ Mbits/sec , (b) $R_2(x) = 2.48\, R_1(x)$)

**Solution:**

(a) $p(\text{level}) = \frac{1}{10}$

information/element $= -\log_2 \frac{1}{10} = \log_2 10$ bits/element

information/picture $= H(x) = 5 \times 10^5 \log_2 10$ bits/picture

$\therefore R_1(x) = H(x) * \text{No. of pictures per sec.}$
$= 5 * 10^5 \log_2 10 * 30 = 49.8$ Mbits/sec.

(b) $p(\text{level}) = \frac{1}{10}$ & $p(\text{color}) = \frac{1}{30}$

$p(x,y) = p(x) \cdot p(y/x)$
$p(\text{level}, \text{color}) = \frac{1}{10} * \frac{1}{30} = \frac{1}{300}$

information/element $= -\log_2 \frac{1}{300} = \log_2 300$ bits/element

$H(x) =$ information/picture $= 5 * 10^5 \log_2 300 = 4.1$ M bits/picture

$\therefore R_2(x) = H(x) * \text{No. of pictures/sec.}$

$= 4.1 \times 10^6 \times 30 = 123.4$ Mbits/sec.

$\therefore$ the relation between $R_1(x)$ & $R_2(x)$ is

$$\frac{R_2(x)}{R_1(x)} = \frac{123.4}{49.8} \Rightarrow R_2(x) = 2.48\, R_1(x)$$

Q3 : An alphabet consists of the letters A, B, C and D. For transmission each letter is coded into a sequence of two binary pulses. A is represented as 00, B as 01, C as 10 and D as 11. Each individual pulse interval is 5 msec.

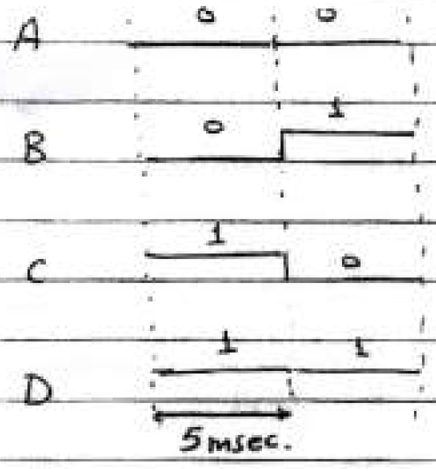
(a) Calculate the average rate of transmission of information if the different letters are equiprobable

(b) The probability of occurance of each letter is respectively, $P_A = 1/5$, $P_B = 1/4$, $P_C = 1/4$ and $P_D = 3/10$ Find the average rate of transmission of information in bits/sec.

(Ans: (a) 200 bits/sec (b) 198.00 bits/sec.)

**Solution:**

(a)



equally likely (equal prob.)

$\therefore p(A) = p(B) = p(C) = p(D)$

$= \frac{1}{4}$

$$\text{information/letter} = -\log_2 \frac{1}{4} = \log_2 4 = 2 \text{ bits/letter}$$

$$\therefore R(x) = \frac{\text{bits/letter}}{\text{sec/letter}}$$

$$t_{av} = 5 + 5 = 10 \text{ msec./letter}$$

$$\therefore R(x) = \frac{2}{10 \times 10^{-3}} = 200 \text{ bits/sec.}$$

16

(b) $p(A) = \frac{1}{5}$ $p(B) = \frac{1}{4}$ $p(C) = \frac{1}{4}$ $p(D) = \frac{3}{10}$

$$H(X) = -\left[\frac{1}{5}\log_2\frac{1}{5} + 2*\frac{1}{4}\log_2\frac{1}{4} + \frac{3}{10}\log_2\frac{3}{10}\right]$$

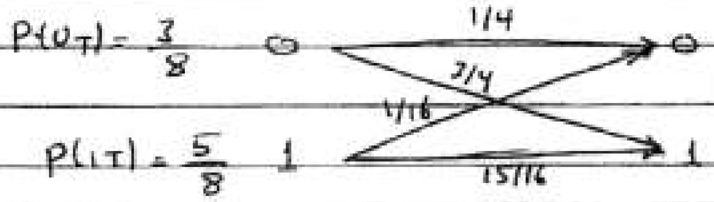
$= 1.98$ bits/letter

$t_{av} = 10$ msec./letter

$$R(Y) = \frac{1.98 \text{ bits/letter}}{10*10^{-3} \text{ sec./letter}} = 198 \text{ bits/sec.}$$

Q4: A binary data source has $P(0_T) = \frac{3}{8}$. Due to intersymbol interference of the channel, then $P(0_R|1_T) = \frac{1}{16}$ and $p(1_R|0_T) = \frac{3}{4}$. Calculate the noise and losses entropies and compare with source entropy.
(Ans: $H(Y/X) = 0.5156$ bits/symbol
$H(X|Y) = 0.9047$ bits/symbol)

**Solution:**



Noise entropy $H(Y/X)$
Losses entropy $H(X|Y)$

$$P(Y/X) = \begin{array}{c|cc} & y_0 & y_1 \\ \hline X_0 & \frac{1}{4} & \frac{3}{4} \\ X_1 & \frac{1}{16} & \frac{15}{16} \end{array}$$

$$p(X) = \begin{array}{cc} x_0 & x_1 \\ \frac{3}{8} & \frac{5}{8} \end{array}$$

$$P(Y/X) = \frac{P(X,Y)}{P(X)} \rightarrow P(X,Y) = P(X).P(Y/X)$$

$$P(X,Y) = \begin{array}{c|cc} X_0 & \frac{3}{32} & \frac{9}{32} \\ X_1 & \frac{5}{128} & \frac{75}{128} \end{array}$$

$$p(y) = \begin{array}{cc} y_0 & y_1 \\ 0.1328 & 0.8671 \end{array}$$

$$H(x) = \text{Source entropy} = -\sum_{i=1}^{2} p(x_i) \log_2 p(x_i)$$

$$= -\left[\frac{3}{8}\log_2\frac{3}{8} + \frac{5}{8}\log_2\frac{5}{8}\right] = 0.9544 \ \frac{\text{bits}}{\text{symbol}}$$

$$H(x,y) = -\sum_{j=1}^{2}\sum_{i=1}^{2} P(x_i,y_j)\log_2 P(x_i,y_j)$$

$$= -\left[\frac{3}{32}\log_2\frac{3}{32} + \frac{5}{128}\log_2\frac{5}{128} + \frac{9}{32}\log_2\frac{9}{32} + \right.$$

$$\left.\frac{75}{128}\log_2\frac{75}{128}\right] = 1.47 \text{ bits/symbol}$$

$$\therefore H(X,Y) = H(X) + H(Y/X)$$

$$\Rightarrow H(Y/X) = H(X,Y) - H(X)$$

$$= 1.47 - 0.9544 = 0.5156 \text{ bits/symbol}$$

$$H(Y) = -\sum_{j=1}^{2} P(y_j)\log_2 P(y_j)$$

$H(Y) = -\left[0.1328 \log_2(0.1328) + 0.867 \log_2(0.867)\right]$

$= 0.5653$ bits/symbol

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

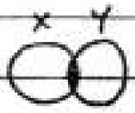
$\therefore H(X/Y) = H(X,Y) - H(Y)$

$= 1.47 - 0.5653 = 0.9047$

we note that losses entropy > noise entropy

i.e $H(X/Y) > H(Y/x)$

& $H(X/Y) \sim H(X)$



Q5: A message source generates one of four messages randomly every microsecond. If prob. of these messages are 0.4, 0.3, 0.2 and 0.1. Find the rate of information produced.

(Ans: $1.846 * 10^6$ bits/sec)

**Solution:**

Q6 $H(X) = -\sum_{i=1}^{4} p(x_i) \log_2 p(x_i)$

$= 0.4 \log_2 0.4 + 0.3 \log_2 0.3 + 0.2 \log_2 0.2 + 0.1 \log_2 0.1$

$= 1.846$ bits/message

$R(x) = \dfrac{H(x)}{\text{average time duration of the message}}$

$= \dfrac{1.846}{10^{-6}} = 1.846 * 10^6$ bits/sec.

<u>Q6</u>: A binary channel matrix is given by $\begin{array}{c|cc} & y_1 & y_2 \\ \hline x_1 & \frac{2}{3} & \frac{1}{3} \\ x_2 & \frac{1}{10} & \frac{9}{10} \end{array}$

Find : source entropy, noise entropy and transinformation if $p(x_1)=\frac{1}{3}$

(Ans : $H(X)=0.9183$ bits/sym; $H(Y/X)=0.6187$ bits/symbol
$I(X,Y)=0.25$ bits/symbol.

**Solution:**

$$p(x_2)=1-p(x_1)=1-\frac{1}{3}=\frac{2}{3}$$

$$p(x,y)=p(x)\cdot p(y/x)=\begin{array}{c}x_1\\x_2\end{array}\begin{bmatrix}\frac{2}{9} & \frac{1}{9}\\ \frac{2}{30} & \frac{18}{30}\end{bmatrix}$$

$$p(y)=\begin{array}{cc} y_1 & y_2 \\ \left[0.29\right. & \left.0.71\right]\end{array}$$

$$H(x)=-\left[\frac{1}{3}\log_2\frac{1}{3}+\frac{2}{3}\log_2\frac{2}{3}\right]=0.9183\ \frac{\text{bit}}{\text{symbol}}$$

$$H(Y/X)=-\sum_i\sum_j p(x_i,y_j)\log_2 P(y_j/x_i)$$

$$=-\left[\frac{2}{9}\log_2\frac{2}{3}+\frac{1}{9}\log_2\frac{1}{3}+\frac{2}{30}\log_2\frac{1}{10}+\frac{18}{30}\log_2\frac{9}{10}\right]=0.6187\ \text{bits/symbol}$$

$$H(y)=-\left[0.29\log_2 0.29+0.71\log_2 0.71\right]$$
$$=0.8687\ \text{bits/symbol}$$

$$I(X,Y)=H(Y)-H(Y/X)$$
$$=0.8687-0.6187$$
$$=0.25\ \text{bits/symbol}$$

Q7: The transition matrix of a channel is given by :

$$P(Y/X) = \begin{array}{c|ccc} & y_1 & y_2 & y_3 \\ \hline x_1 & 0.1 & 0.3 & 0.6 \\ x_2 & 0.2 & 0.25 & 0.55 \end{array}$$

If $P(X_1) = 0.4$, find (a) noise entropy (b) losses entropy (c) rate of information transmission if each symbol lasts 0.1 msec. (d) Source entropy rate.

(Ans : (a) 1.38 bits/symbol (b) 0.95 bits/symbol
(c) 200 bits/sec (d) 9700 bits/sec.

**Solution:**

$P(X_1) + P(X_2) = 1$

$\therefore P(X_2) = 1 - P(X_1) = 1 - 0.4 = 0.6$

$$\Rightarrow P(X) = \begin{array}{cc} x_1 & x_2 \\ \hline 0.4 & 0.6 \end{array}$$

$$P(X,Y) = P(X).P(Y/X) = \begin{array}{c|ccc} & y_1 & y_2 & y_3 \\ \hline x_1 & 0.04 & 0.12 & 0.24 \\ x_2 & 0.12 & 0.15 & 0.33 \end{array}$$

(a) noise entropy $H(Y/X)$

$$H(Y/X) = -\left[0.04\log_2 0.1 + 0.12\log_2 0.3 + 0.24\log_2 0.6 + 0.12\log_2 0.2 + 0.15\log_2 0.25 + 0.33\log_2 0.55\right]$$

$= 1.38$ bits/symbol

(b) losses entropy $H(X/Y)$

$$P(y) = \begin{array}{ccc} y_1 & y_2 & y_3 \\ \hline 0.16 & 0.27 & 0.57 \end{array}$$

$$H(Y) = -\left[0.16 \log_2 0.16 + 0.27 \log_2 0.27 + 0.57 \log_2 0.57\right]$$
$$= 1.4 \text{ bits/symbol}$$

$$H(X,Y) = -\left[0.04 \log_2 0.04 + 0.12 \log_2 0.12 + 0.24 \log_2 0.24 + 0.12 \log_2 0.12 + 0.15 \log_2 0.15 + 0.33 \log_2 0.33\right]$$
$$= 2.35 \text{ bits/symbol}$$

$$\therefore H(X/Y) = H(X,Y) - H(Y) = 2.35 - 1.4 = 0.95 \frac{\text{bits}}{\text{symbol}}$$

(c) $I(X,Y) = H(X) - H(X/Y) = H(Y) - H(Y/X)$
$$= 1.4 - 1.38 = 0.02 \text{ bits/symbol}$$

$$R(X,Y) = \frac{I(X,Y)}{\tau_{av}} = \frac{0.02}{0.1 \times 10^{-3}} = 200 \text{ bits/sec}$$

(d) $H(X) = -[0.4 \log_2 0.4 + 0.6 \log_2 0.6] = 0.97$

$$\therefore R(X) = \frac{H(X)}{\tau_{av}} = \frac{0.97}{0.1 \times 10^{-3}} = 9700 \text{ bits/sec}$$

<u>Q8</u>: Asymmetric channel has
Find (a) $P_1$, $P_2$ and $P_3$
(b) channel capacity
(c) channel efficiency

$$P(X,Y) = \begin{array}{c|ccc} & y_1 & y_2 & y_3 \\ x_1 & P_1 & P_2 & P_3 \\ x_2 & 0.05 & 0.35 & 0.1 \\ x_3 & 0.06 & 0.03 & 0.21 \end{array}$$

(Ans: (a) $P_1 = 0.14$ ; $P_2 = 0.04$ ; $P_3 = 0.02$
(b) 0.42 bits/symbol
(c) 92%

**Solution:**

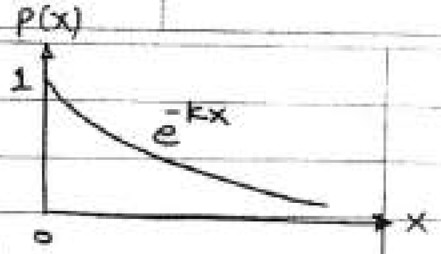
**Q9:** The PDF of a continous random Variable is

$$p(x) = \begin{cases} e^{-kx} & x > 0 \\ 0 & \text{elsewhere} \end{cases}$$

find K and entropy of x

(Ans: $k = 1$ ; $H(x) = 1/\ln 2$ bits/symbol)

**Solution:**



$$\int_{-\infty}^{\infty} p(x)\,dx = 1$$

$$\int_{0}^{\infty} e^{-kx}\,dx = 1 \Rightarrow -\frac{1}{k} e^{-kx} \Big|_{0}^{\infty} = 1$$

$$-\frac{1}{k}[0-1] = 1 \Rightarrow \boxed{k=1}$$

$$H(x) = -\int_{-\infty}^{\infty} p(x) \log_2 p(x)\,dx$$

$$= -\int_{0}^{\infty} e^{-x} \log_2 e^{-x}\,dx$$

$$= \int_{0}^{\infty} x e^{-x} \log_2 e\,dx$$

$$= \log_2 e \int_{0}^{\infty} \underbrace{x e^{-x}}_{udv} dx$$

$$\therefore H(x) = \log_2 e\,[-xe^{-x} - e^{-x}]_{0}^{\infty}$$

$$= \log_2 e\,[1]$$

$$= \frac{\ln e}{\ln 2} = \frac{1}{\ln 2} \quad \frac{\text{bits}}{\text{symbol}}$$

**Q10:** A ternary source has $P(X_0) = \frac{1}{8}$, self information of $X_1 = 3.5$ bits. If the source produces 100 symbol/sec. Find the source entropy rate and the redundancy of this source.

(Ans: $H(x) = 0.956$ bits/symbol; Redundancy $= 0.396$)

**Solution:**

$P(X_0) = \frac{1}{8}$ ; $I(X_1) = 3.5$ bits

$I(X_1) = -\log_2 P(X_1)$

$3.5 = -\log_2 P(X_1) \Rightarrow -3.5 = \log_2 P(X_1)$

$P(X_1) = 2^{-3.5} = 0.0883$

$P(X_2) = 1 - P(X_0) - P(X_1) = 1 - \frac{1}{8} - 0.0883$

$= 0.7867$

$H(X) = -\left[\frac{1}{8}\log_2\frac{1}{8} + 0.0883\log_2 0.0883 + 0.7867\log_2 0.7867\right]$

$= 0.956$ bits/symbol

Redundancy of the source $= 1 - \dfrac{H(x)}{H(x)|_{max}}$

$= 1 - \dfrac{0.956}{\log_2 3} = 1 - \dfrac{0.956}{1.58}$

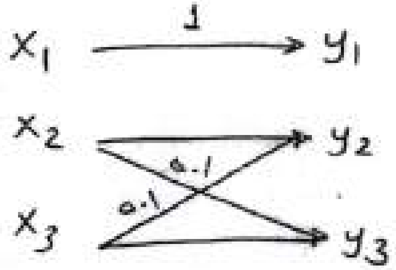
$= 0.396$

**Q11**: A source produces the symbols $x_1, x_2$ and $x_3$ with $p(x) = [\frac{1}{2} \;\; \frac{1}{4} \;\; \frac{1}{4}]$ If the time duration of each symbol is $\tau = [1 \;\; 2 \;\; 2]$ sec. These symbols are transmitted through a channel having the model shown below

Find:

(a) Source entropy rate

(b) Rate of information transmission



(Ans: (a) 1 bits/sec ; (b) 0.8436 bits/sec).

**Solution:**

$$p(x,y) = p(x).p(y/x) = \begin{array}{c|ccc} & y_1 & y_2 & y_3 \\ \hline x_1 & 0.5 & 0 & 0 \\ x_2 & 0 & 0.225 & 0.025 \\ x_3 & 0 & 0.025 & 0.225 \end{array}$$

$$p(y) = \begin{array}{ccc} y_1 & y_2 & y_3 \\ [0.5 & 0.25 & 0.25] \end{array}$$

(a) $H(x) = -\sum_{i=1}^{3} p(x_i) \log_2 p(x_i) = 1.5$ bits/symbol

$\bar{\tau} = \sum_{i=1}^{3} p(x_i)\tau_i = \frac{1}{2} * 1 + \frac{1}{4} * 2 + \frac{1}{4} * 2$

$= 1.5$ sec./symbol

$$R(x) = \frac{H(x)}{\text{average time duration of the symbol}} = \frac{1.5}{1.5} = 1 \frac{\text{bits}}{\text{sec.}}$$

$$(b)\ I(X,Y) = +\sum_{j=1}^{3}\sum_{i=1}^{3} p(x_i,y_j)\log_2 \frac{p(y_j/x_i)}{p(y_j)}$$

$$= 1.2655022 \text{ bits/symbol}$$

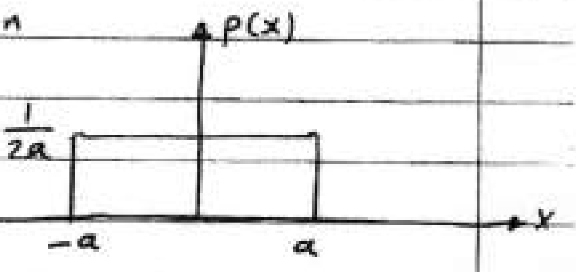
$$R(X,y) = \frac{I(X,Y)}{\text{average time duration of the symbol}}$$

$$= 0.8436 \text{ bits/sec.}$$

<u>Q12</u>: The input to a communication channel is a zero mean uniformly distributed random variable with variance of 3, find source entropy.

(Ans: 2.585 bits/symbol)

**Solution:**



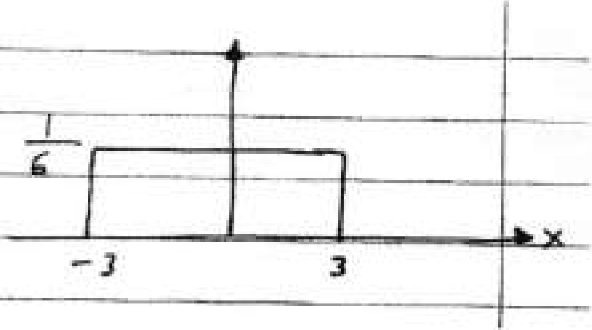
$$(a)\ \overset{ac}{\sigma_x^2} = \overset{total}{E(x^2)} - \overset{\text{zero mean (dc)}}{\cancel{[E(x)]^2}}$$

$$3 = \int_{-a}^{a} \frac{1}{2a} x^2 dx$$

$$3 = \frac{1}{6a} x^3 \Big|_{-a}^{a} \Longrightarrow 3 = \frac{2a^3}{6a} \Longrightarrow 3 = \frac{a^2}{3}$$

$$\Longrightarrow \boxed{a = 3}$$

$$H(x) = -\int_{-3}^{3} p(x)\log_2 p(x)\,dx$$



$$= -\int_{-3}^{3} \frac{1}{6}\log_2 \frac{1}{6}\,dx$$

$$= 2.585 \text{ bits/symbol}$$

# Chapter Three

# Channel Capacity

## 3.1 Channel capacity

This is defined as the maximum of I(X,Y):

$\boxed{\text{C=channel capacity=max[I(X,Y)]}}$ bits /symbol.

Physically it is the maximum amount of information each symbol can carry to the receiver. Sometimes this capacity is also expressed in bits/sec if related to the rate of producing symbols r :

$\boxed{C = r * \max[I(X,Y)]}$ bits/sec

where r is the number of symbols produced per second.

C is also expressed as:

$\boxed{C=\max[R(X,Y)]}$ bits/sec

where R(X,Y)=rate of information transmission :

R(X,Y)= r * I(X,Y) bits/sec or $R(X,Y)=\dfrac{I(X,Y)}{\bar{\tau}}$ where :

$\bar{\tau}=\sum_{i=1}^{n}\tau_i p(xi)$ = average time duration of symbols, $\tau_i$ is the time duration of the symbol $x_i$.

The maximization of I(X,Y) is done with respect to input prob p(X) or output prob p(Y) for a constant channel conditions, i.e. with p(Y/X) being a constant.

## 3.2 Channel capacity of discrete symmetric channels

- **Def: Symmetric channels:**

  Previously we mention some symmetric channels. A more general definition of symmetric channel is that channel where:

  1-n=m, equal number of symbols in X & Y, i.e. p(Y/X) is a square matrix.

  2-Any row in p(Y/X) matrix comes from some permutation of other rows.

**Example 3.1**

1- $p(Y/X)=\begin{bmatrix}0.9 & 0.1\\ 0.1 & 0.9\end{bmatrix}$ is a BSC where n=m=2 and the 1st row is the permutation of the 2nd row.

2- $p(Y/X)=\begin{bmatrix}0.9 & 0.05 & 0.05\\ 0.05 & 0.9 & 0.05\\ 0.05 & 0.05 & 0.9\end{bmatrix}$ is TSC where n=m=3 and each row is a permutation of the others.(same numbers appear)

3- $p(Y/X)=\begin{bmatrix}0.8 & 0.1 & 0.1\\ 0.1 & 0.8 & 0.1\end{bmatrix}$ is a nonsymmetric since n≠m( not square) although the 1st row is permutation of the 2nd row.

4- $p(Y/X)=\begin{bmatrix}0.8 & 0.1 & 0.1\\ 0.1 & 0.7 & 0.2\\ 0.1 & 0.1 & 0.8\end{bmatrix}$ is a nonsymmetric since the 2nd row is not a permutation of some other row, although n=m=3.

Channel capacity of such symmetric channel is easy to find using the following derivation:

To find max[I(X,Y)], then:

I(X,Y)=H(Y) - H(Y/X)

$$I(X,Y) = H(Y) + \sum_{j=1}^{m}\sum_{i=1}^{n} p(xi)p(yj/xi)\log_2 p(yj/xi)$$

If the channel is symmetric then the quantity $\sum_{j=1}^{m} p(yj/xi)\log_2 p(yj/xi)$ is a constant independent of the row number i, so if this comes out of the double summation, the remaining is $\sum_{i=1}^{n} p(xi)$ which is equal to unity, hence:

$$\boxed{\begin{aligned} I(X,Y) &= H(Y) + \sum_{j=1}^{m} p(yj/xi)\log_2 p(yj/xi) \\ &= H(Y) + K \end{aligned}}$$

Where K= $\sum_{j=1}^{m} p(yj/xi)\log_2 p(yj/xi)$

Hence: I(X,Y)=H(Y)+K for symmetric channels only

Now to find max of I(X,Y)=max[H(Y)+K]=max[H(Y)]+K

And since max[H(Y)]=$\log_2$m when Y has equiprobable symbols, then:

$\boxed{C = \log_2 m + K}$ bits / symbol

## 3.3 Channel efficiency and redundancy

Channel efficiency: $\boxed{\eta = \frac{I(X,Y)}{C}}$

Channel redundancy: $\boxed{R = 1 - \eta = 1 - \frac{I(X,Y)}{C}}$

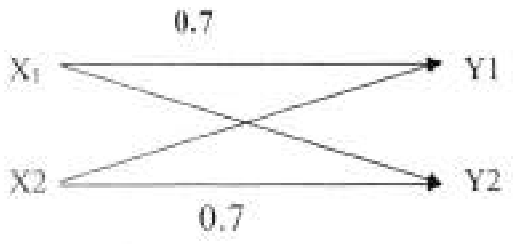
Notes:

1- I(X,Y) becomes maximum equals C only if the condition for maximization is satisfied, i.e. only if Y has equiprobable symbols. This condition yields that X has also equiprobable symbols since if the output of a symmetric channel is equiprobable, then its input X is also symmetric.

2- For symmetric channel only, and to ease calculations, we can use the formula I(X,Y)=H(Y)+K.

**Example 3.2**

For the BSC shown:



Find the channel capacity and efficiency if $I(x_1)$=2bits

**Solution:**

First we write p(Y/X), as:

$p(Y/X)=\begin{bmatrix} 0.7 & 0.3 \\ 0.3 & 0.7 \end{bmatrix}$ and since symmetric, then C=$\log_2$m+K, n=m=2 and

$K = 0.7\log_2 0.7 + 0.3\log_2 0.3$ = - 0.88129, then:

C = $\log_2 2$ + K = 1 - 0.88129 = 0.1187 bits/symbol.

To find the channel efficiency, then we must find I(X,Y). First, we find $p(x_1)$ from $I(x_1)$ = - $\log_2 p(x_1)$ = 2, giving $p(x_1) = 2^{-2}$ = 0.25, then :

p(X) = [0.25 0.75], multiplying with p(Y/X) get:

$$p(X,Y)=\begin{bmatrix}0.7*0.25 & 0.3*0.25\\ 0.3*0.75 & 0.7*0.75\end{bmatrix}=\begin{bmatrix}0.175 & 0.075\\ 0.225 & 0.525\end{bmatrix}$$, then summing

the columns to give p(Y) = [0.4   0.6],

from which H(Y) = 0.97095 bits/symbol. Then:

I(X,Y) = H(Y) + K = 0.97095 - 0.88129 = 0.0896 bits/symbol.

Then: η = I(X,Y)/C = 0.0896/0.1187 = 75.6%.

### H.W 3.1

Repeat previous example for the channel having transition prob.

$$p(Y/X)=\begin{bmatrix}0.7 & 0.2 & 0.1\\ 0.1 & 0.7 & 0.2\\ 0.2 & 0.1 & 0.7\end{bmatrix}$$

### 3.4 Entropies of continuous signals

If x and y are continuous random variables, with probability density functions p(x) and p(y), then in analogy with discrete sources the differential entropies of X & Y are given by:

$$H(X)=-\int_{-\infty}^{\infty} p(x)\log_2 p(x)\,dx$$ in bits/sample of the random variable x

$$H(Y)=-\int_{-\infty}^{\infty} p(y)\log_2 p(y)\,dy$$ in bits/sample of the random variable y

And other entropies are also differential entropies and are given by:

$$H(X,Y)=-\iint_{-\infty} p(x,y)\log_2 p(x,y)\,dx\,dy$$ in bits/sample

$$H(Y/X)=-\iint_{-\infty} p(x,y)\log_2 p(y/x)\,dx\,dy$$ in bits/sample.

24

$$H(X/Y) = -\iint_{-\infty} p(x,y)\log_2 p(x/y)\,dx\,dy \text{ in bits/sample.}$$

$$I(X,Y) = \iint_{-\infty} p(x,y)\log_2 \frac{p(x/y)}{p(x)}\,dx\,dy \text{ in bits/sample.}$$

Note that all above entropies are differential entropies and not an absolute measure of information since all probabilities are in fact probability density functions.

### 3.5 Channel capacity of continuous Gaussian channel

A Gaussian channel is that channel affected by the Gaussian noise.

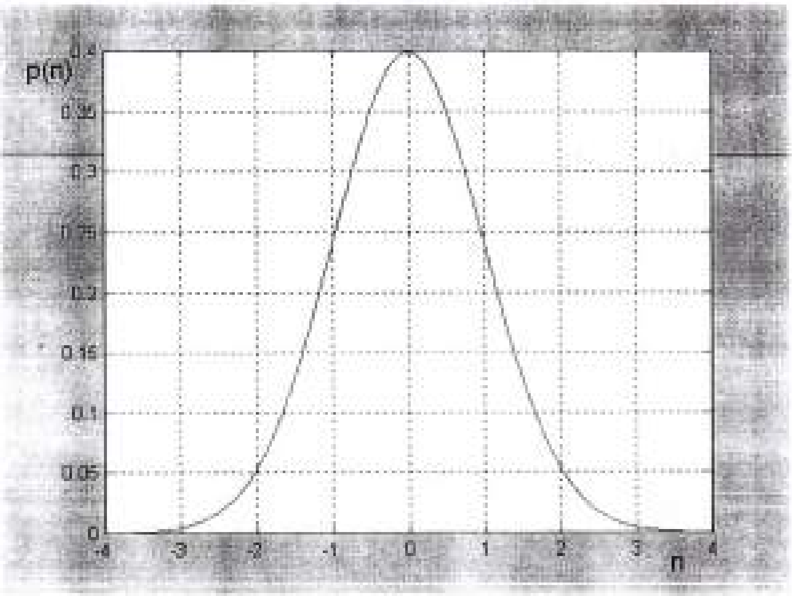
- **Review of Gaussian signal**

If the noise signal n(t) is Gaussian then its PDF(prob density function):

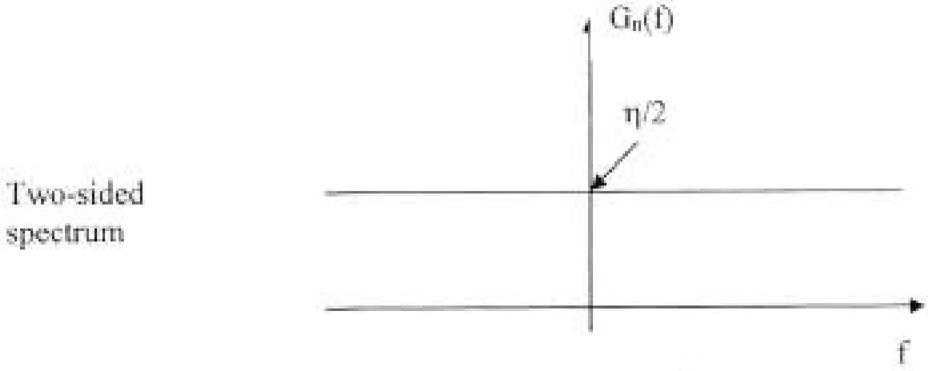
$$\boxed{p(n) = \frac{1}{\sqrt{2\pi}\,\sigma} e^{-0.5\left(\frac{n-\mu}{\sigma}\right)^2}}$$

where $\mu$ is the mean of n(t)

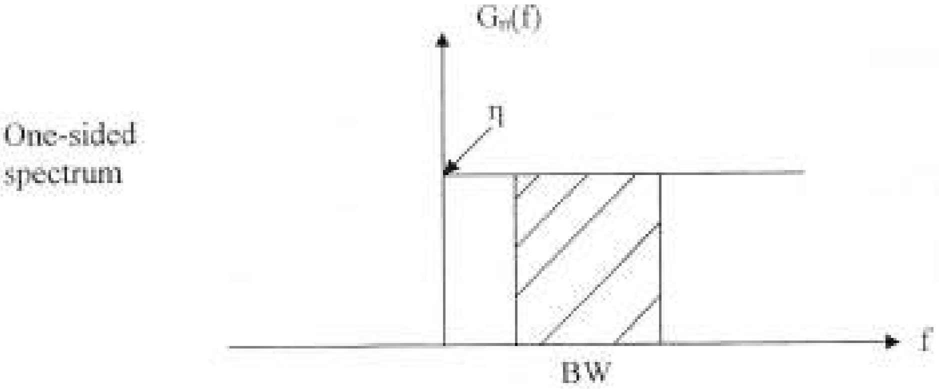
$\sigma^2$ is the variance of n(t).



If n(t) is a thermal noise then we can assume that $\mu=0$, and the frequency spectrum of this noise is flat over wide range of frequencies as shown.

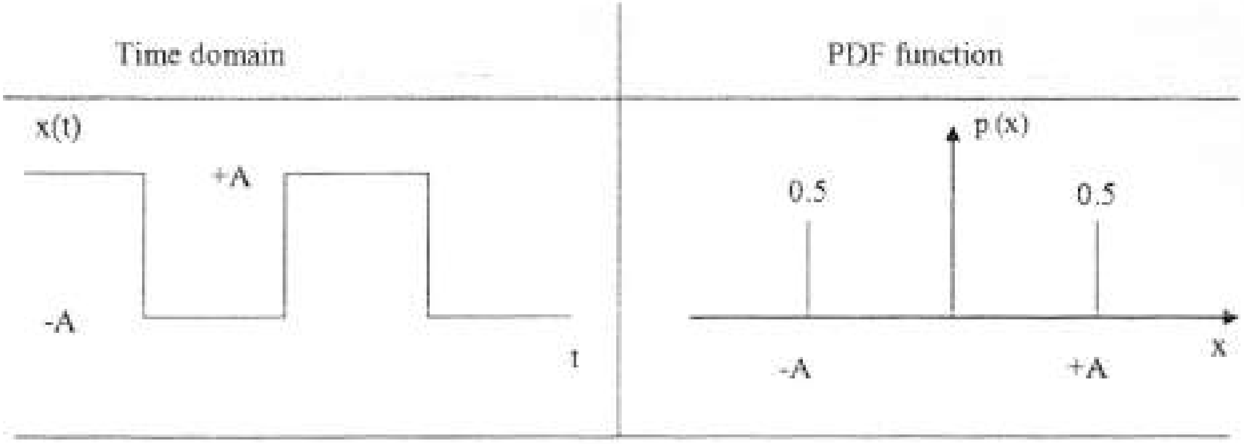


This has two sided power spectral density $G_n(f)=\eta/2$ W/Hz and one-sided power spectral density $G_n(f)=\eta$ W/Hz



From $G_n(f)$, we can find the noise power as $N= \eta\ BW$ in watts.

Since the spectrum is flat, we call this noise white noise. This white noise affects the signal x(t) as additive term, i.e., the received signal $y(t)=x(t)+n(t)$. A very popular name of <u>A</u>dditive, <u>W</u>hite, <u>G</u>aussian, <u>N</u>oise (AWGN) is used for such thermal noise. The figure below shows how this AWGN affects equiprobable bipolar ±A signal.



## 3.6 Entropy of Gaussian noise

Mathematically, we can prove that if x(t) is a random variable, then the entropy of x is maximum if x(t) has Gaussian PDF. To find this entropy, then (and assuming μ=0)

$$H(X) = -\int_{-\infty}^{\infty} p(x)\,\ln[\frac{1}{\sqrt{2\pi}\,\sigma} e^{-0.5\frac{x^2}{\sigma^2}}]dx \quad \text{nats/sample}$$

$$H(X) = \int_{-\infty}^{\infty} p(x)\ln\sqrt{2\pi}\,\sigma \quad dx + \frac{1}{2\sigma^2}\int_{-\infty}^{\infty} x^2 p(x)dx$$

But: $\int_{-\infty}^{\infty} x^2 p(x)dx = \textit{mean square of } x = \mu^2 + \sigma^2 = \sigma^2$

*and* $\int_{-\infty}^{\infty} p(x)\,dx = 1$ then $H(X) = \ln\sqrt{2\pi}\,\sigma + 0.5 = \ln\sqrt{2\pi}\,\sigma + \ln\sqrt{e}$

$H(X) = \ln(\sqrt{2\pi e}\,\sigma)$ nats/sample

or

$\boxed{H(X) = \log_2(\sqrt{2\pi e}\,\sigma)}$ bits/sample

## 3.7 Channel capacity of Gaussian channels

A Gaussian channel is a channel affected by Gaussian noise n(t).

Then: $C = [H(Y) - H(Y/X)]_{max}$ = [receiver entropy – noise entropy]$_{max}$

It should be noted that, maximization is already included when we take the case of Gaussian noise, then: $C = \log_2(\sqrt{2\pi e}\,\sigma_y) - \log_2(\sqrt{2\pi e}\,\sigma_n)$

Using previous expression of H(X) for Gaussian signal for the signal y with variance $\sigma_y^2$ then for the noise n(t) with variance $\sigma_n^2$ (noise power):

$$C = \log_2 \frac{\sigma_y}{\sigma_n} = \frac{1}{2}\log_2 \frac{{\sigma_y}^2}{{\sigma_n}^2}$$ But $\sigma_y^2=\sigma_x^2+\sigma_n^2$ sum of power,

But $\sigma_x^2$ = S=signal power and $\sigma_n^2$ = N=noise power, then:

$$C = \frac{1}{2}\log_2 \frac{S+N}{N} = \frac{1}{2}\log_2(1+\frac{S}{N})$$ bits/sample

For an analogue signal sampled at the Nyquist rate, then the sampling frequency is $f_s$= 2 B samples/sec, where B is the bandwidth of the signal,

hence: $C = \frac{1}{2}\log_2 \frac{S+N}{N} * 2B$ bits/sec, or:

$$\boxed{C = B\log_2(1+SNR)}$$ bit/sec

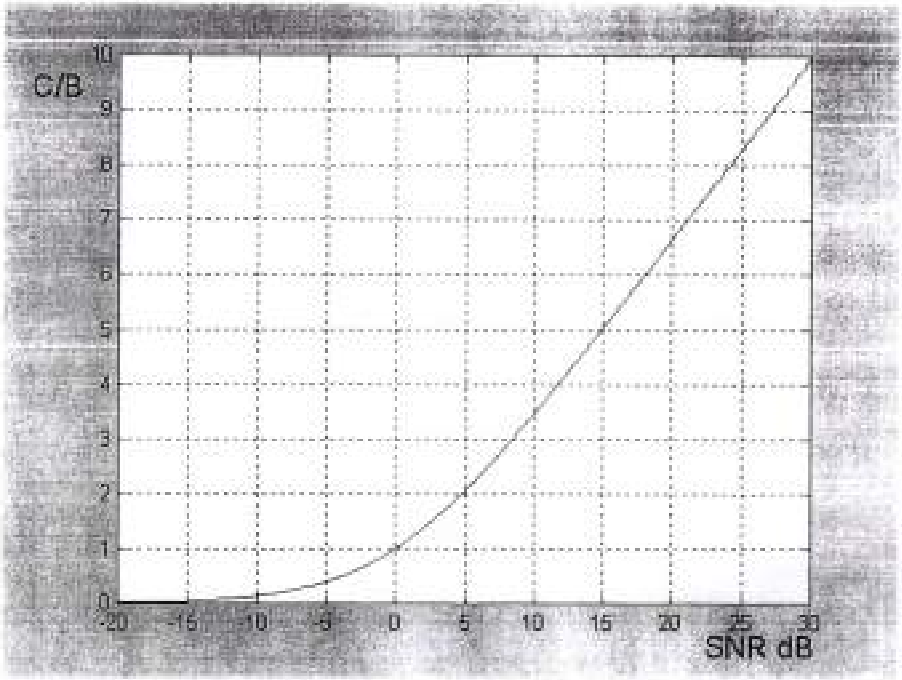
This is a very important formula known as SHANNON EQUATION named after C. E. Shannon, it is sometimes called Shannon-Hartly equation.

Notes on Shannon equation:

1- Care must be taken regarding the units, here B is in Hz., SNR=signal to noise power ratio is in absolute, then, C is in bits/sec. If SNR is given in dB, then: SNR(absolute)=$10^{0.1(\text{SNR in dB})}$.

2- The ratio [C/B]=$\log_2(1+SNR)$ gives what is called channel utilization ratio ( bps per Hz) that increases with SNR as shown.

3- The equation C = B $\log_2(1+SNR)$ gives the maximum theoretical performance in terms of maximum bit rate that can be transmitted over a channel having a bandwidth B and SNR ratio.



**Example 3.3**

Find the channel capacity of a Gaussian channel if its bandwidth increases without a limit.

**Solution:**

B increases without a limit means B→∞, then:

$$\lim_{B\to\infty} C = \lim_{B\to\infty} B\log_2(1+SNR)$$

Note that SNR itself is a function of B:

N=η B (η is the one-sided noise spectral density), then:

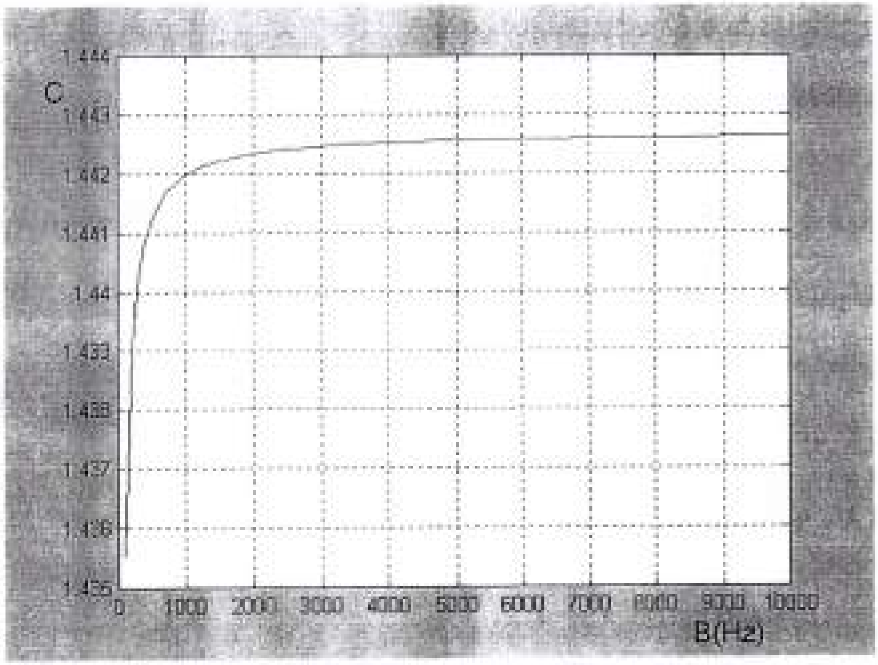
$$\lim_{B\to\infty} C = \lim_{B\to\infty} B\log_2(1+(S/\eta B)$$

To find this limit, let x=S/(ηB), then:

$$\lim_{B\to\infty} C = \lim_{x\to 0} [S/(\eta\, x)][\log_2(1+x)]$$

as B→∞ and (S/η) is a constant, then

$$\boxed{\lim_{B\to\infty} C = \lim_{x\to 0}\frac{S}{\eta}\frac{\log_2(1+x)}{x} = \frac{S}{\eta}\lim_{x\to 0}\frac{1/(1+x)}{\ln 2} = \frac{S}{\eta \ln 2} = 1.44\frac{S}{\eta}}$$



(S/η=1)

Note:

The result of previous example indicates that the channel capacity C approaches a limit of 1.44S/η even if B is very large. This result is very important for bandwidth unlimited channels, but power limited channels such as satellite channels, where the bandwidth may be large but signal power is a very important parameter.

**Example 3.4**

Find the maximum theoretical information rate that can be transmitted over a telephone channel having 3.5KHz bandwidth and 15dB SNR.

**Solution**

C is the maximum theoretical information rate, using Shannon eq, then:

$C = B \log_2(1+ SNR)$, where, SNR=15dB, changing into absolute

$SNR=10^{0.1*15}=31.$, then:

$C =3500 \log_2(1+31)=17500$ bps.

**Example 3.5**

A source produces 16 equiprobable symbols at a rate of 500 symbols/sec, check the possibility of transmitting this rate over the telephone channel of previous example.

**Solution**

First, we find the rate of information from the source, which is the source entropy rate R(X):

$R(X)= H(X)*$ rate of symbols.

$H(X)=H(X)|_{max}=\log_2 16=4$bits (equiprobable case)

Then: $R(X)=4 * 500= 2000$ bps. Now since $R(X) < 17500$, then yes it is possible to transmit source output over this channel.

**Example 3.6:**

Find the minimum theoretical time it would take to transmit 2500 octal digits over the telephone channel of the previous example.

**Solution:**

From previous example then C=17500 bps. A minimum theoretical transmission time is obtained if the channel operates at the maximum rate which is C, then:

$T_{min}$= [amount of information to be transmitted]/C

Amount of information = 2500 * $\log_2 8$ =7500 bits

(note each octal digit has $\log_2 8 = 3$ bits of information), then:

$T_{min}$= 7500/17500=0.428sec.

**Example 3.7**

Find the minimum theoretical SNR required to transmit a compressed video information at a rate of 27Mbps over a channel having 5MHz bandwidth.

**Solution**

For the minimum theoretical SNR, then put C=source bit rate =27Mbps, then:

$C= B \log_2(1+SNR)$

$27* 10^6 = 5* 10^6 \log_2(1+SNR)$, or

$1+SNR = 2^{5.4} \rightarrow$ SNR = 41.2 absolute or SNR=16.1 dB

# Chapter 3 Tutorial Problems

## Q1

A coloured monitor screen consists of $2*10^5$ pixels. Each pixel has 8 equiprobable Colours and 8 equiprobable levels of brightness. If 25 pictures are produced per second. Find the rate of information produced and the possibility of transmitting this rate over an AWGN channel having a BW of 5MHz and SNR of 55 dB.

## Solution

$p(\text{color}) = \frac{1}{8} \quad p(\text{level}) = \frac{1}{8}$

$p(X,Y) = p(Y)\, p(X/Y) = \frac{1}{8}\,\frac{1}{8} = \frac{1}{64}$

$\text{information / pixel} = -\log_2 \frac{1}{64} = \log_2 64 = 6 \text{ bits / pixel}$

$\text{information / picture} = 2*10^5 * 6 = 12*10^5 \text{ bits / picture}$

$R(x) = \frac{\text{bits}}{\text{picture}} * \frac{\text{Picture}}{\text{sec.}} = 12*10^5 * 25 = 30 \frac{\text{Mbits}}{\text{sec.}}$

$C = B\log_2(1+SNR) = 5*10^6 \log_2(1+10^{5.5})$

$C = 91.353$ Mbits/sec.

$\because C > R(x) \Rightarrow$ it is possible to transmit

## Q2

Asymmetric channel has

$$P(X,Y) = \begin{array}{c|ccc} & y_1 & y_2 & y_3 \\ X_1 & P_1 & P_2 & P_3 \\ X_2 & 0.05 & 0.35 & 0.1 \\ X_3 & 0.06 & 0.03 & 0.21 \end{array}$$

Find (a) $P_1$, $P_2$ and $P_3$

(b) channel Capacity

(c) channel efficiency

**Solution**

$$p(x) = \begin{array}{c} \\ \left[ \right. \end{array}\begin{array}{ccc} x_1 & x_2 & x_3 \\ P_1+P_2+P_3 & 0.5 & 0.3 \end{array}\begin{array}{c} \\ \left. \right] \end{array}$$

$$p(X_1) = 1 - p(X_2) - p(X_3)$$

$$P_1+P_2+P_3 = 1-0.5-0.3 = 0.2$$

$$p(Y/X) = p(X,Y)/p(X) = \begin{array}{c|ccc} & y_1 & y_2 & y_3 \\ X_1 & \frac{P_1}{0.2} & \frac{P_2}{0.2} & \frac{P_3}{0.2} \\ X_2 & \frac{0.05}{0.5} & \frac{0.35}{0.5} & \frac{0.1}{0.5} \\ X_3 & \frac{0.06}{0.3} & \frac{0.03}{0.3} & \frac{0.21}{0.3} \end{array}$$

$$\therefore p(Y/X) = \begin{array}{c|ccc} X_1 & \frac{P_1}{0.2} & \frac{P_2}{0.2} & \frac{P_3}{0.2} \\ X_2 & 0.1 & 0.7 & 0.2 \\ X_3 & 0.2 & 0.1 & 0.7 \end{array}$$

$\because$ Symmetrical channel

$$\therefore P_1/0.2 = 0.7 \Longrightarrow P_1 = 0.14$$

$$P_2/0.2 = 0.2 \Longrightarrow P_2 = 0.04$$

$$P_3/0.2 = 0.1 \Longrightarrow P_3 = 0.02$$

$$\therefore p(Y/X) = \begin{array}{c|ccc} X_1 & 0.7 & 0.2 & 0.1 \\ X_2 & 0.1 & 0.7 & 0.2 \\ X_3 & 0.2 & 0.1 & 0.7 \end{array}$$

$$C = \log_2 m + K$$

$$K = \sum_{j=1}^{3} p(y_j/x_i) \log_2 p(y_j/x_i)$$

$= 0.7 \log_2 0.7 + 0.2 \log_2 0.2 + 0.1 \log_2 0.1$

$= -1.16$

$C = \log_2 3 - 1.16 = 0.42$ bits/symbol

$p(y_1) = p_1 + 0.05 + 0.06 = 0.14 + 0.05 + 0.06 = 0.25$

$p(y_2) = p_2 + 0.35 + 0.03 = 0.04 + 0.35 + 0.03 = 0.42$

$p(y_3) = p_3 + 0.1 + 0.21 = 0.02 + 0.1 + 0.21 = 0.33$

$\therefore p(y) = [0.25 \quad 0.42 \quad 0.33]$

$H(y) = -[0.25 \log_2 0.25 + 0.42 \log_2 0.42 + 0.33 \log_2 0.33]$

$= 1.55$ bits / symbol

$I(X,Y) = H(Y) + K = 1.55 - 1.16$

$= 0.39$ bits/symbol

$$\eta = \frac{I(X,Y)}{C} = \frac{0.39}{0.42} = 92\%$$

Q3

A channel has the joint probability matrix

$$P(X,Y) = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{ccc} y_1 & y_2 & y_3 \end{array} \\ \begin{bmatrix} 0.03 & 0.05 & 0.12 \\ 0.1 & 0.24 & 0.06 \\ 0.24 & 0.06 & 0.1 \end{bmatrix} \end{array}$$

Find the channel efficiency and redundancy.

**Solution**

$p(x) = [0.2 \quad 0.4 \quad 0.4]$

$p(y) = [0.37 \quad 0.35 \quad 0.28]$

$$p(X,Y) = p(X) \cdot p(Y/X) \Rightarrow p(Y/X) = \frac{P(X,Y)}{P(X)}$$

$$p(y/x) = \begin{bmatrix} 0.15 & 0.25 & 0.6 \\ 0.25 & 0.6 & 0.15 \\ 0.6 & 0.15 & 0.25 \end{bmatrix}$$

it is a symmetric channel

$$C = \log_2 m + \sum_{j=1}^{3} p(y_j/x_i) \log_2 p(y_j/x_i)$$

$$= \log_2 3 + [0.15 \log_2 0.15 + 0.25 \log_2 0.25 + 0.6 \log_2 0.6]$$

$= 0.232$ bits/symbol

$$I(X,Y) = H(Y) + \sum_{j=1}^{3} p(y_j/x_i) \log_2 p(y_j/x_i)$$

$$H(Y) = -[0.37 \log_2 0.37 + 0.35 \log_2 0.35 + 0.28 \log_2 0.28]$$

$= 1.575$ bits/symbol

$I(X,Y) = 1.575 - 1.352 = 0.223$ bits/symbol

$$\eta = \frac{I(X,Y)}{C} = \frac{0.223}{0.232} = 0.9612 = 96\%$$

$R = 1 - \eta \cong 4\%$

## Q4

Find the minimum theoretical time required to transmit 600 decimal digits on a Continous channel having a BW of 8 KHz and SNR of 31.

**Solution**

decimal digits $(0 \to 9) \Rightarrow 10$ digits

$L = \log_2 n = \log_2 10$ bits / digits

amount of information = no. of digits $*$ L

$= 600 \cancel{\text{digits}} * \log_2 10 \ \frac{\text{bits}}{\cancel{\text{digits}}}$

$= 1993$ bits

$C = B \log_2 (1 + SNR) = 8 * 10^3 \log_2 (1 + 31)$

$= 40000$ bits/sec.

$t_{min} = \frac{1993 \text{ bits}}{40000 \text{ bits/sec}} = 50$ msec.

## Q5

check if it is possible to transmit 32 K bits/sec. information rate over an AWGN channel having a BW of 8 KHz and SNR of 14.9 dB.

**Solution**

$C = B \log_2 (1 + SNR)$

$= 8 * 10^3 \log_2 (1 + 10^{1.49}) = 40$ K bits/sec.

$\therefore c > R(x) \Longrightarrow R(x)$ is possible to transmit

**Q6**

A Ternary source has $P(X_0) = P(X_1) = \frac{1}{4}$ produces symbols at a rate of 500 symbol/sec. These are transmitted through a channel having:

$$P(y_j/X_i) = \begin{cases} 0.9 & \text{if } i=j \\ p & \text{if } i \neq j \end{cases} \quad , \; i=0,1,2 \quad j=0,1,2$$

Find the source entropy rate, rate of information transmission and the channel efficiency.

**Solution**

$$P(Y/X) = \begin{array}{c} \\ X_0 \\ X_1 \\ X_2 \end{array} \begin{array}{c} \begin{array}{ccc} y_0 & y_1 & y_2 \end{array} \\ \begin{bmatrix} 0.9 & p & p \\ p & 0.9 & p \\ p & p & 0.9 \end{bmatrix} \end{array} = \begin{bmatrix} 0.9 & 0.05 & 0.05 \\ 0.05 & 0.9 & 0.05 \\ 0.05 & 0.05 & 0.9 \end{bmatrix}$$

$$p(X_2) = 1 - p(X_0) - p(X_1) = 1 - \frac{1}{4} - \frac{1}{4} = \frac{1}{2}$$

$$\therefore p(X) = \begin{array}{c} \begin{array}{ccc} X_0 & X_1 & X_2 \end{array} \\ \left[ \begin{array}{ccc} \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{array} \right] \end{array}$$

$$H(X) = -\left[0.25 \log_2 0.25 + 0.25 \log_2 0.25 + 0.5 \log_2 0.5\right]$$

$$= 1.5 \text{ bits/symbol}$$

$$R(X) = H(X) * \text{no. of symbols/sec.}$$

$$= 1.5 \frac{\text{bits}}{\cancel{\text{symbol}}} * 500 \frac{\text{symbol}}{\text{sec}}$$

$$= 750 \text{ bits/sec.}$$

$$p(x,y) = p(x).p(y/x) = \begin{array}{c|ccc} & y_0 & y_1 & y_2 \\ \hline x_0 & 0.225 & 0.0125 & 0.0125 \\ x_1 & 0.0125 & 0.225 & 0.0125 \\ x_2 & 0.025 & 0.025 & 0.45 \end{array}$$

$$p(y) = \begin{array}{ccc} y_0 & y_1 & y_2 \\ [0.2625 & 0.2625 & 0.475] \end{array}$$

$$H(y) = -[2 * 0.2625 \log_2 0.2625 + 0.475 \log_2 0.475]$$
$$= 1.52 \text{ bits/symbol}$$

$$K = \sum_{j=1}^{3} p(y_j/x_i) \log_2 p(y_j/x_i)$$

$$= 0.9 \log_2 0.9 + 2 * 0.05 \log_2 0.05 = -0.57$$

$$I(X,Y) = H(Y) + K = 1.52 - 0.57$$
$$= 0.95 \text{ bits/symbol}$$

$$R(X,Y) = I(X,Y) * \text{no. of symbol/sec.}$$
$$= 0.95 \frac{\text{bits}}{\cancel{\text{symbol}}} * 500 \frac{\cancel{\text{symbol}}}{\text{sec}} = 475 \text{ bits/sec.}$$

①

# Chapter Four

# Source Coding of Discrete Sources

## 4.1 Source Coding

A discrete source is a source that produces finite set of messages $x_1, x_2, x_3, \dots\dots\dots, x_n$ with probabilities $p(x_1)$, $p(x_2)$, $p(x_3)$,....., $p(x_n)$. The source coder will transform these messages into a finite sequence of digits, called the codeword of the message. If binary digits (bits) are used in this codeword, then we obtain what is called "Binary Source Coding". Nonbinary (such as ternary, quaternary,...etc) source coding is also possible if the elements of this codeword are nonbinary digits.

The selection of codewords for different messages $x_i$, is done according to the following two considerations:

1- **The average code length $L_c$** must be as minimum as possible. This average length is given by:

$$\boxed{L_c = \overline{\ell}_i = \sum_{i=1}^{n} \ell_i \, p(x_i)} \text{ digits/message}$$

Where $\ell_i$ is the length of the codeword for message $x_i$ ($\ell_i$ is in bits for binary coding, or in digits for nonbinary coding).

2- The codewords at the receiver must be **uniquely decodable**.

To understand the above two considerations, the following example is given:

②

## Example 4.1

The code table for a certain binary code is given as:

| Message $x_i$ | $p(x_i)$ | Codeword $C_i$ | $\ell_i$(bits) |
|---|---|---|---|
| $x_1$ | 0.2 | 0 | 1 |
| $x_2$ | 0.1 | 10 | 2 |
| $x_3$ | 0.4 | 110 | 3 |
| $x_4$ | 0.3 | 111 | 3 |

[1]-Find the average code length, then comment.

[2]-If the received data stream is 1 0 1 1 0 0 0 1 1 1 1 1 0…….., check if this code is uniquely decodable or not, then comment.

**Solution:**

[1]-

$$L_c = \overline{\ell}_i = \sum_{i=1}^{n} \ell_i \ p(x_i) = 0.2+2*0.1+3*0.4+3*0.3=2.5\text{bits/message}$$

[2]- using the given code table, then:

1 0 | 1 1 0 | 0 | 0 | 1 1 1 | 1 1 0 |……..,

$x_2$ | $x_3$ | $x_1$| $x_1$| $x_4$ | $x_3$ |…….,

Hence the code is uniquely decodable, since the receiver get at only one possible message stream.

**Notes:**

[1]- For previous example, the code is not optimum in terms of $L_c$, i.e. it could be less by another redistribution of the codewords. In fact, we can reduce $L_c$ by giving less $\ell_i$ for $x_i$ with higher $p(x_i)$ such that $L_c$ is reduced. For example, the given code table is modified as:

③

| Message $x_i$ | $p(x_i)$ | Codeword $C_i$ | $\ell_i$(bits) |
|---|---|---|---|
| $x_3$ | 0.4 | 0 | 1 |
| $x_4$ | 0.3 | 10 | 2 |
| $x_1$ | 0.2 | 110 | 3 |
| $x_2$ | 0.1 | 111 | 3 |

This gives $L_c$=0.4+0.3*2+0.2*3+0.1*3=1.9 bits/message which is less than before.

[2]- Condition for uniquely decodable code: The condition for uniquely decodable code is that if $x_i$ is given a codeword $C_i$ of length $\ell_i$ bits, then these $\ell_i$ bits must not be the beginning (from the left) of any other codeword $C_j$ of higher length $\ell_j$ for message $x_j$. Applying this for previous example, then if "0" is a codeword, then no other codeword of higher length starts with "0". Also if "10" is a codeword, then no other codeword of higher length starts with "10" and so on.

**Example 4.2**

Check if the following code is uniquely decodable or not:

| | |
|---|---|
| $x_1$ | 0 |
| $x_2$ | 10 |
| $x_3$ | 101 |
| $x_4$ | 111 |

**Solution**

This code is not uniquely decodable since "10" is a codeword for $x_2$ , while the codeword for $x_3$ starts with "10".

④

## 4.2 Coding efficiency and redundancy:

A code with average code length $L_c$ digits has coding efficiency:

$$\boxed{\eta = \frac{H(x)}{L_c \log_2 r}}$$ where:

H(x) is source entropy in bits/message,

r=coding size (r=2 for binary coding, r=3 for ternary coding, and so on….).

$L_c$ has the units of the code size, (i.e. bits/message if r=2, ternary digits/message if r=3, and so on…..).

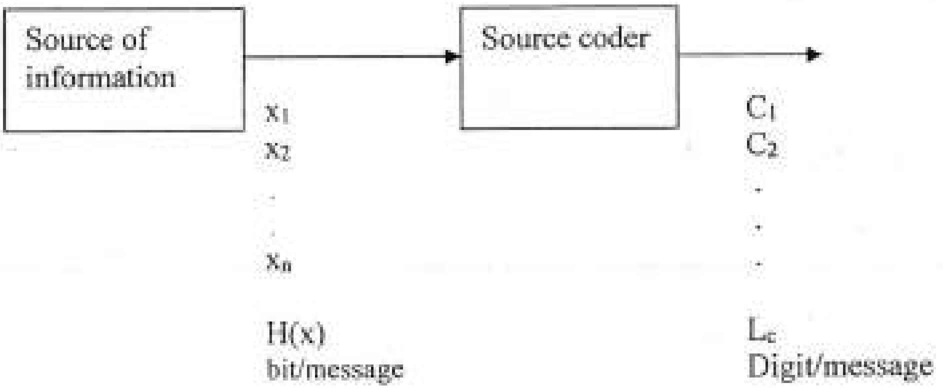
For **binary coding** only (D=2), then: $\boxed{\eta = \frac{H(X)}{L_c}}$

(Note: If the type of the code is not given, then assume it BINARY).

The code redundancy is simply R=1-η.

**Note:**

The interpretation of code efficiency comes from the following discussion:



The average amount of information from the source output is H(X) bits/message. The average amount of information at the source coder is $L_c$ digit/message or $L_c$*$\log_2$(r) bits/message. The factor $\log_2$(r) changes the

5

units from digits of D-sized into bits. Hence the ratio between H(X) and $L_c*\log_2(r)$ will represent the efficiency of the source coder.

Note:

When $p(xi)=2^{-li}$ , the efficiency is 100% $[2^{-li}$ in binary case]

where $l_i$ is +ve integer

## 4.3 Source Coding Methods:

### a) Shannon-Fano Code ( Fano Code):

The procedure for binary Fano code is given as follows:

Step 1: arrange the messages in a decreasing order of prob.

Step 2: find out a point in the decreasing order such that the sum of probabilities upward is *almost* equal to the sum of prob downward.

Step 3: assign all messages upward as "0" and all messages downward as "1".

Step 4: repeat steps 2 & 3 many times on the upward and downward parts until all the messages are separated.

**Example 4.3**

Develop Fano code for the following set of messages:

$$\begin{array}{rcccccc} & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ p(X) = [ & 0.25 & 0.2 & 0.18 & 0.15 & 0.12 & 0.1] \end{array}$$

then find coding efficiency and redundancy.

**Solution**

6

messages are already given in a decreasing order of prob. To carry out step 2, then we notice that point between $x_2$ and $x_3$ is the best choice since the sum of prob upward is 0.45 while the sum of prob downward is 0.55. we assign upward by "0" and downward by "1".

| | | |
|---|---|---|
| $x_1$ | 0.25 | 0 |
| $x_2$ | 0.2 | 0 |
| $x_3$ | 0.18 | 1 |
| $x_4$ | 0.15 | 1 |
| $x_5$ | 0.12 | 1 |
| $x_6$ | 0.1 | 1 |

Next we repeat the step above on the upward and downward portions, where the upward is simply separated into two parts assigning up( message $x_1$) by "0" and down (message $x_2$) by "1" where these two messages are completely separated.

| | | |
|---|---|---|
| $x_1$ | 0.25 | 00 |
| $x_2$ | 0.2 | 01 |
| $x_3$ | 0.18 | 1 |
| $x_4$ | 0.15 | 1 |
| $x_5$ | 0.12 | 1 |
| $x_6$ | 0.1 | 1 |

The remaining downward part consists of $x_3$, $x_4$, $x_5$, $x_6$, where the best split is between $x_4$ and $x_5$ (partial sum up is 0.33 and partial sum down is 0.22), ⑦

then assign up (messages $x_3$ and $x_4$) by "0" and down (messages $x_5$ and $x_6$) by "1":

| | | |
|---|---|---|
| $x_1$ | 0.25 | 00 |
| $x_2$ | 0.2 | 01 |
| $x_3$ | 0.18 | 10 |
| $x_4$ | 0.15 | 10 |
| $x_5$ | 0.12 | 11 |
| $x_6$ | 0.1 | 11 |

Finally $x_3$ and $x_4$ are directly separated by "0" and "1". And $x_5$ and $x_6$ are also directly separated by "0" and "1".

| $x_i$ | $p(x_i)$ | $C_i$ | $l_i$ |
|---|---|---|---|
| $x_1$ | 0.25 | 00 | 2 |
| $x_2$ | 0.2 | 01 | 2 |
| $x_3$ | 0.18 | 100 | 3 |
| $x_4$ | 0.15 | 101 | 3 |
| $x_5$ | 0.12 | 110 | 3 |
| $x_6$ | 0.1 | 111 | 3 |

(numbers appear on arrows represent the order of plotting that splitting arrow in the procedure).

Then: $H(X)=2.519$ bits/message and:

$$L_c= 2*(0.25+0.2)+3*(0.18+0.15+0.12+0.1)=2.55 \text{ bits/message}$$

And $\eta=H(X)/L_c = 2.519/2.55=98.7\%$

8

**Example 4.4**

Develop Fano code for the following set of messages:

$$\begin{array}{lcccccccc} & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ p(x) = [ & 0.4 & 0.2 & 0.12 & 0.08 & 0.08 & 0.04 & 0.04 & 0.04] \end{array}$$

then find coding efficiency.

**Solution:**

using previous steps, then the following code table is obtained:

| $x_i$ | $p(x_i)$ | $C_i$ | $L_i$ |
|---|---|---|---|
| $x_1$ | 0.4 | 0 | 1 |
| $x_2$ | 0.2 | 100 | 3 |
| $x_3$ | 0.12 | 101 | 3 |
| $x_4$ | 0.08 | 1100 | 4 |
| $x_5$ | 0.08 | 1101 | 4 |
| $x_6$ | 0.04 | 1110 | 4 |
| $x_7$ | 0.04 | 11110 | 5 |
| $x_8$ | 0.04 | 11111 | 5 |

Note that less $\eta$ is obtained (higher $L_c$) if starting arrow is made between $x_2$ and $x_3$ which gives the same balance of sum of prob compared with that used in above solution. 0.4 ------- 0.6.

(numbers appear on arrows represent the order of plotting that splitting arrow in the procedure).

$H(X) = 2.5$ bits/message, $L_c = 2.56$ bits/message, then:

$\eta = H(X)/L_c = 2.5/2.56 = 97.6\%$

## Example 4.6

Modify Fano procedure for ternary coding.

**Solution:**

First, we find out two points(arrows) in each step that split the sum of prob into almost three equal parts assigning them as "0", "1", and "2". Applying this onto previous example, then:

| $x_i$ | $p(x_i)$ | $C_i$ |
|---|---|---|
| $x_1$ | 0.4 | 0 |
| $x_2$ | 0.2 | 1 |
| $x_3$ | 0.12 | 1 |
| $x_4$ | 0.08 | 2 |
| $x_5$ | 0.08 | 2 |
| $x_6$ | 0.04 | 2 |
| $x_7$ | 0.04 | 2 |
| $x_8$ | 0.04 | 2 |

Then $x_1$ is directly separated. Messages $x_2$ and $x_3$ are directly separated by one arrow.

| $x_i$ | $p(x_i)$ | $C_i$ |
|---|---|---|
| $x_1$ | 0.4 | 0 |
| $x_2$ | 0.2 | 10 |
| $x_3$ | 0.12 | 11 |
| $x_4$ | 0.08 | 2 |
| $x_5$ | 0.08 | 2 |
| $x_6$ | 0.04 | 2 |
| $x_7$ | 0.04 | 2 |
| $x_8$ | 0.04 | 2 |

10

The remaining messages are separated by two arrows, one between $x_4$ and $x_5$ and the other between $x_5$ and $x_6$

| $x_i$ | $p(x_i)$ | $C_i$ |
|---|---|---|
| $x_1$ | 0.4 | 0 |
| $x_2$ | 0.2 | 10 |
| $x_3$ | 0.12 | 11 |
| $x_4$ | 0.08 | 20 |
| $x_5$ | 0.08 | 21 |
| $x_6$ | 0.04 | 22 |
| $x_7$ | 0.04 | 22 |
| $x_8$ | 0.04 | 22 |

Finally the last three messages are separated by two arrows:

| $x_i$ | $p(x_i)$ | $C_i$ |
|---|---|---|
| $x_1$ | 0.4 | 0 |
| $x_2$ | 0.2 | 10 |
| $x_3$ | 0.12 | 11 |
| $x_4$ | 0.08 | 20 |
| $x_5$ | 0.08 | 21 |
| $x_6$ | 0.04 | 220 |
| $x_7$ | 0.04 | 221 |
| $x_8$ | 0.04 | 222 |

11

(Numbers appear on arrows represent the order of plotting that splitting arrow in the procedure).

## b) Huffman code:

Procudure(Binary coding):

Step1: Arrange messages in a decreasing order of prob.

Step2: The two lowest prob messages are joined (sum their prob), assign "0" for one of them and "1" for the other.

Step3: rewrite messages once again in a decreasing order replacing the sum of prob of step2 as a prob of one message, hence reducing number of messages by one.

Step4: repeat steps 2 and 3 many times until you end up with total prob of unity 1.00.

Step5: the codeword for each message is read from marked "0" and "1" following the arrows from left to right and writing codeword bits from right to left (this is done to satisfy the condition for uniquely decodable code).

### Example 4.7:

Develop binary Huffman code for the following set of messages:

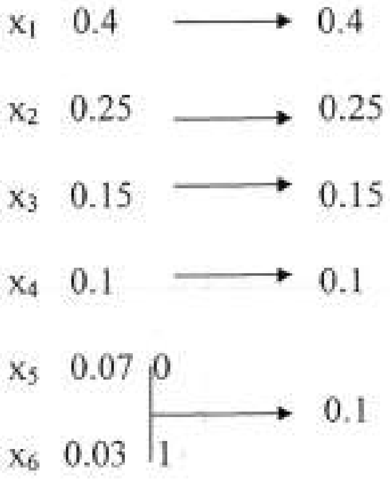
$$\begin{array}{lcccccc} & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ p(x) = [ & 0.4 & 0.25 & 0.15 & 0.1 & 0.07 & 0.03] \end{array}$$

then find coding efficiency.

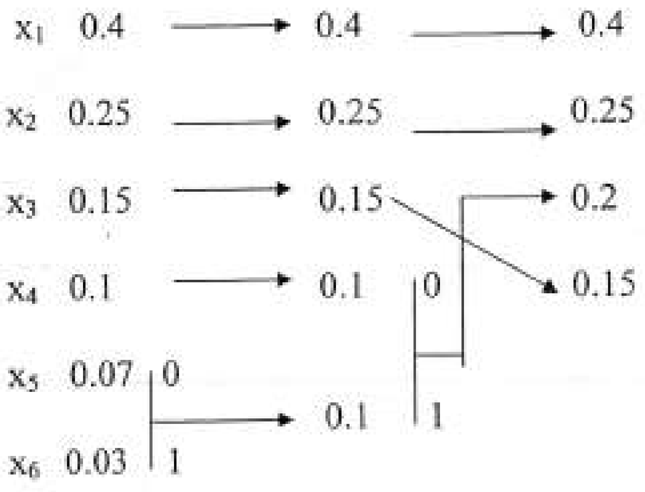
⑫

**Solution**

The sum of the last two lowest prob is 0.1, rewrite messages and replace these two messages by their sum of prob.

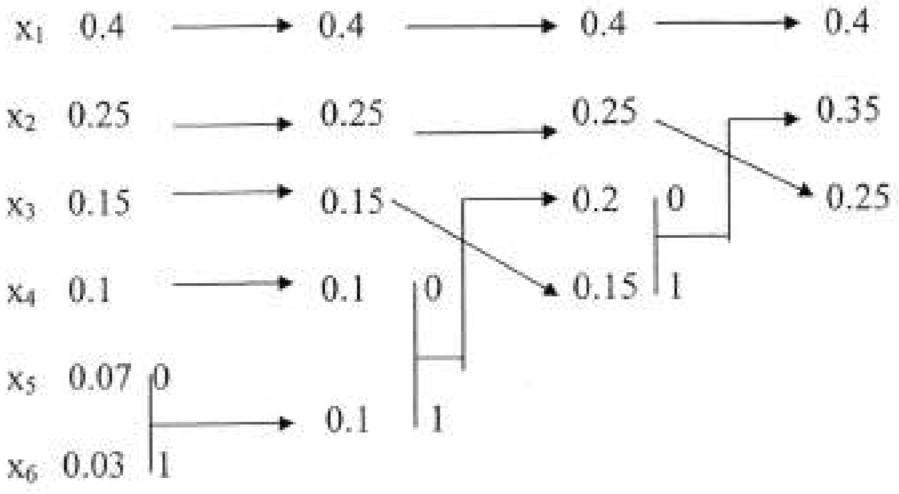


In the new sequence, the sum of the two lowest prob is 0.2, so we rewrite replacing them by their sum whose position in the new sequence is between 0.25 and 0.15, then:

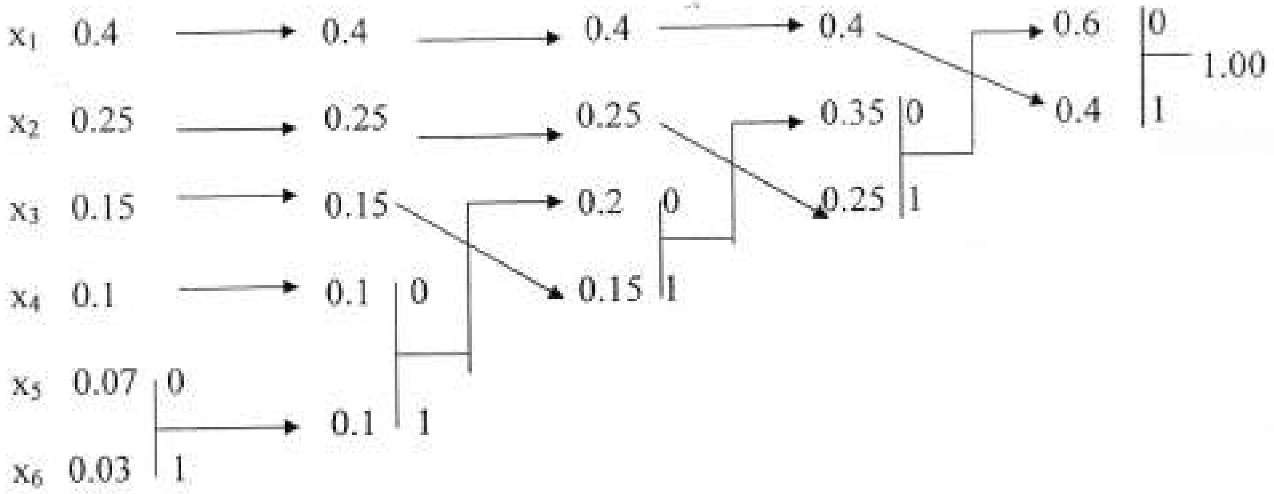


In the new sequence, the sum of the two lowest prob is 0.35, so we rewrite replacing them by their sum whose position in the new sequence is between 0.4 and 0.25, then:

⑬



Finally, in new sequence, the sum of the two lowest prob is 0.6, so we rewrite replacing them by their sum whose position in the new sequence is at the 1st position, then:



To read codewords, then the codeword for $x_1$ is simply "1" following the arrow from the left to the right. The codeword for $x_2$ is "01", following the arrows from the left to the right and writing codeword bits from the right to the left. The codeword for $x_3$ is "001" following the arrows from the left to the right and writing codeword bits from the right to the left, and so on we can arrange the code table as shown below:

| $x_i$ | $p(x_i)$ | $C_i$ | $l_i$ |
|---|---|---|---|
| $x_1$ | 0.4 | 1 | 1 |
| $x_2$ | 0.25 | 01 | 2 |
| $x_3$ | 0.15 | 001 | 3 |
| $x_4$ | 0.1 | 0000 | 4 |
| $x_5$ | 0.07 | 00010 | 5 |
| $x_6$ | 0.03 | 00011 | 5 |

This code has $L_c$=2.25 bits/message.

H(X)=2.1918 bits/message.

And $\eta=H(X)/L_c$ = 2.198/2.25=97.4%

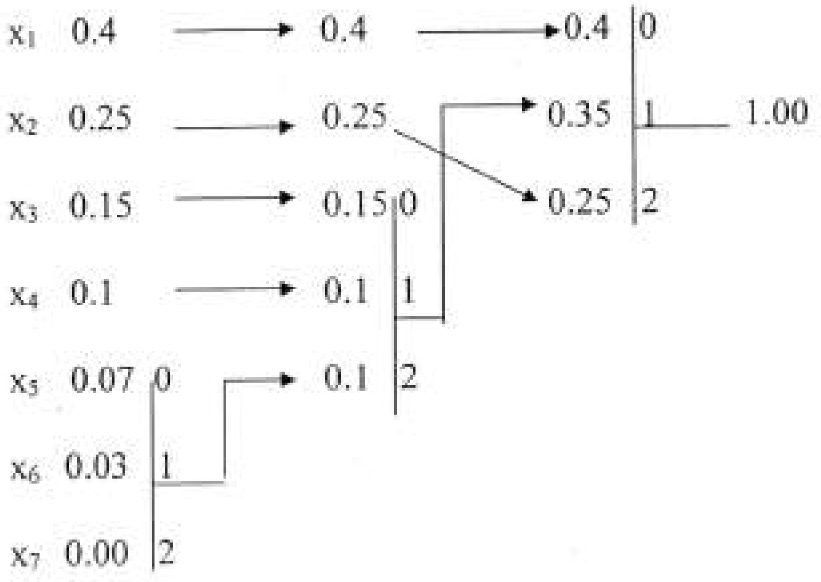
### Example 4.8

Modify Huffman binary coding into ternary coding, then repeat previous example using ternary Huffman coding.

**Solution:**

For ternary Huffman coding, then we join or sum the last three lowest prob messages. This will reduce no of messages in each step by two, so to ensure ending up the procedure with 3 messages corresponding to "0","1"', and "2", then we must notice the number of messages from the beginning. If the number of messages is even, then add a dummy message with prob of zero so that we end up with 3 messages. If the number of messages is already odd, then leave it as it is.

To apply above on the previous example, we notice that there are 6 messages (even), then we add another message $x_7$ with prob of 0.00, and carry out the same previous procedure joining up 3 lowest prob messages at a time.



this gives a code table as shown below:

| $x_i$ | $p(x_i)$ | $C_i$ | $l_i$ (ternary digit) |
|---|---|---|---|
| $x_1$ | 0.4 | 0 | 1 |
| $x_2$ | 0.25 | 2 | 1 |
| $x_3$ | 0.15 | 10 | 2 |
| $x_4$ | 0.1 | 11 | 2 |
| $x_5$ | 0.07 | 120 | 3 |
| $x_6$ | 0.03 | 121 | 3 |

Hence $L_c$=0.4+0.25+2*(0.15+0.1)+3*(0.07+0.03)=1.45 ternary digit/message.

And $\eta$=H(X)/ ($\log_2(3)$*$L_c$) = 2.198/(1.58*1.45)=95.6%

Note that it is less than the efficiency for binary coding. This makes us think of what is the necessary and sufficient condition to make the coding efficiency 100%. This will be given in the next example.

⑯

**Example 4.9**

show that in any coding procedure the coding efficiency is 100% if:

$p(x_i) = (\frac{1}{r})^k$ ( k is an integer for all i=1,2,3,….n).

**Solution:**

Note that if $p(x_i) = (\frac{1}{r})^k$ then:

$l_i = -\log_r(p(x_i)) = \log_r(r^k) = k$ which is an integer for all i.

Take for example, the source:

p(x)=[1/2 1/4 1/8 1/16 1/16], which satisfies the condition for 100% binary coding efficiency. Using say Fano code, then:

| | | | |
|---|---|---|---|
| $x_1$ | 0.5 | 0 | 1 |
| $x_2$ | 0.25 | 10 | 2 |
| $x_3$ | 0.125 | 110 | 3 |
| $x_4$ | 0.0625 | 1110 | 4 |
| $x_5$ | 0.0625 | 1111 | 4 |

$L_c$=0.5+2*0.25+3*0.125+4*(0.0625+0.0625)=1.875 bits/message =H(X)

Hence $\eta = H(X)/L_c = 100\%$

**H.W 1**

Repeat previous example for the source using ternary coding:

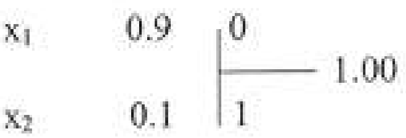
p(X)=[1/3 1/3 1/9 1/9 1/27 1/27 1/27]

17

## 4.4 Source Extension:

Sometimes, the source produces symbols with very extreme probabilities like p(X)=[0.9  0.1] or p(X)=[ 0.9  0.08  0.02]. ..etc. In such a case and using any of the previous variable length coding methods, the efficiency obtained is so small. Take for example, the source:

p(x)=[0.9  0.1]: , then using say Huffman procedure, then:

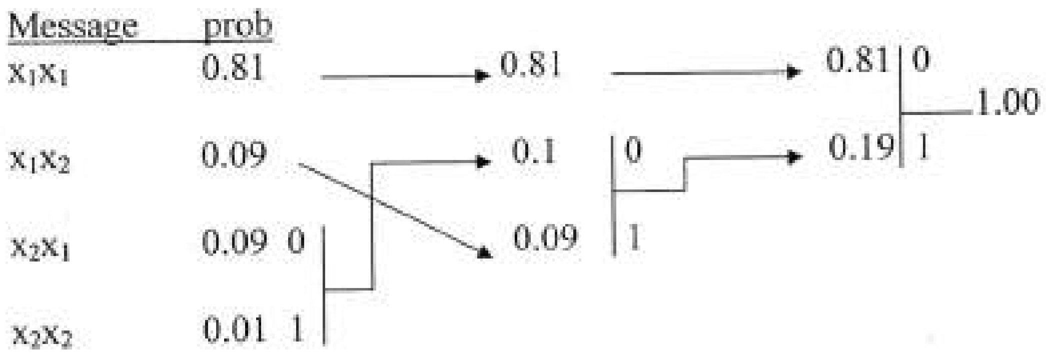


$x_1$ is "0"
$x_2$ is "1"

This gives $L_c$=1 bit/symbol, while:

H(X)=0.469 bits/symbol. $\eta$=H(X)/ $L_c$=0.469/1=46.9%

Now if we group two symbols and regard them as one message (this grouping is called source extension), then and assuming statistically independent symbols, then, the prob of a group of two symbols will be the joint prob:



this gives the code table:

| | | | |
|---|---|---|---|
| $x_1x_1$ | 0.81 | 0 | 1 |
| $x_1x_2$ | 0.09 | 11 | 2 |
| $x_2x_1$ | 0.09 | 100 | 3 |
| $x_2x_2$ | 0.01 | 101 | 3 |

18

$L_c$=0.81+0.18+3*0.1=1.29 bits/message

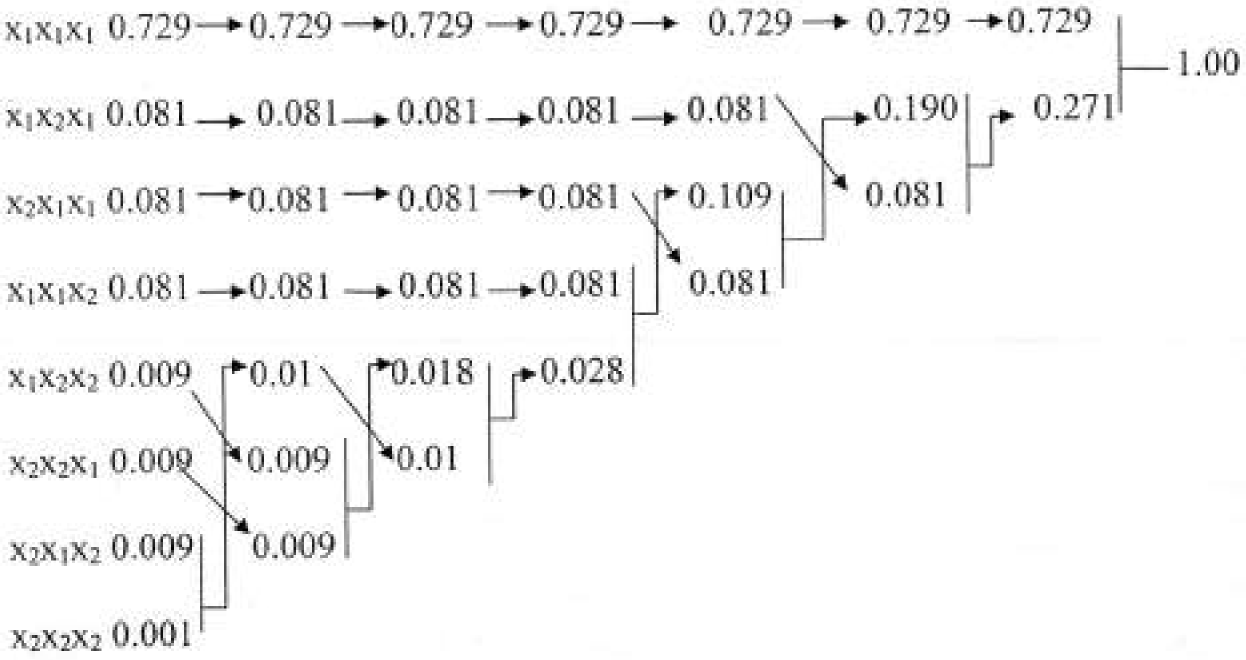
=1.29 bits/2symbols=0.645 bits/symbol

η=H(X)/ $L_c$=0.469/0.645=72.7% which is better than one symbol/message.

Shannon showed that increasing the number of symbols/message will increase the efficiency approaching the 100% as a limit. To check this, let us group 3 symbols/message, then:

| Message | prob | | Message | prob |
|---|---|---|---|---|
| $x_1x_1x_1$ | 0.729 | | $x_1x_1x_1$ | 0.729 |
| $x_1x_1x_2$ | 0.081 | arranging in decreasing order | $x_1x_2x_1$ | 0.081 |
| $x_1x_2x_1$ | 0.081 | | $x_2x_1x_1$ | 0.081 |
| $x_1x_2x_2$ | 0.009 | | $x_1x_1x_2$ | 0.081 |
| $x_2x_1x_1$ | 0.081 | | $x_1x_2x_2$ | 0.009 |
| $x_2x_1x_2$ | 0.009 | | $x_2x_2x_1$ | 0.009 |
| $x_2x_2x_1$ | 0.009 | | $x_2x_1x_2$ | 0.009 |
| $x_2x_2x_2$ | 0.001 | | $x_2x_2x_2$ | 0.001 |

using Huffman coding then:



⑲

this gives the code table:

| | | | |
|---|---|---|---|
| $x_1x_1x_1$ | 0.729 | 0 | 1 |
| $x_1x_2x_1$ | 0.081 | 11 | 2 |
| $x_2x_1x_1$ | 0.081 | 101 | 3 |
| $x_1x_1x_2$ | 0.081 | 1000 | 4 |
| $x_1x_2x_2$ | 0.009 | 100100 | 6 |
| $x_2x_2x_1$ | 0.009 | 100101 | 6 |
| $x_2x_1x_2$ | 0.009 | 100110 | 6 |
| $x_2x_2x_2$ | 0.001 | 100111 | 6 |

This gives

$L_c$=0.729+0.081(2+3+4)+6*(3*0.009+0.001)=1.626 bits/messgae

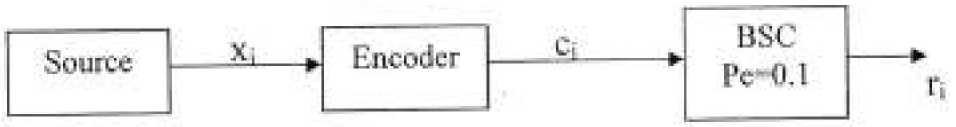
=1.626 bits/3 symbols=0.542 bits/symbol

$\eta$=H(X)/ $L_c$=0.469/0.542=86.5%, which is better than before.

**Example 4.10**

Given the following information system. Find the entropy at the output of each stage in system given in Fig. below

| $x_i$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ |
|---|---|---|---|---|---|
| $p(x_i)$ | 0.15 | 0.2 | 0.1 | 0.3 | 0.25 |



**Solution**

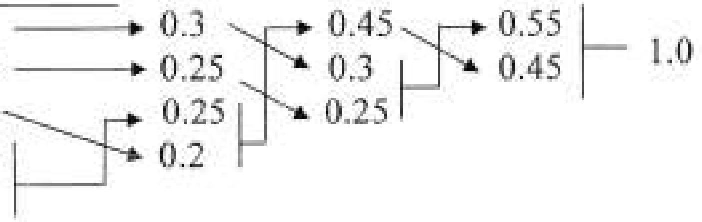
$$H(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \qquad \text{bits / symbol}$$

$$= -\ 0.3\log_2 0.3+2*0.25\log_2 0.25+0.2\log_2 0.2+0.15\log_2 0.15+0.1\log_2 0.1]$$

$$= 2.22 \text{ bits/symbol}$$

29

| $\ell_{i0}$ | $\ell_{i1}$ | $\ell_i$ | code | $x_i$ | $p_i$ |
|---|---|---|---|---|---|
| 0 | 2 | 2 | 11 | $x_4$ | 0.3 |
| 1 | 1 | 2 | 10 | $x_5$ | 0.25 |
| 2 | 0 | 2 | 00 | $x_2$ | 0.2 |
| 1 | 2 | 3 | 011 | $x_1$ | 0.15 |
| 2 | 1 | 3 | 010 | $x_3$ | 0.1 |



$$L_c = \overline{\ell}_i = \sum_{i=1}^{5} \ell_i \, p(x_i) = 2*(0.3+0.25+0.2)+3*(0.15+0.1)$$
$$= 2.25 \text{ bit/symbol}$$

$$\left.\begin{aligned} p(0) &= \frac{\sum_{i=1}^{5} 0_i p(x_i)}{L_c} = \frac{0.25+0.4+0.15+0.2}{2.25} = 4/9 \\ p(1) &= \frac{\sum_{i=1}^{5} 1_i p(x_i)}{L_c} = \frac{0.6+0.25+0.3+0.1}{2.25} = 5/9 \end{aligned}\right\} \quad p(c)$$

$$H(c) = -\sum_{i=1}^{n} p(c_i)\log_2 p(c_i) \qquad \text{bits/symbol}$$
$$= -[(4/9)\log_2(4/9)+(5/9)\log_2(5/9)]=1.035 \text{ bits/symbol}$$

$$p(r/c) = \begin{bmatrix} 0.9 & 0.1 \\ 0.1 & 0.9 \end{bmatrix}$$

$p(r,c) = p(r/c).\ p(c)$

$$p(r,c) = \begin{bmatrix} 0.9*(4/9) & 0.1*(4/9) \\ 0.1*(5/9) & 0.9*(5/9) \end{bmatrix}$$

$p(r) = [0.4555 \quad 0.5444]$

$$H(r) = -\sum_{i=1}^{n} p(r_i)\log_2 p(r_i) \qquad \text{bits/symbol}$$
$$= -[0.4555\log_2 0.4555+0.5444\log_2 0.5444]=0.994 \text{ bits/symbol}$$

# Chapter 4 Tutorial Problems

**Q1**: A source produces the following messages:

$P(X) = [0.18 \quad 0.17 \quad 0.14 \quad 0.12 \quad 0.2 \quad 0.11 \quad 0.08]$

at a rate of 1500 message/sec. If these are coded using Shannon-Fano code then transmitted through a 1.5 KHz AWGN channel. Find coding efficiency and the minimum theoretical SNR required at the channel

(Ans: $\eta_{coding} = 98.2\%$ ; $SNR_{min} = 7.75\,dB$)

## Solution

(a)

| $X_i$ | $P(X_i)$ | Codeword | $l_i$ |
|---|---|---|---|
| $X_5$ | 0.2 | 0 0 | 2 |
| $X_1$ | 0.18 | 0 1 0 | 3 |
| $X_2$ | 0.17 | 0 1 1 | 3 |
| $X_3$ | 0.14 | 1 0 0 | 3 |
| $X_4$ | 0.12 | 1 0 1 | 3 |
| $X_6$ | 0.11 | 1 1 0 | 3 |
| $X_7$ | 0.08 | 1 1 1 | 3 |

$$L = \sum_{i=1}^{7} l_i p(X_i) = 2(0.2) + 3(0.18 + 0.17 + 0.14 + 0.12 + 0.11 + 0.08)$$
$$= 2.8 \text{ bits/symbol}$$

$$H(X) = -\sum_{i=1}^{7} p(x_i)\log_2 p(X_i) = 2.75 \text{ bits/symbol}$$

$$\eta_c = \frac{H(X)}{L} = \frac{2.75}{2.8} = 98.2\,\%$$

(b) $R(x) = 2.75 \frac{\text{bits}}{\text{symbol}} \times 1500 \frac{\text{symbol}}{\text{sec.}} = 4125 \frac{\text{bits}}{\text{Sec.}}$

$R = B \log_2(1+SNR)$ $(SNR_{min}$ when $C = R)$

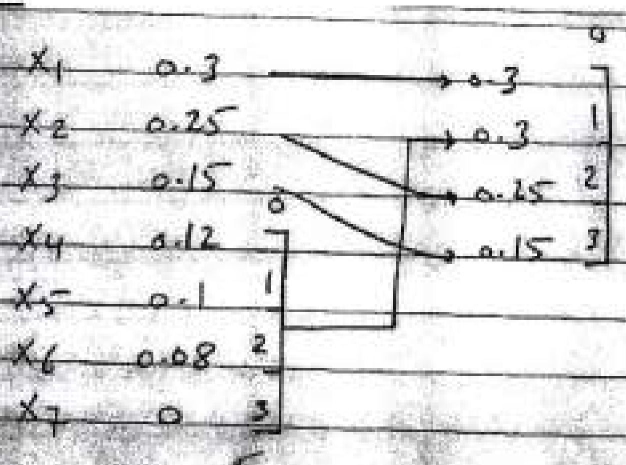
$4125 = 1500 \log_2(1+SNR_{min})$

$1+SNR_{min} = 2^{\frac{4125}{1500}} \Rightarrow SNR_{min} = 5.7272$

$SNR_{min} = 7.57$ dB

Q2: A source emits six messages with prob. 0.3, 0.25, 0.15, 0.12, 0.1 and 0.08. Find the quaternary Huffman code used to encode these messages. Find its efficiency and redundancy. (Ans: $\eta = 93\%$ ; $R = 7\%$)

**Solution**



تم اضافة رمز لإكمال احتمالات الشجرة الرباعية quaternary

| $X_i$ | $P(X_i)$ | Code word | $l_i$ |
|---|---|---|---|
| $X_1$ | 0.3 | 0 | 1 |
| $X_2$ | 0.25 | 2 | 1 |
| $X_3$ | 0.15 | 3 | 1 |
| $X_4$ | 0.12 | 10 | 2 |
| $X_5$ | 0.1 | 11 | 2 |
| $X_6$ | 0.08 | 12 | 2 |

$L = \sum_{i=1}^{6} l_i P(X_i) = 1.3$ quaternary / symbol

$$H(x) = -\sum_{i=1}^{6} p(x_i)\log_4 p(x_i) = 1.2112 \text{ quaternary/symbol}$$

$$\eta = \frac{H(x)}{L} = \frac{1.2112}{1.3} = 93.17\%$$

$$R = 1 - \eta = 6.83\%$$

Q3: A source emits symbols $m_1$ & $m_2$ with prob. 0.8 & 0.2 respectively. Find a Shannon-Fano code used to encode messages containing 1 symbol, 2 symbols and 3 symbols / message. Find the code efficiency in each case.

(Ans: 1 symbol: $\eta = 72.2\%$ ; 2 symbol: $\eta = 92.56\%$
3 symbol : $\eta = 99.17\%$

**Solution**

(a) for one symbol/message

| $m_i$ | $p(m_i)$ | Codeword | $l_i$ |
|---|---|---|---|
| $m_1$ | 0.8 | 0 | 1 |
| $m_2$ | 0.2 | 1 | 1 |

$$L = \sum_{i=1}^{2} l_i p(x_i) = 1 \text{ bits/symbol}$$

$$H(x) = -\sum_{i=1}^{2} p(x_i)\log_2 p(x_i) = 0.722 \text{ bits/symbol}$$

$$\eta = \frac{H(x)}{L} = \frac{0.722}{1} = 72.2\%$$

(b) for 2 symbols/message

| $m_i m_j$ | $p(m_i m_j)$ | Codeword | $l_i$ |
|---|---|---|---|
| $m_1 m_1$ | 0.64 | 0 | 1 |
| $m_1 m_2$ | 0.16 | 1 0 | 2 |
| $m_2 m_1$ | 0.16 | 1 1 0 | 3 |
| $m_2 m_2$ | 0.04 | 1 1 1 | 3 |

$$L = 0.64 + 2(0.16) + 3(0.16) + 3(0.04) = 1.56 \ \frac{\text{bits}}{2\text{symbols}}$$

$$H(X) = -\left[0.64 \log_2 0.64 + 2 * 0.16 \log_2 0.16 + 0.04 \log_2 0.04\right]$$

$$= 1.4439 \ \frac{\text{bits}}{2\text{symbols}}$$

$$\eta = \frac{H(x)}{L} = \frac{1.4439}{1.56} = 92.56\,\%$$

(c) for 3 symbols/message

يجب ترتيب الاحتمالات تنازلياً

| $m_i m_j m_k$ | $p(m_i m_j m_k)$ | Codeword | $l_i$ |
|---|---|---|---|
| $m_1 m_1 m_1$ | 0.512 | 0 | 1 |
| $m_1 m_1 m_2$ | 0.128 | 100 | 3 |
| $m_1 m_2 m_1$ | 0.128 | 101 | 3 |
| → $m_2 m_1 m_1$ | 0.128 | 110 | 3 |
| → $m_1 m_2 m_2$ | 0.032 | 11100 | 5 |
| $m_2 m_1 m_2$ | 0.032 | 11101 | 5 |
| $m_2 m_2 m_1$ | 0.032 | 11110 | 5 |
| $m_2 m_2 m_2$ | 0.008 | 11111 | 5 |

$$L = \sum l_i p(m_i m_j m_k) = 2.184 \ \text{bits}/3\text{symbols}$$

$$H(X) = 2.166 \ \text{bits}/3 \text{ symbols}$$

$$\eta = \frac{H(x)}{L} = \frac{2.166}{2.184} = 99.17\,\%$$

**Q4**: Find the efficiency of a shannon ternary code used to encode the message

$$P(X) = \left[ \frac{1}{3} \ \frac{1}{3} \ \frac{1}{9} \ \frac{1}{9} \ \frac{1}{27} \ \frac{1}{27} \ \frac{1}{27} \right]$$

(Ans: 100%)

**Solution**

| $x_i$ | $P(x_i)$ | Codeword | $l_i$ |
|---|---|---|---|
| $x_1$ | 1/3 | 0 | 1 |
| $x_2$ | 1/3 | 1 | 1 |
| $x_3$ | 1/9 | 2 0 | 2 |
| $x_4$ | 1/9 | 2 1 | 2 |
| $x_5$ | 1/27 | 2 2 0 | 3 |
| $x_6$ | 1/27 | 2 2 1 | 3 |
| $x_7$ | 1/27 | 2 2 2 | 3 |

$$L = (1/3) + (1/3) + (1/9)2 + (1/9)2 + (1/27)3 + (1/27)3 + (1/27)3$$

$$= 1.4444 \text{ ternary / symbol}$$

$$H(X) = -\left[ 2\times\frac{1}{3}\log_3\frac{1}{3} + 2\times\frac{1}{9}\log_3\frac{1}{9} + 3\times\frac{1}{27}\log_3\frac{1}{27} \right]$$

$$= 1.4444 \text{ ternary/symbol}$$

$$\eta = \frac{H(X)}{L} = \frac{1.4444}{1.4444} = 100\%$$

<u>Q5</u> : A source emits 3 equiprobable symbols randomly & independently.

(a) Find the efficiency & redundancy of a ternary Huffman Code for 1 symbol/message.

(b) Repeat (a) for binary Huffman Code.

(c) Repeat (a) for binary Huffman Code with 2 symbol/message

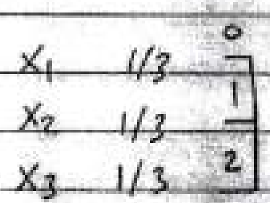
(Ans : (a) $\eta = 100\%$ (b) 95% (c) $\eta = 98.37\%$

## Solution

The symbols are equiprobable

$p(X_1) = p(X_2) = p(X_3) = \frac{1}{3}$

(a)



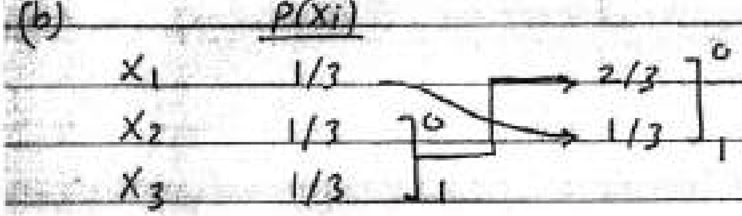
| $X_i$ | $P(X_i)$ | Codeword | $l_i$ |
|---|---|---|---|
| $X_1$ | 1/3 | 0 | 1 |
| $X_2$ | 1/3 | 1 | 1 |
| $X_3$ | 1/3 | 2 | 1 |

$L = \sum_{i=1}^{3} l_i p(X_i) = 1$ ternary / symbol

$H(X) = -\left[3 \times \frac{1}{3} \log_3 \frac{1}{3}\right] = 1$ ternary / symbol

$\eta = \frac{H(X)}{L} = 100\%$ ; $R = 1 - \eta = 0\%$

(b)



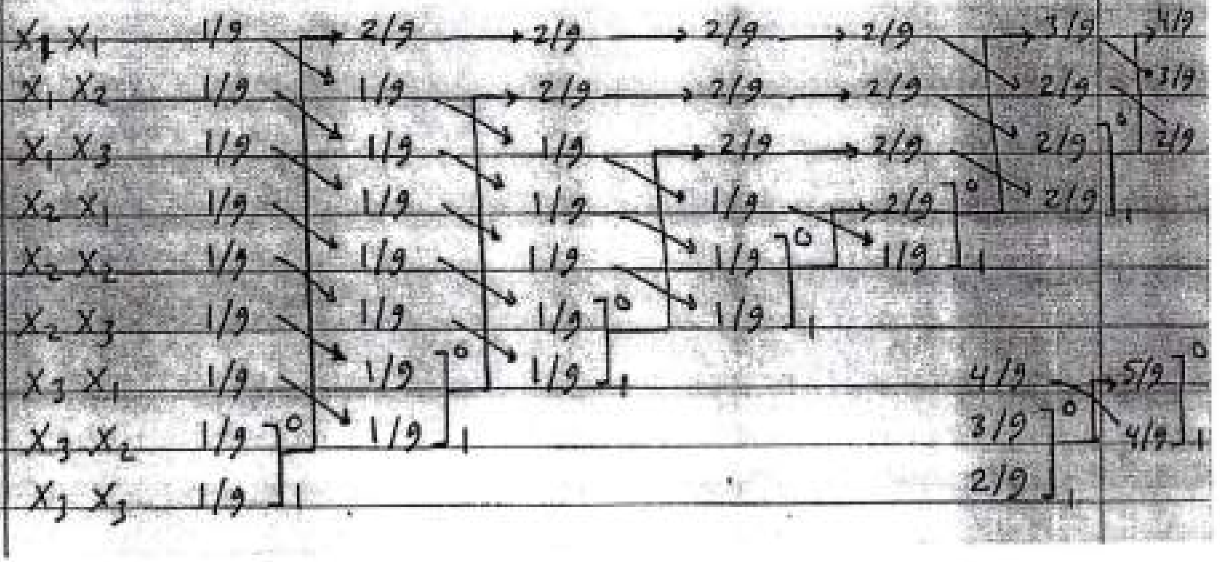
| $X_i$ | P(Xi) | Codeword | $l_i$ |
|---|---|---|---|
| $X_1$ | 1/3 | 1 | 1 |
| $X_2$ | 1/3 | 0 0 | 2 |
| $X_3$ | 1/3 | 0 1 | 2 |

$$L = \sum l_i p(x_i) = \frac{1}{3} + \frac{2}{3} + \frac{2}{3} = 1.667 \text{ bits/symbol}$$

$$H(X) = -\left[3 \times \frac{1}{3} \log_2 \frac{1}{3}\right] = 1.58 \text{ bits/symbol}$$

$$\eta = \frac{H(x)}{L} = \frac{1.58}{1.667} = 95\% \quad ; \; R = 5\%$$

(c)



| $X_i X_j$ | $P(X_i X_j)$ | Codeword | $l_i$ |
|---|---|---|---|
| $X_1 X_1$ | 1/9 | 001 | 3 |
| $X_1 X_2$ | 1/9 | 0000 | 4 |
| $X_1 X_3$ | 1/9 | 0001 | 4 |
| $X_2 X_1$ | 1/9 | 110 | 3 |
| $X_2 X_2$ | 1/9 | 111 | 3 |
| $X_2 X_3$ | 1/9 | 100 | 3 |
| $X_3 X_1$ | 1/9 | 101 | 3 |
| $X_3 X_2$ | 1/9 | 010 | 3 |
| $X_3 X_3$ | 1/9 | 011 | 3 |

$$L = \sum_{i=1}^{9} l_i p(x_i) = 3.22 \text{ bits / 2 symbols}$$

$$H(x) = 3.17 \text{ bits}/\overset{2}{\text{symbols}}$$

$$\eta = \frac{H(x)}{L} = \frac{3.17}{3.22} = 98.37\ \%$$

$$R = 1 - \eta = 1.623\ \%$$

**Q6:** A discrete source produces the symbols

$p(x) = [0.31\ \ 0.17\ \ 0.15\ \ 0.1\ \ 0.05\ \ 0.07\ \ 0.06\ \ 0.04\ \ 0.02]$

These are encoded using ternary Shannon - Fano code, then transmitted through a discrete ternary symmetric channel having a transition matrix

$$p(Y/X) = \begin{array}{c|ccc} & y_0 & y_1 & y_2 \\ \hline x_0 & 0.8 & 0.1 & 0.1 \\ x_1 & 0.1 & 0.8 & 0.1 \\ x_2 & 0.1 & 0.1 & 0.8 \end{array}$$

Find coding efficiency, channel redundancy and the information losses.

(Ans: $\eta_{coding} = 99.11\ \%$ ; $H(X/Y) = 1.8373\ \frac{\text{bits}}{\text{symbol}}$ )

**Solution**

| $X_i$ | $p(X_i)$ | Codeword | $l_i$ | $O_i$ | $1_i$ |
|---|---|---|---|---|---|
| $X_1$ | 0.31 | 0 | 1 | 1 | 0 |
| $X_2$ | 0.17 | 1 0 | 2 | 1 | 1 |
| $X_3$ | 0.15 | 1 1 | 2 | 0 | 2 |
| $X_4$ | 0.1 | 1 2 | 2 | 0 | 1 |
| $X_5$ | 0.08 | 2 0 | 2 | 1 | 0 |
| $X_6$ | 0.07 | 2 1 | 2 | 0 | 1 |
| $X_7$ | 0.06 | 2 2 0 | 3 | 1 | 0 |
| $X_8$ | 0.04 | 2 2 1 | 3 | 0 | 1 |
| $X_9$ | 0.02 | 2 2 2 | 3. | 0 | 0 |

$$L = \sum_{i=1}^{9} l_i\, p(x_i) = 1.81 \quad \text{ternary/symbol}$$

$$H(x) = \sum_{i=1}^{9} p(x_i) \log_3 p(x_i) = 1.7722 \quad \text{ternary/symbol}$$

$$\eta_c = \frac{H(x)}{L} = \frac{1.7722}{1.81} = 97.72\%$$

$$p(0) = \frac{\sum_{i=1}^{9} O_i\, p(x_i)}{L} = 0.3425414$$

$$p(1) = \frac{\sum_{i=1}^{9} 1_i\, p(x_i)}{L} = 0.3757$$

$$p(2) = 1 - p(0) - p(1) = 0.28177$$

$$p(x,y) = p(x).\,p(y/x) = \begin{array}{c|ccc} & y_0 & y_1 & y_2 \\ \hline x_0 & 0.274 & 0.03425 & 0.03425 \\ x_1 & 0.03767 & 0.3 & 0.03757 \\ x_2 & 0.0282 & 0.0282 & 0.2254 \end{array}$$

$$p(y) = [\overset{y_0}{0.34} \quad \overset{y_1}{0.363} \quad \overset{y_2}{0.297}]$$

$$C = \log_2 m + \sum_{j=1}^{3} P(y_j/x_i) \log_2 P(y_j/x_i)$$

$$= \log_2 3 - 0.922 = 0.663 \text{ bits/symbol}$$

$$I(X,Y) = H(Y) + \sum_{j=1}^{3} P(y_j/x_i) \log_2 P(y_j/x_i)$$
$$= 0.65817 \text{ bits/symbol}$$

$$\eta_{channel} = \frac{I(X,Y)}{C} = 99\% \Rightarrow R = 1 - \eta = 1\%$$

$$H(X/Y) = H(X,Y) - H(Y)$$
$$= 2.4955 - 0.65817$$
$$= 1.8373 \text{ bits/symbol}$$

**Q7**: A source produces the symbols with probabilities:
$p(x) = [0.4 \quad 0.2 \quad 0.12 \quad 0.08 \quad 0.08 \quad 0.04 \quad 0.04 \quad 0.04]$
these are encoded using Shannon-Fano code then the source encoder o/p is transmitted through a BSC having BER of 0.1. Find (a) Coding efficiency
(b) receiver entropy (c) information lost in the channel
(d) channel efficiency
(Ans: (a) 96.17% (b) 0.99929 bits/symbol (c) 0.4686 $\frac{bits}{symbol}$
(d) $\eta_{Chanel} = 99.8\%$

**Solution**

(a)

| $x_i$ | $p(x_i)$ | codeword | $l_i$ | $O_i$ |
|---|---|---|---|---|
| $x_1$ | 0.4 | 00 | 2 | 2 |
| $x_2$ | 0.2 | 01 | 2 | 1 |
| $x_3$ | 0.12 | 100 | 3 | 2 |
| $x_4$ | 0.08 | 101 | 3 | 1 |
| $x_5$ | 0.08 | 110 | 3 | 1 |
| $x_6$ | 0.04 | 1110 | 4 | 1 |
| $x_7$ | 0.04 | 11110 | 5 | 1 |
| $x_8$ | 0.04 | 11111 | 5 | 0 |

$$L = \sum_{i=1}^{8} l_i \, p(x_i) = 2.6 \text{ bits/symbol}$$

$$H(x) = -\sum_{i=1}^{8} p(x_i) \log_2 p(x_i) = 2.5 \text{ bits/symbol}$$

$$\therefore \eta = \frac{H(x)}{L} = \frac{2.5}{2.6} = 96.17\%$$

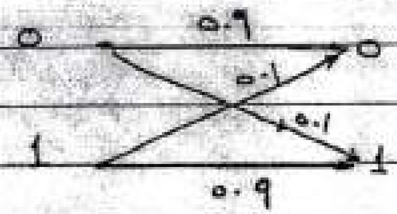
(b) $$p(0) = \frac{\sum_{i=1}^{8} O_i \, p(x_i)}{L} = 0.48$$

$$p(1) = 0.52$$

$$p(Y/X) = \begin{array}{c} \\ x_0 \\ x_1 \end{array} \begin{array}{c} \begin{array}{cc} y_0 & y_1 \end{array} \\ \begin{bmatrix} 0.9 & 0.1 \\ 0.1 & 0.9 \end{bmatrix} \end{array}$$

$p(0) = 0.48$

$p(1) = 0.52$



$$p(x,y) = p(x)\,p(y/x) = \begin{array}{c|cc} & y_0 & y_1 \\ \hline x_0 & 0.432 & 0.048 \\ x_1 & 0.052 & 0.468 \end{array}$$

$$p(y) = \begin{array}{cc} y_0 & y_1 \\ [\,0.484 & 0.516\,] \end{array}$$

$$H(y) = -\sum_{j=1}^{2} p(y_j)\log_2 p(y_j) = 0.99926 \text{ bits/symbol}$$

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

$= 1.4686 - 0.99926$

$= 0.4686$ bits/symbol

(d) $I(X,Y) = H(Y) + \sum_{j=1}^{2} p(y_j/x_i)\log_2 p(y_j/x_i)$

$= 0.99926 - 0.469$

$= 0.53$ bits/symbol

$C = \log_2 m + K = \log_2 2 - 0.469$

$= 0.531$ bits/symbol

$$\eta = \frac{I(X,Y)}{C} = 99.8\%$$

# Chapter Five

# Channel Coding

## 5.1 Introduction:

The purpose of channel coding is:

1-either to protect information from channel noise, distortion and jamming, which is the subject of error detecting and correcting codes. Or,

2-to protect information from the 3rd party (enemy) which is the subject of encryption, scrambling.

In this course, only error detecting and correcting codes are discussed.

## 5.2 Error Detecting and Correcting Codes

The basic idea behind error detecting or correcting codes is to **add extra bits** (or digits) to the information such that the receiver can use it **to detect or correct errors** with limited capabilities. These extra redundant bits are called **parity** or **check** or **correction** bits. So, if for each **k** digits, **r** parity digits are added then, the transmitted **k+r=n** digits will have r redundant digits and the code is called **(n,k) code** with **code efficiency or rate of (k/n).** In general, the ability of detection or correction depends on the techniques used and the n, k parameters.

## 5.3 Error Detecting Codes

### 5.3.1 Odd/Even Parity codes:

The simplest error detection schemes are the well- known **even and odd parity** generators. For even parity, an extra bit is added for each k information bits such that the total number of 1's is even. At the receiver, an error is detected if the number of 1's is odd.

However, if the number of 1's is **even**, then either no error occurs or even number of errors occur. Hence:

probability(detecting errors)=probability(odd number of errors)

and

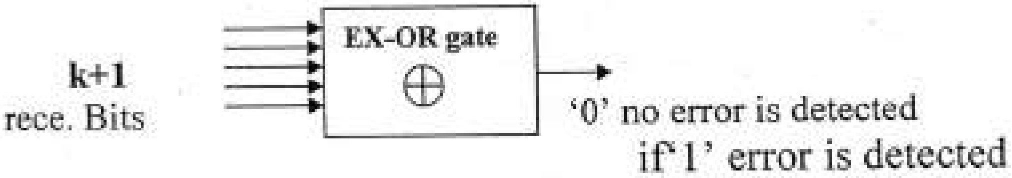
probability(undetected errors)=probability(even number of errors)

The same idea can be applied when number of 1's is adjusted to be odd.

The code rate (efficiency) is k/(k+1).

To implement these parity generators, simple Ex-OR gates are used at Tx and Rx as shown below:

| Information bits | even parity bit |
|---|---|
| 1 0 1 0 1 1 1 | 1 |
| 0 1 1 0 1 0 1 | 0 |
| 1 0 1 1 1 1 1 | 0 |
| 1 1 0 1 0 0 0 | 1 |



Hence, we can conclude that error detection is not ideal. It does not detect errors with 100% probability, since **even number of errors behaves exactly the same as no error.** However, and for practical channels, the single bit error probability (bit error rate BER) is of the order of p=$10^{-3}$ or less. Assuming, say k=7 and n=7+1=8 bits, then the probability of undetected errors will be:

$$\boxed{P(undet\ \ error)=C_2^8 p^2(1-p)^6+C_4^8 p^4(1-p)^4+C_6^8 p^6(1-p)^2+C_8^8 p^8 \approx 28\times10^{-6}}$$

- for p<<1. $C_n^m$ is the combination factor $C_n^m=\frac{m!}{n!\,(m-n)!}$

The probability of detected errors will be:

$$\boxed{P(\text{detected}\quad error\mathrm{s})=C_1^8p^1(1-p)^7+C_3^8p^3(1-p)^5+C_5^8p^5(1-p)^3+C_7^8p^7(1-p)\approx 8\times 10^{-3}}$$

Note that, although the code used for detection is so simple (few EX-OR gates) but still we have big advantage since probability of detecting errors is much higher than probability of undetected errors. The advantage of error detection is clear when used together with ARQ (Automatic Repeat Query) systems. In these systems, two channels are used, the usual forward channel with error detection and a backward channel. Data are transmitted through the forward channel. These data are protected against errors with parity error detection. If the receiver detects errors then a backward channel will be used to inform the transmitter to retransmit (repeat) the same data so that in the next transmission, data is received correctly since errors occur randomly (may occur or may not occur).

### 5.3.2 Binary Repetition Codes (BRC):

Here

k=1, n=r+1

Code rate=1/n=1/(1+r)

The encoder repeats every message digits n times (n:odd) while the decoder uses majority logic decoding to decide the digit value as follows:

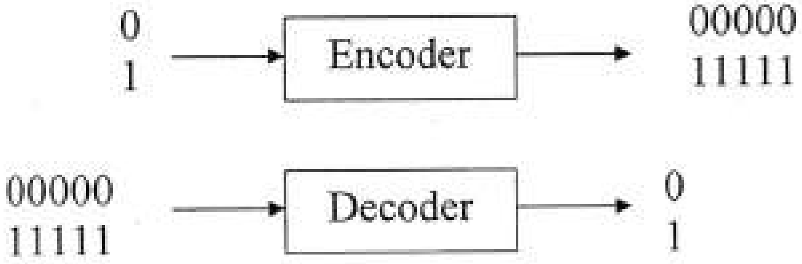
If No. of 0's > No. of 1's → message is "0"

If No. of 0's < No. of 1's → message is "1"

**Example 5.1**

Show the generated codewords from binary repition code with n=5 and calculate code rate

**Solution**



Code rate=1/5

The error probability of binary repetition code $P_{BRC}$ over binary symmetric channel with error probability per hop $P_e$ is given by:

$$\boxed{P_{BRC} = \sum_{j=Int[\frac{n}{2}]+1}^{n} C_j^n P_e^j (1-P_e)^{n-j}}$$

**Example 5.2**

Consider BSC with error prob. Per hop $P_e$=0.1. Find $P_{BRC}$ if BRC with n=3 is used.

**Solution**

$$Int[\frac{n}{2}]+1=2$$

$$P_{BRC} = \sum_{j=2}^{3} C_j^3 P_e^j (1-P_e)^{n-j} = C_2^3 P_e^2 (1-P_e)^1 + C_3^3 P_e^3 (1-P_e)^0$$

$$= \frac{3!}{2!1!}(0.1)^2(0.9)^1 + \frac{3!}{3!0!}(0.1)^3(0.9)^0 = 0.028$$

## 5.4 Error Correcting Codes

In order to make the receiver have the ability to detect and correct errors, then not only a single parity bit is used, but in stead r bits are used giving what is called the (n,k) code.

### Basic definitions:

### 1-systematic and nonsystematic codes:

If information bits (a's) are unchanged in their values and positions at the transmitted codeword, then this code is said to be systematic.

Input data [D]=[$a_1$ $a_2$ $a_3$ …….$a_K$],

Output systematic (n,k) codeword is [C]=[ $a_1$ $a_2$ $a_3$ …….$a_K$ $c_1$ $c_2$ $c_3$ …….$c_r$]

However if data bits are spread or changed at the output codeword then, the code is said to be nonsystematic:

Output nonsystematic(7,4) codeword is [C]=[$c_2$ $a_1$ $c_3$ $a_2$ $c_1$ $a_4$ $a_3$]

### 2- Hamming distance:

The ability of error detection and correction codes depends on this parameter. The Hamming distance between two codewords $C_i$ and $C_j$ is denoted by $d_{ij}$ which is the number of bits that differ. For a binary (n,k) code with $2^k$ possible codewords then the minimum Hamming distance (HD) is the min($d_{ij}$). Of course

$n \geq d_{ij} \geq 0$.

### Example 5.3:

Find the Hamming distance between the two codewords: [C1]=[1011100] and [C2]=[1011001].

**Solution:**

Here, the no. of bits that differ is 2, hence $d_{12}=2$.

**Example 5.4:**

Find the minimum Hamming distance for the 3 codewords:

[C1]=[1011100], [C2]=[1011001] and [C3]=[1011000].

**Solution:**

Here $d_{12}=2$, $d_{13}=1$ and $d_{23}=1$. Hence $\min(d_{ij})=1=(HD)$. Note that the calculation of HD becomes more difficult if no of codewords increases.

### 3-Hamming weight:

This is the number of 1's in the non zero codeward $C_i$. It is denoted by $\omega_i$ . As will be shown later, and for linear codes, $\omega_{min}=HD=\min(d_{ij})$. This simplifies the calculation of HD. As an example, if [C1]=[1011000], then $\omega_1=3$, and for [C2]=[0001010], then $\omega_2=2$, and so on.

### 4-Linear and nonlinear codes:

when the r parity bits are obtained from a linear function of the k information bits then the code is said to be linear, otherwise it is a nonlinear code.

**Notes:**

1-A linear code can correct t=Int[(HD-1)/2] of random (isolated) errors and detect (HD-1) random (isolated errors).

2- HD is the min Hamming distance= $\omega_{min}$

### 5.4.1Linear Block Codes:

Only systematic binary codes will be described. The r parity bits are obtained using a linear function of the a's data. Mathematically, this can be described by the set of equations:

$$\left.\begin{array}{l} C_1=h_{11}a_1+h_{12}a_2+h_{13}a_3+\ldots\ldots+h_{1k}a_k \\ C_2=h_{21}a_1+h_{22}a_2+h_{23}a_3+\ldots\ldots+h_{2k}a_k \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_r=h_{r1}a_1+h_{r2}a_2+h_{r3}a_3+\ldots\ldots+h_{rk}a_k \end{array}\right| \quad \ldots\ldots\ldots\ldots\ldots(1)$$

Where + is mod-2 addition (EX-OR), product is the AND multiplication and $h_{ij}$ coefficients are binary variables for a binary coding. The complete output codeword can be written in matrix form as:

[C]= [D][G] where:

$$[G]=\begin{bmatrix} 1 & 0 & 0 & 0 & h_{11} & h_{21} & h_{31} & . & h_{r1} \\ 0 & 1 & 0 & 0 & h_{12} & h_{22} & h_{32} & . & h_{r2} \\ 0 & 0 & 1 & 0 & . & . & . & . & . \\ 0 & 0 & 0 & 1 & h_{1k} & h_{2k} & h_{3k} & . & h_{rk} \end{bmatrix}=[\, I_k : P_{kxr} \,]$$

which is kxn matrix.

This matrix is called the generator matrix of the linear block code (LBC). Equation(1) can also be written in matrix form as:

$$[\,H\,]\,[C]^T=[0] \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

where: $[C]=[\ a_1\ a_2\ a_3\ \ldots\ldots a_k\ c_1\ c_2\ c_3\ \ldots\ldots c_r]$ and [H] matrix is in fact related with [G] matrix by: $[\,H\,]=[-P^T : I_r]$, and for binary coding this – sign drops out.

This rxn [H] matrix is called the **parity check matrix**. As will be shown, encoding can be done either using eq(1) ( [G] matrix ) or eq(2) ([H] matrix), but decoding is done using [H] matrix only.

**Hamming Bound:**

The question here is how to choose the number of parity bits r so that, a certain error correction capability is obtained. The answer to this question is given by R. W.Hamming. as an inequality called Hamming bound. For binary codes, this is given by:

$$\boxed{2^r \geq \sum_{j=0}^{t} C_j^{\,n}}$$

where t is the number of bits to be corrected.

**For example** if k=4, then to correct single error (t=1) then:

$2^r \geq C_0^{\,4+r} + C_1^{\,4+r}$. This gives $2^r \geq 1+(4+r)$ and the minimum r is r=3 (take minimum r to have max code efficiency). This is the (7,4) code. Note that equality is satisfied in this example, when this is the case, the code is said to be perfect code.

**Another example** if k=5 and up to 3 errors are to be corrected then:

$2^r \geq C_0^{\,5+r} + C_1^{\,5+r} + C_2^{\,5+r} + C_3^{\,5+r}$ that gives:

$2^r \geq 1+(5+r)+(5+r)(4+r)/2+(5+r)(4+r)(3+r)/6$, then min r here is r=10, and the code is the (15,5) non perfect code(equal sign is not satisfied ).

**Note:**

If the (n,k) codewords are transmitted through a channel having error prob=$p_e$, then prob. of decoding a correct word at the Rx for t-error correcting code will be:

P(correct words)=p(no error)+p(1 error)+……..p(t errors)

$$\boxed{P(correct\ word) = \sum_{i=0}^{t} C_i^n\ p_e^{\ i}\ (1-p_e)^{n-i}}$$

and
prob(erroneous word)=1-P(correct word).

## Hamming code:

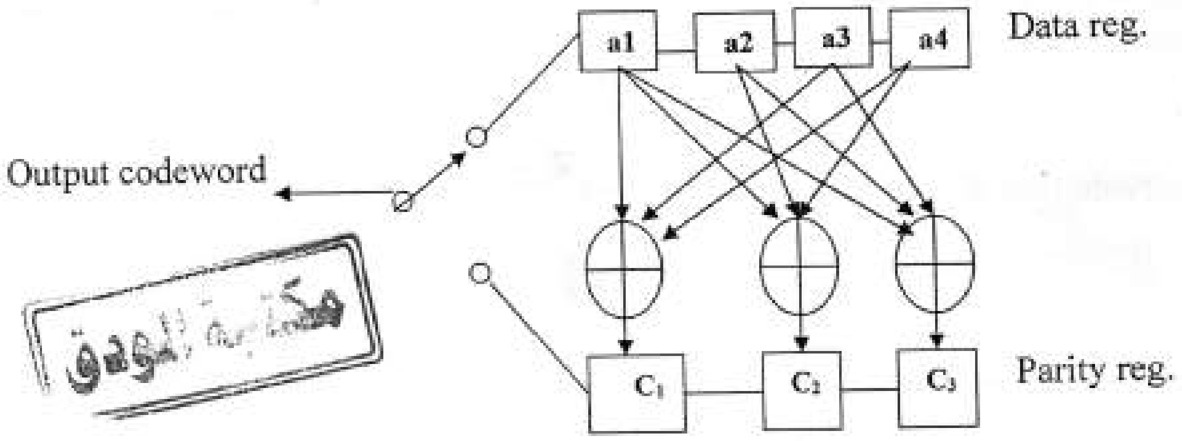
The first example given above is the Hamming code. It is a **single error correcting** perfect code with the following parameters: $n=2^r-1$, HD=3, t=1. The (7,4), (15,11), (31,26) …..are examples of Hamming codes. Hamming codes are encoded and decoded as a linear block codes.

## Encoding of Linear Block codes:

Eq(1) or eq(2) can be implemented using EX-OR gates. Take for example a binary (7,4) Hamming code with a parity check matrix:

$$[H]=\begin{bmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}$$ , then using eq(2), $[H][C]^T=[0]$ will give:

$C_1=a_1+a_3+a_4$, $C_2=a_1+a_2+a_4$, $C_3=a_1+a_2+a_3$.



Above equations for C's are used to find the code table for this code as:

| $a_1$ | $a_2$ | $a_3$ | $a_4$ | $c_1$ | $c_2$ | $c_3$ | $\omega_i$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | -- |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 3 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 3 |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 4 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 3 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 4 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 4 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 3 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 4 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 3 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 3 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 4 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 3 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 4 |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 4 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 7 |

$\omega i(\min)=3=HD$, i.e. $t= \mathrm{int}(3-1)/2=1$ bit. Hence, this is a single error correcting code (Hamming code).

---

**Example 5.5:**

Find the generator matrix for the previous LBC.

**Solution:**

$$[G]=[I_k\ P^T]=\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Note that the equation [C]=[D][G] gives:

$[C]=[a_1\ \ a_2\ \ a_3\ \ a_4\ \ (a_1+a_3+a_4)\ \ (a_1+a_2+a_4)\ \ (a_1+a_2+a_3)]=[\ a_1\ \ a_2\ \ a_3\ \ a_4\ c_1\ c_2\ c_3]$ as obtained before.

**Decoding of linear block codes:**

If [R]=[C]+[E] is the received codeword, where [E] is the error word, if [E]=[0] then no error occurs but if [E]=[0 0 …0 0 1 0] then single error occurs at 2nd position (from the right), or if [E]=[0 0 0…0 1 0 0 1 0 1] then triple errors occur at 1st, 3rd and 6th positions. Depending on t not all of these errors can be corrected. If [R] is multiplied by [H] (the receiver must know [H]) then:

$[H]\,[R]^T=[H][C]^T+[H]\,[E]^T=[H][E]^T$ since $[H][C]^T$ is set to [0] at the Tx.

Then define [S] vector :

$[S]=[H]\,[R]^T=[H][E]^T$ ……………..(4)

This [S] r-vector is called the syndrome. **If [S]=[0], the RX decides on no error** but if $[S]\neq[0]$, then the receiver must use [S] to find [E] and hence the corrected [C]=[R]+[E] binary coding). Of course, [S] is calculated from [R]. The problem is now how to find [E] from [S]?. In Eqs(4) we have n unknowns in r equations (n>r). To solve this problem, maximum likelihood criterion is used. i.e, most probable error words are chosen and usually the most probable errors are those with less number of errors. So the RX finds [E] that matches [S] such that the less number of errors solution is chosen.

## Simple decoding procedure for single error:

For single error Hamming codes, above mathematical solution is reduced into comparing the [S] r-vector with all columns of the [H] matrix ($2^r$-1 non zero and non repeated columns). That column similar to [S] is the position of error. This is mathematically equivalent to multiply $[H][E]^T$ such that [E] has only one nonzero element at the ith position or at the ith column. Hence, for single error correction, the parity check matrix [H] must satisfy the following:

i. No all zero columns so as not to mix with the no error case.
ii. No repeated columns so that the decoder can decode any received word correctly with single error assumption.

**Example 5 :**

For previous example, [1]-Find the corrected word at the receiver, for the previous example, if the received word [R]=[1001111]. [2]-Find the syndrome vector if double errors occur at 1st and last positions, comment. [3]- Draw the decoder cct used to find the syndrome vector[S].

**Solution:**

[1] If the received word is [R]=[1001111] then,

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

which is similar to the 4th column in [H].

Hence the corrected word=[R]+[0001000]= [1 0 0 0 1 1 1]

which checks with the table shown besides.

---

[2]-To find the syndrome vector[S] for double errors, then $[S]=[H][E]^T$.

Where [E]=[1000001] corresponding to double errors at 1st and last positions. Then:

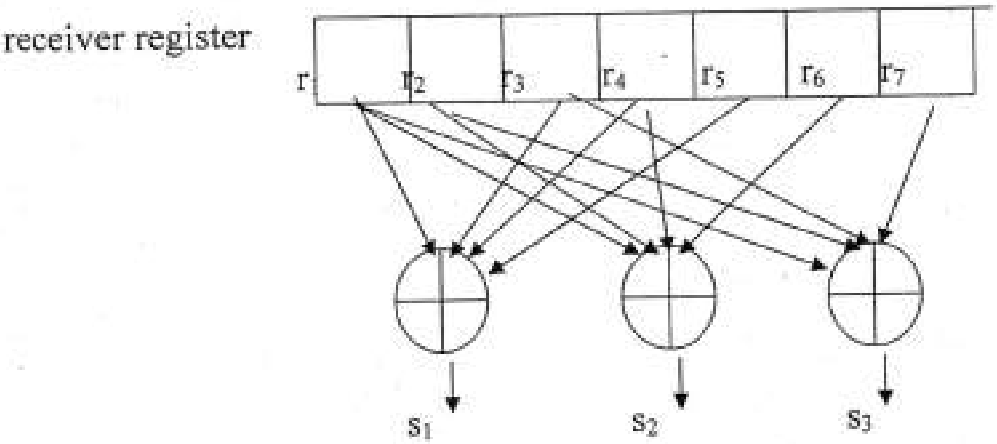
$$[S] = [H][E]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Note that the syndrome for single error at the 4th position is the same as the syndrome for double errors at 1st and last positions. This indicates that the code is only capable of correcting single error as expected.

[3]- To draw the decoder cct, then :

$$[S]=[H][R]^T=\begin{bmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}\begin{bmatrix}r_1\\r_2\\r_3\\r_4\\r_5\\r_6\\r_7\end{bmatrix}=\begin{bmatrix}s_1\\s_2\\s_3\end{bmatrix}$$ which gives:

$s_1=r_1+r_3+r_4+r_5$, $s_2=r_1+r_2+r_4+r_6$, $s_3=r_1+r_2+r_3+r_7$ implemented as shown:



**Example 5.7:**
The generator matrix of a LBC is given by:

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

a- Use Hamming bound to find error correction capability.

b- Find the parity check matrix.

c- find the code table, Hamming weight and the error correction capability then compare with part(a).

d- If the received word is [R]=[1011110011], find the corrected word at the Rx.

**Solution:**
(a) n=10, k=3, r=7 , (10,3) code. Using Hamming bound, then:

$2^7 \geq C_0^{10}+C_1^{10}+C_2^{10}+........\pm C_t^{10}$ that gives 128>1+10+(10*9/2), i.e t=2 double error correction.

(b)

$$[H]=[P^T\ I]=\begin{bmatrix} 1&0&0&1&0&0&0&0&0&0\\ 1&1&0&0&1&0&0&0&0&0\\ 0&1&1&0&0&1&0&0&0&0\\ 1&0&1&0&0&0&1&0&0&0\\ 1&1&1&0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0&0&0&1 \end{bmatrix}$$

with no 'zero' or repeated columns.

The equation $[H][C]^T=[0]$ gives $c_1=a_1$, $c_2=a_1+a_2$ and $c_3=a_2+a_3$, $c_4=a_1+a_3$, $c_5=a_1+a_2+a_3$ $c_6=a_2$, $c_7=a_3$.

| a1 | a2 | a3 | c1 | C2 | c3 | c4 | c5 | c6 | c7 | wi |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | --- |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 5 |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 5 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 6 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 5 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 6 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 6 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 7 |

(c) $\omega_i(min)=5=HD$, i.e. t= int(5-1)/2=2 bits. Hence, this is a double error correcting code which checks with part(a).

(d) If [R]=[1011110011], then:

$$[S]=[H][R]^T=\begin{bmatrix}1&0&0&1&0&0&0&0&0&0\\1&1&0&0&1&0&0&0&0&0\\0&1&1&0&0&1&0&0&0&0\\1&0&1&0&0&0&1&0&0&0\\1&1&1&0&0&0&0&1&0&0\\0&1&0&0&0&0&0&0&1&0\\0&0&1&0&0&0&0&0&\underset{\uparrow}{0}&1\end{bmatrix}\begin{bmatrix}1\\0\\1\\1\\1\\1\\0\\0\\1\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\\0\\1\\0\end{bmatrix}$$

which is similar to the 9th. column in [H](from the left), hence corrected word will be [1011110001].

# Chapter 5 Tutorial Problems

**Q1:** A source produces information in blocks of 3 bits. If the probability of a block $b_i$ is given by $P(b_i) = \frac{i}{36}$, $i = 1, 2, \ldots, 8$. These block are preselected against errors using a linear block code having the generator matrix

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

Find prob. of logic zero at channel encoder o/p and the corrected word at the Rx for the received word $[R] = [1110011]$

**Solution**

$G = [I_k : P^T]$

from $G \rightarrow k = 3$ ; $r = 4$ ; $n = 7$

$\Rightarrow (7,3)$ LBC

$C = dG$

$$[d_1 d_2 d_3 \; c_4 c_5 c_6 c_7] = [d_1 \; d_2 \; d_3] \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right]$$

$c_4 = d_1 \oplus d_2 \oplus d_3$

$c_5 = d_1 \oplus d_3$

$c_6 = d_2 \oplus d_3$

$c_7 = d_1 \oplus d_2$

| $d_1$ | $d_2$ | $d_3$ | $C_4$ | $C_5$ | $C_6$ | $C_7$ | $\omega_i$ | $O_i$ | $P(x_i)$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | – | 7 | 1/36 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 4 | 3 | 2/36 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 4 | 3 | 3/36 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 4 | 3 | 4/36 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 4 | 3 | 5/36 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 4 | 3 | 6/36 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 4 | 3 | 7/36 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 4 | 3 | 8/36 |

$d_{min} = (\omega_i)_{min} = 4$

no. of detected errors = $d_{min} - 1$ = 3 errors

no. of corrected errors = $Int\left(\frac{d_{min}-1}{2}\right)$

$= Int\left(\frac{4-1}{2}\right) = 1$ error

$$p(o) = \frac{\sum O_i\,P(x_i)}{l} = \frac{\frac{7}{36}+\frac{3\times2}{36}+\frac{3\times3}{36}+\frac{3\times4}{36}+\frac{3\times5}{36}+\frac{3\times6}{36}+\frac{3\times7}{36}+\frac{3\times8}{36}}{7}$$

$= 0.4444$

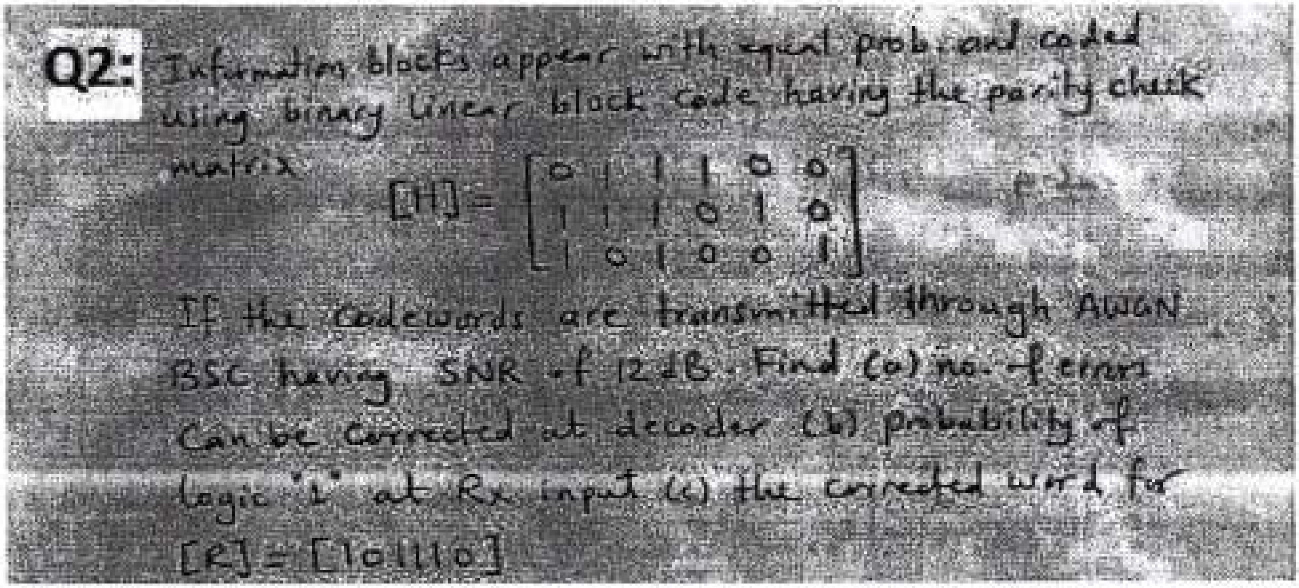
from $G = [I_k : P^T]$

we find $H = [P : I_m]$

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

$$S = RH^T = [1110011]\begin{bmatrix} 1101 \\ \underline{1011} \\ 1110 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix} = [1011]$$

∴ Corrected word $[R] = [1\underline{0}10011]$

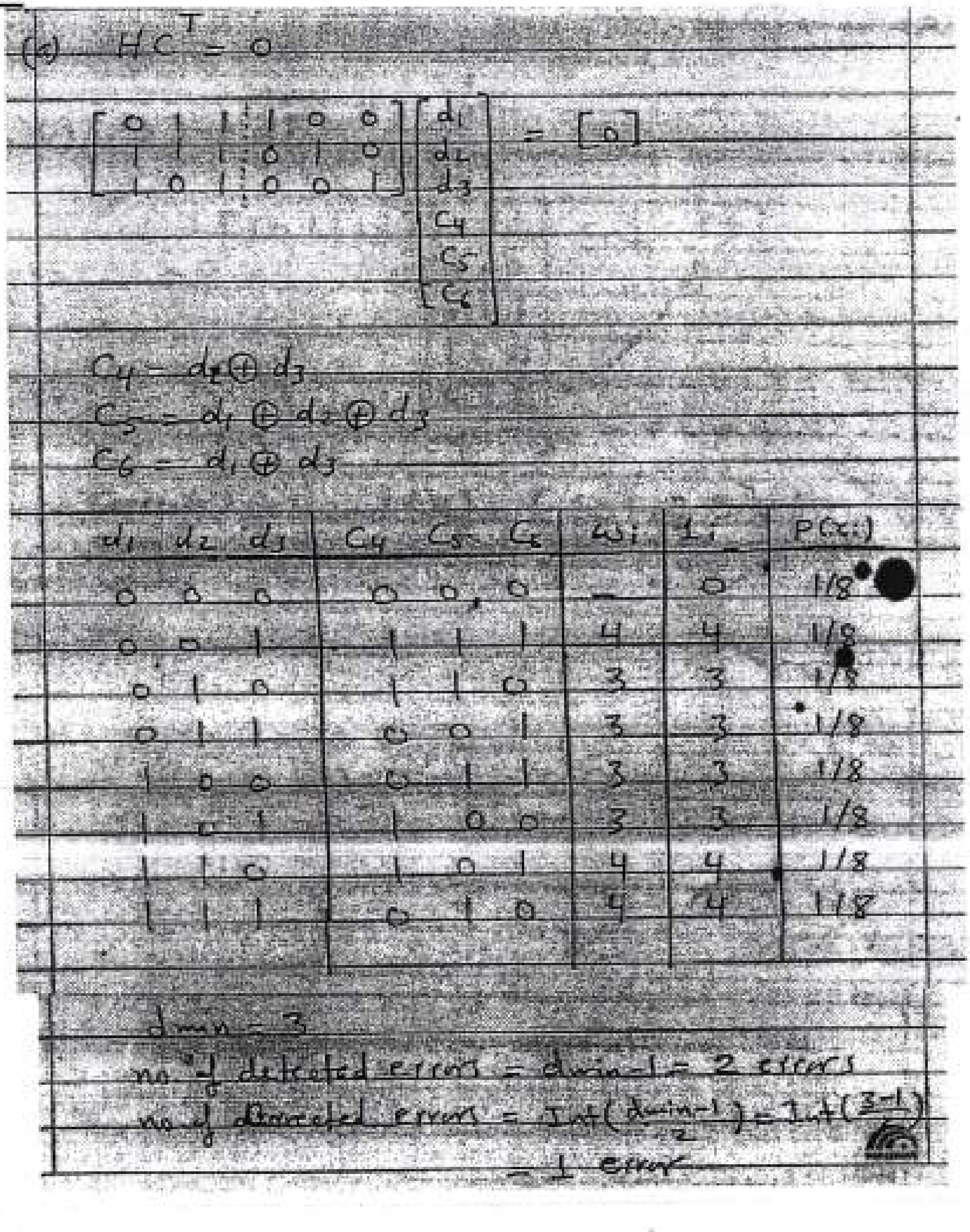


**Q2:** Information blocks appear with equal prob. and coded using binary linear block code having the parity check matrix

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

If the codewords are transmitted through AWGN BSC having SNR of 12 dB. Find (a) no. of errors can be corrected at decoder (b) probability of logic '1' at Rx input (c) the corrected word for $[R] = [101110]$

**Solution**



(a) $HC^T = 0$

$$\left[\begin{array}{ccc:ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \begin{bmatrix} d_1 \\ d_2 \\ d_3 \\ C_4 \\ C_5 \\ C_6 \end{bmatrix} = [0]$$

$C_4 = d_2 \oplus d_3$

$C_5 = d_1 \oplus d_2 \oplus d_3$

$C_6 = d_1 \oplus d_3$

| $d_1$ | $d_2$ | $d_3$ | $C_4$ | $C_5$ | $C_6$ | $W_i$ | $1_i$ | $P(x_i)$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | – | 0 | 1/8 |
| 0 | 0 | 1 | 1 | 1 | 1 | 4 | 4 | 1/8 |
| 0 | 1 | 0 | 1 | 1 | 0 | 3 | 3 | 1/8 |
| 0 | 1 | 1 | 0 | 0 | 1 | 3 | 3 | 1/8 |
| 1 | 0 | 0 | 0 | 1 | 1 | 3 | 3 | 1/8 |
| 1 | 0 | 1 | 1 | 0 | 0 | 3 | 3 | 1/8 |
| 1 | 1 | 0 | 1 | 0 | 1 | 4 | 4 | 1/8 |
| 1 | 1 | 1 | 0 | 1 | 0 | 4 | 4 | 1/8 |

$d_{min} = 3$

no. of detected errors $= d_{min} - 1 = 2$ errors

no. of corrected errors $= \text{Int}\left(\frac{d_{min}-1}{2}\right) = \text{Int}\left(\frac{3-1}{2}\right)$

$= 1$ error

(b) $P(1) = \dfrac{\sum 1_i \times P(x_i)}{l} = \dfrac{\frac{1}{8}[4+3+3+3+3+4+4]}{6} = 0.5$

(c) $S = RH^T$

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

Corrected Codeword $[R] = [1\,0\,1\,1\,\underline{0}\,0]$

**Q3:** A source of information produces equiprobable blocks of 4-bits. The encoder circuits adds an even parity bit for error detection. Prepare the encoder table then find the prob. of the logic pair "10" at the encoder output

**Solution**

| information bits | | | | extra bit | | |
|---|---|---|---|---|---|---|
| $d_1$ | $d_2$ | $d_3$ | $d_4$ | (even parity) | "10" | $P(x_i)$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 1/16 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1/16 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1/16 |
| 0 | 0 | 1 | 1 | 0 | 1 | " |
| 0 | 1 | 0 | 0 | 1 | 1 | " |
| 0 | 1 | 0 | 1 | 0 | 2 | " |
| 0 | 1 | 1 | 0 | 0 | 1 | " |
| 0 | 1 | 1 | 1 | 1 | 0 | " |
| 1 | 0 | 0 | 0 | 1 | 1 | " |
| 1 | 0 | 0 | 1 | 0 | 2 | " |
| 1 | 0 | 1 | 0 | 0 | 2 | " |
| 1 | 0 | 1 | 1 | 1 | 1 | " |
| 1 | 1 | 0 | 0 | 0 | 1 | " |
| 1 | 1 | 0 | 1 | 1 | 1 | " |
| 1 | 1 | 1 | 0 | 1 | 1 | " |
| 1 | 1 | 1 | 1 | 0 | 1 | " |

$l = n - k + 1 = 4 + 1 = 5$ bits

$$p(\text{"10"}) = \frac{\sum \text{"10"}_i \cdot P(x_i)}{l} = \frac{\frac{1}{16}\left[1+1+1+2+1+1+2+2+1+1+1+1+1\right]}{5}$$

$= 0.2$

**Q4:** A linear systematic (6,3) LBC has been observed to give the following the o/p codewords:

Codeword1 : 100101
Code word2 : 010011
Code word3 : 001111
Find the parity check matrix of the code and find the corrected word at Rx if [R] = [110001]

**Solution**

$HC^T = 0$

$$\begin{bmatrix} h_{11} & h_{12} & h_{13} & 1 & 0 & 0 \\ h_{21} & h_{22} & h_{23} & 0 & 1 & 0 \\ h_{31} & h_{32} & h_{33} & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = [0]$$

$h_{11} + 1 = 0 \rightarrow h_{11} = 1$

$h_{21} = 0$

$h_{31} + 1 = 0 \rightarrow h_{31} = 1$

$$\begin{bmatrix} 1 & h_{12} & h_{13} & 1 & 0 & 0 \\ 0 & h_{22} & h_{23} & 0 & 1 & 0 \\ 1 & h_{32} & h_{33} & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \boxed{0}$$

$h_{12} = 0$

$h_{22} + 1 = 0 \Rightarrow h_{22} = 1$

$h_{32} + 1 = 0 \rightarrow h_{32} = 1$

$$\begin{bmatrix} 1 & 0 & h_{13} & 1 & 0 & 0 \\ 0 & 1 & h_{23} & 0 & 1 & 0 \\ 1 & 1 & h_{33} & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \boxed{0}$$

$h_{13} = 1$

$h_{23} = 1$

$h_{33} = 1$

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

$S = eH^T$

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

Corrected word $[R] = [1\,1\,\underline{1}\,0\,0\,1]$

**Q5:** Consider a BSC with error probability per hop $p = 0.05$, Find error probability if binary repition code is used with $n = 5$ is used

**Solution**

$$j = Int\left[\frac{n}{2}\right] + 1 = Int\left[\frac{5}{2}\right] + 1 = 3$$

$$P_e = \sum_{j=3}^{5} C_j^5 \, p^j (1-p)^{5-j}$$

$$= C_3^5 p^3 (1-p)^2 + C_4^5 p^4 (1-p) + C_5^5 p^5 (1-p)^0$$

$$= \frac{5!}{3!2!}(0.05)^3(0.95)^2 + \frac{5!}{4!1!}(0.05)^4(0.095) + \frac{5}{5!0!}(0.05)^5$$

$$= 10(0.05)^3(0.95)^2 + 5(0.05)^4(0.95) + (0.05)^5$$

$$= 0.0011 + 2.9688 \times 10^{-5} + 3.125 \times 10^{-7}$$

$$= 0.0011$$

**Q6:** The generator matrix of a (7,3) systematic LBC is Constructed as follows:

1- the first row is the action of a 2 i/p OR gate

2- the Second row is the decimal of 15

3- the third row is the action of a 2 i/p EX-OR gate

Find the code table & discuss the Correction Capability

**Solution**

$$G = \underbrace{[\,I_k}_{k} : \underbrace{P^T\,]}_{m} \updownarrow k$$

| A | B | OR | Ex-OR |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |

first row

$2nd\ row = 15_{10} = 1111$

3rd row

$$[G] = \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right] \begin{array}{l} \text{OR gate} \\ (15)_{10} \\ \text{Ex OR gate} \end{array}$$

$$\underset{k=3}{\longleftrightarrow} \qquad \underset{m=4}{\longleftrightarrow}$$

$$C = dG$$

$$= [d_1\ d_2\ d_3] \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$C_4 = d_2$

$C_5 = d_1 \oplus d_2 \oplus d_3$

$C_6 = d_1 \oplus d_2 \oplus d_3$

$C_7 = d_1 \oplus d_2$

| $d_1$ | $d_2$ | $d_3$ | $C_4$ | $C_5$ | $C_6$ | $C_7$ | $w_i$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | – |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 3 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 5 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 4 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 4 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 3 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 3 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 6 |

$d_{min} = 3$

no of detected errors $= d_{min} - 1 = 2$ errors

no of corrected errors $= \text{Int}\left(\frac{d_{min}-1}{2}\right)$

$= \text{Int}\left(\frac{3-1}{2}\right) = 1$ error

# Chapter Six

# Cyclic codes

## 6.1 Introduction:

These are subclass from the linear block codes. The name cyclic comes from the fact that any **cyclic shift of a codeword is another codeword**. i.e, if $[C_1]=[0011010]$ is a codeword then $[C_2]=[0001101]$ is another codeword obtained from $[C_1]$ by a right circular shift.

## 6.2 Generation of cyclic codes:

The cyclic code generation depends on the type of such code. Cyclic codes can be either systematic or nonsystematic.

### a)Nonsystematic cyclic codes: (multiplicative ):

As mentioned before a nonsystematic code is that code in which the information and parity bits are mixed and **not separated** at the output codeword [C]. A nonsystematic cyclic code is generated using polynomial multiplication:

**Procedure:**

(1) For $[D]=[a_1\ a_2\ \ldots..\ a_k]$ data word, write the data word in terms of a power of a dummy variable x with $a_1$ weighted as MSB (Most Significant Bit) and $a_k$ as LSB (Least Significant Bit). This arrangement is chosen similar to what we have in logic where the LSB lies in the right and the MSB lies in the left. Hence:

$$\boxed{D(x)=a_k+a_{k-1}\,x+a_{k-2}\,x^2+\ldots\ldots+a_2\,x^{k-2}+a_1\,x^{k-1}}$$

D=[1000101]
$D(x)=x^{6}+x^{2}+1$

where "+" sign is mod-2 addition(Ex-OR). For example if [D]=[11101], then $D(x)=1+x^2+x^3+x^4$ and if $D(x)= x^6+x^2+1$ then [D]=[1000101], and so on.

(2) Multiply D(x) by what is called generator polynomial g(x) of order r=n-k. This g(x) is one or the multiplication of some factors of $x^n+1$. Factorization of $x^n+1$ is not always easy and is **usually taken from tables**. **For example** if n=7, then $x^7+1=(x+1)(x^3+x^2+1)(x^3+x+1)$ in mod-2 addition, (i.e. these terms are multiplied together and similar terms cancels each other). Then for n=7, r=3, we can choose either $g_1(x)= x^3+x^2+1$ or $g_2(x)= x^3+x+1$. Also note that for n=7, r=4, we can choose either $g_1(x)=(x+1)(x^3+x^2+1)$ or $g_2(x) =(x+1)(x^3+x+1)$.

(3) The output codeword polynomial will be

$$\boxed{C(x)=D(x)\,g(x)}$$

from which we can find the output codeword [C].

**<u>Example 6.1:</u>**

Write down the code table for the (7,4) nonsystematic cyclic code with generator polynomial $g(x)=x^3+x+1$.

**<u>Solution:</u>**

Here n=7, k=4, r=3, $[D]=[a_1\ a_2\ a_3\ a_4]$, so the table has 16 rows:

where:

--if [D]=[0001], then D(x)=1 and $C(x)=D(x)g(x)=x^3+x+1$ or
[C]=[0001011]

--if [D]=[0010], then D(x)=x and $C(x)=D(x)g(x)=x(x^3+x+1)=x^4+x^2+x$ or
[C]=[0010110].

| i/p [D] | | | | o/p [C] | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_1$ | $a_2$ | $a_3$ | $a_4$ | $c_1$ | $c_2$ | $c_3$ | $c_4$ | $c_5$ | $c_6$ | $c_7$ | $w_i$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | --- |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 3 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 3 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 4 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 3 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 4 |
| 0 | 1 | 1 | 0 | | | | | | | | |
| 0 | 1 | 1 | 1 | | | | | | | | |
| 1 | 0 | 0 | 0 | | | | | | | | |
| 1 | 0 | 0 | 1 | | | | | | | | |
| 1 | 0 | 1 | 0 | | | | | | | | |
| 1 | 0 | 1 | 1 | | | | | | | | |
| 1 | 1 | 0 | 0 | | | | | | | | |
| 1 | 1 | 0 | 1 | | | | | | | | |
| 1 | 1 | 1 | 0 | | | | | | | | |
| 1 | 1 | 1 | 1 | | | | | | | | |

--if [D]=[0011], then $D(x)=1+x$ and

$C(x)=D(x)g(x)=(1+x)(x^3+x+1)=x^3+x+1+x^4+x^2+x=x^4+x^3+x^2+1$ or

[C]=[0011101]

--if [D]=[0100], then $D(x)=x^2$ and $C(x)=D(x)g(x)=x^2\ (x^3+x+1)=x^5+x^3+x^2$

or [C]=[0101100].

--if [D]=[0101], then $D(x)=1+x^2$ and $C(x)=D(x)g(x)=(1+x^2)(x^3+x+1)=$

$x^3+x+1+x^5\ +x^3\ +x^2=x^5+x^2+x+1$, or [C]=[0100111].

And so on, the rest of the table is left as a homework. Note that the Hamming weight $w_i$ is found from the output codeword [C].

### b) Systematic Cyclic codes (Division):

The polynomial representation is also used here. The same method is used to choose the generator polynomial g(x) as in nonsystematic cyclic code. The procedure for the generation of (n,k) systematic cyclic code is as follows:

(1) Find D(x) from [D] as before.

(2) As before, select a generator polynomial g(x) of order r from the factorization table of $x^n+1$.

(3) The output codeword will be: $\boxed{C(x) = x^r\ D(x) + \mathrm{Re}\,m\,\frac{x^r\ D(x)}{g(x)}}$

where Rem is the remainder of the long division of $x^r$ D(x) by g(x).

(4) Use C(x) to find [C].

The output codeword [C] is now in systematic form since C(x) consists of two parts, the 1st is $x^r$ D(x) which is the same as information data bits shifted to the left by r positions. The 2nd is the remainder of the long division of $[x^r D(x)/g(x)]$ of order (r-1) which is the r LSB bits of the output codeword or the parity bits, hence:$[C]=[a_1\ a_2\ \ldots\ldots a_k\ c_1\ c_2\ldots\ldots c_r]$ which in systematic form.

**Example 6.2:**

Write down the code table for the (7,4) systematic cyclic code generated by the generator polynomial $g(x)=x^3+x^2+1$.

**Solution:**

Here n=7, k=4, r=3:

| o/p [C] | | | | | | | |
|---|---|---|---|---|---|---|---|
| i/p [D] | | | | | | | |
| $a_1$ | $a_2$ | $a_3$ | $a_4$ | $c_1$ | $c_2$ | $c_3$ | $w_i$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | --- |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 3 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 4 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 3 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 3 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 4 |
| 0 | 1 | 1 | 0 | | | | |
| 0 | 1 | 1 | 1 | | | | |
| 1 | 0 | 0 | 0 | | | | |
| 1 | 0 | 0 | 1 | | | | |
| 1 | 0 | 1 | 0 | | | | |
| 1 | 0 | 1 | 1 | | | | |
| 1 | 1 | 0 | 0 | | | | |
| 1 | 1 | 0 | 1 | | | | |
| 1 | 1 | 1 | 0 | | | | |
| 1 | 1 | 1 | 1 | | | | |

---for [D]=[0001], D(x)=1, $x^rD(x)=x^3$

$$\left.\begin{array}{r|l} & \quad 1 \\ \hline x^3+x^2+1 & x^3 \\ & x^3+x^2+1 \\ \cline{2-2} & \quad x^2+1 \end{array}\right\} \text{mod 2 add}$$

$(x^2+1)$ is the remainder and the long division stops since $x^2+1$ has an order less than r. Hence: $C(x)=x^3+x^2+1$, or $[C]=[\underbrace{0\,0\,0\,1}_{\text{Data}}\ \underbrace{1\,0\,1}_{\text{parity}}]$.

```
remainder since significant bits  ------------->  00010
are less then (r+1)
                                        take r bits as remainder
```

[C]=[0011010], check with previous code table.

for [D]=[0010], then divide [0010000] by [1101]

```
                                   1101 |0010000
                                          1101
                                          01010
                                           1101
remainder since significant bits  ------> 00111
are less then (r+1)
                                   take r bits as remainder
```

[C]=[0010111] as before(check with the code table).

Note:

Since the remainder is put as LSB of [C] then we expect that if [C] is divided by g(x) or [G], then the result is always [0].

Check the note by selecting any [C] from precious table and divide by [G]:

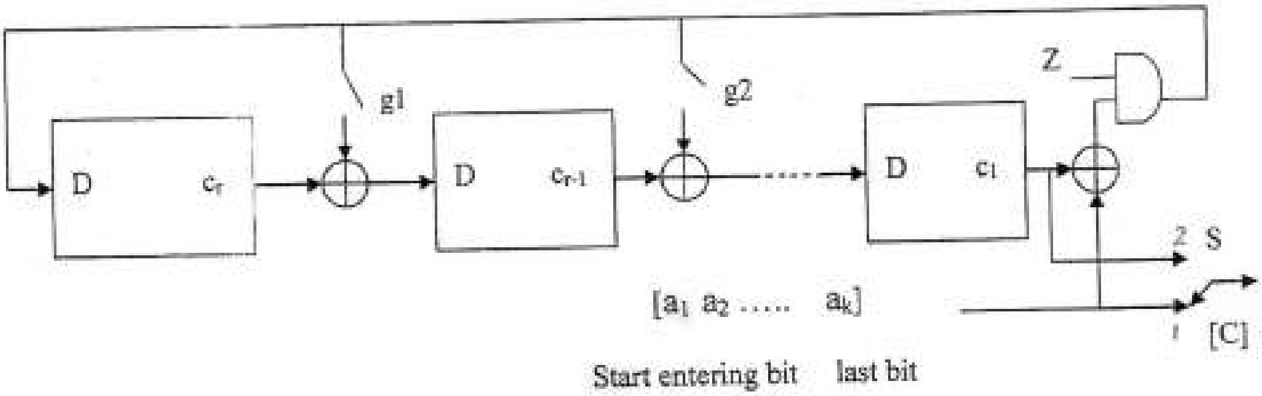
```
1101 |  0101110
         1101
         01101
          1101
          00000
```

## 6.3 Implementation of systematic cyclic encoder:

Practically, the previous long division required in long division is done using logic circuit that implements the division by g(x). In general, if:

$g(x)=g_o+g_1 x+g_2 x^2+........+g_r x^r$,

then we must note that for any factorization of $x^n+1$, $g_o=g_r=1$ always, hence only $g_1, g_2, \dots g_{r-1}$ is shown in the implementation below:



This logic circuit is called modular feedback shift register implemented using D-type flip-flop with synchronized master data clock (not shown).

**Circuit operation:**

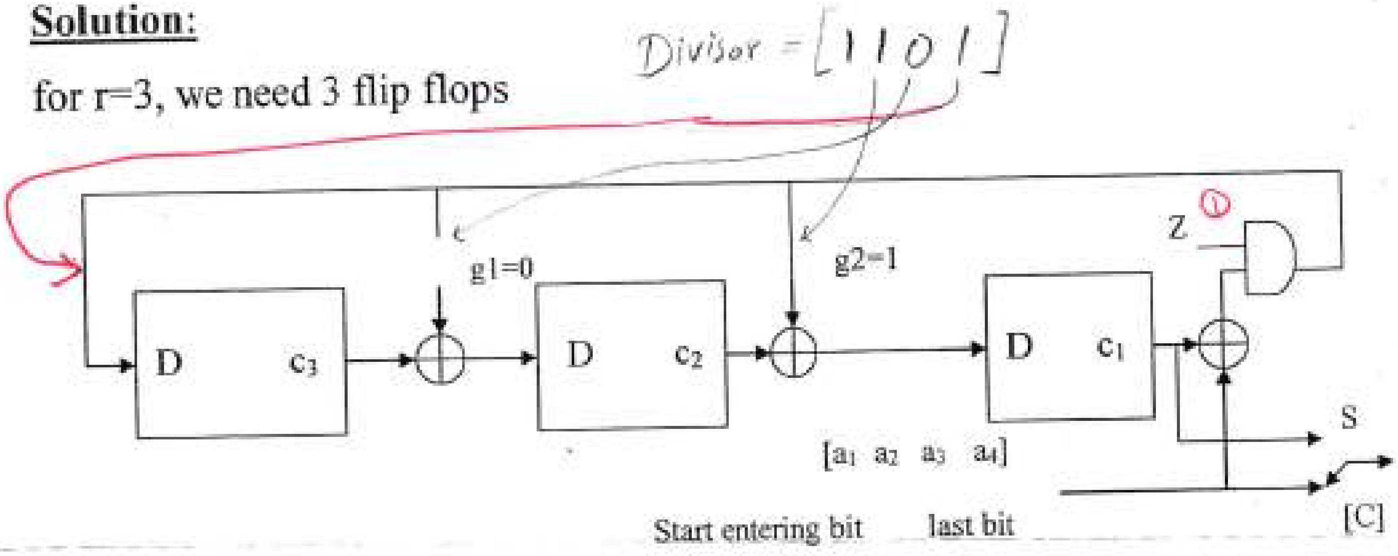
Switch S at position (1) giving the data bits to [C] output and at the same time for k clock pulses the control Z is enabled (Z=1) to feedback the content to the register to produce $c_1c_2\dots c_r$ bits at the end of the last k^th clock pulse. Then Z is disabled (Z=0) and switch S is changed to position (2) to shift out the **r** parity bits to [C] and at the same time **r** 0's will be fed back to the register to initialize the register to the next data block.

**Example 6.4:**

Using the encoder circuit, find the output codeword for systematic cyclic code with $g(x)=x^3+x^2+1$ for data words [D]=[0101] and [0010].

**Solution:**

for r=3, we need 3 flip flops



Here $g_1$=0, $g_2$=1 (note the Ex-OR gate for $g_1$ can be omitted).

First, we write the transition eqs for $c_3$, $c_2$, and $c_1$, i.e. we write the next state of them in terms of the present state and the input $a_i$ and this is done when the feedback is enabled by Z=1.

$c_3^+ = a_i + c_1^-$ where $c_3^+$ is the next state of $c_3$. and $c_1^-$ is the present state of $c_1$

$c_2^+ = c_3^-$ and

$c_1^+ = c_2^- + c_1^- + a_i = c_2^- + c_3^+$

For [D]=[0101] with always zero initial states, then:

| $a_i$ |
|---|
| 0 |
| 1 |
| 0 |
| 1 |

initial

| $c_3$ | $c_2$ | $c_1$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |
| 0 | 0 | 0 |
| 0 | 0 | 0 |

Then $c_1c_2c_3$=110 and [C]=[0101110] (check with the code table)

For [D]=[0010] with always zero initial states, then:

initial

| $a_i$ |
|---|
| 0 |
| 0 |
| 1 |
| 0 |

| $c_3$ | $c_2$ | $C_1$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 0 | 0 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |
| 0 | 0 | 0 |

Then $c_1c_2c_3$=111 and [C]=[0010111] ( check with the code table)

## 6.4 Decoding of systematic cyclic code:

At the receiver [R]=[C]+[E] where [C] is the transmitted codeword, [E] is the error word, writing above in polynomial form, then:

R(x)=C(x)+E(x)

Dividing both sides by g(x) taking the remainder, then:

$\mathrm{Re}\,m\frac{R(x)}{g(x)}=\mathrm{Re}\,m\frac{C(x)}{g(x)}+\mathrm{Re}\,m\frac{E(x)}{g(x)}$ and since $\mathrm{Re}\,m\frac{C(x)}{g(x)}=0$ from transmitter side, then:

$\boxed{\mathrm{Re}\,m\frac{R(x)}{g(x)}=\mathrm{Re}\,m\frac{E(x)}{g(x)}=s(x)}$ = syndrome polynomial of order (r-1).

Above syndrome equation shows that the same remainder you obtain if you divide R(x) by g(x) or E(x) by g(x).

1- if s(x)=0, then the receiver decides on no error.

2-if s(x)≠0, then errors occur. To find the location(s) of errors, the receiver may prepare a syndrome table and store it in its memory as a look up table, use it to find [E] from [s]. This look up syndrome table starts with most probable errors(less no of errors).

**Example 6.5:**

Prepare the syndrome table for the (7,4) systematic cyclic code with $g(x)=x^3+x^2+1$ for single error.

**Solution:**

[G]=[1101].

| Error word | [E] | | | | | | [s] | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |

No error

One error

2 errors

Each [s] is found from [E] by finding Rem[E(x)/g(x)]. For example if [E]=[0100000] which corresponds to a single error at the 2nd position from the left, then:

$$1101\overline{)\,0100000}$$

```
 1101
 01010
  1101
  01110
   1101
   0011
```

Hence [s]=[011], and so on

Note that no repeated syndromes are observed for single error. This is expected since $w_i(min)=3$ and the given (7,4) code is a single error correction. Note also that when you start to find the syndromes for double error say [E]=[0000011], then [s]=[011] which similar to a single error at the 2nd position(from the left), hence these two errors can not be corrected since the receiver will choose the most probable case of the single error. Try other more than one error pattern and find [s] and see that [s] obtained is similar to one of the single error case.

**Example 6.6:**

Using previous syndrome table, find the corrected word for the received word [R]=[1011001].

**Solution:**

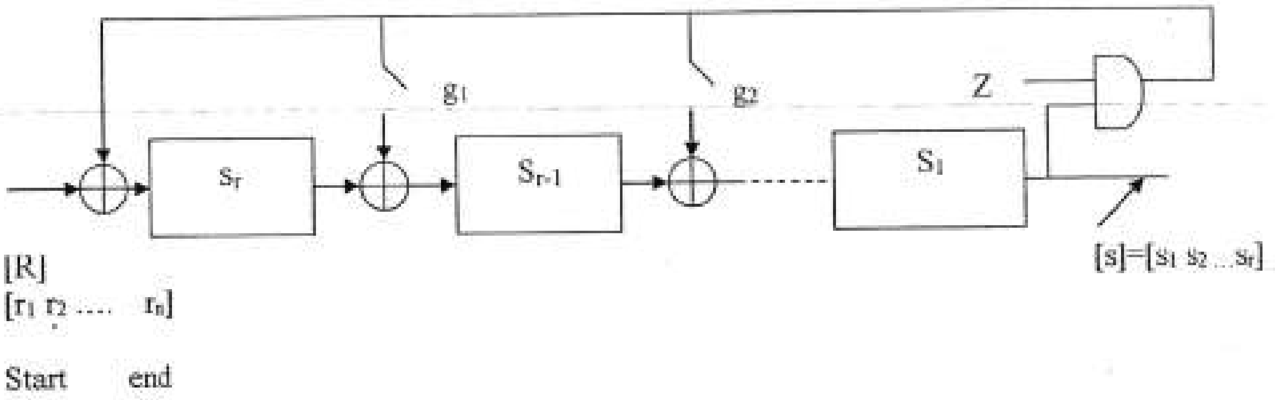
As soon as the receiver receives [R], then this [R] is divided by [G] to find [s] as the remainder of R(x)/g(x).

```
1101 | 1011001
       1101
       01100
        1101
        000101
```

hence, [s]=[101], using previous syndrome table and for [s]=[101], then and for single error, then [E]=[0001000], i.e. a single error at the 4th position from the left. Hence corrected [R] will be [1010001].

### 6.6 Implementation of systematic cyclic decoder:

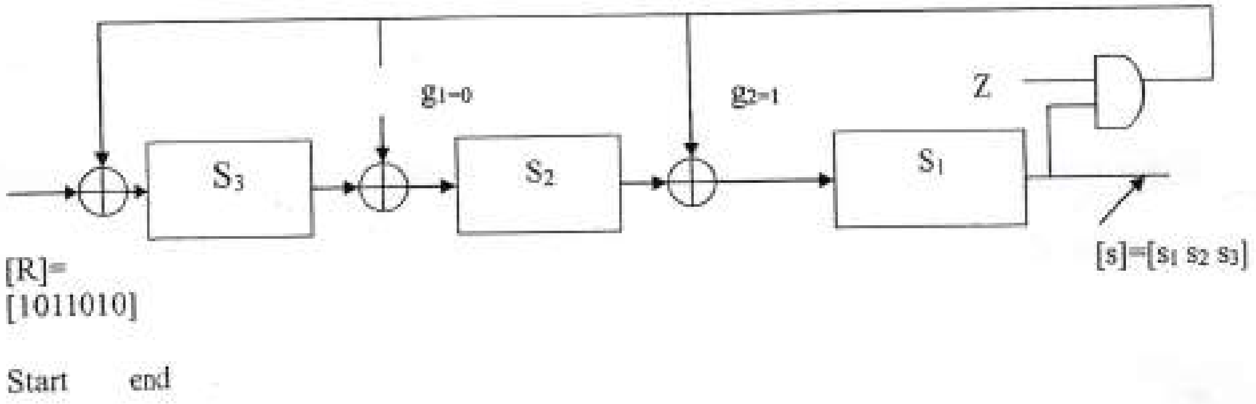
The long division of R(x) by g(x) to obtain the remainder is implemented using a modular feedback shift register as shown. The control Z is set (Z=1) for n clock pulses and reset (Z=0) for r clock pulses.



**Example 6.7:**
Use the decoder circuit to find the syndrome and hence correct the received word [R]=[1011010] for generator polynomial g(x)=$x^3+x^2+1$.

**Solution:**

Above circuit will be as shown for g(x)=$x^3+x^2+1$.



When Z=1, the transition eqs for s will be:

$s_3^+ = r_i + s_1^-$

$s_2^+ = s_3^-$

$s_1^+ = s_2^- + s_1^-$ for zero initial states, then:

| [R] |
|---|
| 1 |
| 0 |
| 1 |
| 1 |
| 0 |
| 1 |
| 0 |

| S3 | S2 | S1 | |
|---|---|---|---|
| 0 | 0 | 0 | ← initial |
| 1 | 0 | 0 | |
| 0 | 1 | 0 | |
| 1 | 0 | 1 | |
| 0 | 1 | 1 | |
| 1 | 0 | 0 | |
| 1 | 1 | 0 | |
| 0 | 1 | 1 | |

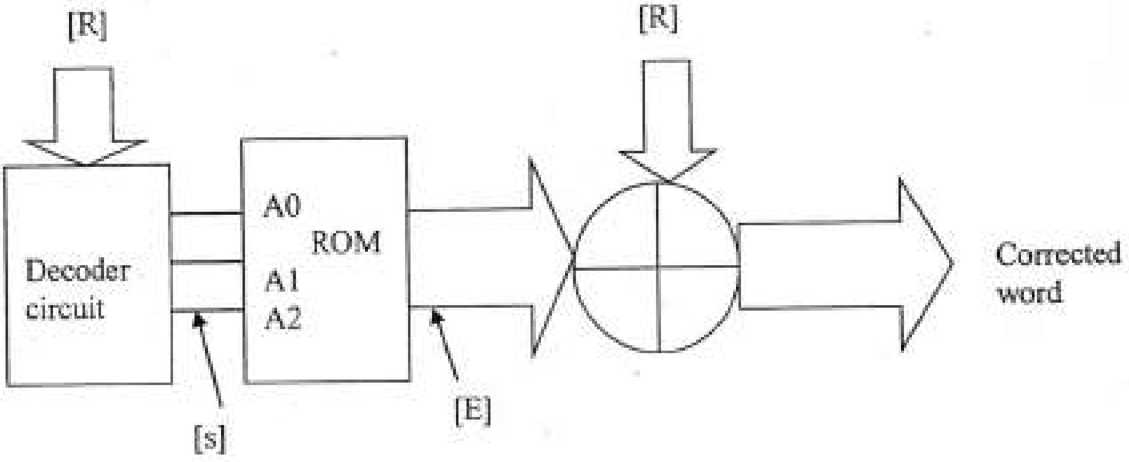
Then [s]=[$s_1$ $s_2$ $s_3$]=[110] and using previous syndrome table then: [E]=[1000000] single error at the 1st position from the left, i.e. corrected word will be [0011010].

**H.W 6.1:**

Repeat previous example for [R]=[1110110].

Note:

The complete circuit diagram of the systematic cyclic decoder that includes the syndrome generator logic circuit and the look up table that stores the syndrome table will be as shown:



## Chapter 6 Tutorial Problems

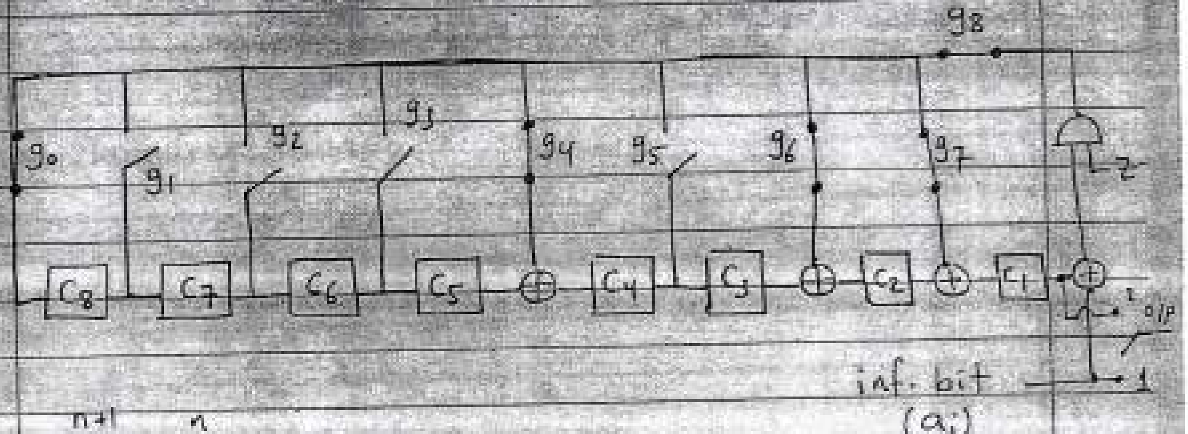
Q1. A (15,7) cyclic code has the generator polynomail
$g(x) = 1 + x^4 + x^6 + x^7 + x^8$
(a) use the encoder cct to find the o/p codeword for information word [1011011]
(b) Discuss error correction and detection capability of this code.

**Solution**

**Q1** (a)

$g(x) = 1 + x^4 + x^6 + x^7 + x^8$

$g_0 = 1,\ g_1 = g_2 = g_3 = 0,\ g_4 = 1,\ g_5 = 0,\ g_6 = g_7 = g_8 = 1$



$C_8^{n+1} = C_1^n + a_i$

$C_7^{n+1} = C_8^n$

$C_6^{n+1} = C_7^n$

$C_5^{n+1} = C_6^n$

$C_4^{n+1} = C_5^n + C_1^n + a_i = C_5^n + C_8^{n+1}$

$C_3^{n+1} = C_4^n$

$C_2^{n+1} = C_3^n + C_1^n + a_i = C_3^n + C_8^{n+1}$

$C_1^{n+1} = C_2^n + C_1^n + a_i = C_2^n + C_8^{n+1}$

| | $C_8$ | $C_7$ | $C_6$ | $C_5$ | $C_4$ | $C_3$ | $C_2$ | $C_1$ |
|---|---|---|---|---|---|---|---|---|
| $\alpha_i$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | $\boxed{1}$ | $\boxed{0}$ | $\boxed{1}$ | $\boxed{1}$ | $\boxed{0}$ | $\boxed{1}$ | $\boxed{1}$ | $\boxed{0}$ |

$\therefore$ o/p $= [C] = [\underbrace{1011011}_{\text{data}}\underbrace{01101101}_{\text{parity}}]$

(b) Hamming bound

$$2^r \geqslant \sum_{i=0}^{t} C_i^n \rightarrow 2^8 \geqslant \sum_{i=0}^{t} C_i^{15}$$

$$2^8 \geqslant C_0^{15} + C_t^{15}$$

$$256 \geqslant 1 + \frac{15!}{t!(15-t)!}$$

$$t!(15-t)! \geqslant \frac{15!}{255}$$

$t = 2$

$\therefore$ no. of correction errors $= \underline{\underline{2}}$

$d_{min} = 2t+1 = 2*2+1 = 5$

no. of detection errors $= d_{min} - 1$
$= \underline{\underline{4}}$

Q2: A cyclic code has the diviser 10100110111 is used to protect information in blocks of 5 bits. The encoded information is sent through channel having $Pe = 0.01$

(a) Discuss error correction and detection capability of the code

(b) Find the probability decoding erronous word.

## Solution

Q2 The divisor is $g(x)$. $g(x)$ has $r+1$ elements since the length of $g(x)$ is 11, then $r = 10$ bits

$K$ = length of information = 5 bits

$\therefore n = K + r = 15$ bits i.e $(15, 5)$ code

(a) using Hamming bound

$$2^r \geq \sum_{i=1}^{t} C_i^n$$

$$2^{10} \geq C_0^{15} + C_1^{15} + C_2^{15} + C_3^{15} + \dots$$

$$1024 \geq 1 + \frac{15!}{1! \times 14!} + \frac{15!}{2! \times 13!} + \frac{15!}{3! \times 12!} + \dots$$

$$1024 \geq \underbrace{\underbrace{\underbrace{1 + 15}_{16} + \overset{105}{\frac{15 \times 14}{2!}}}_{121} + \overset{455}{\frac{15 \times 14 \times 13}{3!}}}_{576} + \overset{1365}{}$$

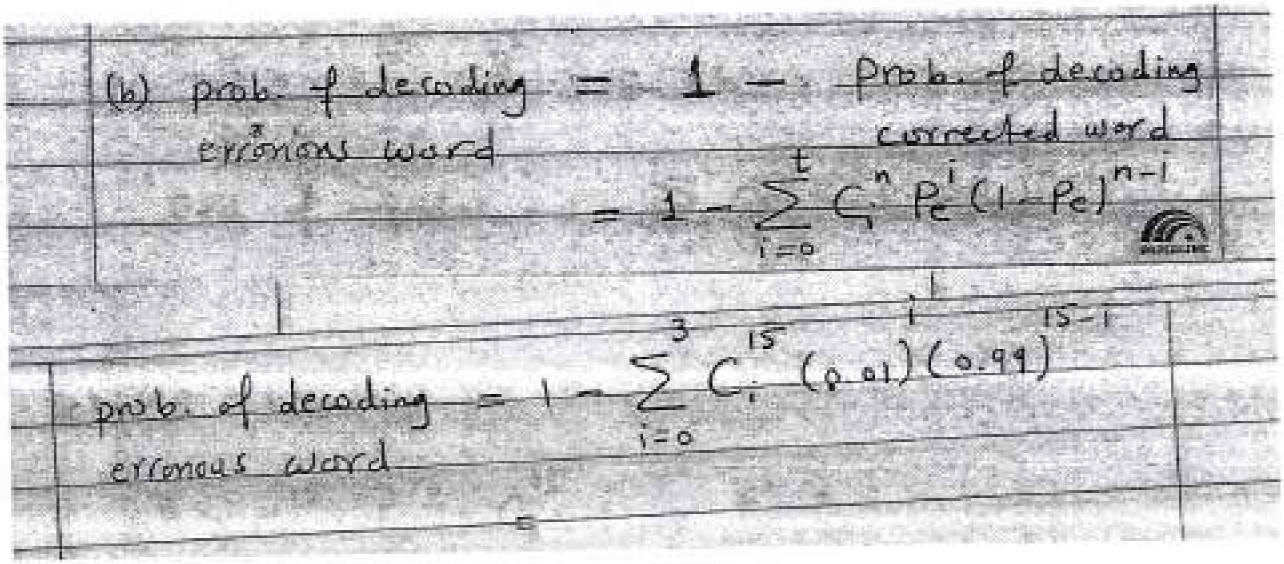
$$1024 \geq 560$$

$\therefore t = 3$

No of errors can be corrected = 3 errors

$d_{min} = 2t + 1 = 7$

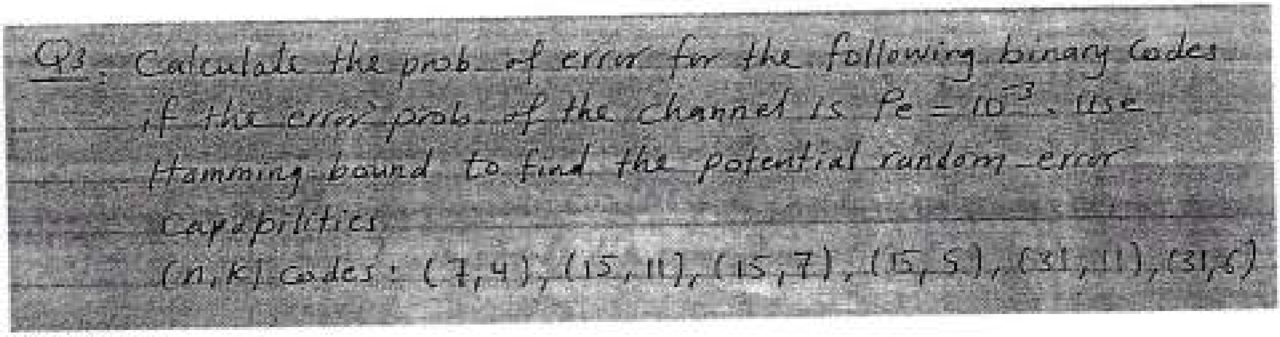
No. of errors can be detected = $d_{min} - 1$ = 6 errors



(b) prob. of decoding erronous word = 1 − Prob. of decoding corrected word

$$= 1 - \sum_{i=0}^{t} C_i^n P_e^i (1-P_e)^{n-i}$$

prob. of decoding erronous word $= 1 - \sum_{i=0}^{3} C_i^{15} (0.01)^i (0.99)^{15-i}$



Q3: Calculate the prob. of error for the following binary codes if the error prob. of the channel is $P_e = 10^{-3}$. Use Hamming bound to find the potential random-error capabilities.
(n, k) codes: (7,4), (15,11), (15,7), (15,5), (31,11), (31,6)

**Solution**

**Q3** $P_e = 10^{-3}$ & by using Hamming Bound $2^r \geqslant \sum_{i=0}^{t} C_i^n$

(a) (7,4) code $\longrightarrow r = 7-4 = 3$

$$2^3 \geqslant \sum_{i=0}^{t} C_i^7 \rightarrow 8 \geqslant C_0^7 + C_1^7$$

$\therefore t = 1$ (one error correction)

$\therefore$ prob. of erroneous $= 1 - \sum_{i=0}^{1} C_i^7 P_e^1 (1-P_e)^{n-1}$

<u>hint</u>

when $P_e \ll 10^{-2}$

Prob. of erroneous word $\simeq P_e(t+1)$

$\therefore$ Prob. of erroneous word $= P_e(t+1) = 10^{-3}(2) = 2 \times 10^{-3}$

(b) (15,11) code $\longrightarrow r = 15-11 = 4$

$$2^4 \geqslant C_0^{15} + C_1^{15} \rightarrow t = 1$$

Prob. of erroneous $= 1 - \sum_{i=0}^{t} C_i^n P_e^i (1-P_e)^{n-i}$

(c) (15,7) Code $\Rightarrow r = 15-7 = 8$

$$2^8 \geqslant C_0^{15} + C_1^{15} + C_2^{15} \Rightarrow t = 2$$

Prob. of erroneous $= 1 - \sum_{i=0}^{t} C_i^n Pe^i (1-Pe)^{n-i}$

(d) (15,5) Code $\Rightarrow r = 15-5 = 10$

$$2^{10} \geqslant C_0^{15} + C_1^{15} + C_2^{15} + C_3^{15} \Rightarrow t = 3$$

prob. of erroneous $= 1 - \sum_{i=0}^{t} C_i^n Pe^i (1-Pe)^{n-i}$

(e) (31,11) Code $\Rightarrow r = 31-11 = 20$

$$2^{20} \geqslant C_0^{31} + C_1^{31} + C_2^{31} + C_3^{31} + C_4^{31} + C_5^{31} + C_6^{31}$$

$\Rightarrow t = 6$

prob. of erroneous word $= 1 - \sum_{i=0}^{t} C_i^n Pe^i (1-Pe)^{n-i}$

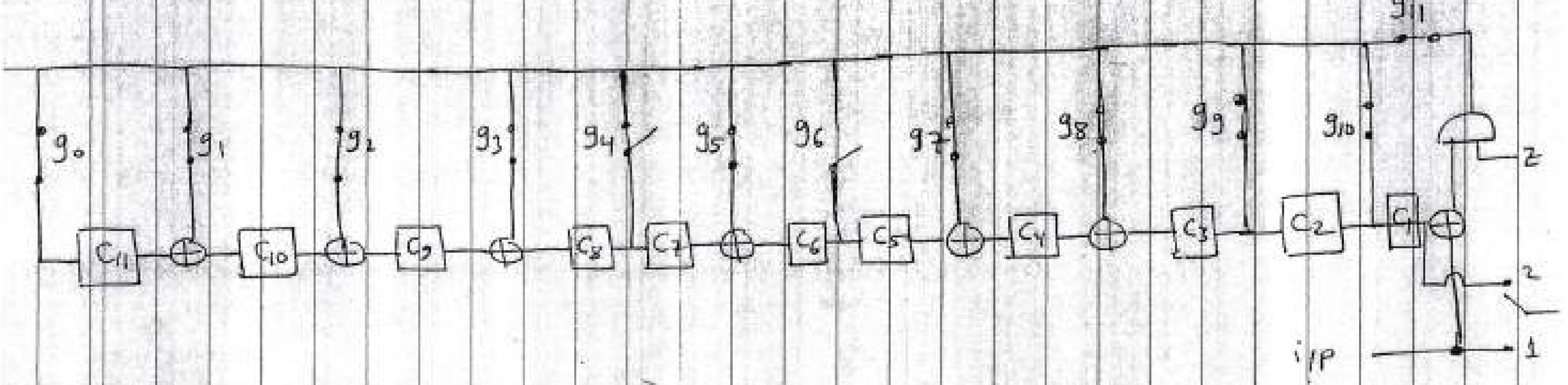
Q4:- A cyclic Code can be implemented by the parity check polynomail $h(x)$ of order $k$ and can be obtained by $h(x) = \frac{X^n+1}{g(x)}$ where $g(x)$ is the generator polynomial of the Code. Find the parity check polynomial $h(x)$ of a (15,11) Cyclic Code having $g(x) = X^4+X+1$. Implement $h(x)$ as a k-stage shift register initially loaded with the k-information bits then n clock pulses are used to produce the code word.

## Solution

Q4 $h(x) = \frac{X^n+1}{g(x)} = \frac{X^{15}+1}{X^4+X+1}$

$$
\begin{array}{r|l}
 & X^{11}+X^8+X^7+X^5+X^3+X^2+X+1 \\
\hline
X^4+X+1 & X^{15}+1 \\
 & \underline{X^{15}+X^{12}+X^{11}} \\
 & X^{12}+X^{11}+1 \\
 & \underline{X^{12}+X^9+X^8} \\
 & X^{11}+X^9+X^8+1 \\
 & \underline{X^{11}+X^8+X^7} \\
 & X^9+X^7+1 \\
 & \underline{X^9+X^6+X^5} \\
 & X^7+X^6+X^5+1 \\
 & \underline{X^7+X^4+X^3} \\
 & X^6+X^5+X^4+X^3+1 \\
 & \underline{X^6+X^3+X^2} \\
 & X^5+X^4+X^2+1 \\
 & \underline{X^5+X^2+X} \\
 & X^4+X+1 \\
 & \underline{X^4+X+1} \\
 & 0
\end{array}
$$

$\therefore h(x) = X^{11}+X^8+X^7+X^5+X^3+X^2+X+1$


g11
g0
g1
g2
g3
g4
g5
g6
g7
g8
g9
g10
C11
C10
C9
C8
C7
C6
C5
C4
C3
C2
C1
z
2
1
i/p

**Q5:** Consider a single-error correcting code for 4-bit message bits. How many check bits are required?

**Solution**

**Q5**

$t=1$ , $K=4$

(a) Hamming bound

$$2^r \geqslant \sum_{i=0}^{t} C_i^{n}$$

$$2^r \geqslant \sum_{i=0}^{1} C_i^{4+r}$$

$$2^r \geqslant C_0^{4+r} + C_1^{4+r}$$

$$2^r \geqslant 1+(4+r)$$

$$\Rightarrow 2^r \geqslant 5+r \Rightarrow r=3$$

$n=K+r=4+3 \Rightarrow (7,4)$ code

**Q6:** Consider the (7,3) code with $g(x)=x^4+x^3+x^2+1$

(a) Construct code table and minimum Hamming weight

(b) use Hamming bound and find the error correction capability

(c) Implement the encoder using $g(x)$ polynomial

## **Solution**

encoder o/p

(7,3) code

**Q6**

| information | | | Parity check bits | | | | |
|---|---|---|---|---|---|---|---|
| $a_1$ | $a_2$ | $a_3$ | $c_1$ | $c_2$ | $c_3$ | $c_4$ | $\omega_i$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | – |
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 4 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 4 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 4 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 4 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 4 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 4 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 | 4 |

$g(x) = x^4 + x^3 + x^2 + 1$

①

```
11101 | 001 0000   r=4
          11101
          -----
           1101
```

②

```
11101 | 010 0000
          11101
          -----
          11010
          11101
          -----
          00111
```

③

```
11101 | 011 0000
         11 101
         ------
           1010
```

④

```
11101 | 100 0000
        11101
        -----
         110100
         11101
         -----
          1110
```

⑤

```
11101 | 1010000
        11101
        -----
         100100
         11101
         -----
          11110
          11101
          -----
          00011
```

⑥

```
11101 | 110 0000
        11101
        -----
         10100
         11101
         -----
          1001
```

⑦

$$11101 \overline{)\,1110000}$$
$$\frac{11101}{\underline{0100}}$$

يمكن ايجاد C(x) بطريقة ثانية

$C(x) - x^r D(x) + \text{Rem}\left[\frac{x^r D(x)}{g(x)}\right]$

أو باستخدام خاصية الترميز

from table $d_{min} = 4$ (by calculating $d_{ij}$ for all codes)

$t = \text{Int}\left(\frac{d_{min}-1}{2}\right) = \text{Int}\left(\frac{4-1}{2}\right)$

$= \text{Int}\left(\frac{3}{2}\right) = 1$

(b)

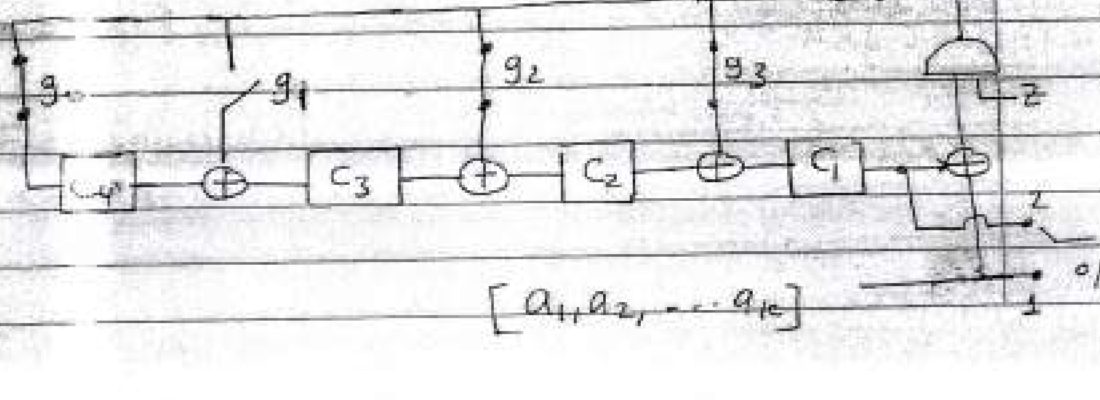
$2^r \geqslant \sum_{i=0}^{t} C_i^n$

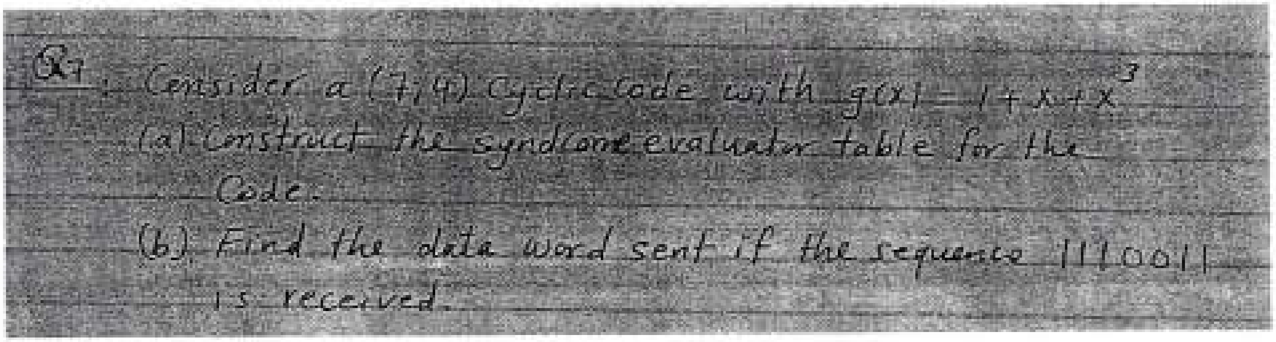
$2^4 \geqslant \sum_{i=0}^{t} C_i^7$

$2^r \geqslant C_0^7 + C_1^7 + \cancel{C_2^7}$

$2^r \geqslant C_0^7 + C_1^7$ ok $\Rightarrow t=1$

(c)





Q7. Consider a (7,4) Cyclic code with $g(x) = 1 + x + x^3$

(a) Construct the syndrome evaluator table for the Code.

(b) Find the data word sent if the sequence 1110011 is received.

**Solution**

Q7

(a) $E =$ 0010000] $\longrightarrow s = [000]$

$E =$ 100 000]

$s =$ 10'|

$$x^3+x+1$$
$$x^3+x+1 \overline{)\, x^6}$$
$$\underline{x^6+x^4+x^3}$$
$$x^4+x^3$$
$$\underline{x^4+x^2+x}$$
$$x^3+x^2+x$$
$$\underline{x^3+x+1}$$
$$x^2+1 \Rightarrow [101]$$

$\bar{E} =$ 0100000]

$s =$ [111]

$$x^2+1$$
$$x^3+x+1 \overline{)\, x^5}$$
$$\underline{x^5+x^3+x^2}$$
$$x^3+x^2$$
$$\underline{x^3+x+1}$$
$$x^2+x+1 \Rightarrow [111]$$

$\bar{E} =$ [00 0000]

$s =$ [110]

$$x$$
$$x^3+x+1 \overline{)\, x^4}$$
$$\underline{x^4+x^2+x}$$
$$x^2+x \Rightarrow [110]$$

$E =$ 0001000]

$s =$ [011]

$$1$$
$$x^3+x+1 \overline{)\, x^3}$$
$$\underline{x^3+x+1}$$
$$x+1 \Rightarrow [011]$$

$E =$ [0000100]

$s$ [100]

$$x^3+x+1 \overline{)\, x^2}$$
$$\Rightarrow [100]$$

$\bar{E} = [0000010]$ $\qquad x^3+x+1 \overline{)\, x}$

$s = [010]$ $\qquad \Rightarrow [010]$

$\bar{E} = [0000001]$ $\qquad x^3+x+1 \overline{)\, 1}$

$s = [001]$ $\qquad \Rightarrow [001]$

(a)

| $\bar{E}$ vector | $s = \text{Rem}\,[E(x)/g(x)]$ |
|---|---|
| 0000000 | 000 |
| 1000000 | 101 |
| 0100000 | 111 ← |
| 0010000 | 110 |
| 0001000 | 011 |
| 0000100 | 100 |
| 0000010 | 010 |
| 0000001 | 001 |

(b) $s(x) = \text{Rem}\left[\frac{R(x)}{g(x)}\right]$

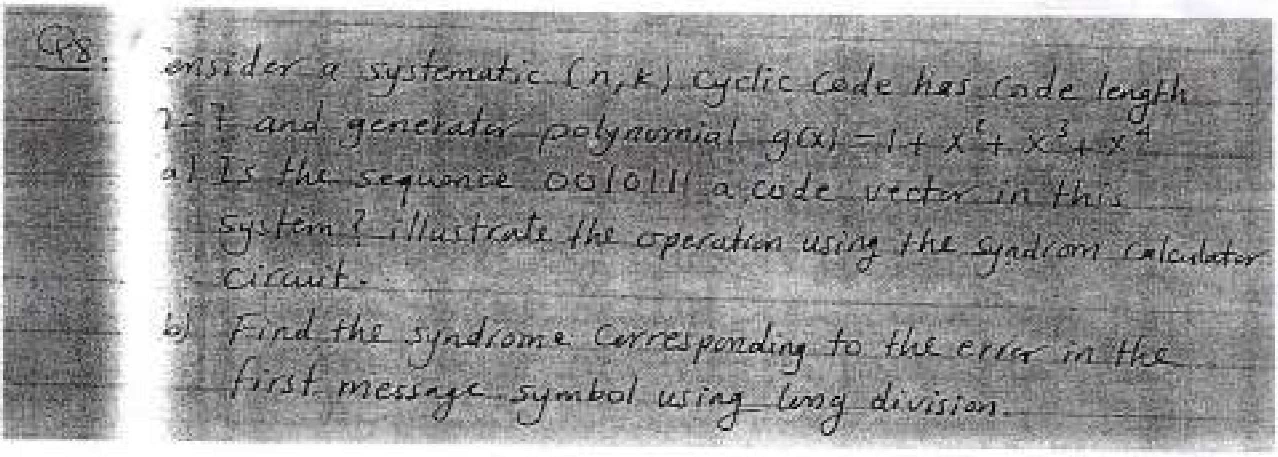
$R(x) = x^6 + x^5 + x^4 + x + 1$

$$\begin{array}{r} x^3+x^2 \\ x^3+x+1 \overline{)\, x^6+x^5+x^4+x+1} \\ x^6+x^4+x^3 \\ \hline x^5+x^3+x+1 \\ x^5+x^3+x^2 \\ \hline x^2+x+1 \Rightarrow [111] \end{array}$$

$s = [111]$

This means that the 6th bit is received in error

The corrected received vector $= [\,1\underline{0}10011\,]$



Q8. onsider a systematic $(n,k)$ cyclic code has code length $n=7$ and generator polynomial $g(x)=1+x^2+x^3+x^4$

a) Is the sequence 0010111 a code vector in this system? illustrate the operation using the syndrom calculator circuit.

b) Find the syndrome corresponding to the error in the first message symbol using long division.

**Solutio**