SOLUTIONS FOR CHAPTER 1

Q.1.1 DMS with source probabilities : {0.30 0.25 0.20 0.15 0.10}

Entropy $H(X) = \sum_i p_i \log \frac{1}{p_i}$

$= 0.30 \log 1/0.30 + 0.25 \log 1/0.25 + \ldots\ldots\ldots\ldots$

$= 2.228$ bits

Q.1.2 Define $D(p||q) = \sum_i p_i \log \frac{q_i}{p_i}$ (1)

p_i, q_i – probability distributions of discrete source X.

$$D(p||q) = \sum_i p_i \log \frac{q_i}{p_i} \leq \sum_i P_i \left(\frac{q_i}{p_i} - 1 \right) \quad \text{[using identity ln x} \leq \text{x} - 1\text{]}$$

$$= \sum_i (q_i - p_i) = 0$$

$\therefore D(p||q) \geq 0$

Put $q_i = 1/n$ in (1) where n = cardinality of the distance source.

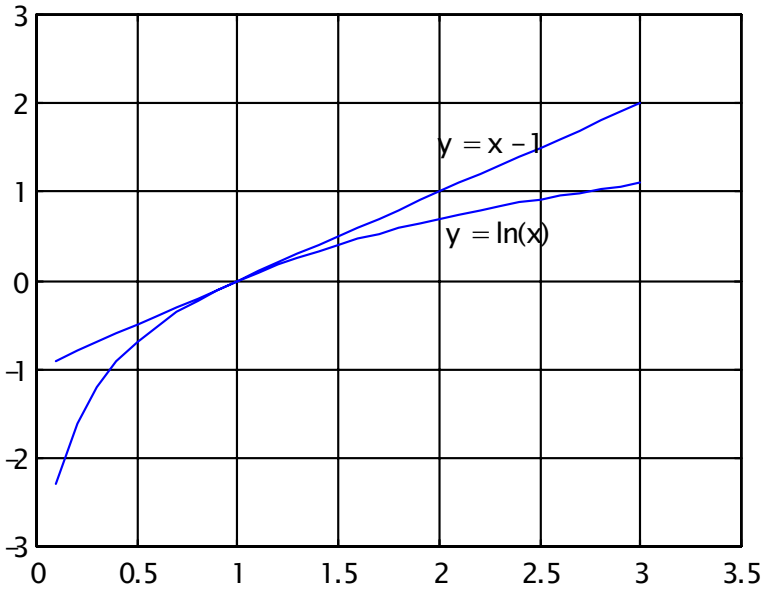
$$D(p||q) = \sum_i p_i \log p_i + \sum_i p_i \log n$$

$$= \sum_i p_i \log p_i + \log n = -H(X) + \log n \geq 0$$

$$-H(X) \leq \log n$$

$H(X)$ = log n for uniform probability distribution. Hence proved that entropy of a discrete source is maximum when output symbols are equally probable. The quantity $D(p||q)$ is called the Kullback-Leibler Distance.

Q. 1.3 The plots are given below:



Q 1.4 Consider two probability distributions: $\{p_0, p_1, , p_{K-1}\}$ and $\{q_0, q_1, , q_{K-1}\}$.

We have $\sum_{k=0}^{K-1} p_k \log_2\left(\frac{q_k}{p_k}\right) = \frac{1}{\ln 2}\sum_{k=0}^{K-1} p_k \ln\left(\frac{q_k}{p_k}\right)$. Use $\ln x \le 1 - x$,

$$\sum_{k=0}^{K-1} p_k \log_2\left(\frac{q_k}{p_k}\right) \le \frac{1}{\ln 2}\sum_{k=0}^{K-1} p_k\left(\frac{q_k}{p_k} - 1\right)$$

$$\le \frac{1}{\ln 2}\sum_{k=0}^{K-1}(q_k - p_k)$$

$$\le \frac{1}{\ln 2}\left(\sum_{k=0}^{K-1} q_k - \sum_{k=0}^{K-1} p_k\right) = 0$$

Thus, $\sum_{k=0}^{K-1} p_k \log_2\left(\frac{q_k}{p_k}\right) \le 0$. (1)

Now, $I(X; Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j)\log\frac{P(x_i, y_j)}{P(x_i)P(y_j)}$ (2)

From (1) and (2) we can conclude (after basic manipulations) that $I(X;Y) \ge 0$. The equality holds if and only if $P(x_i, x_j) = P(x_i)P(x_j)$, i.e., when the input and output symbols of the channel are statistically independent.

Q.1.5 Source X has infinitely large set of outputs $P(x_i) = 2^{-i}$, $i = 1, 2, 3, \ldots\ldots$

$$H(X) = \sum_{i=1}^{\infty} p(x_i) \log \frac{1}{p(x_i)} = \sum_{i=1}^{\infty} 2^{-i} \log 2^{-i}$$

$$= \sum_{i=1}^{\infty} i.2^{-i} = 2 \text{ bits}$$

Q.1.6 Given: $P(x_i) = p(1-p)^{i-1}$ $\quad i = 1, 2, 3, \ldots\ldots..$

$$H(X) = -\sum_i p(1-p)^{i-1} \log\left\{p(1-p)^{i-1}\right\}$$

$$= -\sum_i p(1-p)^{i-1} \left\{\log p + (i-1) \log(1-p)\right\}$$

$$= -p \log p \sum_{i=1} p(1-p)^{i-1} - p \log(1-p) \sum_i (i-1)(1-p)^{i-1}$$

$$= -p \log p \times \frac{1}{p} - p \log(1-p) \times \frac{1-p}{p^2}$$

$$= -\log p - \left(\frac{1-p}{p}\right) \log(1-p) = \frac{p \log p - (1-p)\log(1-p)}{p} = \frac{1}{p} H(p) \text{ bits}$$

Q 1.7 Hint: Same approach as the previous two problems.

Q 1.8 Yes it is uniquely decodable code because each symbol is coded uniquely.

Q 1.9 The relative entropy or Kullback Leibler distance between two probability mass functions $p(x)$ and $q(x)$ is defined as

$$D(p \| q) = \sum_{x \in X} p(x) \log\left(\frac{p(x)}{q(x)}\right). \tag{1.76}$$

(i) Show that $D(p \| q)$ is non negative.

Solution: $-D(p \| q) = -\sum_{x \in X} p(x) \log\left(\frac{p(x)}{q(x)}\right) = \sum_{x \in X} p(x) \log\left(\frac{q(x)}{p(x)}\right)$

$$\leq \log \sum_{x \in X} p(x) \frac{q(x)}{p(x)} \text{ (from Jensen's Inequality: } Ef(X) \geq f(EX))$$

$$= \log \sum_{x \in X} q(x) = \log(1) = 0.$$

Thus, $-D(p \| q) \leq 0$ or $D(p \| q) \geq 0$.

(ii) $D(p \| q) = \sum p(x) \log \frac{p(x)}{q(x)}$

Symmetry Property:

$D(p \| q) = D(q \| p)$

$\sum p(x) \log \frac{p(x)}{q(x)} = \sum q(x) \log \frac{q(x)}{p(x)}$

$\sum p(x) \log p(x) - \sum p(x) \log q(x) \neq \sum q(x) \log q(x) - \sum q(x) \log p(x)$

Therefore Kullback Leibler distance does not follow symmetry property.

Triangle Inequality:

$D(p \| q) + D(q \| r) \geq D(p \| r)$

$\sum p(x) \log \frac{p(x)}{q(x)} + \sum q(x) \log \frac{q(x)}{r(x)} \geq \sum p(x) \log \frac{p(x)}{r(x)}$

On solving this we get

$\sum (-p(x) + q(x)) \log \frac{q(x)}{r(x)} \geq 0$

This relation does not hold if $p(x) > q(x)$.

Therefore Kullback Leibler distance does not follow triangle inequality property.

(iii) $I(X;Y) = \sum p(x,y) I(x;y)$

$= \sum p(x,y) \frac{\log(x,y)}{\log p(x) p(y)}$

$= D(p(x,y) \| p(x)p(y))$

Q.1.10

a) Compute the entropy of this source.

The entropy is

$$-0.4999999 \log_2(0.4999999) - 0.4999999 \log_2(0.4999999) - 0.0000002 \log_2(0.0000002) = 1.000004539$$

b) Find an optimal code for this source, and compute its expected codeword length.

One optimal code is the following:

$$a_1 : 0$$
$$a_2 : 10$$
$$a_3 : 11$$

Its expected codeword length is

$$0.4999999 \times 1 + 0.4999999 \times 2 + 0.0000002 \times 2 = 1.5000001$$

c) Find an optimal code for the second extension of this source (ie, for blocks of two symbols), and compute its expected codeword length, and the expected codeword length divided by two.

Here is one optimal code:

$$\begin{aligned}
(a_1, a_1) &: 00 \\
(a_1, a_2) &: 01 \\
(a_2, a_1) &: 10 \\
(a_2, a_2) &: 110 \\
(a_1, a_3) &: 11100 \\
(a_2, a_3) &: 11101 \\
(a_3, a_1) &: 11110 \\
(a_3, a_2) &: 111110 \\
(a_3, a_3) &: 111111
\end{aligned}$$

Its expected codeword length is approximately 2.2500012, which divided by two is approximately 1.1250006.

d) Prove (without any tedious calculations) that in order to compress to within 1% of the entropy by encoding blocks of size N from this source, N will have to be at least 5.

When N is less than 5, the 2^N blocks in which all symbols are either a_1 or a_2 will be much more probable than all other blocks. An optimal code for the N-th extension will assign codewords of length N to all but one of these high-probability blocks, and a codeword of length $N+1$ to the remaining high-probability block. (Other blocks will have codewords of length greater than $N+1$. The expected codeword length for such a code will be greater than

$$N \times (2^N - 1) \times 0.4999999^N + (N+1) \times 0.4999999^N \;=\; N \times 2^N \times 0.4999999^N + 0.4999999^N$$

The expected codeword length divided by N will be greater than $2^N \times 0.4999999^N + 0.4999999^N/N$. For $N = 1$, $N = 2$, $N = 3$, and $N = 4$, the values of this expression are 1.4999997, 1.1249996, 1.0416660, and 1.0156242. The entropy plus 1% is 1.0100046. Since the expected codeword length divided by N is greater than this for $N < 5$, a block size of at least five will be needed to compress to within 1% of the entropy.

Q.1.11 The codeword lengths are possible if and only if they satisfy Kraft-McMillan inequality, which in this case is

$$\frac{1}{2^3} + \frac{1}{2^3} + \frac{1}{2^3} + \frac{d}{2^8} \le 1$$

$$\frac{d}{256} \le \frac{5}{8}$$

$$d \le 160$$

Q. 1.12 First note that it is a discrete random variable with a valid probability distribution, since $\sum_n P_n = \sum_{n=2}^{\infty} \frac{1}{An\log^2 n} = 1$.

However, $H(X) = \sum_n -P_n \log P_n = +\infty$ (the series does not converge!).

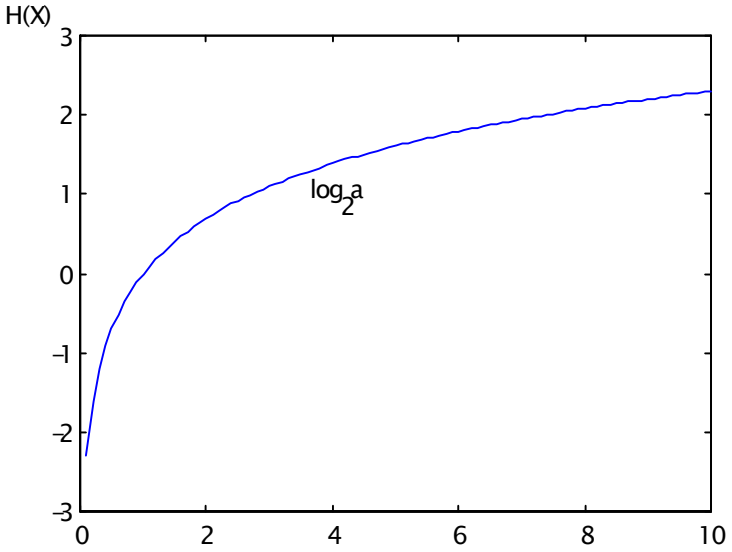
Thus the entropy of a discrete random variable can also be infinite.

Q.1.13 $P(x) = \begin{cases} a^{-1} & 0 \le x \le a \\ 0 & otherwise \end{cases}$

Differential entropy $= -\int_0^a p(x)\log\ p(x)\,dx$

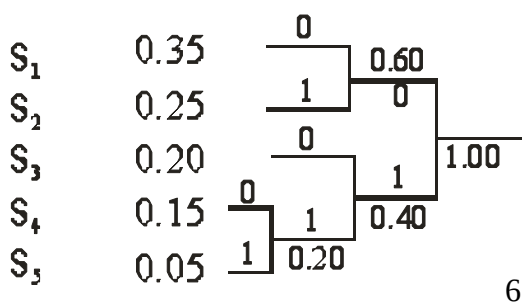
$$= -\int_0^a \frac{1}{a}\log a\,dx\ = \log_2 a$$

The plot is given below. Note that the differential entropy can be negative.



Q.1.14 DMS with source probabilities {0.35, 0.25, 0.20, 0.15, 0.05}

(i) Huffman code



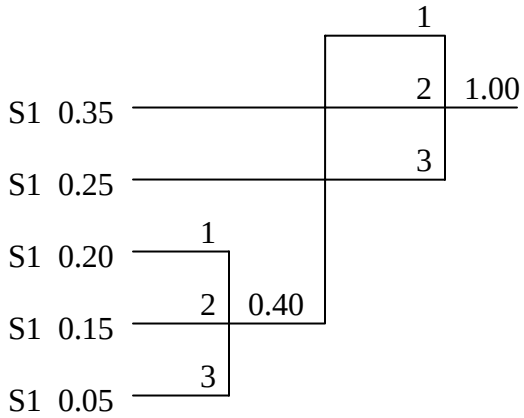
	Codes
S_1	00
S_2	01
S_3	10
S_4	110
S_5	111

(ii) $\overline{R} = \sum_i p_i l_i = 0.35 \times 2 + 0.25 \times 2 + 0.20 \times 2 + 0.15 \times 3 + 0.05 \times 3 = 2.2$ bits.

(iii) $\eta = \dfrac{H(X)}{\overline{R}}$ $\quad H(X) = \sum p_i \log \dfrac{1}{p_i} = 2.121$

$$\eta = \frac{2.121}{2.2} = 0.964 = 96.4\% .$$

Q.1.15 (i)



	Codes
S1	2
S2	3
S3	11
S4	12
S5	13

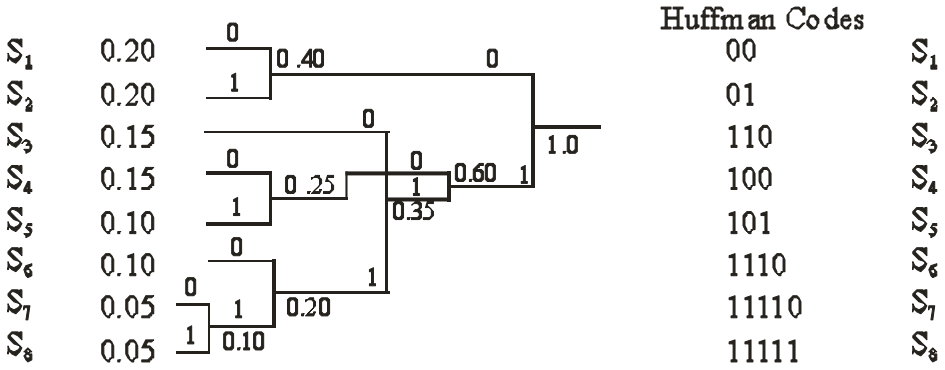
(ii) $\overline{R} = \sum_i p_i l_i = 0.35 + 0.25 + 0.20 \times 2 + 0.15 \times 2 + 0.05 \times 2 = 1.40$ ternary digits/ symbol

Q.1.16 (i) DMS with source probabilities :

Symbols	Prob.	Efficient fixed length code
S_1	0.20	000
S_2	0.20	001
S_3	0.15	010
S_4	0.15	011
S_5	0.10	100
S_6	0.10	101
S_7	0.05	110
S_8	0.05	111

Average code length = $\overline{R} = \sum_{k=1}^{L} n(x_k)P(x_k) = 3$

(ii) Huffman code



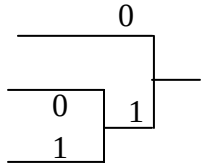
$$\overline{R} = \sum_{k=1}^{L} n(x_k)P(x_k) = 2.9 \text{ bits.}$$

(iii) The entropy $H(X) = -\sum_{i=1}^{n} P(x_i)\log P(x_i) = 2.8464$ bits

Huffman code gives shorter code length ($\eta = 98.15\%$)

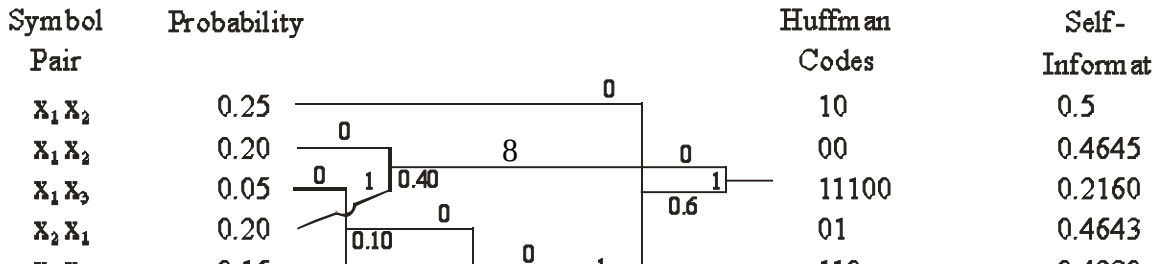
Q.1.17

Symbol	Probability	Self information	Code
x_1	0.5	0.5	0
x_2	0.4	0.528	10
x_3	0.1	0.332	11



$H(X) =$ 1.36 bits / symbol pair
$\overline{R}_1 =$ 1.5 bits / symbol pair
$\eta =$ 90.66 %

(ii)



$H(X)$ = 2.72 bits / symbol pair

$\overline{R}_2$ = 2.78 bits / symbol pair

η = 97.84 %

Symbol Triple	Self Information	Huffman Codes	Probability
$x_1\ x_1\ x_1$	0.375	000	0.125
$x_1\ x_1\ x_2$	0.3322	110	0.1
$x_1\ x_2\ x_1$	0.3322	100	0.1
$x_2\ x_1\ x_1$	0.3322	101	0.1
$x_1\ x_2\ x_2$	0.2915	0100	0.08
$x_2\ x_1\ x_2$	0.2915	0110	0.08
$x_2\ x_2\ x_1$	0.2915	0111	0.08
$x_2\ x_2\ x_2$	0.2538	0010	0.064
$x_1\ x_1\ x_3$	0.1330	11100	0.025
$x_1\ x_3\ x_1$	0.1330	11101	0.025
$x_3\ x_1\ x_1$	0.1330	010100	0.025
$x_1\ x_2\ x_3$	0.11287	010101	0.02
$x_1\ x_3\ x_2$	0.11287	010110	0.02
$x_2\ x_3\ x_1$	0.11287	010111	0.02
$x_2\ x_1\ x_3$	0.11287	001100	0.02
$x_3\ x_1\ x_2$	0.11287	001101	0.02
$x_3\ x_2\ x_1$	0.11287	001110	0.02
$x_2\ x_2\ x_3$	0.09545	111100	0.016
$x_2\ x_3\ x_2$	0.09545	111101	0.016
$x_3\ x_2\ x_2$	0.09545	111110	0.016
$x_1\ x_3\ x_3$	0.0382	1111110	0.005
$x_3\ x_1\ x_3$	0.0382	1111111	0.005
$x_3\ x_3\ x_1$	0.0382	00111110	0.005
$x_2\ x_3\ x_3$	0.03186	00111100	0.004
$x_3\ x_2\ x_3$	0.03186	00111101	0.004
$x_3\ x_3\ x_2$	0.03186	001111110	0.004
$x_3\ x_3\ x_3$	0.00996	001111111	0.001

$H(X)$ = 4.0826 bits / triple

$\overline{R}_2$ = 4.118 bits / symbol triple

$$\eta = \frac{H(X)}{\overline{R}_3} = 99.14\%$$

Q.1.18 For a B-symbol block $x_1\ x_2\ \ldots\ldots\ x_B$,

$$H(x_1\ x_2\ \ldots\ldots\ x_B) = -\sum_{j_1=1}^{n}\sum_{j_2=1}^{n} - \sum_{j_B=1}^{n} p(x_{j_1}\ x_{j_2}\ldots..\ x_{j_B})\ \log p(x_{j_1}\ x_{j_2}\ldots...x_{j_B})$$

$P(x_1\ x_2\ \ldots..\ x_B) = p(x_1)\ p(x_2|\ x_1)\ p(x_3|\ x_1\ x_2)\ \ldots\ldots\ p(x_B|x_1\ x_2\ \ldots.\ x_{B-1})$

Assuming the B r, vs to be statistically independent

$\therefore\ H(x_1\ x_2\ \ldots\ldots\ x_B) = H(x_1) + H(x_2) + \ldots.. + H(x_B)$

$= BH(X)$

Q 1.19 Hint: Apply equation 1.27.

Q.1.20 Lempel Ziv Code for

0100111110010100000101010110011000 0

Parsing 0,1,00,11,111,001,01,000,0010,10,101,100,110

gives

Dictionary	Dictionary Location	Contents	Codeword
1	0001	0	00000
2	0010	1	00001
3	0011	00	00010
4	0100	11	00101
5	0101	111	01001
6	0110	001	00111
7	0111	01	00011
8	1000	000	00110
9	1001	0010	01100
10	1010	10	00100
11	1011	101	10101
12	1100	100	10100
13	1101	110	01000

Encoded stream

00000 00001 00010 00101 01001 00111 00011 00110 01100 00100 10101 10100 01000 00110

Q.1.21 (i) Lempel Ziv Code for

13300202111300002212223 3

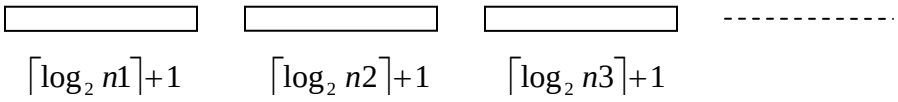
Parsing 13,30,02,021,11,300,00,22,12,223

gives

Dictionary	Dictionary Location	Contents	Codeword

Q.1.22 (i) For run length code we encode a run in terms of [how many] and [what]. Therefore to encode a run of n bits we require $= \lceil \log_2 n \rceil + 1$ bits.

The run length code is therefore



Compression it will provide:

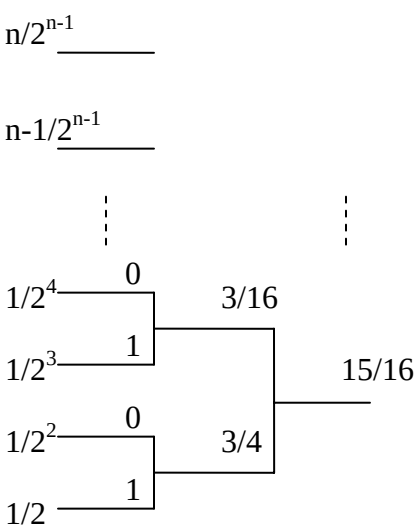
Every run requires $\lceil \log_2 n \rceil + 1$ bits.

Average length of a run = $1\frac{1}{2} + 2\frac{1}{2^2} + 3\frac{1}{2^3} + - - - - - + (n-1)\frac{1}{2^{(n-1)}} + n\frac{1}{2^{(n-1)}}$

$$= \frac{(n+1)2^{2n} - 2^{3n}}{2^{(n-1)}\left[2^{n+1} - 2^n\right]^2}$$

$$\text{Average Compression} = \frac{\lceil \log_2 n \rceil + 1}{\left[\frac{(n+1)2^{2n} - 2^{3n}}{2^{(n-1)}\left[2^{n+1} - 2^n\right]^2}\right]}$$

(ii) Huffman Coding



Q.1.23 For example, let us assume a run of 2^{14} 1's. For first level of run length coding we require 14+1=15 1's. For second level of run length coding we need 4+1=5 1's. This multi-layer run length coding is useful when we have large runs.

To encode n 1's maximum possible compression can be calculated as:

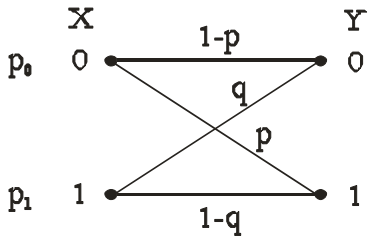
For first run required bits = $\lceil \log_2 n \rceil + 1$

For second run required bits = $\lceil \log \lceil \log_2 n \rceil + 1 \rceil + 1$

So for a run of n 1's maximum possible compression = $\frac{n}{\lceil \log_2 \lceil \log_2 \lceil \log_2 n+1 \rceil +1 \rceil +1 \rceil ------+1}$

SOLUTIONS FOR CHAPTER 2

Q.2.1



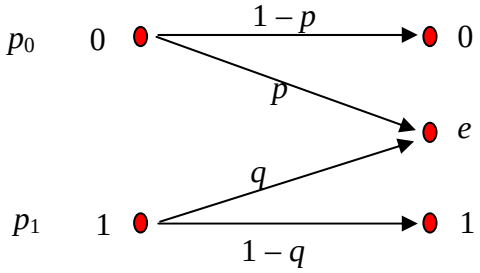
$$p(y=0) = p(y=0 \mid x=0)\, p(x=0) + p(y=0 \mid x=1)\, p(x=1)$$
$$= (1-p)\, p_0 + q p_1$$
$$= (1-p)\, p_0 + q(1-p_0)$$

$$p(y=1) = p(y=1 \mid x=0)\, p(x=0) + p(y=1 \mid x=1)\, p(x=1)$$
$$= p p_0 + (1-q)\,(1-p_0)$$

$$p(x=0 \mid y=0) = \frac{p(y=0 \mid x=0)\, p(x=0)}{p(y=0)} = \frac{(1-p)\, p_0}{(1-p)\, p_0 + q(1-p_0)}$$

$$p(x=1 \mid y=1) = \frac{p(y=1 \mid x=1)\, p(x=1)}{p(y=1)} = \frac{(1-q)(1-p_0)}{p p_0 + (1-q)(1-p_0)}$$

Q 2.2



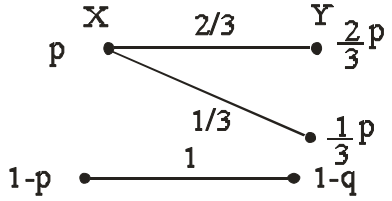
$$p(y=0) = (1-p)\, p_0$$
$$p(y=e) = p\, p_0 + q(1-p_0)$$
$$p(y=1) = (1-q)\,(1-p_0)$$

$$I(x;y) = \sum_{i=1}^{2}\sum_{j=1}^{3} P(y_j \mid x_i)\, P(x_j) \log \frac{P(y_j \mid x_i)}{P(y_j)}$$

$$= (1-p)\, p_0 \log \frac{1}{p_0} + p p_0 \log \frac{p}{p p_0 q (1-p_0)} + (1-q)(1-p_0) \log \frac{1}{(1-p_0)} + q(1-p_0) \log \frac{q}{p p_0 + q(1-p_0)}$$

Hint: For capacity find value of p_0 by $\frac{dI(X;Y)}{dp_0} = 0$ and then substitute it in above equation.

Q 2.3 (a)



$C_A = \max_{p} I(x; y)$

$$I(x; y) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j)\log\frac{P(x_i, y_j)}{P(x_i)P(y_j)}$$

$$I(x,y) = \frac{2}{3}p\log\frac{1}{p} + \frac{1}{3}p\log\frac{1}{p} + (1-p)\log\left(\frac{1}{1-p}\right)$$

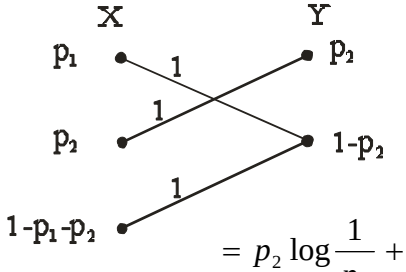
$$= p\log\frac{1}{p} + (1-p)\log\left(\frac{1}{1-p}\right) = -p\log p - (1-p)\log(1-p)$$

$$\frac{dI(x,y)}{dp} = -\log p - 1 + \log(1-p) + 1 = 0$$

$\Rightarrow$ - log p = log (1 - p) $\Rightarrow$ p = 1/2

$\therefore$ C_A = ½ log 2 + ½ log 2 = log 2 = 1 bit/use.

(b)



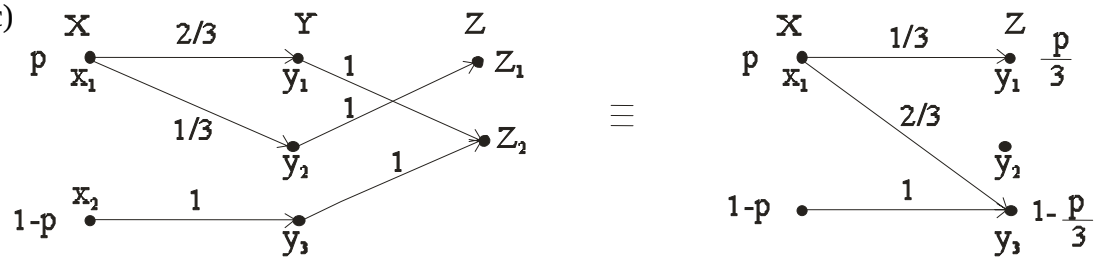
$$I(x; y) = p_2\log\frac{1}{p_2} + p_1\log\left(\frac{1}{1-p_2}\right) + (1-p_1-p_2)\log\left(\frac{1}{1-p_2}\right)$$

$$= p_2\log\frac{1}{p_2} + (1-(1-p_2)\log\frac{1}{1-p_2}$$

I(x; y) is maximized for p_2 = ½.

$\therefore C_B$ = log 2 = 1 bit/use.

(c)



$$H(Z) = -\frac{p}{3}\log\frac{p}{3} - \left(1-\frac{p}{3}\right)\log\left(1-\frac{p}{3}\right)$$

$$H(Z \mid X) = -\frac{p}{3}\log\frac{1}{3} - \frac{2p}{3}\log\frac{2}{3}$$

$I(X; Z) = H(Z) - H(Z|X)$

$$I(X; Z) = \frac{1}{3}p\log\frac{1}{p} + \frac{2}{3}p\log\left(\frac{2}{3-p}\right) + (1-p)\log\left(\frac{3}{3-p}\right)$$

$$= \frac{-p}{3}\log p + \frac{2p}{3}\log 2 - \frac{2p}{3}\log p(3-p) + (1-p)\log 3 - (1-p)\log(3-p)$$

$$= \frac{-p}{3}\log p + \frac{2p}{3}\log 2 - \frac{2p}{3} + (1-p)\log 3 - \left(1-\frac{p}{3}\right)\log(3-p)$$

$$\frac{dI(x;z)}{d_p} = \frac{-1}{3}\log p - \frac{1}{3} + \frac{2}{3} - \log 3 + \frac{1}{3}\log(3-p) + \frac{1}{3} = 0$$

$$\Rightarrow \frac{2}{3} - \log 3 + \frac{1}{3}\log\left(\frac{3-p}{p}\right) = 0$$

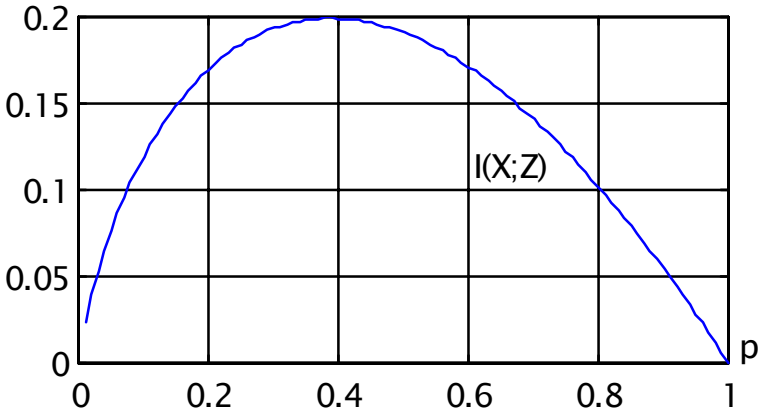
$$\Rightarrow 2 - 3\log 3 + \log\left(\frac{3-p}{p}\right) = 0$$

$$\Rightarrow \log\left(\frac{3-p}{p}\right) = 3\log 3 - 2 = 2.755$$

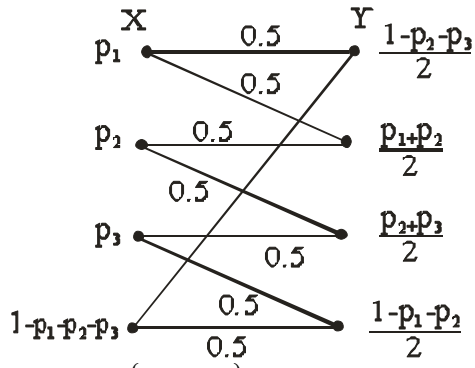
$$\Rightarrow \frac{3-p}{p} = 6.75 \qquad \Rightarrow p = 0.387.$$

$C_{AB} = 0.199$ bit/use

(d) C_{AB} is less than both C_A and C_B. This is because we don't have the flexibility to choose the input symbol probabilities for the second half of the composite channel. The plot of $I(X; Z)$ versus probability p is given below.



Q.2.4



Probabilities of different output symbols

$$C = \max_{p_i} \{I(x; y)\}$$

$$I(x;y) = \sum_j \sum_i p(x_j)\, p(y_i|x_j) \log\left[\frac{p(y_i|x_j)}{p(y_i)}\right]$$

$$= 0.5\, p_1 \log\frac{0.5}{0.5(1-p_2-p_3)} + 0.5(1-p_1-p_2-p_3)\log\frac{0.5}{0.5(1-p_2-p_3)}$$

$$+ 0.5\, p_1 \log\frac{0.5}{0.5(p_1+p_2)} + 0.5\, p_2 \log\frac{0.5}{0.5(p_1+p_2)}$$

$$+ 0.5\, p_2 \log\frac{0.5}{0.5(p_2+p_3)} + 0.5\, p_3 \log\frac{0.5}{0.5(p_2+p_3)}$$

$$+ 0.5\, p_3 \log\frac{0.5}{0.5(1-p_1-p_2)} + 0.5(1-p_1-p_2-p_3)\log\frac{0.5}{0.5(1-p_1-p_2)}$$

$$= -0.5\,[p_1 \log(1-p_2-p_3) + (1-p_1-p_2-p_3)\log(1-p_2-p_3) + p_1\log(p_1+p_2)$$
$$+ p_2\log(p_1+p_2) + p_2\log(p_2+p_3) + p_3\log(p_2+p_3) + p_3\log(1-p_1-p_2)$$
$$+ (1-p_1-p_2-p_3)\log(1-p_1-p_2)\,]$$

$$= -0.5\,[(1-p_2-p_3)\log(1-p_2-p_3) + (p_1+p_2)\log(p_1+p_2) + (p_2+p_3)$$
$$\log(p_2+p_3) + (1-p_1-p_2)\log(1-p_1-p_2)\,]$$

$$\frac{\partial I(x;y)}{\partial p_1} = \frac{1}{2}\left[\log(p_1+p_2)+1-\log(1-p_1-p_2)-1\right]=0$$

$$\Rightarrow \log(p_1+p_2) = \log(1-p_1-p_2) \quad \Rightarrow \quad p_1+p_2=\frac{1}{2} \qquad (1)$$

$$\frac{\partial I(x;y)}{\partial p_3} = -0.5\left[-\log(1-p_2-p_3)-1+\log(p_2+p_3)+1\right]=0$$

$$\Rightarrow \log(p_2+p_3) = \log(1-p_2-p_3)$$

$$\Rightarrow \quad p_2+p_3 = 1-p_2-p_3 \qquad \Rightarrow \quad p_2+p_3=\frac{1}{2} \qquad (2)$$

Substituting (1) & (2) in I(x; y) we get

C = -0.5 [0.5 log 0.5 + 0.5 log 0.5 + 0.5 log 0.5 + 0.5 log 0.5]

= - 4/2 × ½ log ½ = log 2 = 1 bit/use.

Q.2.5 (a) $C = B\log_2(1+SNR)$ SNR = 20 dB = 100

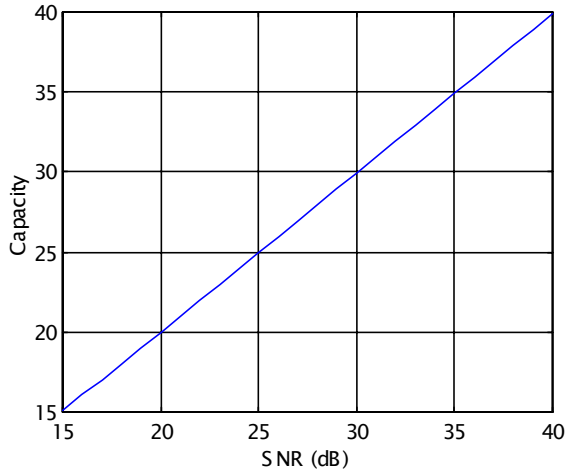
$= 3000 \log_2(1+100)$

$= 19{,}974.6$ bits/sec ≈ 20 kb/s.

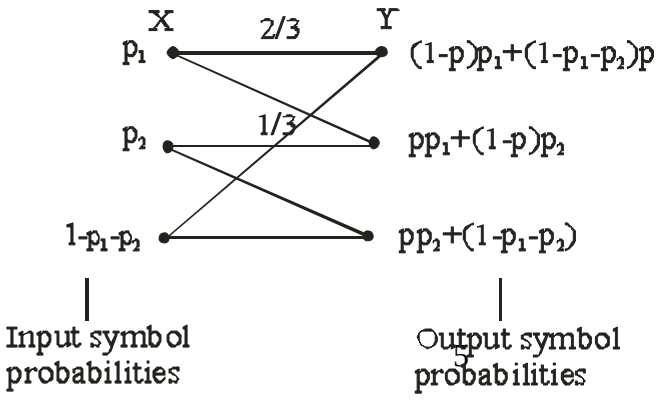
(b) SNR = 25 dB = 316.2

$C = 3000 \log_2(1+316.2) = 24{,}927.7$ bits/sec ≈ 25 kb/s.

It is interesting to note that for this telephone channel under consideration, the SNR (in dB) directly translates to the capacity (in kb/s). See the graph below!



Q.2.6



$$Capacity = \max_{\{p_i\}} \{I(x;\, y)\}$$

$$I(x;\, y) = p_1(1-p)\log\left\{\frac{1-p}{(1-p)p_1 + p(1-p_1-p_2)}\right\} + p(1-p_1-p_2)\log\left\{\frac{p}{(1-p)p_1 + p(1-p_1-p_2)}\right\}$$

$$+\ p_2(1-p)\log\left\{\frac{1-p}{pp_1 + p(1-p-p_2)}\right\} + pp_1\log\left\{\frac{p}{pp_1 + p(1-p)p_2)}\right\}$$

$$+\ (1-p_1-p_2)\ (1-p)\log\left\{\frac{1-p}{pp_2 + (1-p)(1-p_1-p_2)}\right\} + pp_2\log\left\{\frac{p}{pp_2 + (1-p)(1-p_1-p_2)}\right\}$$

$I(x; y) = -[p_1(1-p) + p(1-p_1-p_2)] \log [(1-p)p_1 + p(1-p_1-p_2)] + p_1(1-p) \log (1-p)$
$+ p(1-p_1-p_2)] \log p - [p_2(1-p) + pp_1] \log[pp_1 + (1-p)p_2] + p_2[(1 - p) \log (1-p)$
$+ pp_1 \log p - [1-p_1-p_2)(1-p) + pp_2] \log[pp2 + (1-p)(1-p_1-p_2) (1-p) \log(1-p)$
$+ pp_2 \log p$

$$\frac{\partial I(x;y)}{\partial p_1} = 0 \quad \Rightarrow (2p\text{-}1) \log [(1\text{-}p)p_1 + p(1\text{-}p_1\text{-}p_2)] - p\log [pp_1 + p_2(1\text{-}p)]$$
$$+ (1\text{-}p) \log[pp_2 + (1\text{-}p) (1\text{-}p_1\text{-}p_2)] = 0$$

$$\frac{\partial I(x;y)}{\partial p_2} = 0 \quad \Rightarrow p \log [(1\text{-}p)p_1 + p(1\text{-}p_1\text{-}p_2)] - (1\text{-}p)\log [pp_1 + (1\text{-}p)p_2]$$
$$- (2p\text{-}1) \log [pp_2 + (1\text{-}p) (1\text{-}p_1\text{-}p_2)] = 0$$

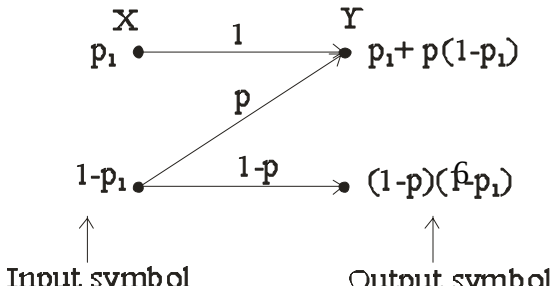
Q.2.7 A TV displays 30 frames /second
2×10^5 pixels /frame
16 bits / pixel

$\therefore$ Transmission rate = $30 \times 2 \times 105 \times 16$ bits /second
$= 96 \times 10^6$ bits / second.

$C = B \log_2 (1 + SNR)$ SNR = 25dB = 316.22

$$\text{Bandwidth required} = \frac{96\times10^6}{\log_2(1+316.22)} = 11.55\times10^6 \text{ Hz}$$

Q.2.8



(a) $I(x;y) = p_1 \log \frac{1}{p_1 + p(1-p_1)} + p(1-p_1) \log \frac{p}{p_1 + p(1-p_1)}$

$$+ (1-p)(1-p_1) \log \frac{p}{(1-p)(1-p_1)}$$

$= - [p_1 + p(1-p_1)] \log[p_1 + p(1-p_1)] - (1-p) - p(1-p_1) \log p - (1-p)(1-p_1) \log(1-p_1)$

$$\frac{dI(x;y)}{dp_1} = - (1-p) \log [p_1 + p(1-p_1)] - (1-p) - p \log p + (1-p) [1 + \log (1-p_1)]$$

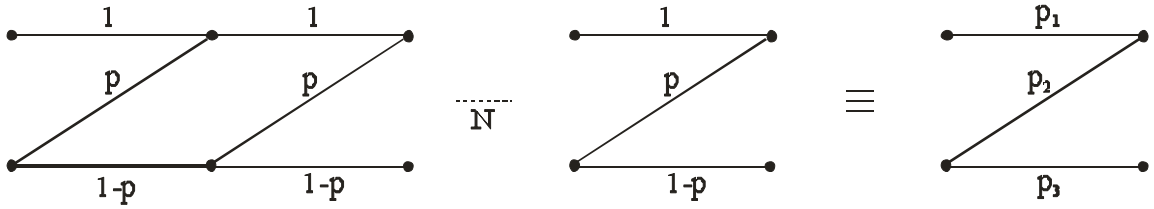
$$= - (1-p) \log (1-p_1) - (1-p) \log [p_1 + p (1-p_1) - p \log p$$

$$\Rightarrow \log \left[\frac{1-p_1}{p_1 + p(1-p_1)} \right] = \frac{p}{1-p} \log p$$

$$\Rightarrow \frac{1-p_1}{p_1 + p(1-p_1)} = (P)^{\frac{p}{1-p}} = \alpha$$

$$p_1 = \frac{1-\alpha p}{1-\alpha p + p\alpha} \qquad \rightarrow \text{Input probability that results in capacity}$$

(b)



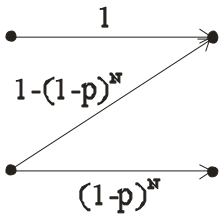
$p_1 = 1, 1 \ldots$. N times $= 1$

$p_2 = p + (1-p)p + (1-p)^2.p + \ldots.. + (1-p)^{N-1} p$

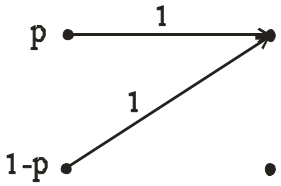
$$= \left[\frac{1-(1-p)^N}{1-(1-p)} \right] = 1 - (1-p)^N$$

$p_3 = (1-p)^N$

Equivalent channel for combination of N Z channels



(c) As $N \to \infty$, the equivalent channel tends to (provided $p \neq 0$)



I(x; y) = p log 1/1 + (1-p) log 1/1 = 0
Thus, the capacity $\to 0$ as $N \to \infty$, provided $p \neq 0$.
Of course, the capacity $\to 1$ as $N \to \infty$, for $p = 0$.

Q.2.9 Given: SNR=20dB

(i) Cutoff rate $R_0 = 1 - \log_2\left(1 + e^{-E/N_0}\right)$

$= 0.99$

(ii) $\overline{P_e} < 2^{n(R_0 - R_c)}$

Assuming binary antipodal signaling-

$10^{-6} < 2^{-(0.99-R_c)}$

$R_c < 18.94$

(iii) n is based on the cutoff rate. Cutoff rate is a design parameter.

Q.2.10 Consider $D(p\|q) \triangleq \int_{-\infty}^{\infty} p(x) \log \frac{p(x)}{q(x)} dx$

Where p(x) and q(x) are two probability distributions.

$$-D(p\|q) \triangleq \int_{-\infty}^{\infty} p(x) \log \frac{q(x)}{p(x)} dx \leq \int_{-\infty}^{\infty} p(x) \left(\frac{q(x)}{p(x)} - 1 \right) dx$$

$$= \int_{-\infty}^{\infty} q(x)\, dx - \int_{-\infty}^{\infty} p(x)\, dx = 0$$

$$\Rightarrow D(p\|q) \geq 0$$

Now, let q(x) be the Gaussian distribution : $\frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma}}$

Let p(x) $\to$ arbitrary distribution with variance σ^2.

$$D(p\|q) \triangleq \int_{-\infty}^{\infty} p(x)\log\frac{p(x)}{q(x)}dx$$

$$= \int_{-\infty}^{\infty} p(x)\log_2\left(\frac{1}{q(x)}\right)dx + \int_{-\infty}^{\infty} p(x)\log_2\, p(x)\,dx$$

$$= \int_{-\infty}^{\infty} p(x)\,\frac{1}{2}\log_2\left(\sqrt{2\pi\sigma^2}\,e^{\frac{x^2}{2\sigma^2}}\right)dx \;-\; H(X)$$

Differential entropy for Gaussian distribution

differential entropy

$$= \frac{1}{2}\log\,(2\pi\sigma^2) + \frac{1}{2}\log 3 \;-\; H(X)$$

$$= \frac{1}{2}\log_2\,(2\pi e\sigma^2) \;-\; H(X)$$

$$D(p\|q) \;\Rightarrow\; H(X) \le \frac{1}{2}\log_2\,(2\pi e\sigma^2)$$

Differential entropy for Gaussian distribution.

SOLUTIONS FOR CHAPTER 3

Q3.1 C = {0000, 1100, 0011, 1111}

Since:

(i) All zero codeword {0000} is a valid code word.

Sum of any two code is also a valid code word. Hence 'C' is a linear code.

(ii) Minimum distance = Minimum weight = 2

$$\begin{array}{ccc} 1100 & 1100 & 0011 \\ +\,0011 & +\,1111 & +\,1111 \\ \hline 1111 & 0011 & 1100 \end{array}$$

Q3.2 (i) $(6, 1, 6) \Leftrightarrow (n, k, d^*)$

$$t = \left[\frac{d-1}{2}\right] = \left[\frac{6-1}{2}\right] = 2$$

Hamming bound for binary codes

$$\left[1 + \binom{n}{1} + \binom{n}{2} + \ldots\ldots + \binom{n}{t}\right] \leq 2^{n-k}$$

$$\Rightarrow 1 + \binom{6}{1} + \binom{6}{2} \leq 2^5$$

$\Rightarrow 22 < 32.$

Hence (6, 1, 6) is a valid code word and it is simply the repetition code with n = 6.

(ii) $(3, 3, 1) \Rightarrow d^* = 1 \Rightarrow t = 0.$

By Hamming bound $[1 + 0] \leq 2^o \leq 1 = 1.$

Hence (3, 3, 1) is also valid code construction.

This code is equivalent to sending information bits as such with no change, hence does not have any error detecting or correction capability.

(iii) $(4, 3, 2) \Rightarrow d^* = 2 \Rightarrow t = 0.$

By Hamming bound $1 < 2$.
Hence it is a valid code construct (Parity code)

Q3.3 $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}_{3x5}$

$\Rightarrow k = 3,\ n = 5.$

(i) All possible code words

$\boldsymbol{C} = \boldsymbol{I} \,.\, \boldsymbol{G}$

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

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

(ii) $\boldsymbol{G}$ in systematic form:

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

$\underbrace{\quad\quad}_{J_k} \quad \underbrace{\quad\quad}_{P}$

Parity check matrix $\mathbf{H} = [-\mathbf{P}^T, \mathbf{I}_{n-k}]$

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

(iii) Generator matrix of an equivalent systematic code

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

(iv) $d^* = 2$; Hence it can detect 1 error but can't correct that error

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

$$\text{Syndrome} = eH^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

We can choose 4 error patterns with distinct syndrome which can be corrected using this syndrome table.

0 0 0 0 0	$\rightarrow$	0 0
0 0 1 0 0	$\rightarrow$	0 1
0 1 0 0 0	$\rightarrow$	1 1
1 0 0 0 0	$\rightarrow$	1 0

Standard Array

00000	01010	10011	11001	10100	11110	00111	01101
00100	01110	10111	11101	10000	11010	00017	01001
01000	00010	11011	10001	11100	10110	01111	00101
10000	11010	00011	01001	00100	01110	10111	11101

(v) Minimum distance, $d^* = 2$.

(vi) Since $d^* = 2$, number of errors it can detect = $d^* - 1 = 1$.

(vii) The error patterns that can be detected:

00001
00010
00100
01000
10000

(viii) Number of errors it can correct = $\frac{d^* - 1}{2} = 0$

(ix) Since it cannot correct any error. The symbol error is *same as* uncoded probability of error. However, since 1 bit error can be detected, a request for repeat transmission can be made on this basis. This scheme will also fail if 2 or more bits are in error. Thus, if automatic repeat request (ARQ) is used, the probability of error will be

$$p(e) = \binom{5}{2} p^2 (1-p)^5 + \binom{5}{3} p^3 (1-p)^2 + \binom{5}{4} p^4 (1-p) + \binom{5}{5} p^5$$

(x) Since all zero is a valid codeword and sum of any two code words is also a valid codeword, it is a linear code.

Q3.4 C = {00000, 10100, 01010, 11111}
For this, $(n, k) = (5, 2)$

By observation if we use the mapping as follow

Information Word		Codeword
0 0	$\rightarrow$	0 0 0 0 0
0 1	$\rightarrow$	1 0 1 0 1
1 0	$\rightarrow$	0 1 0 1 0
1 1	$\rightarrow$	1 1 1 1 1

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

Q3.5 Given: (n, k, d^*) is a binary code with d^* even. We need to show that there exists a (n, k, d^*) code in which all codewords have even weight.

Construct a code with all codewords of even weight by adding even a parity bit to all the codewords of the given binary (n, k, d^*) code with d^* even. By adding an even parity, all code words will become even weight and also since d^* is even.

This process of adding a parity bit will not alter the minimum weight. Hence, the d^* will be even for this new code.

Q3.6 Let C be a linear code (binary).
If the codewords $C_1, C_2 \in C$, then, $C_1 \oplus C_2 = C_3 \in C$.
Let us now add a parity check bit to the codewords of C.
Let P_i be the parity bit of C_i and let this new augmented codeword be denoted by $\overline{C}_i$. By definition, the parity bit is the binary sum of all the elements of the codeword vector, i.e.:

$P_1 = C_{11} \oplus C_{12} \oplus \ldots. \oplus C_{1n}$
$P_2 = C_{21} \oplus C_{22} \oplus \ldots. \oplus C_{2n}$
$P_3 = C_{31} \oplus C_{32} \oplus \ldots. \oplus C_{3n}$
Now, $C_3 = C_1 \oplus C_2$
$= (C_{11} \oplus C_{12} \oplus \ldots. \oplus C_{1n}) \oplus (C_{21} \oplus C_{22} \oplus \ldots. \oplus C_{2n})$
$P_3 = P_1 \oplus P_2$.

Hence even after adding an overall parity bit,
$\overline{C}_1 \oplus \overline{C}_2 = \overline{C}_3$
Thus the modified code is also binary linear code.

Q3.7 (i) New codeword C_3 consists of $U_1\ U_2\ U_3$----- $U_n\ V_1\ V_2\ V_3$ ------- V_n
So in new code there are total 2n codewords.
As $U_1\ U_2\ U_3$----- U_n encodes 2^{k1} words and $V_1\ V_2\ V_3$ ------- V_n encodes 2^{k2} words, the new code encodes $2^{k1}.2^{k2} = 2^{k1+k2}$ words.
Therfore C_3 is (2n, k1+k2) code.

(ii) $U_1\ U_2\ U_3$----- U_n => minimum distance $d1$
$V_1\ V_2\ V_3$ ------- V_n => minimum distance $d2$
For C_3 $(U|U+V)$ if U is all zero codeword then minimum distance is $d2$.
If V is all zero codeword then minimum distance is $2d1$.
Therefore minimum distance of C_3 is min{$2d1, d2$}

Q3.8 (a) S = {0101, 1010, 1100}
<S> = {0000, 0101, 1010, 1100, 1111, 1001, 0110, 0011}

(b) S = {1000, 0100, 0010, 0001}
<S> = {0000, 1000, 0100, 0010, 0001, 1100, 1010, 1001, 0110, 0101, 0011, 1110, 1101, 1011, 0111, 1111}

(c) S = {11000, 01111, 11110, 01010}
<S> = {00000, 11000, 01111, 01010, 10111, 00110, 10010, 10001, 00101, 10100, 01001, 11101, 01100, 11011, 11110, 00011}

Q3.9 Binary code (23, 12, 7)

$t = \dfrac{d^* - 1}{2} = 3$, errors that can be corrected.

p = 0.01.

$$P(e) = \binom{23}{4} p^4 (1-p)^{19} + \binom{23}{5} p^5 (1-p)^{18} + \ldots\ldots\ldots + \binom{23}{23} p^{23}$$

$$= 1 - \binom{23}{0}(1-p)^{23} - \binom{23}{1} p(1-p)^{22} - \binom{23}{2} p^2 (1-p)^{21} - \binom{23}{3} p^3 (1-p)^{20}$$

$$= 1 - 079361 - 0.18437 - 0.02048 - 0.00144$$

$$= 1 - 0.99992 \approx 0.00008.$$

Q3.10 $\boldsymbol{C}$ is a binary code with parity check matrix $\boldsymbol{H}$.

$\boldsymbol{C}_1 \rightarrow \boldsymbol{H}_1 \Rightarrow \boldsymbol{C}\boldsymbol{H}^T = 0 \Rightarrow \boldsymbol{G}\boldsymbol{H}^T = 0$

$\boldsymbol{C}_1 = [\boldsymbol{C} : P]$

$\boldsymbol{G}_1 = [\boldsymbol{G} : \boldsymbol{P}]$

$$G_1 H_1^T = [G : P] H_1^T$$

$$= [\boldsymbol{G} : \boldsymbol{P}] \begin{bmatrix} & & & & | & 1 \\ & H^T & & & | & 1 \\ & & & & | & 1 \\ - & - & - & - & - & - \\ 0 & 0 & .... & 0 & | & 1 \end{bmatrix}$$

$$= [\boldsymbol{G}\boldsymbol{H}^T \quad \boldsymbol{G} \oplus \boldsymbol{P}]$$

$$= \boldsymbol{0}.$$

Hence $\boldsymbol{H}_1 = \begin{pmatrix} \boldsymbol{H} & : & 0 \\ & : & 0 \\ \ldots\ldots & : & : \\ 1\ 1\ 1\ 1 \ldots & & 1 \end{pmatrix}$

is the parity check matrix of the extended code $\boldsymbol{C}$, obtained from $\mathbf{C}$ by adding an overall parity bit.

Q3.11 (5, 3) code over *GF* (4)

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}$$

I P

(i) Parity check matrix

$$H = \begin{bmatrix} -1 & -1 & -1 & 1 & 0 \\ -1 & -2 & -3 & 0 & 1 \end{bmatrix}$$

$$\Rightarrow H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{bmatrix}$$ since -1 = 1, -2 = 2, -3 = 3 over *GF* (4).

(ii) Minimum distance, $d^* = 3$.

Hence this code can detect 2 errors.

(iii) This code can correct 1 error.

(iv) With erasures $d^* \geq 2t + 1 + r$

As $t = 1$
$r = 0$

(v) Check for the condition for perfect code:

$$M\left\{\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{t}(q-1)^t\right\} = q^n$$

Here, $n = 5$, $k = 3$, $t = 1$, $q = 4$, $M = 4^3$. Yes, it's a perfect code!

3.13 Hamming bound for non-binary.

$$\left[1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}\right] = 2^{n-k}$$

if $n = 7\ [1 + 7 + 21 + 35] = 2^{7\text{-k}}$

$64 = 2^{7-k}$

which can be satisfied for k = 1.

$\therefore$ binary perfect code with $d^* = 7$ & $n = 7$ is possible.

If $n = 23$

$1 + 23 + 253 + 1771 = 2^{23\text{-k}}$

$2048 = 2^{23\text{-k}}$

$\Rightarrow k = 12.$

$\therefore$ binary perfect code with $d^* = 7$ & $n = 23$ is possible.

Q3.14 $r_H = \dfrac{k}{n} = \dfrac{2^m - 1}{2^m - 1 - m}$

$$\lim_{k\to\infty} r_H = \lim_{m\to\infty} \frac{2^m - 1}{2^m - 1 - m}$$

Since 2^m terms goes toward ∞, exponentially. Hence we can neglect the effect of m & 1 both

$$\Rightarrow \lim_{k\to\infty} r_H = \lim_{m\to\infty} \frac{2^m}{2^m} = 1.$$

Q3.15 Hint: Check for the optimality of codes with a larger value of *n*, but same *k* and *t*, or with a smaller value of *k* with the same *n* and *t*. Then draw a conclusion.

Q.3.16 For orthogonality every column must be orthogonal to other column i.e. inner product of 2 column vectors must be 0.

Column(1,2) inner product

$(x_1, x_2, x_3).(-x_2^*, x_1^*, 0) = 0$

Column(1,3) inner product

$(x_1, x_2, x_3).(-x_3^*, 0, x_1^*) = 0$

Column(1,4) inner product

$(x_1, x_2, x_3).(0, -x_3^*, x_2^*) = 0$

Column(2,3) inner product

$(-x_2^*, x_1^*, 0).(-x_3^*, 0, x_1^*) \neq 0$

Therefore the given STBC code is not orthogonal.

SOLUTIONS FOR CHAPTER 4

Q4.1 (a) → Not a linear cyclic block code since {1111} missing.
(b) → Not cyclic.
(c) → Not cyclic.
(d) → Cyclic equivalent.
(e) → Cyclic.

Q4.2 (a) $\frac{F[x]}{x^2+1}$ over $GF(2)$ contains {0, 1, x, 1 + x}.

The addition and multiplication tables are given below:

+	0	1	x	1+x
0	0	1	x	1+x
1	1	0	x+1	1
x	x	x+1	0	1
1+x	1+x	x	1	0

.	0	1	x	1+x
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
1+x	0	x+1	x+1	0

$\frac{F[x]}{x^2+1}$ over $GF(2)$ is not a field because of the absence of a multiplicative inverse for 1+x.

Also, $\frac{F[x]}{x^2+1}$ over $GF(2)$ is not a field because (x^2+1) in not prime polynomial over $GF(2)$.

(b) $\frac{F[x]}{x^2+1}$ over $GF(3)$ is a field because $(x^2 + 1)$ is prime over $GF(3)$.

$\frac{F[x]}{x^2+1}$ over $GF(3)$ contains {0, 1, 2, x, x +1, x + 2, 2x, 2x+1, 2x+2}.

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

.	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

This is a field because it satisfies all the eight conditions stated in Definition 3.9.

Q4.3 (a) Irreducible polynomials over $GF(2)$ of degree 1 to 5.
x, $x+1$, x^2+x+1, $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$, $x^5 + x^4 + x^3 + x + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x^3 + x^2 + x + 1$, $x^5 + x^3 + 1$, $x^5 + x^2 + 1$.

(b) Irreducible polynomials over $GF(3)$ of degree 1 to 3.
x, $2x$, $x+1$, $x+2$, $2x+1$, $x^2 + 2x + 2$, $x^2 + 1$, $+ x^2 + x + 2$, $2x^2 + x + 1$, $2x^2 + 2x + 1$, $x^3 + x^2 + 2$, $2x^3 + x + 1$, $2x^3 + x + 2$, $x^3 + 2x + 1$, $x^3 + 2x + 2$, $x^3 + x^2 + x + 2$, $x^3 + x^2 + 2x + 1$, $x^3 + 2x^2 + 1$, $x^3 + 2x^2 + 2x + 2$, $2x^3 + x^2 + 2$, $2x^3 + x^2 + x + 1$, $2x^3 + x^2 + 2x + 2$, $2x^3 + 2x^2 + 1$, $2x^3 + 2x^2 + x + 2$, $2x^3 + 2x^2 + 2x + 1$.

Q4.4 $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$, hence two cyclic nontrivial codes of length 5 are possible.
(i) With $g(x) = x^4 + x^3 + x^2 + x + 1$
$n = 5$, $n - w = 4$ $k = 1$
$G = [1\ 1\ 1\ 1\ 1\ ]_{1x5}$
Min distance $d^* = 5$.

(ii) With $g(x) = x+1$.

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{4x5}$$

Systematic form of G.

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

$d^* = 2$.

Q4.5 $x^n - 1$ is product of r distinct irreducible polynomials over $GF(q)$.

Hence $2^r - 2$, different nontrivial cyclic codes of length n exits (excluding trivial case of $g(x) = 1$ & $g(x) = x^n - 1$.

If g(x) is given, then
Minimum distance of codes $\leq$ Weight of generator matrix.

Q4.6 **(a)** To factorize $x^8 - 1$ over $GF(3)$

$$\begin{aligned}(x^8 - 1) &= (x^4 - 1)(x^4 + 1) \\ &= (x^2 - 1)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2) \\ &= (x - 1)(x + 1)(x^2 + x + 2)(x^2 + 2x + 2)(x^2 + 1) \\ &= (x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)\end{aligned}$$

(b) Hence $2^5 - 2 = 30$ non-trivial ternary code exists.

(c) For $GF(4)$:
$(x^2 - y^2) = (x^2 + y^2)$
$x^8 - 1 = x^8 + 1 = (x+ 1)^8$
Hence 7 non-trivial quaternary cyclic codes exist. The generator polynomials are: $g_r(x) = (x+ 1)^r$ for r = 1, 2,…,7.

Q4.7 $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ $\quad n = 15 \quad \Rightarrow \quad k = 5$, since degree of g(x) is (n – k).

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

Minimum distance, $d^* = 7$.
(b) See at the end of the solution for this question.

(c) Errors that can be detected = 7 – 1 = 6

(d) Errors that can be corrected (7-1)/2 = 3.

(e) Systematic form of G

$$G = \left[\begin{array}{ccccc|ccccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

I P

(b) $\boldsymbol{H} = [-\ P^T \quad I_{n-k}]$

$$= \left[\begin{array}{cccccccccccccc} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Q4.8 $g(x) = x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 2x + 1$ over $GF(4)$

$n - k = 6, n = 15, \Rightarrow \quad k = 9$

(a) Check the validity of g(x)

$x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 2x + 1)\ x^{15} + 1\ (x^9+3x^8+3x^7+2x^5+x^4+2x^2 + 2x + 1$

$x^{15} + 3x^{14} + x^{13} + x^{12} + 2x^{11} + 2x^{10} + x^9$

$3x^{14} + x^{13} + x^{12} + 2x^{11} + 2x^{10} + x^9 + 1$

$3x^{14} + 2x^{13} + 3x^{12} + 3x^{11} + x^{10} + x^9 + 3x^8$

$3x^{13} + 2x^{12} + x^{11} + 3x^{10} + 3x^8 + 1$

$3x^{13} + 2x^{12} + 3x^{11} + 3x^{10} + x^9 + x^8 + 3x^7$

$2x^{11} + x^9 + 2x^8 + 3x^7 + 1$

$2x^{11} + x^{10} + 2x^9 + 2x^8 + 3x^7 + 3x^6 + 2x^6$

$x^{10} + 3x^9 + 3x^6 + 2x^6 + 1$

$x^{10} + 3x^9 + x^8 + x^7 + 2x^6 + 2x^5 + x^4$

$x^8 + x^7 + x^6 + x^4 + 1$

$x^8 + 3x^7 + x^6 + x^5 + 2x^4 + 2x^3 + x^2$

$2x^7 + x^5 + 3x^4 + 2x^3 + x^2 + 1$

$$\begin{array}{r} 2x^7 + x^6 + 2x^5 + 2x^4 + 3x^3 + 3x^2 + 2x \\ \hline x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 2x + 1 \\ x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 2x + 1 \\ \hline \end{array}$$

No remainder.

Hence g(x) is a valid generator polynomial.

(b) $x^{15} + 1 = (x^9 + 3x^8 + 3x^7 + 2x^5 + x^4 + 2x^2 + 2x + 1).g(x) = h(x).g(x)$

$$H = \begin{bmatrix} 1 & 3 & 3 & 0 & 2 & 1 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 3 & 0 & 2 & 1 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 & 3 & 0 & 2 & 1 & 0 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 3 & 0 & 2 & 1 & 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 3 & 0 & 2 & 1 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 & 3 & 0 & 2 & 1 & 0 & 1 & 2 & 1 \end{bmatrix}$$

(c) $d^* = 5$ (five columns of $\boldsymbol{H}$ add up to the zero vector).

(d) Code rate = k/n = 9/15 = 3/5.

(e) $v(x) = x^8 + x^5 + 3x^4 + x^3 + 3x + 1$.

V = [0 0 0 0 0 0 1 0 0 1 3 1 0 3 1]

$$H^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 \\ 3 & 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 3 & 1 & 0 & 0 \\ 2 & 0 & 3 & 3 & 1 & 0 \\ 1 & 2 & 0 & 3 & 3 & 1 \\ 0 & 1 & 2 & 0 & 3 & 3 \\ 1 & 0 & 1 & 2 & 0 & 3 \\ 2 & 1 & 0 & 1 & 2 & 0 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

VH^T = [1 _ _ _ _ _] non zero.
Hence $v(x) = x^8 + x^6 + 3x^4 + x^5 + 3x + 1$ is not a valid code word.
Also we can check this by dividing $x^8 + x^6 + 3x^4 + x^3 + 3x + 1$ by $x^6 + 3x^6 + x^4 + x^3 + 2x^2 + 2x + 1$ and since reminder is not zero, so it is not valid code word.

Q4.9 Since we are working over $GF(2)$, -1 = +1.
For Hamming code, $g_H(x) = (x^3 + x + 1)$
$g_1(x) = (x+1)(x^3 + x + 1)$
$= x^4 + x^3 + x^2 + 1.$
n = 7, n – k = 4, k = 3

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

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

$$H_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad d_{\min} = 4$$

$$t = \left| \frac{4-1}{2} \right| = 1$$

So this code can correct one bit error.

$S = eH^T$

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

The first matrix contains ALL single errors and adjacent double errors. The second matrix is the H^T. The matrix on the RHS is the syndrome matrix.

Since we can map all the two adjacent possible errors to *district* syndrome vectors, we will be able to correct all the two adjacent double error.

Q4.10 Hint: Work along similar lines as Example 4.28.

Q4.11 Hint: Start from the basic definition of the Fire code.

Q4.12 (i) Assuming this Fire code over GF(2). For a valid generator polynomial of a Fire code $g(x) = (x^{2t-1}-1)\, p(x)$ where $p(x)$ does not divide $(x^{2t-1}-1)$.

$$\begin{array}{r} x^6 + x + 1 \;\big)\; x^{11} + 1 \;\big(\; x^5 + 1 \\ \underline{x^{11} + x^6 + x^5} \\ x^6 + x^5 + 1 \\ \underline{x^6 + x + 1} \\ x^5 + x \end{array}$$

Therefore g(x) is a valid generator polynomial.

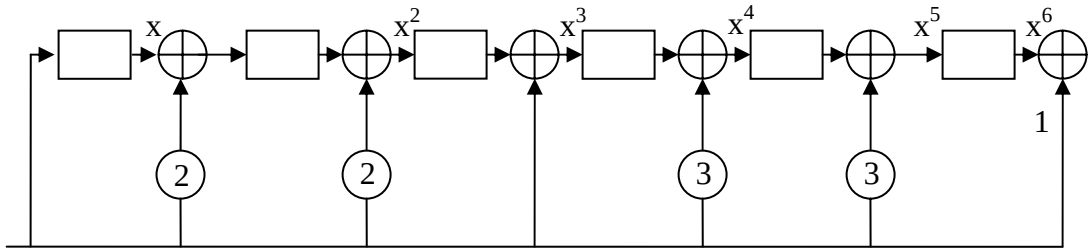
(ii) A Fire code can correct all burst errors of length t or less. So this code can correct all burst of length 6 or less.

Q.4.13 g(x) is a codeword that is a burst of length (n-k)+1. Probability of burst error of length (n-k) + 1 can not be detected is $\frac{1}{2^{(n=k)+1}}$.

Therefore g(x) can detect a fraction $1-2^{-(n-k+1)}$ of all burst pattern of length (n-k+1).

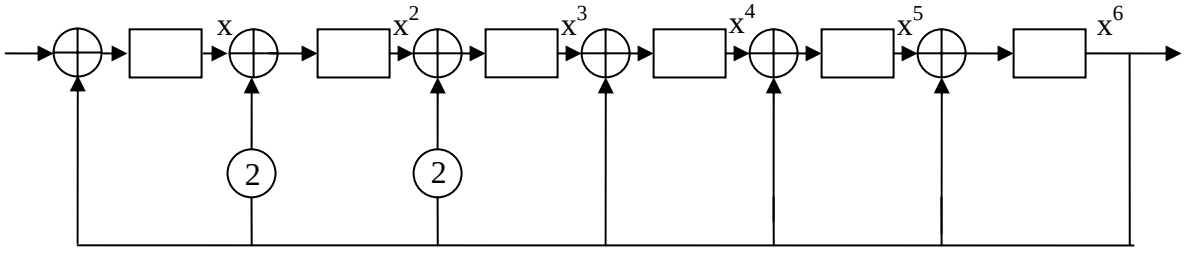
Q.4.14 Shift Register Encoder:

$g(x) = x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 2x + 1$



Meggitt Decoder:

Shift register circuit for dividing by g(x).



For Meggitt decoder refer flow chart of Fig. 4.9.

Q4.15 $g(x) = (x^{23} + 1)(x^{17} + x^3 + 1)$

$g(x) = x^{40} + x^{26} + x^{23} + x^{17} + x^3 + 1$

$n - k = 40$. From Singleton bound
$d^* \leq n - k + 1 = 41$.

(i) Errors that can be corrected $\leq \left\lfloor \frac{41-1}{2} \right\rfloor$

$\leq 20.$

(ii) Burst errors that can be corrected

$\leq \left\lfloor \frac{1}{2}(n-k) \right\rfloor \leq 20.$

However, the actual $d^* = 6$. Thus the Singleton bound is quite loose here. This g(x), however, is excellent for detecting and correcting burst errors

SOLUTIONS FOR CHAPTER 5

Q5.1 The addition and multiplication tables for of *GF*(3) are:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Representation of $GF(3^2)$:
Choose the primitive polynomial $p(x) = x^2 + x + 2$

Table 1

Exponential Notation	Polynomial Notation	Ternary Notation	Decimal Notation	Minimal Notation
0	0	00	0	1
α^0	1	01	1	x + 2
α^1	z	10	3	$X^2 + x + 2$
α^2	2z + 1	21	7	$x^2 + 1$
α^3	2z + 2	22	8	$x^2 + x + 2$
α^4	2	02	2	x + 1
α^5	2z	20	6	$x^2 + 2x + 2$
α^6	Z + 2	12	5	$x^2 + 1$
α^7	Z + 1	11	4	$x^2 + 2x + 2$

GF(9) Addition and Multiplication Tables:

+	0	1	z	2z+1	2z+2	2	2z	z+2	z+1
0	0	1	z	2z+1	2z+2	2	2z	z+2	z+1
1	1	2	z+1	2z+2	2z	0	2z+1	2	z+2
z	z	z+1	2z	1	z	z+2	0	2z+2	2z+1
2z+1	2z+1	2z+2	1	2z+2	z	2z	2z+1	z+2	6
2z+2	2z+2	2z	2	2	Z+1	2z+1	1	2z+2	Z
2	2	0	z+2	2z	2z+1	1	2z+2	Z+1	Z
2z	2z	2z+1	0	z+1	Z+2	1	2z+2	z+1	2
Z+2	z+2	2	2z+2	0	1	z+1	2	2z+1	2z
Z+1	z+1	z+2	2z+1	2	0	2	1	2z	2z+1

.	0	1	z	2z+1	2z+2	2	2z	z+2	z+1
0	0	0	0	0	0	0	0	0	0
1	0	1	z	2z+1	2z+2	2	2z	z+2	z+1
z	0	z	2z+1	2z+2	2	2z	z+2	z+1	1
2z+1	0	2z+1	2z+2	2	2z	z+2	z+1	z+1	Z
2z+2	0	2z+2	2	2z	z+2	z+1	1	z	2z+1
2	0	2	2z	z+2	z+1	1	z	2z+1	2z+2
2z	0	2z	z+2	z+1	1	z	2z+1	2z+2	2
Z+2	0	z+2	Z+1	1	z	2z+1	2z+2	z	2z

Z+1	0	z+1	1	z	2z+1	2z+2	2	2z	z+2

Q5.2 (i) Using the minimal polynomials as calculated previously in Table-1 in the previous solution:

GF(3)
$x^8 - 1 = (x + 1)(x + 2)(x^2 + 1)(x^2 + 2x + 2)(x^2 + x + 2)$

Ternary BCH code with t = 2 (double error correcting code).
$g(x) = \text{LCM}[f_1(x), f_2(x), f_3(x) f_4(x)]$
$= \text{LCM}[x^2 + x + 2, x^2 + 1, x^2 + x + 2, x + 1]$
$= (x^2 + 2x + 2)(x^2+1)(x+2)$
$g(x) = x^5 + 2x^4 + x^3 + x^2 + 2$

Minimum distance $d^* = 5$
$n = 8, \quad n - k = 5 \Rightarrow k = 3.$
Code rate = k/n = 3/8.

(ii) The primitive blocklength = $26 = q^m - 1 = 3^3 - 1$.
$p(x) = x^3 + 2x + 1$
Representation of $GF(3^2)$

Exponential Notation	Polynomial Notation	Ternary Notation	Decimal Notation	Minimal Notation
0	0	000	0	
α^0	1	001	1	x + 1
α^1	2	010	3	$x^3 + 2x + 1$
α^2	22	100	9	$x^3 + 2x^2 + 2x + 1$
α^3	2 + z	012	5	$x^3 + 2x + 2$
α^4	$2^2 + 2z$	120	15	$x^3 + 2x^2 + 1$
α^5	$2z^2 + z + 2$	212	23	$x^3 + x^2 + x + 2$
α^6	$2^2 + 1 + 2$	111	13	$x^3 + 2x^2 + x + 1$
α^7	$2^2 + 2z + 2$	122	17	
α^8	$2z^2 + 2$	202	29	
α^9	z + 1	011	4	$x^3 + 2x + 2$
α^{10}	$2^2 + z$	110	12	$x^3 + 2x + 1$
α^{11}	$2^2 + z + 2$	112	14	
α^{12}	$2^2 + z$	102	11	$x^3 + 2x^2 + 1$
α^{13}	2	002	2	x + 2
α^{14}	2z	020	6	
α^{15}	$2z^2$	200	18	$x^3 + x^2 + x + 2$
α^{16}	2z + 1	021	7	
α^{17}	$2z^2 + 2$	210	21	
α^{18}	$2^2 + 2z + 1$	121	16	$x^3 + 2x^2 + x + 1$

α^{19}	$2z^2 + 2 + 2z$	202	26	$x^3 + x^2 + x + 2$
α^{20}	$2z^2 + z + 1$	211	22	
α^{21}	$2^2 + 1$	101	10	
α^{22}	$2z + 2$	022	8	
α^{23}	$2z^2 + 2z$	220	24	
α^{24}	$2z^2 + 2z + 1$	221	25	
α^{25}	$2z^2 + 1$	201	19	

t = 3 (triple error correcting code)

$g(x) = \text{LCM}[f_1(x), f_2(x), f_3(x), f_4(x)\, f_5(x)\, f_6(x)]$

$= x^{12} + x^{11} + 2x^9 + 2x^8 + 2x^7 + 2x^3 + 2x^2 + x + 1$

$d^* = 9$ (thus the code is over designed).

Q5.3 Representation of $GF(2^5)$

Primitive polynomial $p(x) = x^5 + x^2 + 1$

Table II

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Notation
0	0	00000	0	
α^0	1	00001	1	x + 1
α^1	z	00100	2	$f_1(x)$
α^2	z^2	01000	4	$f_1(x)$
α^3	z^3	10000	8	$f_3(x)$
α^4	z^4	00101	16	$f_1(x)$
α^5	$z^2 + 1$	01010	5	$f_5(x)$
α^6	$z^2 + z$	10100	10	$f_5(x)$
α^7	$z^4 + z^2$	01101	20	$f_7(x)$
α^8	$z^3 + z^2 + 1$	11010	13	$f_1(x)$
α^9	$z^4 + z^3 + z$	10001	26	$f_5(x)$
α^{10}	$z^4 + 1$	10001	17	$f_5(x)$
α^{11}	$z^2 + z + 1$	00111	7	$f_{11}(x)$
α^{12}	$z^3 + z^2 + z$	01110	14	$f_3(x)$
α^{13}	$z^4 + z^3 + z^2 + 1$	11100	28	$f_{11}(x)$
α^{14}	$z^4 + z^3 + z^2 + 1$	11101	29	$f_7(x)$
α^{15}	$z^4 + z^3 + z^2 + z + 1$	11111	31	$f_{15}(x)$
α^{16}	$z^4 + z^3 + 1 + z$	11011	27	$f_1(x)$
α^{17}	$z^4 + z + 1$	10001	19	$f_3(x)$
α^{18}	z +1	00011	3	$f_5(x)$
α^{19}	$z^2 + z$	00110	6	$f_7(x)$
α^{20}	$z^3 + z$	01100	12	$f_3(x)$
α^{21}	$z^4 + z^2$	11000	24	$f_{11}(x)$
α^{22}	$z^4 + z^2 + 1$	10101	21	$f_{11}(x)$

α^{23}	$z^3 + z^2 + z + 1$	01111	15	$f_{15}(x)$
α^{24}	$z^4 + z^3 + z^2 + z$	11110	30	$f_3(x)$
α^{25}	$z^4 + z^3 + 1$	11001	25	$f_7(x)$
α^{26}	$z^4 + z^2 + z + 1$	10111	23	$f_{11}(x)$
α^{27}	$z^3 + z + 1$	010111	11	$f_{15}(x)$
α^{28}	$2^4 + z^2 + 2$	101110	22	$f_7(x)$
α^{29}	$2^3 + 1$	01001	9	$f_{15}(x)$
α^{30}	$2^4 + 2$	10010	18	$f_{15}(x)$

The generator polynomial for correcting at least t errors is given by
$g(x) = \text{LCM}\,[f_1(x)\, f_2(x), ..., f_{2t}(x)]$.
$g(x) = x^5 + (z+1)\, x^4 + (z^2 + z + 1)\, x^3 + (z + 1)\, x^2 + zx + z^4$

Q5.4 Over GF(2) for RS code $N = 2^1 - 1 = 1$
Generator polynomial $(x - \alpha^0) = (x - 1)$

Q5.5 Taking values of 2's from $GF(2^n)$ construction

(i) RS (15, 11) code
$n = 15, k = 11 \quad d^* = n - k + 1 = 5$
$t = (n - k)/2 = 2.$
$g(x) = (x - 2)(x - 2^2)(x - 2^3)(x - 2^4)$
$= x^4 + (2^3 + 2^2 + 1)x^3 + (2^3 + 2^2)x^2 + z^3(x) + (z^2 + 2 + 1)$
$= x^4 + \alpha^{13}\, x^3 + x^6\, x^2 + \alpha^3\, x + \alpha^{10}$

(ii) RS (15, 7) $\quad n = 15, k = 7$
$d^* = 15 - 7 + 1 = 9$
$t = (n - k)/2 = 4$

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)(x - \alpha^5)(x - \alpha^6)(x - \alpha^7)(x - \alpha^2)(x - \alpha^8)$$

(iii) Taking values of α's from Table II RS (31, 21)
$n = 31, \; k = 21, \; d^* = 11, \; t = (n - k)/2 = 5$
$g(x) = (x - \alpha)(x - \alpha 2)(x - \alpha^3) \ldots\ldots\ldots\ldots (x - \alpha^9)(x - \alpha^{10})$

Q5.6 Hint: Similar to example 5.10.

Q5.7 Hint: Start with a RS code over $GF(q^m)$ for a designed distance d. Then show that BCH code is a subfield subcode of a Reed Solomon code of the same designed distance.

Q5.8 The theorem is true if $\mu = 1$. If it is true for all $\mu - 1$ by $\mu - 1$ Vendermonde matrices, then it is also true for all μ by μ Vendermonde matrices. Replace X1 by the indeterminate x and transpose the matrix. Then the determinant is a function of x, given by

$$D(x) = \det \begin{bmatrix} 1 & x & x^2 & \cdots & x^{\mu-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{\mu-1} \\ \vdots & \vdots & & \vdots & \\ 1 & X_\mu & X_\mu^2 & \cdots & X_\mu^{\mu-1} \end{bmatrix}$$

The determinant can be expanded in terms of elements of the first row multiplied by the cofactors of these elements of the first row. This gives a polynomial in x of degree μ - 1, which can be written

$$D(x) = d_{\mu-1}x^{\mu-1} + \cdots + d_1 x + d_0$$

The polynomial *D(x)* has at most μ - 1 zeros. The coefficient $d_{\mu-1}$ is itself the determinant of a Vandermonde matrix, and by the induction hypothesis, is nonzero. If for any *i*, $2 \le i \le \mu$, we set $x = X_i$, then two rows of the matrix are equal, and $D(X_i) = 0$. Thus for each $i \ne 1$, X_i is a zero of $D(X_i)$, and because they are all distinct and there are μ - 1 of them, the polynomial can easily factored:

$$D(x) = d_{\mu-1}\left[\prod_{i=2}^{\mu}(x - X_i)\right].$$

Therefore the determinant of the original Vandermonde matrix is

$$D(X_1) = d_{\mu-1}\left[\prod_{i=2}^{\mu}(X_1 - X_i)\right].$$

This is non zero because $d_{\mu-1}$ is nonzero and X_1 is deferent from each of the remaining X_i. Hence the determinant of the μ by μ Vendermonde matrix is nonzero, and by induction, the theorem is true for all μ.

Q5.9 (i) Given: $\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 10 \\ 1 & 2^2 & 3^2 & 10^2 \\ 1 & 2^3 & 3^3 & 10^3 \\ & & & \\ 1 & 2^8 & 3^8 & 10^8 \end{bmatrix}$.

We observe that $s_r = \left[\sum_{i=1}^{10} i^r\right]_{\text{mod}11} = 0$ for $r = 0, 1, 2, 3, ..,8$.

Thus all the 10 columns of $\boldsymbol{H}$ add up to the zero vector. Hence $d^* = 10 \Rightarrow t = 4$.

(ii) The size of $\boldsymbol{H}$ is $(n\text{-}k)$ x n. Thus $n - k = 9$, $n = 10 \Rightarrow k = 1$.
In this case, $n - k + 1 = 9 + 1 = 10 = d^*$.
Thus, it is optimal in the sense of the Singleton bound.

Q5.10 (i) Given $\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & 2 & 3 & 4 & \ldots & 10 \\ 1 & 2^2 & 3^2 & 4^2 & \ldots & 10^2 \\ 1 & 2^3 & 3^3 & 4^3 & \ldots & 10^3 \\ 1 & 2^4 & 3^4 & 4^4 & \ldots & 10^4 \\ 1 & 2^5 & 3^5 & 4^5 & \ldots & 10^5 \end{bmatrix}$

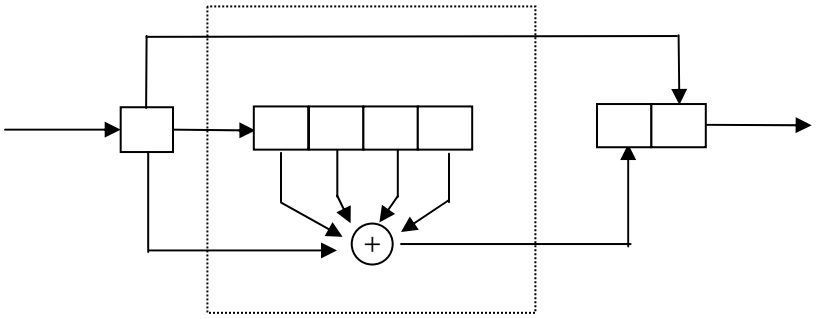
Use the same approach as the previous question.

(ii) First convert the matrix into $\boldsymbol{H} = [-\boldsymbol{P}^{\boldsymbol{T}} \mid \boldsymbol{I}]$ form. Since the math is over $GF(11)$, and $q = 11$ = odd, its simply modulo 11 arithmetic. The generator matrix is given by $\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{P}]$.

Q5.11 (i) $x^8 + x^4 + x^3 + x^2 + 1$

SOLUTIONS FOR CHAPTER 6

Q6.1 R = 1/2 , v = 4, d* = 6



(i) There are $2^4 = 16$ states for this encoder. The state transitions and the output is given in the table below.

Input	Current State				Next State				Output	
0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	0	0	0	1	1
0	0	0	0	1	0	0	0	0	0	0
1	0	0	0	1	1	0	0	0	1	1
0	0	0	1	0	0	0	0	1	0	1
1	0	0	1	0	1	0	0	1	1	0
0	0	0	1	1	0	0	0	1	0	1
1	0	0	1	1	1	0	0	1	1	0
0	0	1	0	0	0	0	1	0	0	1
1	0	1	0	0	1	0	1	0	1	0
0	0	1	0	1	0	0	1	0	0	1
1	0	1	0	1	1	0	1	0	1	0
0	0	1	1	0	0	0	1	1	0	0
1	0	1	1	0	1	0	1	1	1	1
0	0	1	1	1	0	0	1	1	0	0
1	0	1	1	1	1	0	1	1	1	1
0	1	0	0	0	0	1	0	0	0	1
1	1	0	0	0	1	1	0	0	1	0
0	1	0	0	1	0	1	0	0	0	1
1	1	0	0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	0	1	0	0
1	1	0	1	0	1	1	0	1	1	1
0	1	0	1	1	0	1	0	1	0	0
1	1	0	1	1	1	1	0	1	1	1

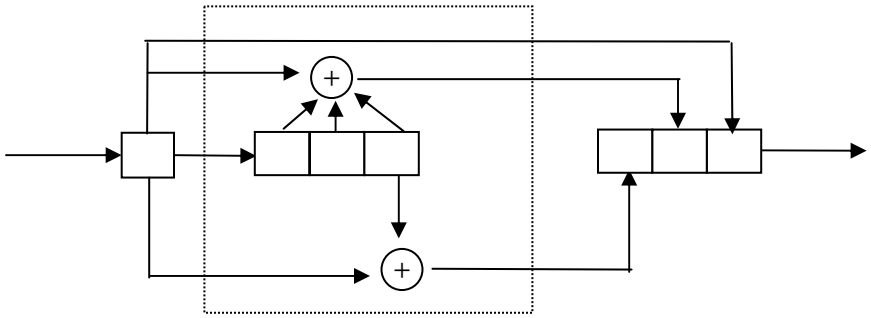
0	1	1	0	0	0	1	1	0	0	0
1	1	1	0	0	1	1	1	0	1	1
0	1	1	0	1	0	1	1	0	0	0
1	1	1	0	1	1	1	1	0	1	1
0	1	1	1	0	0	1	1	1	0	1
1	1	1	1	0	1	1	1	1	1	0
0	1	1	1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1	1	1	0

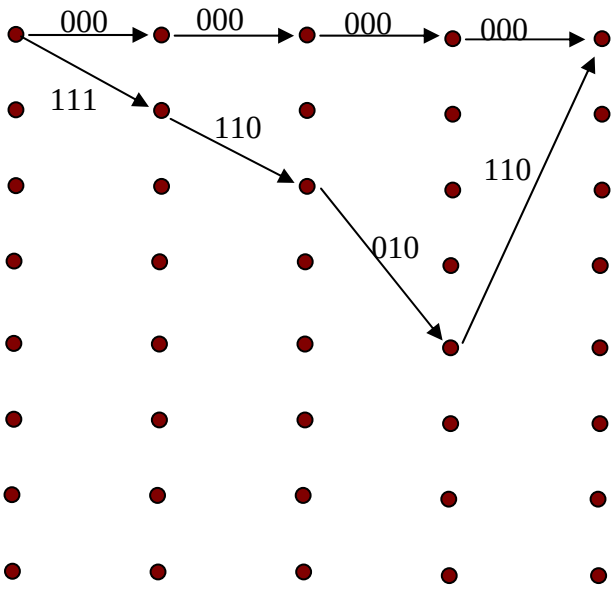
(iii) $d_{free} = 6$.

(iv) $G(D) = [1 \quad D^4+D^3+D^2+D+1]$.

(v) Non catastrophic since GCD $[1 \quad D^4+D^3+D^2+D+1] = 1$.

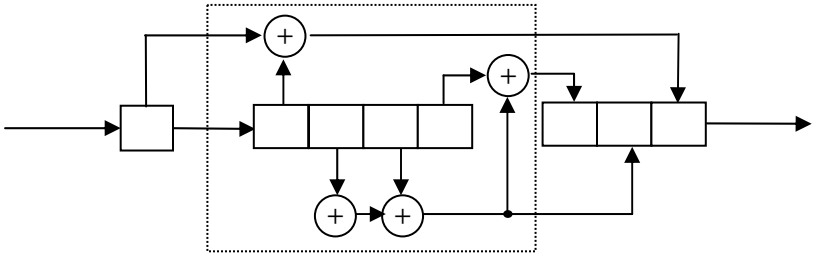
Q 6.2 (i)





(ii) $d_{free} = 8$ (see the trellis diagram).

Q6.3 (i)



Trellis diagram will have 16 states. Generate mechanically, or write a small computer program. The state transitions in a tabular for is given below.

Present state	Next state		Output	
	i/p = 0	i/p = 1	i/p = 0	i/p = 1
0000	0000	1000	000	001
0001	0000	1000	000	001
0010	0001	1001	110	111
0011	0001	1001	110	111
0100	0010	1010	010	011
0101	0010	1010	010	011
0110	0011	1011	100	101
0111	0011	1011	100	101
1000	0100	1100	001	000
1001	0100	1100	001	000
1010	0101	1101	111	110
1011	0101	1101	111	110
1100	0110	1110	011	010
1101	0110	1110	011	010
1110	0111	1111	101	100
1111	0111	1111	101	100

(ii) $k_0 = 1$, $n_0 = 3$, Rate, R = 1/3
$\nu = 4$, m = 1.

(iii) $d^* = 5$, $d_{free} = 5$
(iv) $G(D) = [1 + D \quad D^2 + D^3 \quad D^2 + D^3 + D^4]$

Q6.4 (i) k = 3, n = 4, v = 1 m = 4 + 2 + 2 = 8, R = ¾.

$v = \sum_{i=1}^{k_0} \max_j \left[\deg g_{ij}(D)\right]$ = sum of highest power of $g_{ij}(D)$ in each row of the matrix $G(D)$ = 2 + 2 + 4 = 8. The $G(D)$ is given below.

$$\text{(ii)}\, G(D) = \begin{bmatrix} D+D^2 & D^2 & D+D^2 & 0 \\ D^2 & D & D & D^2 \\ 0 & 0 & D^4 & D^2 \end{bmatrix}_{3x4}$$

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

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad G_2 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$G_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad G_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Q6.5 $$G(D) = \begin{bmatrix} D & 0 & 1 & D^2 & D+D^2 \\ D^2 & 0 & 0 & 1+D & 0 \\ 1 & 0 & D^2 & 0 & D^2 \end{bmatrix}$$

$k_0 = 3$, $n_0 = 5$, R = 3/5

(ii) GCD [G(D)] = 1

$\Rightarrow$ It's a non-catastrophic convolutional code.

Q6.6 Hint:

Use:

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{P}_0^T & -\boldsymbol{I} & & & & & & & & \cdots \\ \boldsymbol{P}_1^T & \mathbf{0} & \boldsymbol{P}_0^T & -\boldsymbol{I} & & & & & & \\ \boldsymbol{P}_2^T & \mathbf{0} & \boldsymbol{P}_1^T & \mathbf{0} & \boldsymbol{P}_0^T & -\boldsymbol{I} & & & & \\ \vdots & & \vdots & & \vdots & & & & & \vdots \\ \boldsymbol{P}_m^T & \mathbf{0} & \boldsymbol{P}_{m-1}^T & \mathbf{0} & \boldsymbol{P}_{m-2}^T & \mathbf{0} & \cdots & \boldsymbol{P}_0^T & -\boldsymbol{I} & \cdots \\ & & \boldsymbol{P}_m^T & \mathbf{0} & \boldsymbol{P}_{m-1}^T & \mathbf{0} & \cdots & & & \\ & & & & \boldsymbol{P}_m^T & \mathbf{0} & \cdots & & & \cdots \end{bmatrix}, \text{ and}$$

$$\boldsymbol{G} = \left[\begin{array}{cc|cc|cc|c|cc|cc|cc|c} \boldsymbol{I} & \boldsymbol{P}_0 & \mathbf{0} & \boldsymbol{P}_1 & \mathbf{0} & \boldsymbol{P}_2 & \cdots & \mathbf{0} & \boldsymbol{P}_m & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots \\ \mathbf{0} & \mathbf{0} & \boldsymbol{I} & \boldsymbol{P}_0 & \mathbf{0} & \boldsymbol{P}_1 & \cdots & \mathbf{0} & \boldsymbol{P}_{m-1} & \mathbf{0} & \boldsymbol{P}_m & \mathbf{0} & \mathbf{0} & \cdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I} & \boldsymbol{P}_0 & \cdots & \mathbf{0} & \boldsymbol{P}_{m-2} & \mathbf{0} & \boldsymbol{P}_{m-1} & \mathbf{0} & \boldsymbol{P}_m & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \mathbf{0} & \boldsymbol{P}_{m-2} & \mathbf{0} & \boldsymbol{P}_{m-1} & \cdots \\ & & & & & & & & & \vdots & \vdots & \mathbf{0} & \boldsymbol{P}_{m-2} & \cdots \\ & & & & & & & & & & & \vdots & \vdots & \end{array}\right],$$

where $\boldsymbol{G}_l = [g_{ijl}]$ and $g_{ij}(D) = \sum_l g_{ijl} D^l$.

Q6.7 (i) $g_1(D) = 2D^3 + 3D^2 + 1$ over GF(4)
$g_2(D) = D^3 + D + 1$

This is a rate ½ encoder.

Hint: You can break up the problem by representing each symbol $\in \{0, 1, 2, 3\}$ by two bits. Thus, this encoder takes in one quaternary symbol (2 bits) and converts it to 2 quaternary symbols (4 bits). The memory unit of this encoder consists of 3 delay elements. Thus the number of states = $4^4 = 256$. In reality, such an encoder will be implemented using a 8-bit shift register, with two bit-shifts at a time. The logic circuit will be implemented using GF(4) arithmetic. It is advisable to write a small computer program to calculate the d_{min} for this code.

(ii) GCD $[g_1, g_2] = 1 \Rightarrow$ non catastrophic

Q6.8 $g_1 = D^3 + D^2 + 1$
$g_2 = D^3 + D$
$g_3 = D^2 + 1$

Input	Present state	Next state	Output
0	000	000	000
1	000	100	101
1	100	110	111
0	110	011	110
0	011	001	011
0	001	000	111
1	000	100	101
0	100	010	111
1	010	101	011
1	001	110	100
0	110	101	110
1	011	101	110
0	101	010	101
1	010	101	001

(i) Encoded Stream for input = 01100011110101 :

000 101 111 110 011 111 101 111
011 100 001 110 101 001

(ii) Encoded Stream for input = 1010101010 .....

101 010 001 101 001 101 001 101

(iii) 0011011

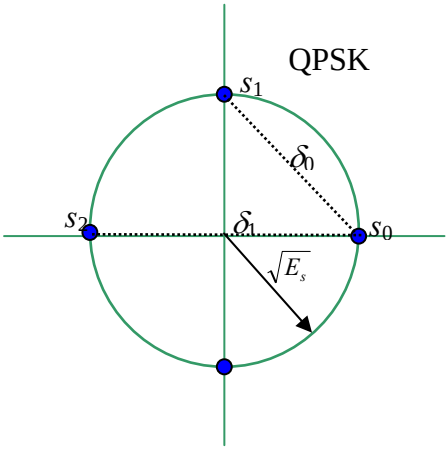
Q6.9 Hint: Solve the problem similar to problem 6.7. You can break up the problem by representing each symbol $\in \{0, 1, 2\}$ by two bits. Thus, this encoder takes in one ternary symbol (2 bits) and converts it to 2 ternary symbols (4 bits). The memory unit of this encoder consists of 4 delay elements. Thus the number of states = $3^4 = 81$. Write a small computer program to calculate the d_{min} for this code.

SOLUTIONS FOR CHAPTER 7

Q7.1 Given 2/3 convolutional encoder with

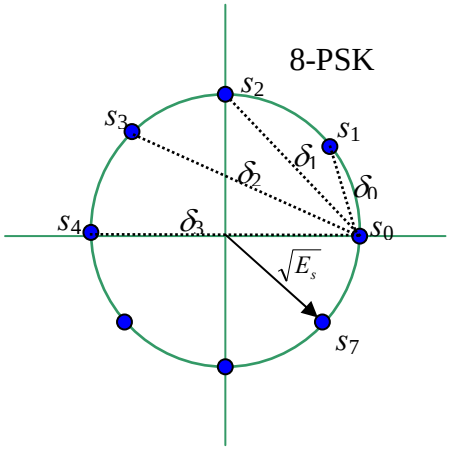
$$G(D)=\begin{pmatrix} 1 & D & D+D^2 \\ D^2 & 1+D & 1+D+D^2 \end{pmatrix}$$

(a) the encoder has 16 states in the Trellis diagram
(b) the free Euclidean distance:



$\delta_0^2 = 2E_s$

$\delta_1^2 = 4E_s$



$\delta_0^2 = 0.586E_s$

$\delta_1^2 = 2E_s$

$\delta_2^2 = 3.414E_s$

$\delta_3^2 = 4E_s$

Gray coded using 8 psk signal constellation

$d_{free}^2 = 2E_s + 2E_s + .586\ E_s = 4.586\ E_s.$

$d_{free} = 2.1415\ \sqrt{E}$

(c) The asymptotic coding gain w.r.t. QPSK

$$g_\infty = g\big|_{SNR\to\infty} = 10\log\frac{\left(d_{free}^2/E_s\right)_{coded}}{\left(d_{free}^2/E_s\right)_{uncoded}},$$

$= 10 \log (4.586/2)$

$= 3.6040$ dB.

Q7.2

(a) The free Euclidean distance:

$d_{free}^2 = 2E_s + 2E_s + 2E_s$

$d_{free} = 2.4495 \sqrt{E}.$

(b) $g_\infty = g|_{SNR\to\infty} = 10\log\frac{\left(d_{free}^2 / E_s\right)_{coded}}{\left(d_{free}^2 / E_s\right)_{uncoded}}$,

= 10 log (6/2)

= 4.7712 dB.

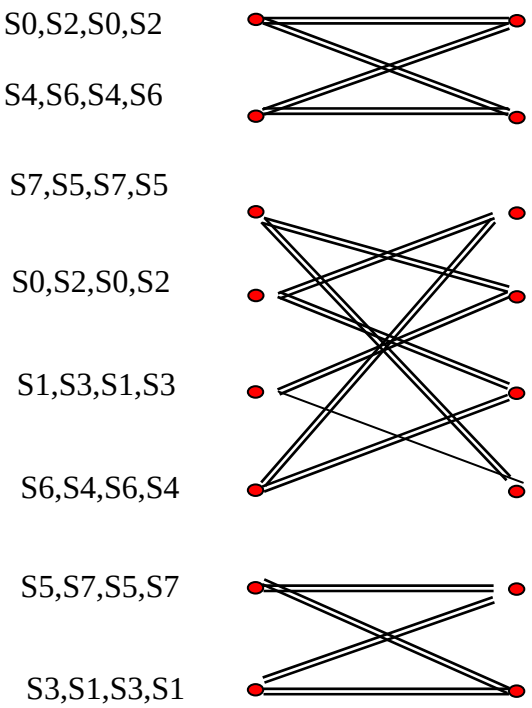
Q7.3

(i)

Present State				Input			Next State				Output		
0	0	0		0	0		0	0	0		0	0	0
0	0	0		0	1		0	0	0		0	1	0
0	0	0		1	0		1	1	0		0	0	0
0	0	0		1	1		1	1	0		0	1	0
0	0	1		0	0		0	1	0		1	0	1
0	0	1		0	1		0	1	0		1	1	1
0	0	1		1	0		1	0	0		1	0	1
0	0	1		1	1		1	0	0		1	1	1
0	1	0		0	0		0	0	1		0	0	0
0	1	0		0	1		0	0	1		0	1	0
0	1	0		1	0		1	1	1		0	0	0
0	1	0		1	1		1	1	1		0	1	0
0	1	1		0	0		0	1	1		1	0	1
0	1	1		0	1		0	1	1		1	1	1
0	1	1		1	0		1	0	1		1	0	1
0	1	1		1	1		1	0	1		1	1	1
1	0	0		0	0		0	0	1		1	0	0
1	0	0		0	1		0	0	1		1	1	0
1	0	0		1	0		1	1	1		1	0	0
1	0	0		1	1		1	1	1		1	1	0
1	0	1		0	0		0	1	1		0	0	1
1	0	1		0	1		0	1	1		0	1	1
1	0	1		1	0		1	0	1		0	0	1
1	0	1		1	1		1	0	1		0	1	1
1	1	0		0	0		0	0	0		1	0	0
1	1	0		0	1		0	0	0		1	1	0
1	1	0		1	0		1	1	0		1	0	0

1	1	0		1	1		1	1	0		1	1	0
1	1	1		0	0		0	1	0		0	0	1
1	1	1		0	1		0	1	0		0	1	1
1	1	1		1	0		1	0	0		0	0	1
1	1	1		1	1		1	0	0		0	1	1

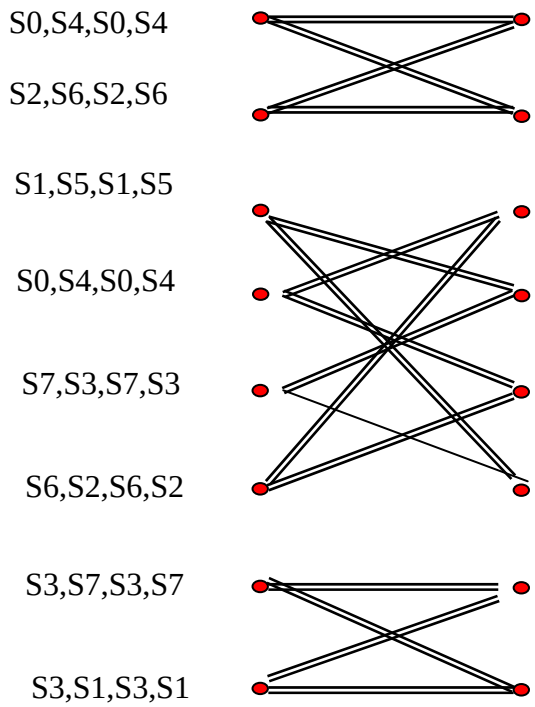
(ii) There are 8 states in the trellis diagram. Construct it using the table above. The trellis diagram has parallel paths. In succinct form, the trellis diagram can be written as



(iii) $d^2_{free} = 2E_s$

$N(d^2_{free}) = 2 \times 8 = 16.$

(iv) After set partitioning: $d^2_{free} = 4E_s$



(v) Encoded symbols for

Natural Mapping: S0, S4, S0, S2, S2

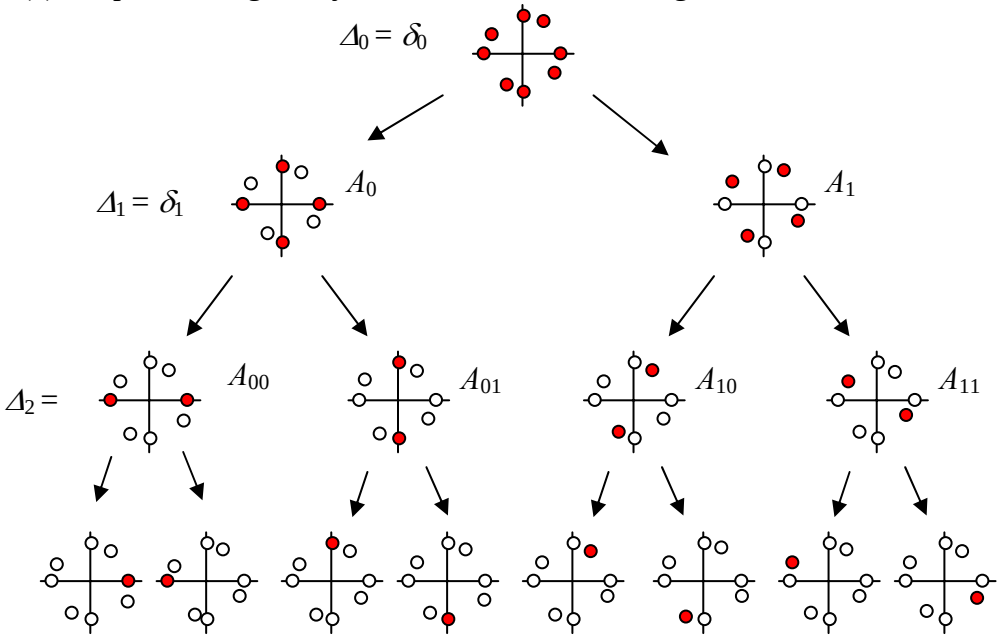
Mapping using set partitioning: S2, S0, S0, S4, S4 .

(vi) Asymptotic coding gain for

Natural Mapping: 10 log (2 / 0.586) = 5.33 dB

Mapping using set partitioning: 10 log (4 / 0.586) = 8.34 dB.

Q7.4(a) Set partitioning of asymmetric constellation diagram:

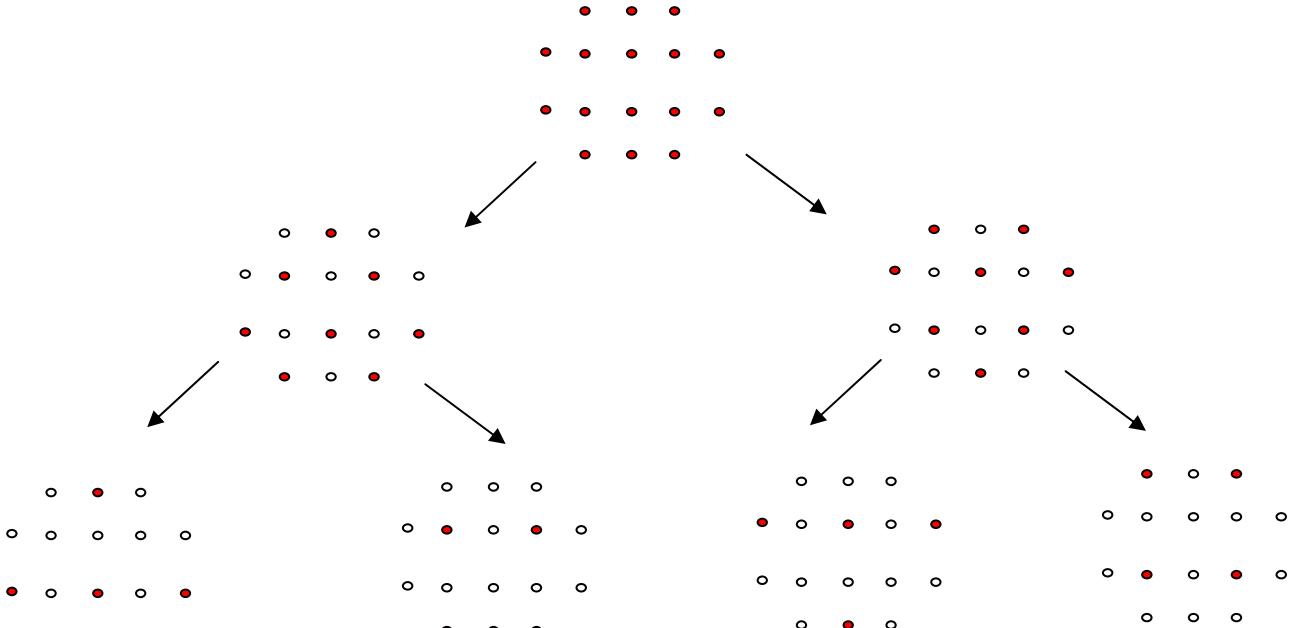


(b) If the minimum Euclidean distance between parallel transitions is given by $\Delta_{\tilde{m}+1}$ and the minimum Euclidean distance between non-parallel paths of the trellis is given by $d_{free}(\tilde{m})$, the free Euclidean distance of the TCM encoder is

$$d_{free} = min[\Delta_{\tilde{m}+1}, d_{free}(\tilde{m})].$$

If all the symbols are used with equal frequency, the asymmetric constellation diagram will result in a smaller value of d_{free} in general (i.e., poorer performance).

Q7.5 Hint: Perform set partitioning as follows;



Q7.6 Hint: For the right hand side of the inequality, divide both the numerator and denominator by K and take lim $K \to \infty$.

Q7.7 Hint: Use equation 7.55.

Q7.8

a) The number of states depends on the desired BER and the computational complexity permissible.
b) The internal memory of the encoder will be decided by the number of states in the trellis.
c) The decision regarding parallel paths can be taken upon calculation of the d_{free}. Parallel paths cannot be ruled out right in the beginning. The number of branches emanating from each node will depend on the constellation size of the modulation scheme.
d) The decision is between MPSK and MQAM. Beyond M = 16 it is better to use MQAM (see their BERs in AWGN!).
e) Since AWGN is under consideration, we will use the Ungerboek's design rules.

Q7.9

Viterbi decoding metric is $m(r_l, s_l) = \ln p(r_l/s_l)$. The metric of the above form is chosen because it behaves like a distance measure between the received signal and the signal associated with the corresponding branch in the trellis. It has an additive property, namely, that the total metric for a sequence of symbols is the sum of the metric for each channel input and output pair.

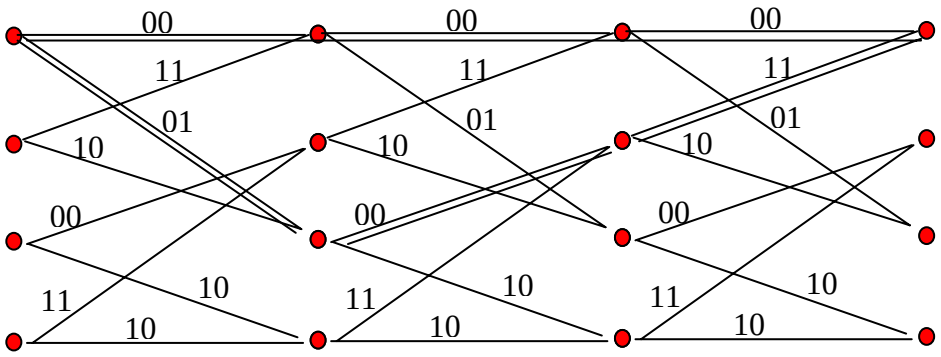
Q7.10.

(a) The direct application of equation 7.55 gives the new $d_p^2(L)$ equal to ten times the previous $d_p^2(L)$. However, to obtain such a large value of $d_p^2(L)$, we need to construct trellis with a larger number of states.

(b) The new d_{free}^2 will be larger resulting in an improvement in the performance of the new TCM scheme over AWGN channels as well.

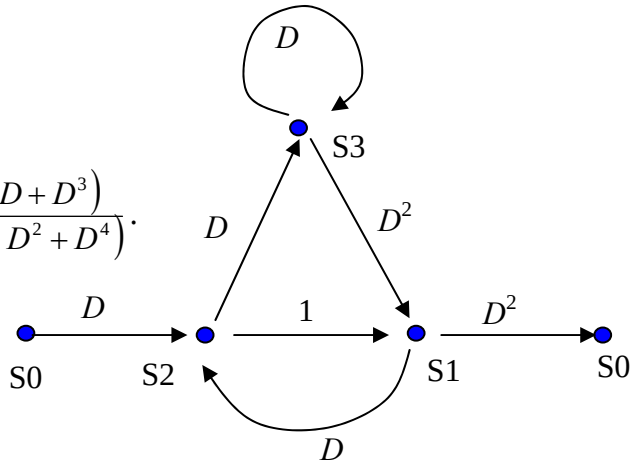
Q7.11

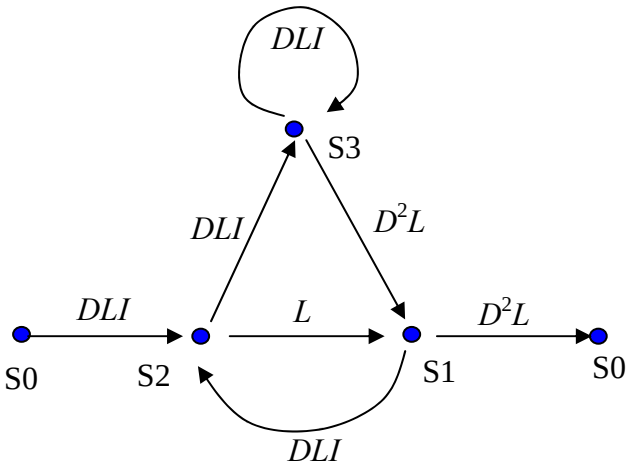
(a) The trellis diagram of the encoder:



(b) $T(D) = \dfrac{D^3\left(1 - D + D^3\right)}{\left(1 - 2D + D^2 + D^4\right)}$.

(c)





$$T(D,L,I)=\frac{L^3ID^3(1-LID)+L^4I^2D^6}{(1-LID-L^2ID+L^3I^2D^2+L^3I^2D^4)}.$$

(d) d_{free}^{H} = 3.

(e) Only one path (see the trellis diagram).

Q7.12: Hint: Carry out the mathematical excercise along the lines in Section 7.6.

Q7.13 (i) TCM2

(iii) For AWGN Channel: TCM2
For Fading Channel: TCM1

SOLUTIONS FOR CHAPTER 8

Q8.1 (a) Let M be the size of alphabet. Then to crack this code we need 'M-1 attempts' by using brute force attack. In this case we require 26 – 1 = 25 attempts.

(b) 25 ms

Q8.2 THE CAT IS OUT OF THE BOX

Q8.3. (a) Assuming plain text is staggered between k rows, we apply brute force attack for each 'k', $1<k<n$, where 'n' is the length of the cipher text.
For each 'k', divide cipher text into $\lfloor n/k \rfloor$ sized blocks (total k blocks).
Number of attacks = (n - 2).
(b) Given k, apply the attack corresponding to k as given in part a) to decrypt.

Q8.4. First stage:
Size of the key < 36 (36 is worst case).
Number of possible rectangular matrices = 36! (Factorial 36).
Second stage:
Key size k < 36 again
We need to attack for key sides from 1 to 36.
So total number of attacks = $36!\left[\sum_{k=1}^{36} k!\right]$.

(b) Given the cipher text, use the second key to form the second matrix (write horizontally, read vertically). After reading horizontally, we get intermediate cipher text. Next, use the first key to form the rectangular matrix. For finding plain text corresponding to XY location, look at X-row and Y-column.

Q8.5. (a) Number of attacks needed < number of vectors = 2n

Q8.6 27!

Q8.7
P = 29, Q = 61
N = PQ = 29 * 61 = 1769
Q(N) = (P-1) (Q-1) = 28 * 60 =1680

Let E = 11 , as 11 * 611 – 4 * 1680 =1
Take D = 611
11 is the public key
611 is the private key.

(b) R = 82, S = 83 , A = 65

822 = 1417 mod 1769
824 = 74 mod 1769
828 = 169 mod 1769
823 = 1209 mod 1769
8211 = 886 mod 1769

832 = 1582 mod 1769
834 = 1358 mod 1769
838 = 166 mod 1769
833 = 1118 mod 1769
8311 = 545 mod 1769

652 = 687 mod 1769
654 = 1415 mod 1769
658 = 1480 mod 1769
6511 = 371 mod 1769

Therefore RSA is encoded as {886, 545, 371}.

(c) P= 37, Q = 67
N=PQ =37 *67 = 2479
Q(N) = (P-1) (Q-1) = 36 * 66 = 2376
E = 5
D = 1901
Public key = 5
Private key = 1901

Q8.8 Hint: Find prime numbers below 1090 and 10100 and subtract from the later.

Q8.9

(i) Each pair should have different keys so total number of distinct keys $= {}^{N}C_2 = \binom{N}{2} = \frac{N(N-1)}{2}$.

(ii) There is 1 public key and N private keys.

Q8.10 1/3

Q8.11 (i) Total number of subblocks = n = p2 / q2
It requires n! brute force attacks.

(ii) Key size = $log_2 n!$