EE512: Error Control Coding

Solution for Assignment on Miscellaneous Topics

April 25, 2007

2. Let $\underline{c}$ be a codeword of the $(n, 1)$ repetition code and $\underline{s} = 1 - 2\underline{c}$ be the symbol vector under BPSK Modulation. Let $\underline{r} = \underline{s} + \underline{z}$ be the received vector over an AWGN channel.

   The decoded codeword obtained from a maximum likelihood decoder for a code C is given by

   $$\hat{\underline{c}} = \arg\max_{\underline{u} \in C} f(\underline{r}|\underline{c} = \underline{u}),$$

   where $f(\underline{r}|\underline{c} = \underline{u})$ is the conditional pdf of the received vector $\underline{r}$ given that the transmitted codeword is $\underline{u}$. Over an AWGN channel the conditional pdf can be written as

   $$f(\underline{r}|\underline{c} = \underline{u}) = \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left(-\frac{\sum_{i=1}^{n}(r_i - s_i)^2}{2}\right),$$

   since given $\underline{u}$ the r_i are independent. Hence, maximum-likelihood decoding in an AWGN channel reduces to minimizing the squared Euclidean distance, and can be written as

   $$\hat{\underline{c}} = \arg\min_{\underline{u} \in C} \sum_{i=1}^{n} (r_i - s_i)^2.$$

   Since $s_i \in \pm 1$ for BPSK modulation, the ML codeword estimate is

   $$\hat{\underline{c}} = \arg\max_{\underline{u} \in C} \sum_{i=1}^{n} r_i s_i.$$

   For the $(n, 1)$ repetiton code $C = \{\underline{c}_0 = 00\ldots0,\ \underline{c}_1 = 11\ldots1\}$, the ML rule is

   $$\begin{aligned} \hat{\underline{c}} &= \arg\max_{\underline{u} \in C} \{r_1 + r_2 + \ldots + r_n, r_1 + r_2 + \ldots + r_n\} \\ &= \begin{cases} 00\ldots0 \text{ if } r_1 + r_2 + \ldots + r_n > 0, \\ 11\ldots1 \text{ if } r_1 + r_2 + \ldots + r_n < 0. \end{cases} \end{aligned}$$

   Probablity of Error:

   $$\begin{aligned} P(\text{error}) &= P(\hat{\underline{c}} = \underline{c}_1|\underline{c} = \underline{c}_0)P(\underline{c} = \underline{c}_0) + P(\hat{\underline{c}} = \underline{c}_0|\underline{c} = \underline{c}_1)P(\underline{c} = \underline{c}_1), \\ &= \frac{1}{2}[P(\hat{\underline{c}} = \underline{c}_1|\underline{c} = \underline{c}_0) + P(\hat{\underline{c}} = \underline{c}_0|\underline{c} = \underline{c}_1)], \\ &= \frac{1}{2}[P(r_1 + r_2 + \ldots + r_n > 0|\underline{c} = \underline{c}_1) + P(r_1 + r_2 + \ldots + r_n < 0|\underline{c} = \underline{c}_0). \end{aligned}$$

   Since $r_i \sim N(s_i, \sigma^2)$ are iid random variables,

   $$\lambda = r_1 + r_2 + \ldots + r_n \ \sim N(s_1 + s_2 + \ldots + s_n, n\sigma^2).$$

   When $\underline{c}_0$ is transmitted, $\lambda \sim N(n, n\sigma^2)$. When $\underline{c}_1$ is transmitted, $\lambda \sim N(-n, n\sigma^2)$. Therefore,

   $$\begin{aligned} P(\text{error}) &= \frac{1}{2}\left[Q\left(\frac{n}{\sqrt{n}\sigma}\right) + Q\left(\frac{n}{\sqrt{n}\sigma}\right)\right], \\ &= Q\left(\frac{\sqrt{n}}{\sigma}\right), \\ &= Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \end{aligned}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-x^2/2} dx$ and $E_b/N_0 = n/(2\sigma^2)$. Hence, no coding gain is obtained by the use of repetition codes.

3.

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

Let C_1 be the $(5, 2)$ code with parity check matrix H. We see that

$$C = \{00000,\ 01110,\ 10101,\ 11011\}.$$

(a) *Soft ML Decoder:* Let the received word over an AWGN Channel under BPSK Modulation be $\underline{r} = \underline{s} + \underline{n}$, where $\underline{s} = 1 - 2\underline{c}$ and $n_i \sim N(0, \sigma^2)$. The soft ML decoding rule for the code C_1 is

$$\hat{\underline{c}} = \begin{cases} 00000, & r_1 + r_2 + r_3 + r_4 + r_5 \text{ is max}, \\ 01110, & r_1 - r_2 - r_3 - r_4 + r_5 \text{ is max}, \\ 10101, & -r_1 + r_2 - r_3 + r_4 - r_5 \text{ is max}, \\ 11011, & -r_1 - r_2 + r_3 - r_4 - r_5 \text{ is max}. \end{cases}$$

(b) *ML hard-decision Decoder:* This is a syndrome decoder. The syndrome $\underline{s} = \underline{r}H^T$ identifies the estimated error vector (coset leader) $\hat{\underline{e}}$, which is added to the received vector $\underline{r}$ to get $\hat{\underline{c}} = \underline{r} + \hat{\underline{e}}$. The syndrome table for C_1 is as follows:

Syndrome, $\underline{s}$	Coset leader $\underline{e}$
000	00000
001	00100
010	01000
011	01100
100	10000
101	00010
110	00001
111	00101

Table 1: Syndrome Table for the $(5, 2)$ code C_1.

4.

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

Let C_2 be the $(5, 3)$ with generator matrix,G. We see that

$$C_2 = \{00000,\ 00110,\ 01001,\ 01111,\ 10011,\ 10101,\ 11010,\ 11100\}.$$

(a) *Soft ML Decoder:*

$$\hat{\underline{c}} = \begin{cases} 00000, & r_1 + r_2 + r_3 + r_4 + r_5 \text{ is max}, \\ 00110, & r_1 + r_2 - r_3 - r_4 + r_5 \text{ is max}, \\ 01001, & r_1 - r_2 + r_3 + r_4 - r_5 \text{ is max}, \\ 01111, & r_1 - r_2 - r_3 - r_4 - r_5 \text{ is max}, \\ 10011, & r_1 - r_2 - r_3 + r_4 + r_5 \text{ is max}, \\ 10101, & -r_1 + r_2 - r_3 + r_4 - r_5 \text{ is max}, \\ 11010, & -r_1 - r_2 + r_3 - r_4 + r_5 \text{ is max}, \\ 11100, & -r_1 - r_2 - r_3 + r_4 + r_5 \text{ is max}, \end{cases}$$

Syndrome, $\underline{s}$	Coset leader $\underline{e}$
00	00000
01	01000 (or) 00010
10	10000 (or) 00001
11	00100

Table 2: Syndrome Table for the $(5, 3)$ code C_2.

(b) *ML Hard-decision Decoder:* See Table 2.

6. Let D_i be the correlation metric for codeword $\underline{c}_i$ i.e.

$$\begin{aligned} D_1 &= r_1 + r_2 + r_3 + r_4 \\ D_2 &= r_1 - r_2 + r_3 - r_4 \\ D_3 &= -r_1 + r_2 - r_3 + r_4 \\ D_4 &= -r_1 - r_2 - r_3 - r_4 \end{aligned}$$

Decide in favour of 0000 if

$$D_1 > D_2 \quad \text{and } D_1 > D_3 \quad \text{and } D_1 > D_4,$$

$$\text{or } r_2 + r_4 > 0 \quad \text{and } r_1 + r_3 > 0 \quad \text{and } r_1 + r_2 + r_3 + r_4 > 0.$$

Decide in favour of 0101 if

$$D_2 > D_1 \quad \text{and } D_2 > D_4 \quad \text{and } D_2 > D_3,$$

$$\text{or } r_2 + r_4 < 0 \quad \text{and } r_1 + r_3 > 0 \quad \text{and } r_1 + r_3 > r_2 + r_4.$$

Decide in favour of 1010 if

$$D_3 > D_4 \quad \text{and } D_3 > D_1 \quad \text{and } D_3 > D_2,$$

$$\text{or } r_2 + r_4 > 0 \quad \text{and } r_1 + r_3 < 0 \quad \text{and } r_2 + r_4 > r_1 + r_3.$$

Decide in favour of 1111 if

$$D_4 > D_3 \quad \text{and } D_4 > D_2 \quad \text{and } D_4 > D_1,$$

$$\text{or } r_2 + r_4 < 0 \quad \text{and } r_1 + r_3 < 0 \quad \text{and } r_1 + r_2 + r_3 + r_4 < 0.$$

Since the third condition in each case above is redundant, we can rewrite the ML decision rule as follows:

$$\hat{\underline{c}} = \begin{cases} 0000, & \text{if } r_1 + r_3 > 0 \text{ and } r_2 + r_4 > 0 \\ 0101, & \text{if } r_1 + r_3 > 0 \text{ and } r_2 + r_4 < 0 \\ 1010, & \text{if } r_1 + r_3 < 0 \text{ and } r_2 + r_4 > 0 \\ 1111, & \text{if } r_1 + r_3 < 0 \text{ and } r_2 + r_4 < 0 \end{cases}$$

Therefore, the necessary number of real-number additions is $N_a = 2$ and the number of real comparisions is $N_c = 2$.

7. (a) A non-systematic encoder is shown in Fig. 1

$$G(D) = [1 + D^3 \;\; 1 + D + D^2 + D^3]$$

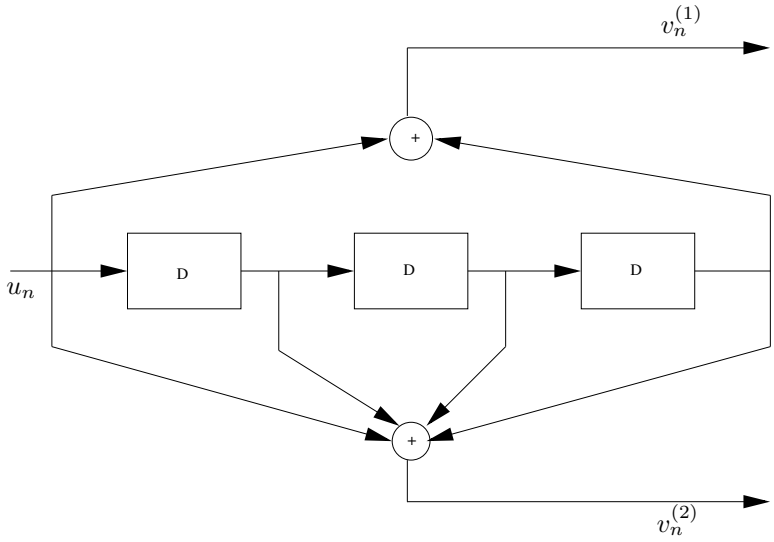

Figure 1: Non- Systematic Encoder.

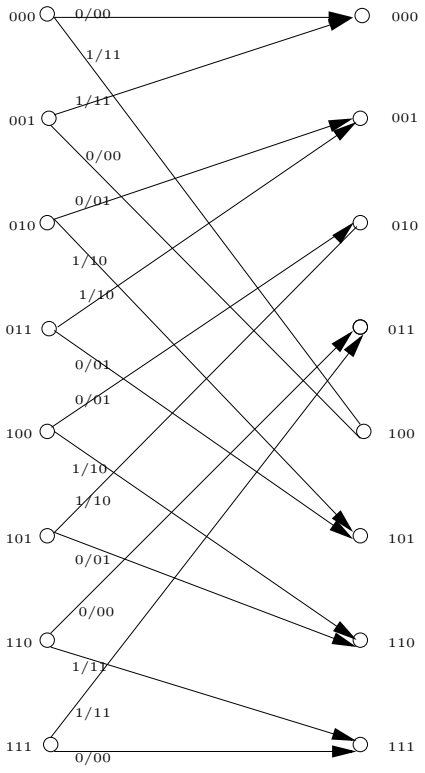

Figure 2: One Stage of Trellis for 1/2 code

(b) One stage of the complete trellis is shown in Fig. 2.

8. (a) The transfer function matrix is seen to be

$$G(D) = [1 + D^3 \;\; 1 + D + D^2 + D^3].$$

The relations between the input sequence $\{u_n\}$ and the output sequences $\{v_n^{(1)}\}$ and $\{v_n^{(2)}\}$

are as follows:

$$v_n^{(1)} = u_n^{(1)} + u_{n-3}^{(1)},$$
$$v_n^{(2)} = u_n^{(1)} + u_{n-1}^{(1)} + u_{n-2}^{(1)} + u_{n-3}^{(1)}.$$

(b) The trellis is the same as that of the previous problem. See Fig. 2.

(c) Encoding of $(11111\ldots\ldots)$:

$$v_n^{(1)} = 111000000\ldots\ldots$$
$$v_n^{(2)} = 101000000\ldots\ldots$$

This encoder is known as a catastrophic encoder, since it produces a finite-weight codeword for an infinite-weight input.

9. (a) The relations between the input sequence $\{u_n\}$ and the output sequences $\{v_n^{(1)}\}$ and $\{v_n^{(2)}\}$ are as follows:

$$v_n^{(1)} = u_n^{(1)},$$
$$v_n^{(2)} = u_n^{(1)} + u_{n-1}^{(1)}.$$

The trellis for 4 message bits is shown in Fig. 3.

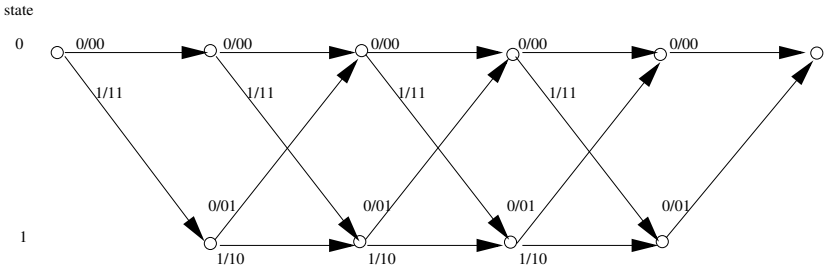

Figure 3: Trellis Diagram for 4 message bits with zero termination.

(b) Number of codewords = Number of possible messages = $2^4 = 16$.

(c) Viterbi decoding over a BSC is shown in Fig. 4. The final survivor is shown in red. The ML decoded message is seen to be 1000.

(d) Viterbi Decoding over AWGN is shown in Fig. 5. The final survivor is shown in red. The ML decoded message is seen to be 0111.

11. (a) Let α be the primitive element of $GF(2^m)$. Parity check matrix of C_R is given by

$$H_R = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \cdots & \alpha^{2t(n-1)} \end{pmatrix}.$$

Parity check matrix of C_B is given by

$$H_R = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(2t-1)} & \alpha^{2(2t-1)} & \cdots & \alpha^{(2t-1)(n-1)} \end{pmatrix}.$$

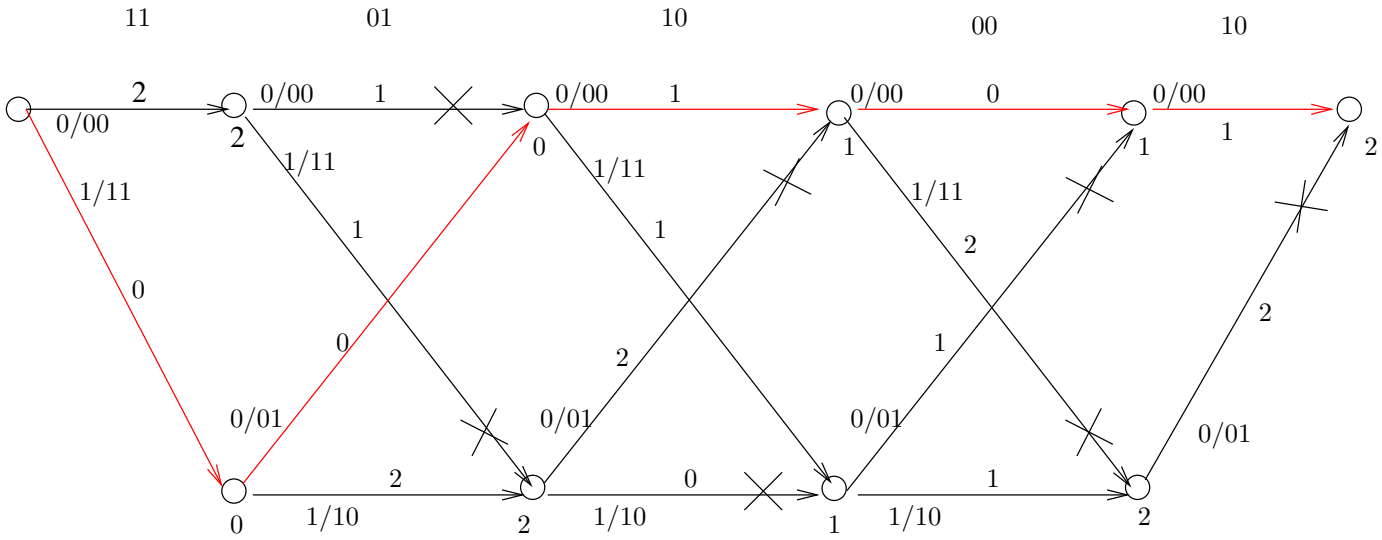

Figure 4: Viterbi Decoding over BSC.

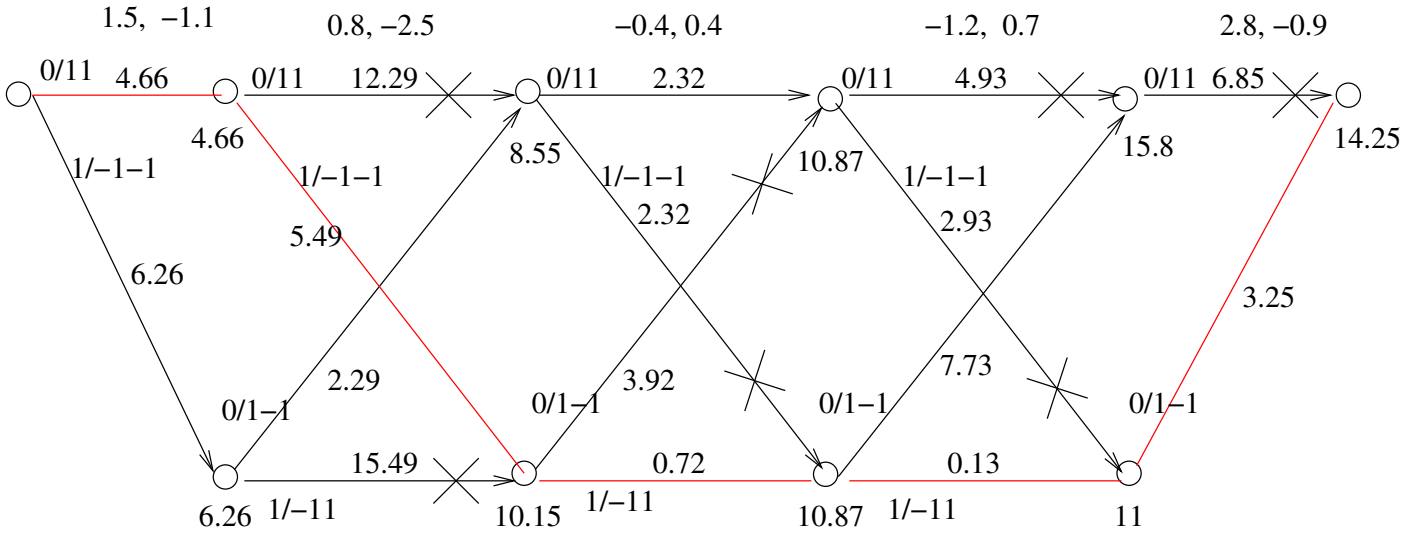

Figure 5: Viterbi Decoding over AWGN.

(b) Given that the codes are transmitted over BSC with transition probability p, the probability of symbol error $p_s = 1-(1-p)^m$. The probability of block error for the RS code C_R is given by

$$p_R = 1 - \sum_{i=0}^{t} \binom{n}{i} p_s^i (1-p_s)^{n-i}.$$

The probability of block error for the BCH code C_B is given by,

$$p_B = 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}.$$

12. The given encoder consists of an encoder E_1 for the $(7,4)$ Hamming code followed by an encoder E_2 for $(127,121)$ RS code over $GF(2^7)$.

(a) A 4 bit message is converted into a 7-bit codeword by E_1. Each 7-bit Hamming codeword forms a single symbol over $GF(2^7)$. 121 such symbols form one message vector for E_2. Thus,

we have to start with $4 \times 121 = 484$ bits at the input of E_1 to get a 121-symbol message vector at the input of E_2. The length of the final coded vector is $7 \times 127 = 889$ bits. Thus, dimension and length of the overall bianry code are, $k = 484$ and $n = 889$.

(b) The given decoder consists of a bounded distance decoder (BDD) for the RS code, followed by the syndrome decoder (SD) for the Hamming code. We assume that if the BDD for the RS code fails, it hands over the received word as such to the SD. The BDD fails when there are more than 3 symbol errors. We need to find the bit error correcting capability t_b of the entire decoder. It is clear that $t_b \geq 3$ since the BDD can correct 3 symbol errors.

Let us check if 4-bit errors are correctable by the concatenated decoder. The only case for which the BDD fails due to a 4-bit error is when the 4-bit error corresponds to a 4-symbol error i.e. a single bit error in 4-symbols. In such a case, the BDD hands over the received word to the Hamming decoder. The Hamming decoder decodes each symbol successfully, as it can correct a single bit error per symbol. Since the 4 erroneous symbols are corrected by the Hamming decoder, all 4-bit errors can be corrected by the combined decoder. All 5-bit errors cannot be corrected, since a 5-bit error can correspond to a 4-symbol error with a single bit error in 3 symbols and a double bit error in 1 symbol. In this case both BDD and SD fail to correct the error.

Thus, the error correcting capability of the entire decoder is $t_b = 4$.

13. C is a RS code of length $n = 2^m - 1$ over $GF(2^m)$.

(a) Let t be the error-correcting capability of the code. The burst-error-correcting capability is $(t-1)m + 1$.

(b) The burst-error-correcting capability after interleaving is $(t-1)mM + (M-1)m + 1$. By interleaving M codewords, the burst-error-correcting capability increases by almost M times.

14. The 2-error correcting $(7, 3)$ RS code over $GF(8)$ is shortened to a $(5, 1)$ code over $GF(8)$. Let α be the primitive element of $GF(8)$. The generator polynomial of the $(7, 3)$ RS code is given by,

$$\begin{aligned} g(x) &= (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4) \\ &= x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3. \end{aligned}$$

The generator matrix for the $(7, 3)$ RS code can be obtained from $g(x)$ as follows:

$$\hat{G} = \begin{pmatrix} 1 & \alpha^3 & 1 & \alpha & \alpha^3 & 0 & 0 \\ 0 & 1 & \alpha^3 & 1 & \alpha & \alpha^3 & 0 \\ 0 & 0 & 1 & \alpha^3 & 1 & \alpha & \alpha^3 \end{pmatrix}.$$

Row transfromation can be done on G to obtain the systematic generator matrix as follows:

$$G = \begin{pmatrix} 1 & 0 & 0 & \alpha^4 & 1 & \alpha^4 & \alpha^5 \\ 0 & 1 & 0 & \alpha^2 & 1 & \alpha^6 & \alpha^6 \\ 0 & 0 & 1 & \alpha^3 & 1 & \alpha & \alpha^3 \end{pmatrix}.$$

The parity check matrix is given by

$$H = \begin{pmatrix} \alpha^4 & \alpha^2 & \alpha^3 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ \alpha^4 & \alpha^6 & \alpha & 0 & 0 & 1 & 0 \\ \alpha^5 & \alpha^6 & \alpha^3 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(a) Shortening is deleting a coordinate in the message vector, which also causes deletion of the corresponding coordinate in the codeword. In other words, the shortened code consists of the codewords which have 0 in a particular coordinate (the coordinate that is deleted). Shortening by one symbol causes deletion of a particular row and column in the generator matrix, or equivalently, deletion of a column in the parity check matrix.

Let the $(7,3)$ RS code be shortened to a $(5,1)$ code by deleting the first 2 co-ordinates. The generator matrix of the shortened code is got by deleting the first 2 rows and columns of G as shown below.

$$G_s = \begin{pmatrix} 1 & \alpha^3 & 1 & \alpha & \alpha^3 \end{pmatrix}.$$

The parity check matrix of the shortened code is given by

$$H_s = \begin{pmatrix} \alpha^3 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ \alpha & 0 & 0 & 1 & 0 \\ \alpha^3 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(b) Minimum distance of the shortened code is 5 (can be deduced from G_s).

(c) Block length and dimension of the binary expanded version of the shortened code are given by $n_s = 3 \times 5 = 15$ and $k = 3 \times 1 = 3$. The $(15,7)$ binary BCH code is a higher rate 2-error correcting code.

15. The 2-error correcting $(7,3)$ RS code over $GF(8)$ is punctured to a $(5,3)$ code over $GF(8)$.

(a) Refer previous Question.

(b) Puncturing results in deletion of a row and column in the parity check matrix (depending on which parity symbol is deleted). Equivalently, it results in the deletion of a column in the generator matrix. Suppose we puncture the last 2 parity symbols of the $(7,3)$ code. The resulting parity check matrix is given by (refer to matrix H in the previous question),

$$H_p = \begin{pmatrix} \alpha^4 & \alpha^2 & \alpha^3 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The generator matrix of the punctured code is given by

$$G_p = \begin{pmatrix} 1 & 0 & 0 & \alpha^4 & 1 \\ 0 & 1 & 0 & \alpha^2 & 1 \\ 0 & 0 & 1 & \alpha^3 & 1 \end{pmatrix}.$$

(c) The punctured code is 1-error correcting since the minimum distance of the punctured code is 3.