Homework-05

CMSC 442/653

Hrudaya Jinna

① (a) Given v be extended Hamming [16,11] d=3 binary linear code

H [16,11] can be written has

$$[2^n, 2^n-1-n)\, d$$

where n=4

H =

0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
add →	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

(b) Given Binary Erasure channel (BEC)

$\vec{r}$ = 10?1 1001 ?001 1001

the possible vectors will be

r_1 = 1001 1001 0001 1001

r_2 = 1001 1001 1001 1001

r_3 = 1011 1001 0001 1001

r_4 = 1011 1001 1001 1001

Multiplying the above possible vectors to H

so we got

$$H\vec{r}_2^{\,T} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \quad H\vec{r}_2^{\,T} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad H\vec{r}_3^{\,T} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$H\vec{r}_4^{\,T} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

If we observe $H\vec{r}_2^{\,T} = 0$ which means it doesnot have any errors so

codevector = 10011001 1001 1001

(2)

(a) For the above [16, 11] $d=3$ by using the parity check matrix construct error/syndrome table for v.

Error pattern	Syndrome
0000 0000 0000 0000	0 0 0 0 0
0000 0000 0000 0001	1 1 1 1 1
0000 0000 0000 0010	1 1 1 0 1
0000 0000 0000 0100	1 1 0 1 1
0000 0000 0000 1000	1 1 0 0 1
0000 0000 0001 0000	1 0 1 1 1
0000 0000 0010 0000	1 0 1 0 1
0000 0000 0100 0000	1 0 0 1 1
0000 0000 1000 0000	1 0 0 0 1
0000 0001 0000 0000	0 1 1 1 1
0000 0010 0000 0000	0 1 1 0 1
0000 0100 0000 0000	0 1 0 1 1
0000 1000 0000 0000	0 1 0 0 1
0001 0000 0000 0000	0 0 1 1 1
0010 0000 0000 0000	0 0 1 0 1
0100 0000 0000 0000	0 0 0 1 1
1000 0000 0000 0000	0 0 0 0 1

error pattern				syndrome
1100	0000	0000	0000	0010
1010	0000	0000	0000	0010
1001	0000	0000	0000	0011
1000	1000	0000	0000	0100
1000	0100	0000	0000	0101
1000	0010	0000	0000	0110
1000	0001	0000	0000	0111
1000	0000	1000	0000	1000
1000	0000	0100	0000	1001
1000	0000	0010	0000	1010
1000	0000	0001	0000	1011
1000	0000	0000	1000	1100
1000	0000	0000	0100	1101
1000	0000	0000	0010	1110
1000	0000	0000	0001	1111
1000	0000			
1000				

(b)

Given stated that overall parity check is 1, the assume that single error has occured, and use the remaining three bits of the syndrome to correct the error.

I feel, this is best method as the codeword's 4 digit, so error maximum will be less than 3 digits.

so as stated if parity check is 1 then only 1 error can occur.

If parity check is 0, then the case will be no error ie 0 or 2errors can occur.

③ P_u = probability of undetectable error

$$= \sum_{j=3}^{9} \binom{n}{j} P_e^j (1-P_e)^{n-j}$$

$n=9 \qquad P_e = \frac{1}{10}$

$$= \binom{9}{3}(10^{-1})^3 (1-10^{-1})^{9-3} + \binom{9}{4}(10^{-1})^4 (1-10^{-1})^5$$

$$+ \binom{9}{5}(10^{-1})^5 (1-10^{-1})^4 + \binom{9}{6}(10^{-1})^6 (1-10^{-1})^3$$

$$+ \binom{9}{7}(10^{-1})^7 (1-10^{-1})^2 + \binom{9}{8}(10^{-1})^8 (1-10^{-1})^1$$

$$+ \binom{9}{9}(10^{-1})^9 (1-10^{-1})^0$$

$= {}^9C_3 = \frac{9!}{3!\times 6!} = \frac{9\times 8\times 7}{3\times 2} = 84$

$= {}^9C_4 = \frac{9!}{4!\times 5!} = \frac{9\times 8\times 7\times 6}{4\times 3\times 2} = 126 = {}^9C_5$

$= {}^9C_6 = \frac{9!}{6!\times 3!} = \frac{9\times 8\times 7}{3\times 2} = 12\times 7 = 84$

$= {}^9C_7 = \frac{9!}{7!\times 2!} = \frac{72}{2} = 36$

$= {}^9C_8 = 9$

So from above

$$= 84(10^{-3})(0.9)^6 + 126(10^{-4})(0.9)^5 + 126(10^{-5})(0.9)^4$$
$$+ 84(10^{-6})(0.9)^3 + 36(10^{-7})(0.9)^2 + 9(10^{-8})(0.9)$$
$$+ 10^{-9}$$

$$= 84\,(10^{-3})(0.9)^3\left[10^{-3} + (0.9)^3\right]$$
$$+ 36\,(10^{-7})(0.9)^2\left[126\,(10^{-4})(0.9)^4\left[0.1+0.9\right]\right.$$
$$+ 10^{-8}\left[8.1+0.1\right]$$
$$= 0.0447 + 0.0083 + 36(8.1 \times e^{-8}) + (8.1 \times e^{-6}) + e^{-9}$$
$$= 0.053.$$

④

(A) Given

let v be cyclic code $R_{15} = GF(2)[x]/x^{15}+1$

by generator polynomial

$$g(x) = x^8+x^4+x^2+x+1$$

Generator polynomial $g(x)$ in $Z(a)$ divides x^n+1

$R_n = 15$

$$x^{15}+1 = f(x)\,g(x)$$

$$= f(x)(x^8+x^4+x^2+x+1)$$

$x^8+x^4+x^2+x+1 \;\big|\; x^{15}+1$

x^7+x^3+x+1

$x^{15}+x^{11}+x^9+x^8+x^7$

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

$x^{11}+x^7+x^5+x^4+x^3$

$x^9+x^8+x^5+x^4+x^3+1$

$x^9+x^5+x^3+x^2+x$

$x^8+x^4+x^2+x+1$

$x^8+x^4+x^2+x+1$

0

(D)

$$(x^{15}+1) = (x^7+x^3+x+1)(x^8+x^4+x^2+x+1)$$

(x^7+x^3+x+1) is not a irreducble polymial we have irreducible factors of $x^{15}+1$,

(a) The length of n of V is 15

as $R_{15} = x^{15} GF(2)(x)/x^{15}+1$

(b) The dimension of V

$k = n - r$

$n = 15$

$r = \deg(g(x)) = 8$

$k = 15 - 8 = 7$

(c) Use the generator polynomial $g(x)$ to construct generator matrix G for V.

Suppose consider

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$$

be a generator polynomial of cyclic code

If divide the above equation

$$G = \begin{bmatrix} g(x) \\ x\,g(x) \\ \vdots \\ x^{n-k} g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & & & & \\ 0 & 0 & \cdots & \cdots & g_0 & \cdots & g_{n-k} \end{bmatrix}$$

Given $g(x) = x^8 + x^4 + x^2 + x + 1$

Generator matrix is right cyclic shift of the row

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

(d) Parity check polynomial $h(x)$ of V

We know that

$$x^n + 1 = h(x) \cdot g(x)$$

$$x^{15} + 1 = h(x) \cdot (x^8 + x^4 + x^2 + x + 1)$$

$$h(x) = \frac{x^{15} + 1}{x^8 + x^4 + x^2 + x + 1}$$

From (a) we got as

$$= x^7 + x^3 + x + 1$$

Hence $h(x) = x^7 + x^3 + x + 1$

(e) Use the parity check polynomial $h(x)$ to construct parity check matrix H of V.

Parity check matrix

If $h(x) = h_0 + h_1 x + \cdots + h_n x^n$

then the parity check matrix

$$H = \begin{bmatrix} h_n & \cdots & h_2 & h_1 & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_2 & & h_2 & h_1 & h_0 & 0 & \cdots & 0 \\ | & & & & & & & & \\ | & & & 0 & 0 & h_n & \cdots & & h_1 h_0 \\ 0 & 0 & & & & & & & \end{bmatrix}$$

Ex 4

Here $h(x) = x^7 + x^3 + x + 1$

$= x^7 + 0.x^6 + 0.x^5 + 0.x^4 + x^3 + 0.x^2 + x + 1$

$=$

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

(5)

Given

$$x^9+1 = (x+1)(x^2+x+1)(x^6+x^3+1)$$

GF(2) of x^9+1

The ideals of $R_9 = GF(2)[x]/(x^9+1)$

$= I/x^9+1 \quad I = GF(2)[x]$

So the complete factorization of x^9+1 is given as list of ideals

$\{ \langle (x+1)\rangle/\langle (x^9+1)\rangle$ ①, $\langle (x^2+x+1)\rangle/\langle (x^9+1)\rangle$ ②,

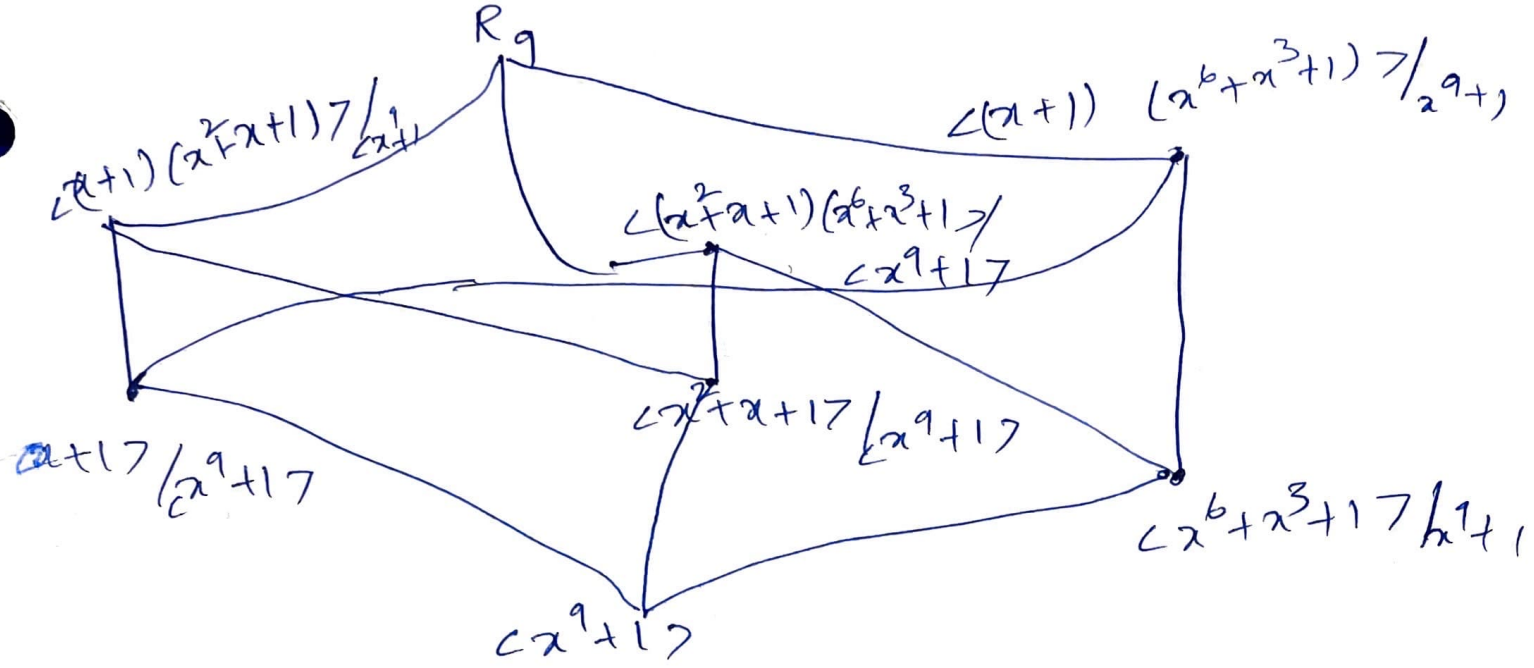
$\langle (x^6+x^3+1)\rangle/\langle (x^9+1)\rangle$ ③, $\langle (x+1)(x^2+x+1)\rangle/\langle (x^9+1)\rangle$ ④,

$\langle (x+1)(x^6+x^3+1)\rangle/\langle (x^9+1)\rangle$ ⑤, $\langle (x^2+x+1)(x^6+x^3+1)\rangle/\langle (x^9+1)\rangle$ ⑥, $\langle x^9+1\rangle \}$

$\langle x+1\rangle \supseteq \langle x^9+1\rangle$, $\langle x^2+x+1\rangle \supseteq \langle x^9+1\rangle$

$\langle x^6+x^3+1\rangle \supseteq \langle x^9+1\rangle$ & so on

the ideal generated by x^9+1 is considered as zero ideal



(b) The dimension of each ideal in R_9 where 2^i is the number of elements in each ideal

$(x+1) / (x^9+1)$ has degree $9-1-1=7$

$(x^2+x+1) / (x^9+1)$ has degree $9-2-1=6$

$(x^6+x^3+1) / (x^9+1)$ has degree $9-6-1=2$

$(x+1)(x^2+x+1) / (x^9+1) = x^3/x^9$ has degree $9-3-1=5$

$(x+1)(x^6+x^3+1) / (x^9+1) = x^7/x^9$ has degree $9-7=2$

$(x^2+x+1)(x^6+x^3+1) / (x^9+1) = x^8/x^9$ has degree $9-8=1$

(c)

elements of $(x+1)/(x^9+1)$ are of form $f(x)(x+1)+x^9+1)$ where $f(x)$ is in $GF(2)[x]$

$(x+1)$ is a 1 degree polynomial

$x^9+1)$ a degree polynomial

$f(x)$ must be $\neq$ degree polynomial $9-1-1=7$

$f(x) = a_0 + a_1 x + a_2 x^{\sim} + \cdots + x^7$

$(x+1)/x^9+1$ has 2^7 elements because has 2 choices

$(x^2+x+1)/x^9+1$ has 2^6 elements because degree of $x^2+x+1=2$

$(x^6+x^3+1)/x^9+1$ has 2^2 element

$((x+1)(x^2+x+1))/(x^9+1)$ has 2^5 elements

$(x+1)(x^6+x^3+1)/(x^9+1)$ has 2 elements

$((x^2+x+1)(x^6+x^3+1))/x^9+1$ has 1 element

$x^9+1)$ is zero elements

(5)(d) (x^6+x^3+1) & $(x+1)(x^6+x^3+1)$

$(x^6+x^3+1) \mid x^9+1$ has 2^2 elements

$f(x)(x^6+x^3+1) + x^9+1)$ where $f(x)$ must form

$a_0 + a_1 x + x^2$

$(x+1)(x^6+x^3+1) \mid x^9+1$

$f(x)(x^6+x^3+1)(x+1) + x^9+1$

where $f(x)$ is form $a_0 + x$ $a_0 + GF(2)$