Cryptography and Codes Assignment 2

1\. a) $w \in F_q^k$

$K(w_1, \ldots w_k) = w_1^3 \ldots w_k^3$

$F_q = \mathbb{Z}_2$

$\underset{k=1}{G} = (111)$ $\quad \underset{k=2}{G} = \begin{pmatrix} 111\ 000 \\ 000\ 111 \end{pmatrix}$ $\quad \underset{k=3}{G} = \begin{pmatrix} 111\ 000\ 000 \\ 000\ 111\ 000 \\ 000\ 000\ 111 \end{pmatrix}$

$$\underset{k>3}{G} = \begin{pmatrix} 111\,000\,000 & \cdots & 000 \\ 000\,111\,000 & \cdots & 000 \\ 000000 & \ddots & \cdots \\ \cdots & \ddots & 000 \\ 000000 \cdots & & 000\,111 \end{pmatrix}$$

G will be $3k \times k$ in size with 111 along its diagon

b) $w \in F_q^k$

$K(w_1, \ldots w_k) = v_1 \ldots v_k$

$v_i = i\,w_i, \quad 1 \le i \le k$

$F_q = \mathbb{Z}_5$

$\underset{k=1}{G} = (1)$ $\quad \underset{k=2}{G} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ $\quad \underset{k=3}{G} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

$$\underset{k>3}{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 3 & 0 & \cdots & \vdots \\ 0 & 0 & & \ddots & & \vdots \\ \vdots & \vdots & \vdots & 0 & (k-1 \bmod 5) & 0 \\ 0 & 0 & 0 & \cdots & 0 & (k \bmod 5) \end{pmatrix}$$

G will be $k \times k$ in size

1 c) $k = 3 \quad F_q = \mathbb{Z}_2$

a) $G = \begin{pmatrix} 111 & 000 & 000 \\ 000 & 111 & 000 \\ 000 & 000 & 111 \end{pmatrix}$ $\quad G' = \begin{pmatrix} 1&0&0&1&0&0&1&0&0 \\ 0&1&0&0&1&1&0&0&0 \\ 0&0&1&0&0&0&0&1&1 \end{pmatrix}$

$-B^T = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&1&0 \\ 1&0&0 \\ 0&0&1 \\ 0&0&1 \end{pmatrix}$ $\quad H' = \begin{pmatrix} 1&0&0&1&0&0&0&0&0 \\ 0&1&0&0&1&0&0&0&0 \\ 0&1&0&0&0&1&0&0&0 \\ 1&0&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&1&0 \\ 0&0&1&0&0&0&0&0&1 \end{pmatrix}$

$$\boxed{H = \begin{pmatrix} 1&1&0&0&0&0&0&0&0 \\ 0&0&0&1&1&0&0&0&0 \\ 0&0&0&1&0&1&0&0&0 \\ 1&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1&0&1 \end{pmatrix}}$$

$GH^T = \begin{pmatrix} 1+1 & 0 & 0 & 1+1 & 0 & 0 \\ 0 & 1+1 & 1+1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1+1 & 1+1 \end{pmatrix}$

$GH^T = \begin{pmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{pmatrix}$

1 c) $k=3$ $F_q = \mathbb{Z}_5$

b) $G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

Since G is $n \times n$ it will have no parity check matrix H as H is $n \times n-k$. Since G is $n \times n$ H will be $n \times 0$ which is not possible.
We can also see that no redundancy is added.

<u>Example</u>

$(1\ 2\ 3)G = 1\ 4\ 4$

With noise say we get 124 which is still in the code

$(1\ 1\ 3)G = 1\ 2\ 4$

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

Decode: 110110
010100

Syndromes	Representatives
000	000000
001	001000
010	000010
011	001010
100	000001
101	000100
110	010000
111	100000

$$H \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

110 -> e = 010000
w - e = 110110 - 010000
= 100110

$$H \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

011 -> e = 001010
w - e = 010100 - 001010
= 011110

3 $G = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{pmatrix}$ $F_q = \mathbb{Z}_3$ Find dual code.

$$-B^T = \begin{pmatrix} -2 & 0 & -1 \\ -2 & -1 & 0 \\ -1 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad GH^T = \begin{pmatrix} 3 & 3 & 3 \\ 6 & 3 & 0 \\ 3 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$K(w) = wH \qquad 000 \leq w \leq 222$

W	k(w)	w	k(w)
000	000000	112	021112
001	201001	120	012120
002	102002	121	210121
010	120010	122	111122
011	021011	200	201200
012	222012	201	102201
020	210020	202	000202
021	111021	210	021210
022	012022	211	222211
100	102100	212	120212
101	000101	220	111220
102	201102	221	012221
110	222110	222	210222
111	120111		

4 $x_1 = x_4$ Find dual code.

$x_2 = x_5$

$x_3 = x_6$

$$G = \begin{pmatrix} 1&0&0&1&0&0 \\ 0&1&0&0&1&0 \\ 0&0&1&0&0&1 \end{pmatrix} \qquad -B^T = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1&0&0&1&0&0 \\ 0&1&0&0&1&0 \\ 0&0&1&0&0&1 \end{pmatrix} \qquad GH^T = \begin{pmatrix} 2&0&0 \\ 0&2&0 \\ 0&0&2 \end{pmatrix} \overset{\mathbb{Z}_2}{=} \begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$$

Since $H = G$ G is a self-dual code

$K(w) = wH \qquad 000 \leq w \leq 111$

W	K(w)
000	000000
001	001001
010	010010
011	011011
100	100100
101	101101
110	110110
111	111111

5. $G = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$ $\quad -B^T = \begin{pmatrix} -2 & 0 & -1 \\ -2 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}$

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

Syndromes generated by $z^T = Ha^T$ where $a \in \{00000, 00001, \dots 22221, 22222\}$ are on next page.

Question 5

00 = 00000, 00110, 00220, 01001, 01111, 01221, 02002, 02112, 02222, 10022, 10102, 10212, 11020, 11100, 11210, 12021, 12101, 12211, 20011, 20121, 20201, 21012, 21122, 21202, 22010, 22120, 22200

01 = 00001, 00111, 00221, 01002, 01112, 01222, 02000, 02110, 02220, 10020, 10100, 10210, 11021, 11101, 11211, 12022, 12102, 12212, 20012, 20122, 20202, 21010, 21120, 21200, 22011, 22121, 22201

02 = 00002, 00112, 00222, 01000, 01110, 01220, 02001, 02111, 02221, 10021, 10101, 10211, 11022, 11102, 11212, 12020, 12100, 12210, 20010, 20120, 20200, 21011, 21121, 21201, 22012, 22122, 22202

10 = 00010, 00120, 00200, 01011, 01121, 01201, 02012, 02122, 02202, 10002, 10112, 10222, 11000, 11110, 11220, 12001, 12111, 12221, 20021, 20101, 20211, 21022, 21102, 21212, 22020, 22100, 22210

11 = 00011, 00121, 00201, 01012, 01122, 01202, 02010, 02120, 02200, 10000, 10110, 10220, 11001, 11111, 11221, 12002, 12112, 12222, 20022, 20102, 20212, 21020, 21100, 21210, 22021, 22101, 22211

12 = 00012, 00122, 00202, 01010, 01120, 01200, 02011, 02121, 02201, 10001, 10111, 10221, 11002, 11112, 11222, 12000, 12110, 12220, 20020, 20100, 20210, 21021, 21101, 21211, 22022, 22102, 22212

20 = 00020, 00100, 00210, 01021, 01101, 01211, 02022, 02102, 02212, 10012, 10122, 10202, 11010, 11120, 11200, 12011, 12121, 12201, 20001, 20111, 20221, 21002, 21112, 21222, 22000, 22110, 22220

21 = 00021, 00101, 00211, 01022, 01102, 01212, 02020, 02100, 02210, 10010, 10120, 10200, 11011, 11121, 11201, 12012, 12122, 12202, 20002, 20112, 20222, 21000, 21110, 21220, 22001, 22111, 22221

22 = 00022, 00102, 00212, 01020, 01100, 01210, 02021, 02101, 02211, 10011, 10121, 10201, 11012, 11122, 11202, 12010, 12120, 12200, 20000, 20110, 20220, 21001, 21111, 21221, 22002, 22112, 22222

We also know that the code words that are generated by the generator matrix G, is the set of representatives for syndrome 00. From this we see the codeword of least weight is 2 (00110) and thus the distance is 2.

6a) $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$

Code words generated by $k(w) = wG$
where $a \in \{000, 001, \ldots 110, 111\}$ are on the next page.

b) $G = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$

This generator matrix, G, is the same one used in question 5. We found the distance of the code given by this G to be 2.

Question 6 a)

000 * G = 00000
001 * G = 11110
010 * G = 00111
011 * G = 11001
100 * G = 11100
101 * G = 00010
110 * G = 11011
111 * G = 00101

Given the above to be the set of all codewords generated by the generator matrix G the codeword of least weight is 1 (00010) and thus the distance is 1.

7. $G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$ $\quad G_2 = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$

$n=5 \quad k=3 \quad d=2 \quad q=2 \qquad n=5 \quad k=3 \quad d=1 \quad q=3$

$t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2-1}{2} \right\rfloor = 0 \qquad t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{1-1}{2} \right\rfloor = 0$

Hamming Bound Formula

$$A_q(n,d) \le \frac{q^n}{\sum_{k=0}^{t} \binom{n}{k}(q-1)^k}$$

$A_q(n,d)$ = number of codewords

Testing perfection of G_1

$$A_2(5,2) \le \frac{2^5}{\sum_{k=0}^{0} \binom{5}{k}(q-1)^k}$$

$$8 \le \frac{32}{\binom{5}{0}(2-1)^0} \longrightarrow 8 \le 32$$

Testing perfection of G_2

$$A_3(5,1) \le \frac{3^5}{\sum_{k=0}^{0} \binom{5}{q}(q-1)^k}$$

$$8 \le \frac{243}{\binom{5}{0}(3-1)^0} \longrightarrow 8 \le 243$$

Since both tests resolt in an inequality neither code is perfect. For a code to be perfect the test must result in an equality.