Solutions to Ex 7

1. 11000
   11000 Hamming distance = 0

   1100101
   0111011 Hamming distance = 5

2. ## Code 1

We show the code is linear by trying to find a basis.
The code contains $8 = 2^3$ vectors and so we need 3 linearly indep. vectors in our basis.

$$0011 + 0101 = 0110$$

$\therefore$ 0011, 0101, 1001 should work.

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

Thus $k = 3$ and $n = 4$

$d = 2$ (min. non-zero weight).

Check

$(000)G = 0000$
$(100)G = 0011$
$(010)G = 0101$
$(001)G = 1001$
$(110)G = 0110$
$(101)G = 1010$
$(011)G = 1100$
$(111)G = 1111$

Code 2 Again this is a code with dimension 3.

$$\begin{array}{r} 001110 \\ 010101 \\ \hline 011011 \end{array}$$

We try the basis 001110, 010101, 100011

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

Check

$(0\,0\,0)\,G = 000000$

$(1\,0\,0)\,G = 001110$

$(0\,1\,0)\,G = 010101$

$(0\,0\,1)\,G = 100011$

$(1\,1\,0)\,G = 011011$

$(1\,0\,1)\,G = 101101$

$(0\,1\,1)\,G = 110110$

$(1\,1\,1)\,G = 111000$

Thus $k = 3$, $n = 6$

d = min weight $= 3$

Code 3 This is a 2 dimensional code. We choose the basis 0101, 1010 and put $G = \begin{pmatrix} 0&1&0&1 \\ 1&0&1&0 \end{pmatrix}$

Check

$(0\,0)\,G = 0000$

$(0\,1)\,G = 1010$

$(1\,0)\,G = 0101$

$(1\,1)\,G = 1111$

$k = 2$, $n = 4$, $d = 2$

Code 4 The dimension is 2. A basis is 1100, 0011.

Put $G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$. Check:

$(00)\,G = 0000$ $\qquad k = 2,\ n = 4,\ d = 2$

$(01)\,G = 0011$

$(10)\,G = 1100$

$(11)\,G = 1111$

In each case, we have to find a parity check matrix H.

Code 1 We need to find a basis for

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

The equations are
$$x_3 + x_4 = 0$$
$$x_2 + x_4 = 0$$
$$x_1 + x_4 = 0$$

x_4 is a free variable. Put $x_4 = \alpha$. Then

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \left\{ \begin{pmatrix} \alpha \\ \alpha \\ \alpha \\ \alpha \end{pmatrix} : \alpha \in \mathbb{Z}_2 \right\} = \left\{ \alpha \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} : \alpha \in \mathbb{Z}_2 \right\}$$

$\therefore\ \underline{H = (1\ 1\ 1\ 1)}$

observe that this works: the sum of the bits in a codeword is always 0

Code 2

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

I shall reorder the rows (doesn't change the nullspace)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

We need to solve the equations

$$\begin{aligned} x_1 + x_5 + x_6 &= 0 \\ x_2 + x_4 + x_6 &= 0 \\ x_3 + x_4 + x_5 &= 0 \end{aligned}$$

the free variables are x_4, x_5, x_6. Put $x_4 = \alpha$, $x_5 = \beta$, $x_6 = \gamma$. Then

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} \beta+\gamma \\ \alpha+\gamma \\ \alpha+\beta \\ \alpha \\ \beta \\ \gamma \end{pmatrix} : \alpha, \beta, \gamma \in \mathbb{Z}_2 \right\}$$

$$= \left\{ \alpha \begin{pmatrix} 0\\1\\1\\1\\0\\0 \end{pmatrix} + \beta \begin{pmatrix} 1\\0\\1\\0\\1\\0 \end{pmatrix} + \gamma \begin{pmatrix} 1\\1\\0\\0\\0\\1 \end{pmatrix} : \alpha,\beta,\gamma \in \mathbb{Z}_2 \right\}$$

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

Check by showing that $HG^T = 0$

<u>Code 3</u> $\quad G = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

Equations $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1\\x_2\\x_3\\x_4 \end{pmatrix} = \begin{pmatrix} 0\\0 \end{pmatrix}$

$$x_1 + x_3 = 0$$
$$x_2 + x_4 = 0$$

free variables $\overset{\alpha}{\overset{\shortparallel}{x_3}}$ and $\overset{\beta}{\overset{\shortparallel}{x_4}}$

$$\left\{ \begin{pmatrix} x_1\\x_2\\x_3\\x_4 \end{pmatrix} = \begin{pmatrix} \alpha\\\beta\\\alpha\\\beta \end{pmatrix} : \alpha,\beta \in \mathbb{Z}_2 \right\} = \left\{ \alpha \begin{pmatrix} 1\\0\\1\\0 \end{pmatrix} + \beta \begin{pmatrix} 0\\1\\0\\1 \end{pmatrix} : \alpha,\beta \in \mathbb{Z}_2 \right\}$$

$H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Check $HG^T = 0$.

This code is said to be <u>self-dual</u>.

<u>Code 4</u> $G = \begin{pmatrix} 1100 \\ 0011 \end{pmatrix}$

Sole $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$x_1 + x_2 = 0$ $\quad x_2 = \alpha, \quad x_4 = \beta$

$x_3 + x_4 = 0$

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha \\ \beta \\ \beta \end{pmatrix} : \alpha, \beta \in \mathbb{Z}_2 \right\}$$

$$= \left\{ \alpha \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} : \alpha, \beta \in \mathbb{Z}_2 \right\}$$

$\therefore H = \begin{pmatrix} 1100 \\ 0011 \end{pmatrix}$

3. $S(\underline{v}, r) = \{ \underline{u} \in \mathbb{Z}_2^n : d(\underline{v}, \underline{u}) \leq r \}$

(a)

Observe $S(\underline{v}, 0) = \{\underline{v}\}$

$S(\underline{v}, 1)$ = all vectors that differ from $\underline{v}$ in one place

$\therefore |S(\underline{v}, 1)| = n$

$S(\underline{v}, 2)$ = all vectors that differ from $\underline{v}$ in 2 places

$\therefore |S(\underline{v}, 2)| = \binom{n}{2}$

In general, $\boxed{|S(\underline{v}, r)| = \binom{n}{r}}$

you are choosing r positions out of n to change

(b) Let $\underline{v} \in C$ be a codeword.

Let the set of all vectors $\underline{u} \in \mathbb{Z}_2^n$ s.t. $d(\underline{v}, \underline{u}) \leq t$ be denoted by $S_{\underline{v}}^t$.

Since C is t-error correcting if $\underline{v}_1 \neq \underline{v}_2$ then

$S_{\underline{v}_1}^t \cap S_{\underline{v}_2}^t = \emptyset$.

$$\therefore \left| \bigcup_{\underline{v} \in C} S_{\underline{v}}^t \right| \leq 2^n.$$

But $|S^t_{\underline{v}_1}| = |S^t_{\underline{v}_2}|$

and $|S^t_{\underline{v}}| = 1 + \binom{n}{1} + \dots + \binom{n}{t}$.

$\therefore \left| \bigcup_{\underline{v} \in C} S^t_{\underline{v}} \right| = M\left(1 + \binom{n}{1} + \dots + \binom{n}{t}\right)$

$\therefore \boxed{M\left(1 + \binom{n}{1} + \dots + \binom{n}{t}\right) \leq 2^n}$

(c) If C is a linear code of dim k then $M = 2^k$, and the above inequality becomes

$$1 + \binom{n}{1} + \dots + \binom{n}{t} \leq 2^{n-k}$$

Let's calculate the LHS for a Hamming code.

Here $t = 1$ and $k = 2^r - 1 - r$ $\quad n = 2^r - 1$

$$1 + \binom{2^r - 1}{1} = 1 + 2^r - 1 = 2^r$$

Whereas the RHS is given by

2^{n-k} where $n-k = 2^r - 1 - 2^r + 1 + r$

$= r$

$\therefore 2^r \therefore$ LHS = RHS.

(d) $(21, 14, 5) = (n, k, d)$

$\therefore t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{4}{2} \rfloor = \underline{\underline{2}}$

$$\text{LHS} = 1 + \binom{21}{1} + \binom{21}{2}$$

$$= 1 + 21 + \frac{21!}{2!\,19!} = 1 + 21 + \frac{21 \times 20}{2}$$

$$= 1 + 21 + 210$$

$$= 232$$

$$\text{RHS} = 2^{21-14} = 2^7$$

$$= 128$$

LHS $\neq$ RHS $\therefore$ no such code exists

(e) This is the information we are given:

$$C \subseteq \mathbb{Z}_2^n, \quad |C| = 100,$$ and is a

2-error correcting code.

We need to determine the smallest value of n for which this inequality holds.

n	$\binom{n}{1}$	$\binom{n}{2}$	$\left(1+\binom{n}{1}+\binom{n}{2}\right)100$	2^n
2	2	1	400	4
3	3	3	800	8
4	4	6	1100	16
5	5	10	1600	32
6	6	15	2200	64
7	7	21	2900	128
8	8	28	3700	256
9	9	36	4600	512
10	10	45	5600	1024
11	11	55	6700	2048
12	12	66	7900	4096
13	13	78	9200	8192
14	14	91	10,600	16384

$\therefore$ $n=14$ is the smallest value for which the Hamming