CODING THEORY: SOLUTIONS 3

(1) A basis must be a linearly independent spanning set. In this case:

$$a(1,2,0,0,1)+b(2,0,1,2,1)+c(0,2,1,2,1)=(0,0,0,0)$$
$$\Leftrightarrow (a+2b, 2a+2c, 2b+2c, a+b+c)=(0,0,0,0)$$
$$\Leftrightarrow a+2b=0\ (1), a+c+0\ (2), b+c=0\ (3), a+b+c=0\ (4))$$

Putting equation (3) into equation (4) we get $a=0$ which putting into equation (1) gives $b=0$ and putting this into equation (3) gives $c=0$. Thus $a(1,2,0,0,1)+b(2,0,1,2,1)+c(0,2,1,2,1)=(0,0,0,0) \Leftrightarrow a=b=c=0$, so the set $\{(1,2,0,0,1),(2,0,1,2,1),(0,2,1,2,1)\}$ is indeed a linearly independent spanning set, and therefore a basis for C. Therefore $\dim(C)=|\text{basis of } C|=3$.

$\{3\ marks\}$

(2)
- S_1: not linear code as $0001+1000=1001 \notin S_1$. $\{1\ marks\}$
- S_2: linear as it is closed under addition in $\mathbb{Z}_2^4$. $\{1\ marks\}$
- S_3: linear as it is closed under addition in $\mathbb{Z}_2^5$. $\{1\ marks\}$
- S_4: not linear as $0001+0001=0002 \in \mathbb{Z}_3^4$ but $0002 \notin S_4$. $\{1\ marks\}$
- S_5: linear as it is closed under addition in $\mathbb{Z}_3^4$. $\{1\ marks\}$

(3) A matrix G is a generator for a code C if the rows of G form a basis for C.

- A possible choice of basis for S_2 is $\{0001, 1000\}$ (it is clearly linearly independent and any other element of S_2 can be made from a linear combination of these two elements). Thus a possible generator matrix is:
$$G_1=\begin{pmatrix}0&0&0&1\\1&0&0&0\end{pmatrix}$$
Note that: $\{2\ marks\}$
$$G_1'=\begin{pmatrix}1&0&0&1\\1&0&0&0\end{pmatrix},\ G_1''=\begin{pmatrix}0&0&0&1\\1&0&0&1\end{pmatrix}$$
are also valid valid generator matrices for S_2.

- For S_3 a possible choice of basis is $\{01000, 00110\}$. Thus a possible generator matrix is:
$$G_2=\begin{pmatrix}0&1&0&0&0\\0&0&1&1&0\end{pmatrix}$$
Other valid choices would be: $\{2\ marks\}$
$$G_2'=\begin{pmatrix}0&1&0&0&0\\0&1&1&1&0\end{pmatrix},\ G_2''=\begin{pmatrix}0&0&1&1&0\\0&1&1&1&0\end{pmatrix}$$

- For S_5, $\{0001\}$ is a possible choice of basis. Therefore a possible generator matrix is:

$$G_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}$$

Another valid choices would be: $\{2\ marks\}$

$$G_2' = \begin{pmatrix} 0 & 0 & 0 & 2 \end{pmatrix}$$

(4) $|C| = n^{\dim(C)}$ where C is n-ary. Thus $|C_1| = |C_2| = 3^2 = 9$, as by question 1 $\dim(C_i) = |\text{basis of } C| = \#$ rows of G_i. For each C_i find its codewords by taking linear combinations of the rows of the respective G_i, knowing that we need 9 codewords for each C_i. $\{1\ marks\}$

- $C_1 = \{0000, 1120, 0112, 1202, 2022, 1011, 2210, 0221, 2101\}$, $\{1\ marks\}$
- $C_2 = \{0000, 1122, 0111, 1200, 2022, 1011, 2211, 0222, 2100\}$. $\{1\ marks\}$

Finally, as we know these are both linear codes, their minimum distance $d(C_i)$ is the same as their minimum weight $w(C_i)$. Therefore $d(C_1) = w(C_1) = 3$ and $d(C_2) = w(C_2) = 2$. $\{2\ marks\}$

(5) To turn G into standard form we use the following operations:

- Swap rows,
- Add one row to another,
- Multiply a row by a scaler,

until we get a copy of the identity matrix on the left hand side.

$$G = \left|\begin{array}{cccc|cc|l} 0 & 1 & 0 & 1 & 0 & 1 & r_1 \\ 0 & 1 & 1 & 1 & 1 & 0 & r_2 \\ 1 & 0 & 0 & 0 & 0 & 1 & r_3 \\ 1 & 1 & 1 & 0 & 0 & 0 & r_4 \end{array}\right. \sim \left|\begin{array}{cccc|cc|l} 1 & 0 & 0 & 0 & 0 & 1 & r_1' = r_3 \\ 0 & 1 & 1 & 1 & 1 & 0 & r_2' = r_2 \\ 0 & 1 & 0 & 1 & 0 & 1 & r_3' = r_1 \\ 1 & 1 & 1 & 0 & 0 & 0 & r_4' = r_4 \end{array}\right.$$

$$\sim \left|\begin{array}{cccc|cc|l} 1 & 0 & 0 & 0 & 0 & 1 & r_1'' = r_1' \\ 0 & 1 & 1 & 1 & 1 & 0 & r_2'' = r_2' \\ 0 & 0 & 1 & 0 & 1 & 1 & r_3'' = r_3' + r_2' \\ 1 & 0 & 0 & 1 & 1 & 0 & r_4'' = r_4' + r_2' \end{array}\right. \sim \left|\begin{array}{cccc|cc|l} 1 & 0 & 0 & 0 & 0 & 1 & r_1''' = r_1'' \\ 0 & 1 & 0 & 1 & 0 & 1 & r_2''' = r_2'' + r_3'' \\ 0 & 0 & 1 & 0 & 1 & 1 & r_3''' = r_3'' \\ 0 & 0 & 0 & 1 & 1 & 1 & r_4''' = r_4'' + r_1'' \end{array}\right.$$

$$\sim \left|\begin{array}{cccc|cc|l} 1 & 0 & 0 & 0 & 0 & 1 & r_1'''' = r_1''' \\ 0 & 1 & 0 & 0 & 1 & 0 & r_2'''' = r_2''' + r_4''' \\ 0 & 0 & 1 & 0 & 1 & 1 & r_3'''' = r_3''' \\ 0 & 0 & 0 & 1 & 1 & 1 & r_4'''' = r_4''' \end{array}\right.$$

Thus G in standard form is:

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

$\{3\ marks\}$

(6) For a code C, $w(C) = min\{x \in C \setminus \{0\}\}$, therefore,

(a) $w(C_1) = 3$, $\{1\ marks\}$

(b) $w(C_2) = 1$, $\{1\ marks\}$

(c) $w(C_3) = 2$, $\{1\ marks\}$

(7) For any two codewords x, y in some linear code C we have,

$$d(x, y) = d(x - y, 0) = w(x - y)$$

by definition of weight. As C is linear, $x - y \in C$ therefore

$$d(C) = \min\{d(x, y)|x, y \in C\} = \min\{w(x - y)|x, y \in C\} = w(C)$$

as required. $\{2\ marks\}$