Problem 1

Given a linear binary code with the following generator matrix

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

What is the error vector belonging to the received vector $\mathbf{v}=(01011)$?

Solution:

First we calculate the parity check matrix by noticing that this code is systematic, because $\mathbf{G}$ contains an identity matrix in its first block, so it is in the form of: $\mathbf{G}_{k\times n}=\left(\mathbf{I}_{k\times k}\,|\,\mathbf{B}_{k\times(n-k)}\right)$

$$\mathbf{G}=\left(\begin{array}{ccc:cc}1&0&0&0&1\\0&1&0&1&0\\0&0&1&1&1\end{array}\right)$$

we know that in case of a systematic code $\mathbf{A}=-\mathbf{B}^T$ which in the binary case is equal to $\mathbf{A}=\mathbf{B}^T$

so $\mathbf{H}_{(n-k)\times n}=\left(\mathbf{A}_{(n-k)\times k}\,|\,\mathbf{I}_{(n-k)\times(n-k)}\right)=\left(\mathbf{B}^T_{(n-k)\times k}\,|\,\mathbf{I}_{(n-k)\times(n-k)}\right)=$

$$\mathbf{H}=\left(\begin{array}{ccc:cc}0&1&1&1&0\\1&0&1&0&1\end{array}\right)$$

Then we use the following relationship: $\mathbf{s}^T=\mathbf{H}\mathbf{v}^T=\mathbf{H}(\mathbf{c}+\mathbf{e})^T=\underbrace{\mathbf{H}\mathbf{c}^T}_{\substack{=0\text{ by}\\\text{definition}\\\text{of }\mathbf{H}}}+\mathbf{H}\mathbf{e}^T=\boxed{\mathbf{H}\mathbf{e}^T=\mathbf{s}^T}$

$$\mathbf{s}^{\mathbf{T}}=\mathbf{H}\mathbf{v}^T=\left(\begin{array}{ccc:cc}0&1&1&1&0\\1&0&1&0&1\end{array}\right)\begin{pmatrix}0\\1\\0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$$

$$\begin{pmatrix}0\\1\end{pmatrix}=\mathbf{H}\mathbf{e}^T=\left(\begin{array}{ccc:cc}0&1&1&1&0\\1&0&1&0&1\end{array}\right)\mathbf{e}^T\rightarrow\mathbf{e}^T=\left\{\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\1\\1\end{pmatrix},\begin{pmatrix}1\\1\\1\\0\\1\end{pmatrix},\begin{pmatrix}1\\0\\1\\1\\1\end{pmatrix}\right\},$$

Problem 2

Given a linear binary code with generator matrix $\mathbf{G}=\begin{pmatrix}1&0&0&0&1\\0&1&0&1&0\\0&0&1&1&1\end{pmatrix}$!

a) Give the type of the code *(n,k)* ?

b) Can this be a Hamming code?

c) How many errors can be detected and corrected by this code?

d) Can the error vectors $\mathbf{e}_1=(10000)$ and $\mathbf{e}_2=(00001)$ be distinguished?

e) Can these error vectors be group leaders?

f) If this code operates over a BSC with error probability $p=0.2$ then what is the probability of these two error vectors occurring?

Solution:

a) n=5, k=3

b) No, because $n+1\neq 2^{n-k}$

c) Based on the generator matrix $\mathbf{G}=\begin{pmatrix}1&0&0&0&1\\0&1&0&1&0\\0&0&1&1&1\end{pmatrix}$ the code words are: $\mathbf{u}\cdot\mathbf{G}=\mathbf{c}$

$(000)\mathbf{G}=(00000)$ $(001)\mathbf{G}=(00111)$; $(010)\mathbf{G}=(01010)$; $(100)\mathbf{G}=(10001)$;

$(011)\mathbf{G}=(01101)$; $(101)\mathbf{G}=(10110)$; $(110)\mathbf{G}=(11011)$; $(111)\mathbf{G}=(11100)$

Knowing the set of code words we can calculate $d_{\min}$

This can be carried out via comparing every two code word and calculating the distance or more simply because this code is <u>linear</u> the weight of the minimal weight code word (except the all zero code word) is the minimal distance. $d_{\min}=w_{\min}=2$

Error detection and correction capability can be calculated via

$l=d_{\min}-1=2-1=1$, so every single error can be detected

$t=\left\lfloor\frac{d_{\min}-1}{2}\right\rfloor=\left\lfloor\frac{2-1}{2}\right\rfloor=0$, but no error can be corrected

d) first to compute the syndrome vectors, we need the parity check matrix:

$\mathbf{H}=\begin{pmatrix}0&1&1&1&0\\1&0&1&0&1\end{pmatrix}$, then we calculate the syndrome vectors as: $\mathbf{s}^{\mathbf{T}}=\mathbf{He}^{T}$

With $\mathbf{e}_1=(10000)$ and $\mathbf{e}_2=(00001)$ we come to the syndrome vector

$\mathbf{s}^{\mathbf{T}}=\mathbf{He}_1^{T}=\mathbf{He}_2^{T}=\begin{pmatrix}0\\1\end{pmatrix}$, so the two error vector <u>cannot</u> be distinguished.

e) It is unnecessary to enumerate the error groups leading to the syndrome vectors because we already know from d) that they cannot be distinguished, so consequently they belong to the same group.

Since the two error vectors have the same weight both of them are equally probable, thus either of them can be the group leader.

f) Since the channel is a BSC the error vector probability is the same for the two error vectors, since they have equal weights.

the error probability can be calculated as:

$$P(\mathbf{e}) = \left(\frac{P_b}{1-P_b}\right)^{w(\mathbf{e})} \cdot (1-P_b)^n = P_b^{\,w(\mathbf{e})}(1-P_b)^{n-w(\mathbf{e})} =$$

$$P(\mathbf{e}_1) = P_b(1-P_b)^4 = 0.2 \cdot 0.8^4 = 0.08192$$

Problem 3

Given a linear binary code with parity check matrix $\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$!

a) Give the type of the code n, k !

b) Give the number of code words !

c) Give the minimum code distance $d_{\min}$!

d) Give the generator matrix $\mathbf{G}$

Solution:

a) Since $\mathbf{H}$ is of type $(n-k)\times n$, $n = 6, k = 5$.

b) The code words are generated as $\mathbf{uG} = \mathbf{c}, \forall \mathbf{u}$ A code word's dimension is *n*, a message word's dimension is *k*. Since the code is binary, there are 2^k different message words and because the coding is a one to one mapping there are the same number of code words: $2^k = 2^5 = 32$

c) Since **H** is linear, $d_{\min} = w_{\min}$. We also know that the code words must satisfy $\mathbf{Hc}^T = \mathbf{0}$, thus in this particular case the code words weight must be an even number. The smallest even number which is not the zero is 2. $d_{\min} = w_{\min} = 2$

d) Since the code is systematic, because $\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \mathbf{H}_{(n-k)\times n} = \left(\mathbf{A}_{(n-k)\times k} \mid \mathbf{I}_{(n-k)\times(n-k)}\right)$

we can construct $\mathbf{G}_{k\times n} = \left(\mathbf{I}_{k\times k} \mid \mathbf{B}_{k\times(n-k)}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$

Problem 4

Given a linear binary code with generator matrix $\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$!

a) Give the code parameters *n*,*k*,*d*
b) Give the standard arrangement table of the code!
c) Give the syndrome decoding table of the code!
d) Is this code MDS and Perfect?
e) Give the probability of a miss-decoding a code word if the channel is a memory free BSC!

Solution:

a) Because $\mathbf{G}_{k\times n}$ the code parameters are $n=5, k=2$

the four code words are: $\begin{pmatrix} \mathbf{c}^{(1)} \\ \mathbf{c}^{(2)} \\ \mathbf{c}^{(3)} \\ \mathbf{c}^{(4)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$, so $d_{\min} = 3$

b) We know that the syndrome vector is $\mathbf{s}^{\mathbf{T}} = \mathbf{H}\mathbf{v}^T = \mathbf{H}(\mathbf{c}+\mathbf{e})^T = \mathbf{H}\mathbf{e}^T$

$$\mathbf{H}_{(n-k)\times n} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

we can write in a table form the mapping of the syndrome vector to the error vector. In the following form:

$\mathbf{s}^{(0)}$	$\mathbf{e}^{(0)} = \mathbf{0}$	$\mathbf{c}^{(1)}$	$\cdots$	$\mathbf{c}^{(2^k-1)}$
$\mathbf{s}^{(1)}$	$\mathbf{e}^{(1)}$	$\mathbf{c}^{(1)} + \mathbf{e}^{(1)}$	$\cdots$	$\mathbf{c}^{(2^k-1)} + \mathbf{e}^{(1)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\mathbf{s}^{(2^{n-k}-1)}$	$\mathbf{e}^{(2^{n-k}-1)}$	$\mathbf{c}^{(1)} + \mathbf{e}^{(2^{n-k}-1)}$	$\cdots$	$\mathbf{c}^{(2^k-1)} + \mathbf{e}^{(2^{n-k}-1)}$

in this specific case

0 0 0	0 0 0 0 0	0 0 0 0 0	1 0 1 1 0	0 1 1 0 1	1 1 0 1 1
1 1 0	1 0 0 0 0	1 0 0 0 0	0 0 1 1 0	1 1 1 0 1	0 1 0 1 1
1 0 1	0 1 0 0 0	0 1 0 0 0	1 1 1 1 0	0 0 1 0 1	1 0 0 1 1
1 0 0	0 0 1 0 0	0 0 1 0 0	1 0 0 1 0	0 1 0 0 1	1 1 1 1 1
0 1 0	0 0 0 1 0	0 0 0 1 0	1 0 1 0 0	0 1 1 1 1	1 1 0 0 1
0 0 1	0 0 0 0 1	0 0 0 0 1	1 0 1 1 1	0 1 1 0 0	1 1 0 1 0
0 1 1	0 0 0 1 1	0 0 0 1 1	1 0 1 0 1	0 1 1 1 0	1 1 0 0 0
1 1 1	1 0 0 0 1	1 0 0 0 1	0 0 1 1 1	1 1 1 0 0	0 1 0 1 0

for demonstrating code performance:

1 0 0	1 1 1 1 1	1 1 1 1 1	0 1 0 0 1	1 0 0 1 0	0 0 1 0 0
0 1 0	1 0 1 0 0	1 0 1 0 0	0 0 0 1 0	1 1 0 0 1	0 1 1 1 1

c) The first two columns of the standard arrangement table is the syndrome decoding table

d) Computing the Singleton and Hamming bound:

$$d_{\min} \overset{?}{=} n - k + 1$$

$3 \overset{?}{=} 5 - 2 + 1,$ not true so the code is not MDS

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$$

$q^k \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \overset{?}{=} q^n,$ in binary case $q = 2$

$$\sum_{i=0}^{t} \binom{n}{i} \overset{?}{=} 2^{n-k} \qquad \binom{n}{k} := \frac{n!}{k!(n-k)!}$$

$$\binom{5}{0} + \binom{5}{1} \overset{?}{=} 2^3$$

$1 + 5 \overset{?}{=} 8,$ not true the code is not Perfect

e) We have totally

1, 0 weight error vector

5, 1 weight error vector

10, 2 weight error vector

10, 3 weight error vector

5, 4 weight error vector

1, 5 weight error vector

since we can correct every single error and two arbitrary but fixed two errors,
the probability of an erroneous decoding is the total probability when the error vector is not among the enumerated values of the syndrome decoding table.

$$P(\mathbf{e}) = P_b^{w(\mathbf{e})} \cdot (1 - P_b)^{n - w(\mathbf{e})}$$

$$P(\text{erroneous decoding}) = P(\text{error vector is not among the enumerated error vectors}) =$$

$$= 8 \cdot P(\mathbf{e} \mid w(\mathbf{e}) = 2) + 10 \cdot P(\mathbf{e} \mid w(\mathbf{e}) = 3) + 5 \cdot P(\mathbf{e} \mid w(\mathbf{e}) = 4) + 1 \cdot P(\mathbf{e} \mid w(\mathbf{e}) = 5) =$$

$$= 8 \cdot P_b^2 (1 - P_b)^3 + 10 \cdot P_b^3 (1 - P_b)^2 + 5 \cdot P_b^4 (1 - P_b)^1 + 1 \cdot P_b^5 (1 - P_b)^0$$