Solutions to Exercise Set #5

1. Suppose the Hamming code is used to detect errors.
   (a) For $i = 0, 1, 2, \ldots, 7$, find the number of error patterns containing exactly $i$ errors that the decoder will fail to detect?
   (b) If the code is used for a binary symmetric channel with bit error probability $p$, find an analytic expression for the probability of an undetected word error as a function of $p$.

Solution: Let $\bar{E}$ be an error pattern. The decoder will not be able to detect error patterns that match non-zero codewords, since

$$H(\bar{E} + \bar{C}) = \bar{0}$$

for any codeword $\bar{C}$. By inspecting the list of codewords for the Hamming $(7, 4)$ code, we find 7 codewords with $W_H = 3$, 7 codewords with $W_H = 4$, and 1 codeword with $W_H = 7$. Hence

$$P(\text{undetected error}) = 7p^3(1-p)^4 + 7p^4(1-p)^3 + p^7.$$  

2. Suppose the Hamming code is used to correct erasures.
   (a) For $i = 0, 1, 2, \ldots, 7$, find the number of erasure patterns containing exactly $i$ erasures that the decoder will fail to correct?
   (b) If the code is used for a binary erasure channel with bit erasure probability $p$, find an analytic expression for the probability of failing to correct the erasures.

Solution: Since the $(7, 4)$ Hamming code has $d_{\text{min}} = 3$, it can correct all erasure patterns with up to 2 erasures. The decoder cannot fill in any pattern with 4 or more erasures since $H$ only has 3 rows. Hence we cannot find 4 or more linearly independent columns in $H$. However, the decoder can correct some patterns with 3 erasures, but not all of them. We are able to fill in patterns that occur in positions that correspond to linearly independent columns in $H$. If we select 3 columns from $H$, there are

$$\binom{7}{3} = 7$$

combinations that are linearly dependent. The reason we divide by $\binom{3}{2}$ is to remove redundant sets of linearly dependent columns.
For 4, 5, 6, and 7 erasures, there are \( \binom{7}{4} = 35 \), \( \binom{7}{5} = 21 \), \( \binom{7}{6} = 7 \), and \( \binom{7}{7} = 1 \) patterns respectively. Hence the analytic expression for the probability of uncorrectable erasures is

\[
P(\text{uncorrectable erasures}) = \sum_{i=3}^{7} e_i p^i (1-p)^{7-i}
\]

where \( e_i \) is the number of patterns with \( i \) erasures that cannot be corrected calculated above, i.e., \( e_3 = 7, e_4 = 35, e_5 = 21, e_6 = 7, e_7 = 1 \).

3. For the \((23,12)\) Golay code given in the notes, calculate the probability of decoding to the wrong codeword if the code is used to correct errors caused by a binary symmetric channel with bit error probability \( p \).

**Solution:** From the lecture, we know that the Hamming \((23,12)\) Golay code has \( d_{\text{min}} = 7 \). Hence it can correct all error patterns of \( \left\lfloor \frac{d_{\text{min}}-1}{2} \right\rfloor \) errors or less. The probability of decoding to a correct codeword \( P_c \) can be given as

\[
P_c = \sum_{i=0}^{3} \binom{23}{i} p^i (1-p)^{23-i}
\]

and the probability of decoding to a wrong codeword \( P_w \) is

\[
P_w = 1 - P_c.
\]

4. Consider the \((15,7)\) parity check code with parity check matrix given below:

\[
H = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1
\end{pmatrix}
\]

(a) Without changing the order of the digits put the parity check matrix in a form with a 8-by-8 identity matrix on the right.

(b) Give the generator matrix of the code with a 7 by 7 unit matrix on the left.

(c) What is the minimum Hamming distance of the code?

(d) Show the form of an encoder using a table look-up. What is the size of the table?

(e) Show a decoder for the code using two tables. What are the size of the tables?
Solution: Let $H = [A|B]$ where $A$ is a $8 \times 7$ matrix and $B$ is a $8 \times 8$ matrix. Then

$$H' = B^{-1}[A|B] = [B^{-1}A|I_{8 \times 8}],$$

where $B^{-1}$ is the modulo 2 inverse of $B$. Using Gaussian elimination (or Matlab), we can find that $B^{-1}A$ is

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

Then the generator matrix is $G = [I_{7 \times 7}|(B^{-1}A)^T]$. By observing the codeword with the minimum Hamming weight, we can find that $d_{\text{min}} = 5$. If a table look-up was used for encoding, the size of the table would be $2^7 \times 8$ where each row corresponds to each message sequence of length 7 and the each column corresponds to each bit of the parity sequence of length 8. The size of a decoding table would be $2^8 \times 15$ where each row corresponds to each syndrome of length 8 and the columns correspond to the error patterns $\bar{e}$. We would decode a received codeword $\bar{r}$ by adding it to $\bar{e}$.