Solutions for Homework 1

1. *Is there room ?*

   Prove or disprove :

   There is a (12,7) binary linear code with $d_{min} = 5$.

   Solution :

   If there were a (12,7) binary linear code with $d_{min} = 5$ then, since $t \stackrel{\Delta}{=} \lfloor \frac{d_{min}-1}{2} \rfloor = 2$, the Hamming balls of radius 2 around the $2^7 = 128$ codewords would have to be disjoint. Each such Hamming ball has $1 + \binom{12}{1} + \binom{12}{2} = 79$ strings of length 12 in it. Now, $128 \times 79 > 2^{12} = 4096$. This means the assumption engenders a contradiction. There isn't enough room $\{0,1\}^{12}$ to allow for the existence of such a code.

2. (*Extended Hamming code*)

   The first problem relates to a specific (8,4) code. This is an *extension* of the (7,4) Hamming code considered in Example 3.1 on pg. 67 of the text, as you will see after constructing a systematic generator matrix for this code. In general, an extension of a linear code is any code got from it by adding more columns to the generator matrix. This process can be thought of as adding more parity check symbols to the code. The various parts of this problem correspond to individual problems on pp. 95 -96 of the text, as indicated below. The first two parts correspond to problem 3.1 on pg. 95 of the text.

   (a) Consider a binary (8,4) code whose parity-check equations are

   $$\begin{aligned} v_0 &= u_1 + u_2 + u_3 \ , \\ v_1 &= u_0 + u_1 + u_2 \ , \\ v_2 &= u_0 + u_1 + u_3 \ , \\ v_3 &= u_0 + u_2 + u_3 \ . \end{aligned}$$

   where $u_0,\ u_1,\ u_2,\ u_3$ are message digits and $v_0,\ v_1,\ v_2,\ v_3$ are parity-check digits. The codeword is $(v_0, v_1, v_2, v_3, u_0, u_1, u_2, u_3)$. Find systematic generator and parity-check matrices for this code.

   Solution :

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

   $$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Strictly speaking this code is not an extension of the (7,4) Hamming code of Example 3.1 on pg. 67. Rather, it is an extension of a (7,4) Hamming code got from the one considered in Example 3.1 on pg. 67 of the text after reordering its coordinates (interchange the first and the third coordinates in that example and then insert an extra column after the second column as in the matrix G above).

(b) Show that the minimum distance of this code is 4.

Solution :

Each column of H is non-zero so no codeword has weight 1. The columns of H are distinct, so no codeword has weight 2. The sum of any two columns of H has even weight, so it cannot equal any column of H, since they all have odd weight. Thus no codeword has weight 3. Thus the minimum weight of a non-zero codeword is at least 4. Further [1 1 1 0 0 1 0 0] is a non-zero codeword of weight 4. Thus the minimum distance of the code is 4.

(c) (*This is problem 3.2 on pg. 95 of the text.*)

Construct (on paper, as a diagram) an encoder for this code.

Solution :

This diagram will look that of figure 3.2 on pg. 71 of the text, with the appropriate choices for the parity check coefficients, which are here given by matrix

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

See equation (3.4) on pg. 69 of the text for the correct indexing of the entries of the parity check coefficients to use in figure 3.2.

(d) (*This is problem 3.3 on pg. 95 of the text.*)

Construct (on paper, as a diagram) a syndrome circuit for this code.

Solution :

This diagram will look that of figure 3.4 on pg. 74 of the text, with the appropriate choices for the coefficients of the parity check matrix.

(e) (*This is problem 3.9 on pg. 96 of the text.*)

Determine the weight profile of this code. Compute the probability of undetected error when this code is used over a binary symmetric channel with crossover probability $p = 10^{-2}$ (assuming maximum likelihood decoding and that all codewords are a priori equiprobable).

Solution :

Since each row of the parity check matrix H has even weight, we see that the all ones word [1 1 1 1 1 1 1 1] is a codeword. Since we have already argued that there are no codewords of weights 1, 2, or 3, it then follows that there are no codewords of weights 7, 6, or 5. Thus all the 14 codewords other than the all zeros codeword and the all ones codeword are of weight 4. The weight enumerator polynomial for this code is therefore

$$A(z) = 1 + 14z^4 + z^8 .$$

The probability of undetected error when this code is used over a binary symmetric channel with crossover probability $p = 10^{-2}$ is then

$$14 \cdot 10^{-8} \cdot (0.99)^4 + 10^{-16} \ .$$

(f) (*This is problem 3.11 on pg. 96 of the text.*)
Construct (on paper, as a diagram) a decoder for this code that is capable of correcting all single-error patterns and simultaneously detecting any combination of double errors. Specifically, if the received vector is at Hamming distance 1 from a codeword, the decoder should return that codeword, while if the received vector is at Hamming distance 2 from a codeword, the decoder should return an indicator that this is the case.

Solution :

The syndrome $\mathbf{s} = [s_0 \ s_1 \ s_2 \ s_3]$ associated to a received word $\mathbf{r} = [r_0 \ \ldots, \ r_7]$ is $\mathbf{s} = \mathbf{r}H^T$. Writing this out, we have the following equations with which to compute the syndrome.

$$\begin{aligned} s_0 &= r_0 + r_5 + r_6 + r_7 \ , \\ s_1 &= r_1 + r_4 + r_5 + r_6 \ , \\ s_2 &= r_2 + r_4 + r_5 + r_7 \ , \\ s_3 &= r_3 + r_4 + r_6 + r_7 \ . \end{aligned}$$

Note that the syndrome depends only on the error pattern $\mathbf{e} = [e_0 \ \ldots, \ e_7]$, and can also be written as $\mathbf{s} = \mathbf{e}H^T$. There are 8 possible error patterns of weight 1 and 28 possible error patterns of weight 2. None of these can result in a zero syndrome, since only error patterns that are codewords can have zero syndrome, and we know that all non-zero codewords have weight at least 4. Further, no two error patterns of weight 1 can have the same syndrome, since if they did their difference would have to be a non-zero codeword, but all non-zero codewords have weight at least 4. The possible syndromes of error patterns of weight 1 are listed below.

$$\begin{array}{cccc} [1\ 0\ 0\ 0] & [0\ 1\ 0\ 0] & [0\ 0\ 1\ 0] & [0\ 0\ 0\ 1] \\ [0\ 1\ 1\ 1] & [1\ 1\ 1\ 0] & [1\ 1\ 0\ 1] & [1\ 0\ 1\ 1] \end{array} \tag{1}$$

The top row lists the syndromes corresponding respectively to single errors at locations 0 through 3, and the bottom row lists those corresponding respectively to single errors at locations 4 through 7 of the received word.

The observations above indicate that a decoder for this code that is capable of correcting all single-error patterns and simultaneously detecting any combination of double errors can be constructed according to the following scheme.

Step 1 : Compute the syndrome.

Step 2 : If the syndrome is zero accept the received word as being a codeword. If the syndrome is non-zero and is *not* one of the eight syndromes listed in (1), declare

an error has been detected. If it is one of these eight syndromes decide that the error pattern is the unique single error pattern that corresponds to this syndrome and correct the error.

(g) (*This is problem 3.14 on pg. 96 of the text.*)
Show that this code is self-dual.
Solution :
Since $GH^T = 0$, the code is self-dual.

3. (*Punctured Reed-Muller code*)

The punctured Reed-Muller code $RM^*(r, m)$ is derived from the Reed-Muller code $RM(r, m)$ by deleting the coordinate corresponding to $v_1 = v_2 = \ldots = v_m = 0$ from all the codewords. In general *puncturing* a code is the term used for the process of getting another code by deleting some of the symbols of the original code. This way the number of message symbols remains the same, but the redundancy is reduced.

(a) Verify that $RM^*(r, m)$ is a $(2^m - 1, 1 + \binom{m}{1} + \ldots + \binom{m}{r})$ code with $d_{min} = 2^{m-r} - 1$.
Solution :
That $n = 2^m - 1$ and $k = 1 + m + \binom{m}{2} + \ldots + \binom{m}{r}$ is immediate. Also, $2^{m-r} - 1 \leq d_{min} \leq 2^{m-r}$. The bounds hold because every codeword in the punctured code is derived from a codeword in the original code by erasing one coordinate - thus its weight is bounded above by the weight of a codeword from which it is derived, and bounded below by this weight less 1. To see that $d_{min} = 2^{m-r} - 1$, it suffices to find a codeword in $\mathcal{R}^*(r, m)$ of weight $2^{m-r} - 1$. For $r = 0$, the bit string of all 1's is such a codeword. For $r > 1$, consider the bit string corresponding to the monomial

$$(1 - v_1)(1 - v_2) \ldots (1 - v_r) \ .$$

It is straightforward to check that this has weight $2^{m-r} - 1$.

(b) Show that it is possible to reorder the transmitted bits in $RM^*(1, 3)$ so that the resulting code is the $(7, 4)$ Hamming code considered in Example 3.1 on pg. 67 of the text.
Hint : Argue that, since $RM^*(1, 3)$ is a $(7, 4, 3)$ binary code, it is perfect. What does this say about its dual code ?
Solution :
The solution using the hint is as follows : from the preceding part of the problem we see that $RM^*(1, 3)$ is a $(7, 4, 3)$ binary code. It then follows that it is perfect, because

$$2^4 \cdot (1 + \binom{7}{1}) = 2^7 \ ,$$

although it is not strictly necessary to observe this. From $d_{min} = 3$ for this code, we see that all nonzero codewords have weight at least 3, from which it follows that no two of the columns of a parity check matrix for this code (which is a generator matrix for the dual code) can be identical, and no column of a parity check matrix for the code can be zero. Since a parity matrix for the code is a 3×7 matrix, it

follows that its columns are precisely all the nonzero bit strings of length 3 in some order. This implies that after reordering the coordinates of $RM^*(1,3)$ we get the $(7,4)$ Hamming code considered in Example 3.1 on pg. 67 of the text.

(c) Is there any relation between the RM(1,3) code and the (8,4) extended Hamming code considered in the preceding problem ? Explain your answer.

Solution :

Let H_b denote the $(7,4)$ Hamming code considered in Example 3.1 on pg. 67 of the text. Let H_h denote the $(7,4)$ Hamming code created from H_b by interchanging its first and third coordinates. Let E denote the $(8,4)$ code considered in problem 2. We argued in problem 2(a) that E is the extension of H_h got by inserting the third column of the generator matrix G of problem 2(a).

RM(1,3) is the extension of $RM^*(1,3)$ got by inserting the first column of the standard generator matrix for RM(1,3). In the preceding part of this problem we argued that rearranging the coordinates of $RM^*(1,3)$ also results in a (7,4) Hamming code. This suggests that RM(1,3) and E should be related by one of them being a rearrangement of the coordinates of the other. This suggestion is reinforced by the respective weight enumerator polynomials : we know that the weight enumerator polynomial of RM(1,3) is $1+14z^4+z^8$, and we have shown in problem 2(e) that this is also the weight enumerator polynomial of E.

Some experimentation will show that it is indeed possible to get RM(1,3) as a rearrangement of the coordinates of E.

4. (*RM(2,5) code*)

(a) Write down a generator matrix for the RM(1,4) code (which is a (16,5) code with $d_{min} = 8$).

Solution :

The standard generator matrix for RM(1,4) is the 5×16 matrix given by the first five rows in Example 4.2 on pg. 106 of the text.

(b) Describe in detail the steps involved in majority logic decoding for this code. Specifically, for each information bit, determine all the check sums whose majority needs to be taken by the majority logic decoder.

Solution :

The discussion for this is identical to that on pp. 108 -109 of the text, starting with the sentence "$\mathbf{r}^{(1)}$ is simply the following codeword" in the bottom half of pg. 108 and ending with the sentence "This step completes the entire decoding." at the middle of pg. 109.