ECE 409 - ERROR CORRECTING CODES - INVESTIGATION 23
INTRODUCTION TO BLOCK CODES - PART III

WINTER 2003 **A.P. FELZER**

To do "well" on this investigation you must not only get the right answers but must also do neat, complete and concise writeups that make obvious what each problem is, how you're solving the problem and what your answer is. You also need to include drawings of all circuits as well as appropriate graphs and tables.

From the last Investigation we know that a block code is linear if the sum of any two codewords is itself a codeword. In particular if a and b are codewords then so is

$$c = a + b$$

The objective of this Investigation is to show how linear codes simplify encoding and decoding of data

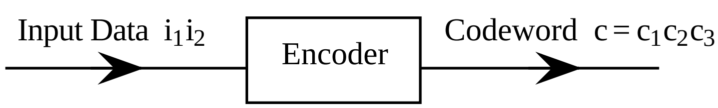
1. We begin with a review problem. Given the even parity code of size (3, 2)
   a. How many valid codewords does the code have
   b. Find all the codewords
   c. Show that the code is linear

2. The objective of this problem is to illustrate how all the codewords of a linear code can be obtained from a subset of them.
   a. Show that all the codewords of an even parity code of size (3, 2) can be obtained as linear combinations of the codewords 101 and 011 as can 101 as follows

$$101 = 1\,(101) + 0\,(011)$$

   b. Note that we say that the codewords 101 and 011 are a **spanning set** of the linear code. **Memorize** this definition. Then find another spanning set of codewords for this code
   c. What can you conclude from parts (a) and (b) about the uniqueness of spanning sets

3. From Problem (2) we have that if an encoder as follows



is linear with spanning set s_1, s_2 then every codeword c can be expressed as a linear combination of s_1 and s_2 as follows

$$c = i_1 s_1 + i_2 s_2$$

The objective of this problem is to illustrate how we can choose the spanning set to obtain codewords that are systematic. The trick is to notice that if we use the spanning set 101, 011 then the resulting code as follows

$$c_1c_2c_3 = i_1(101) + i_2(011)$$

is systematic with

$$c_1 = i_i \quad c_2 = i_2 \quad c_3 = i_i + i_2$$

In matrix form we can write

$$\left(c_1\, c_2\, c_3\right) = \left(i_1\, i_2\right)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \left(i_1\, i_2\right)\mathbf{G}$$

where

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

is called the **generating matrix** of spanning codewords.

a. What is it about the spanning set we chose in this problem that makes the codewords systematic
b. Verify that each of the codewords $c_1c_2c_3$ of the even parity linear code of size (3, 2) can be obtained from the matrix equation above with generating matrix **G**
c. Verify that your result in part (b) is in fact systematic

4. Generalizing on the result of Problem (3) it can be shown that every linear code of size (n,k) has a spanning set of k codewords that can be used to generate the codeword for an input i as follows

$$\mathbf{c} = \mathbf{iG}$$

where $\mathbf{c} = 1 \times n$ codeword
$\mathbf{i} = 1 \times k$ input
$\mathbf{G} = k \times n$ generating matrix of spanning codewords

a. Show that if we pick our spanning set so that the generating matrix **G** can be partitioned as follows

$$\mathbf{G} = \left[\mathbf{I}_k \vdots \mathbf{P}\right]$$

where $\mathbf{I_k}$ is a k by k unit matrix as follows then the code will be systematic. Note that **P** is referred to as the **parity matrix**
b. Find **G** for a (4,3) linear even parity code that is systematic
c. Find **G** for a (7,4) Hamming code for which

$$\begin{aligned} c_5 &= c_1 + c_2 + c_3 = i_1 + i_2 + i_3 \\ c_6 &= c_2 + c_3 + c_4 = i_2 + i_3 + i_4 \\ c_7 &= c_1 + c_2 + c_4 = i_1 + i_2 + i_4 \end{aligned}$$

Note that Hamming codes were the first error detecting codes found. They all detect one error but are different sizes depending on the number of data bits.

5. From Problem (4) we know that we can use the generating matrix **G** to encode data i as follows

$$\mathbf{c} = \mathbf{iG} = \mathbf{i}\left[\mathbf{I}_k \vdots \mathbf{P}\right]$$

where P is the k by n-k parity matrix. But the real problem, of course, is decoding. Luckily there's a straightforward way to decode received signals with what we refer to as the **parity-check matrix H** as follows

$$\mathbf{H} = \left[\mathbf{P^T} \vdots \mathbf{I_{n-k}}\right]$$

where $\mathbf{P^T}$ is the transpose of **P** (each element p_{jk} in **P** trades places with p_{kj})

Find H for the linear code with the following generating matrix **G**

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

6. Now the key result for parity-check matrices **H** is that

$$\mathbf{G}\mathbf{H}^{\mathbf{T}} = \mathbf{0}$$

   a. Make use of this result to show that $\mathbf{c}\mathbf{H}^{\mathbf{T}} = \mathbf{0}$ for any valid codeword **c**. Hint - express **c** in terms of **G**
   b. Do an example to verify that $\mathbf{c}\mathbf{H}^{\mathbf{T}} = \mathbf{0}$

7. Now suppose that the signal at the input to the decoder is equal to

$$\nu = \mathbf{c} + \mathbf{e}$$

where **c** = valid codeword from the encoder **e** = error from transmission. We call $\mathbf{s} = \nu\mathbf{H}^{\mathbf{T}}$ the **error syndrome** of ν

   a. Show that $\nu\mathbf{H}^{\mathbf{T}} = \mathbf{e}\mathbf{H}^{\mathbf{T}}$
   b. Calculate the error syndrome for the linear code with parity-check matrix

$$\mathbf{H} = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

   for $\nu = [1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0]$

   c. What is the error syndrome equal to when there is no error

8. The objective of this problem is to show how parity-check matrices **H** can be used to do error correcting. Suppose in particular that we have a (6,3) code with parity-checking matrix **H** as follows

$$\mathbf{H} = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

that has distance 3 and so can correct one error. The procedure for detecting and correcting these single errors is as follows

(1) Calculate a table of all the error syndromes **s** for errors **e** of weight one
(2) Calculate the error syndrome **s** for the input ν to the decoder
(3) Use the table from Step (1) to find the corresponding error **e**
(4) Calculate our estimate of the correct code as $\nu + \mathbf{e}$

   a. Verify the following table of error syndromes of single bit errors for our **H** as follows

e	**s**
0 0 0 0 0 0	0 0 0
0 0 0 0 0 1	0 0 1
0 0 0 0 1 0	0 1 0
0 0 0 1 0 0	1 0 0
0 0 1 0 0 0	1 1 0
0 1 0 0 0 0	1 0 1
1 0 0 0 0 0	0 1 1

b. Calculate the error syndrome for $\nu = 111110$.
c. Then make use of the table to find what the original code **c** was if there was only one error.
d. What does an error syndrome of value **s** = 111 tell us