Lesson 2

Recall,

HAMMING BOUND. Let C be a code in Z_2^n and t is the number of errors that can be corrected. Then

$$|C|\left[\binom{n}{0}+\cdots+\binom{n}{t}\right] \leq 2^n$$

Another Bound

Let C be a code in Z_2^n. Let d be the designed distance of the code (the shortest distance between code words). If $d > n/2$, then

$$|C| \leq \frac{2d}{2d-n}$$

Ex $C = \{00000000, (11100011), (00011111), (11111100)\}$. $n=8$, $d=5$

$|C|=4$. $d > n/2$.

$$|C| = 4 \leq \frac{2d}{2d-n} = \frac{10}{10-8} = 5$$

See problem 2 at the end of these notes

HADAMARD MATRICIES

let H be an $n \times n$ matrix whose elements are all 1's and -1's with $H H^T = nI$. H is called a Hadamard matrix

Ex 1. $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$

Since $H \frac{1}{n} H^T = I$, $H^{-1} = \frac{1}{n} H^T$

Then $H^T H = nI$. One view is that the dot product of any pair of rows is 0 and of a row with itself is n

Multiplication of ~~H (or H⁻¹)~~ a row of H (or column of H) by -1 is another Hadamard matrix. We can multiply ~~by~~ enough -1 so that the first row of H is all 1's (same for columns). The dot product of two rows (columns) of H is 0. With all 1's in row one, the other rows have $\frac{1}{2}n$ ~~ways~~ ones and $\frac{1}{2}n$ -1's. Using the dot product condition again 2 rows have

a. 1's in $\frac{1}{4}n$ positions at the same time
b. -1's in $\frac{1}{4}n$ positions at the same time
c. 1 in the 1st, -1 in the second $\frac{1}{4}n$ times
d. 1 in the second, -1 in the first $\frac{1}{4}n$ times

Ex 2 See Example 1.

This matrix can be constructed by a general procedure. Let H be the normalized 4×4 matrix in Ex 1. Then $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ is another Hadamard matrix, $2n$ by $2n$.
If H_2 is the matrix in Ex 2 Then $H_3 = \begin{pmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{pmatrix}$ has size 8×8

$H_4 = \begin{pmatrix} H_3 & H_3 \\ H_3 & -H_3 \end{pmatrix}$ is 16×16 Generally

$H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$ is 2^n by 2^n.

$n=1,2,\ldots$ In fact, if H is larger then 2×2, then H has size a multiple of 4

Proof Let $H=(h_{ij})$ be a normalized Hadamard matrix of size >2. Consider

$$\sum_{j=1}^{n}(h_{1j}+h_{2j})(h_{1j}+h_{3j}) = \sum_{j=1}^{n} h_{1j}^2 = n$$

using the dot product of rows condition. But each $h_{1j} + h_{2j}$ is 0 or 2 (remember all $h_{ij} = 1$), same for $h_{1j} + h_{3j}$. So each term in the sum is 0 or 4. Hence 4 divides n.

HADAMARD CODES

Start with a normalized $4n \times 4n$ Hadamard matrix.

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

Remove the first row and column and change all -1 to 0

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

If $n = 4k$, then this last matrix is $(4k-1, 4k-1)$ with $2k-1$ 1's and $2k$ 0's. In each pair of rows there are $2k$ different terms and $2k-1$ terms the same. Assume the rows make up a code C in $4k-1$ space. There are $4k-1$ elements in C and the designed distance is $2k$. Hence $t = k-1$ errors can be corrected. The codes constructed are called Hadamard codes

Reed Muller Codes

Continue the Hadomard code example, calling the matrix in that example J. Let K be the matrix gotten from J by interchanging all 0's and 1's. Put a 1 in front of each row in J and a 0 in front of each row in K. Call these new matrices S and T. Construct $\begin{pmatrix} S \\ \hline T \end{pmatrix} = R$. R has $8k-2$ rows and $4k$ columns. The designed distance is still $2k$. If we add a row of 1's and a row of 0's, then the $8k$ rows are the code words, so $|C| = 8k$, in $4k$ space and has designed distance $2k$ so can correct $k-1$ errors. This is the famous Reed-Soloman code, used in sending information from space.

Continue the last example

$$J = \begin{matrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{matrix}$$

$$K = \begin{matrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{matrix}$$

Fill in the first column of J with 1, the first column of K with 0. The add a row of 1's and a row of 0's

The result is a 16x8 matrix → $|C| = 16$ length $= n = 8$, $d = 4$

PROBLEMS

PAGE 89 #1

1. Let C be the 2 error correcting code in Example 3

a Find 2 vectors that are not codewords but which are guaranteed to be uniquely correctable

b. Find 2 vectors in Z_2^8 that are at least 3 errors from each codeword but which are uniquely correctable to a word in C

c Find 2 vectors in Z_2^8 that are not uniquely correctable

d. How many non-code words in Z_2^8 are either one or two bit errors from a codeword in C

Problems (PAGE 90 # 2)

2 Use the Hamming bound find the maximum number of errors that can be corrected in a code of length 7 ($n=7$) with 4 code words. Then use the other bound to show it is not possible to construct a code with $n=7$, $|C|=4$ that is guaranteed to uniquely correct this number of errors