EE/Ma 127a Error-Correcting Codes - Homework Assignment 2

Ling Li, ling@cs.caltech.edu

October 12, 2000

2.1 $(n, 32)$

The set of correctable error patterns is $E = \{0\}$, and the set of detectable error patterns is $F = \{\text{all error patterns of weight 1, 2 or 3}\}$. Suppose H is the parity-check matrix for the $(n, 32)$ code. Thus for all $\mathbf{z} \in F$, $H\mathbf{z} \neq 0$. That is, no 3 columns of H is linear dependent. This is the same as what we have done in homework assignment 1.5. Here I just list the answer: the smallest n is 39, and one parity-check matrix is

$$H = (\langle 1 \rangle, \langle 3 \rangle, \langle 5 \rangle, \cdots, \langle 77 \rangle),$$

where for convenience, column h_i of H is written as an integer, which is

$$\left\langle \begin{pmatrix} 2^6 & 2^5 & \dots & 1 \end{pmatrix} \cdot h_i \right\rangle.$$

The decoding algorithm is very straightforward:

- When x received, calculate Hx^T;
- If Hx^T is zero, accept x as a valid codeword;
- Otherwise, neglect x and request a retransmission.

2.2 Linear codes

Given parity-check matrix H, the length of the code equals the number of columns of H (denoted here by n), the dimension of the code is $[n - \dim(H)]$, and the minimum distance which is also the minimum weight among all non-zero codewords, is the minimum number of columns with sum 0.

(a) $H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. $n = 7$, $\dim(H) = 4$. So, the length is 7, dimension is 3, and minimum distance of the code is 3. An example is the distance between 0001101 and 0000000.

(b) $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$. $n = 7$, $\dim(H) = 4$. So, the length is 7, dimension is 3, and minimum distance is 4, (Each column of H is different from each other and has odd number of 1. Thus the sum of any 2 or 3 columns of H can not be 0.) with an example 1110100.

2.3 ML decoding

The concept '*match*' will be defined differently for this two channels, and n denotes the length of the code.

(a) The binary erasure channel: We say $\mathbf{y}$ *matches* a codeword $\mathbf{x}$ (or vice versa), if $y_i = x_i$ or $y_i = ?$ for all $i = 0..(n-1)$. Thus,

$$p(\mathbf{y}|\mathbf{x}_i) = \begin{cases} p^d(1-p)^{n-d}, & \text{if } \mathbf{y} \text{ matches } \mathbf{x}_i; \\ 0, & \text{otherwise.} \end{cases}$$

where d is the number of erasures ('?') in $\mathbf{y}$. To find a codeword $\mathbf{x}_i$ with largest $p(\mathbf{y}|\mathbf{x}_i)$ is just to find a codeword $\mathbf{x}_i$ that matches $\mathbf{y}$, since d is a constant for a given $\mathbf{y}$.

(b) The Z-channel: We say $\mathbf{y}$ *matches* a codeword $\mathbf{x}$, if $y_i = 0$ for all i that makes $x_i = 0$. Thus

$$p(\mathbf{y}|\mathbf{x}_i) = \begin{cases} p^d(1-p)^{n-d}, & \text{if } \mathbf{y} \text{ matches } \mathbf{x}_i; \\ 0, & \text{otherwise.} \end{cases}$$

where d is the Hamming distance between $\mathbf{x}_i$ and $\mathbf{y}$. Since p is between 0 and $1/2$, $p^d(1-p)^{n-d}$ decreases when d inceases. So the decoder should first find all the codewords that $\mathbf{y}$ matches, then find the one among them with the minimum Hamming distance with $\mathbf{y}$.

2.4 Decoder error

(a) This is somewhat like what we discussed in 2.2(b). One parity-check matrix of the code is

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

which also has odd number of 1 in every column of H. Thus the minimum distance of the code is bigger than 3. In fact, it is 4, with an example 11100001.

(b) $t = 0$ means the decoder will accept x iff $Hx^T = 0$. Among totally 2^8 error patterns from 00000000 to 11111111, there are 2^4 patterns (the same as 2^4 valid codewords) satisfy $Hx^T = 0$. So, when considered as error patterns, 15 non-zero codewords will cause the decoder make wrong decisions. We can list the 15 non-zero codewords and their weights here.

1 1 1 0 0 0 0 1	*(4)*	0 1 1 0 0 1 1 0	*(4)*	0 1 0 0 1 0 1 1	*(4)*
1 1 0 1 0 0 1 0	*(4)*	1 0 0 0 0 1 1 1	*(4)*	1 1 0 0 1 1 0 0	*(4)*
0 0 1 1 0 0 1 1	*(4)*	0 1 1 1 1 0 0 0	*(4)*	0 0 1 0 1 1 0 1	*(4)*
1 0 1 1 0 1 0 0	*(4)*	1 0 0 1 1 0 0 1	*(4)*	0 0 0 1 1 1 1 0	*(4)*
0 1 0 1 0 1 0 1	*(4)*	1 0 1 0 1 0 1 0	*(4)*	1 1 1 1 1 1 1 1	*(8)*

Thus the probability of decoder error is

$$14p^4(1-p)^4 + p^8.$$