EE/Ma 127a Error-Correcting Codes - Homework Assignment 6

Ling Li, ling@cs.caltech.edu

November 17, 2000

6.1 *Shortened cyclic code.* Use $\mathcal{C}$ and $\mathcal{C}'$ to denote the original cyclic code $(n, n-r)$ and the shortened code $(n_0, n_0 - r)$, respectively.

(a) For any two codewords $[C_0, C_1, \ldots, C_{n_0-1}]$ and $[\tilde{C}_0, \tilde{C}_1, \ldots, \tilde{C}_{n_0-1}]$ in the code $\mathcal{C}'$, we have $C_0 + C_1 x + \cdots + C_{n_0-1}x^{n_0-1}$ and $\tilde{C}_0 + \tilde{C}_1 x + \cdots + \tilde{C}_{n_0-1}x^{n_0-1}$ are multiples of $g(x)$. Thus the sum of them, i.e., $(C_0 + \tilde{C}_0) + (C_1 + \tilde{C}_1)x + \cdots + (C_{n_0-1} + \tilde{C}_{n_0-1})x^{n_0-1}$ is also a multiple of $g(x)$. Thus

$$[C_0 + \tilde{C}_0, C_1 + \tilde{C}_1, \ldots, C_{n_0-1} + \tilde{C}_{n_0-1}] = [C_0, C_1, \ldots, C_{n_0-1}] + [\tilde{C}_0, \tilde{C}_1, \ldots, \tilde{C}_{n_0-1}]$$

is also in $\mathcal{C}'$. So $\mathcal{C}'$ is a linear code.

(b) For the cyclic code $\mathcal{C}$ generated by $g(x) = x^6 + x^4 + x + 1$, the parity-check polynomial is $h(x) = (x^{21} - 1)/g(x) = x^{15} + x^{13} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$. Thus we can design the parity-check matrix H_1 from $\tilde{h}(x)$ and the first $n_0 = 16$ columns of H_1 constitute a parity-check matrix for $\mathcal{C}'$:

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

Since the generating function of $\mathcal{C}'$ is a multiple of $g(x)$, we can design the generator polynomial for $\mathcal{C}'$ as designing G_1 for $\mathcal{C}$:

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

We can verify that any row of G' is orthogonal to any row of H'.

6.2 First, get the parity-check matrix for $\mathcal{C}_1$.

$$h(x) = (x^{15}-1)/g(x) = x^{10}+x^9+x^8+x^6+x^5+x^2+1,$$

and

$$H_1 = \begin{pmatrix} 1&1&1&0&1&1&0&0&1&0&1&0&0&0&0 \\ 0&1&1&1&0&1&1&0&0&1&0&1&0&0&0 \\ 0&0&1&1&1&0&1&1&0&0&1&0&1&0&0 \\ 0&0&0&1&1&1&0&1&1&0&0&1&0&1&0 \\ 0&0&0&0&1&1&1&0&1&1&0&0&1&0&1 \end{pmatrix}.$$

I made a program to get the fraction of burst errors that were detected by H_1:

b	N_a	N_c	N_c/N_a	undetectable error
4	60	60	1	n/a
5	120	120	1	n/a
6	240	225	0.9375	101011
7	480	465	0.96875	1111101
8	960	930	0.96875	11010001,10000111

In the table, N_a is the number of all burst errors with length b, which actually is $n2^{b-2}$, and N_c is the number of detectable burst errors with length b. N_c/N_a is the fraction. I also list examples for undetectable burst errors.

6.3 The minimum distance of this code is 4, and the dimension is 10.

(a) Since the minimum distance for the $(15,11)$ Hamming code is 3, the minimum distance for this code is bigger than or equal to 3. For any 3 distinct columns of H, we have

$$\begin{pmatrix} x_1 \\ f(x_1) \end{pmatrix} + \begin{pmatrix} x_2 \\ f(x_2) \end{pmatrix} + \begin{pmatrix} x_3 \\ f(x_3) \end{pmatrix} = \begin{pmatrix} x_1+x_2+x_3 \\ T(x_1+x_2+x_3)+y \end{pmatrix}.$$

Since y is non-zero, $T(x_1+x_2+x_3)+y = y$ is non-zero when $x_1+x_2+x_3=0$. Thus any 3 distinct columns of H is linearly independent.

However, some combinations of 4 columns of H is linearly dependent. For example, $1+2+5+6=0$, thus

$$\begin{pmatrix} 1 \\ f(1) \end{pmatrix} + \begin{pmatrix} 2 \\ f(2) \end{pmatrix} + \begin{pmatrix} 5 \\ f(5) \end{pmatrix} + \begin{pmatrix} 6 \\ f(6) \end{pmatrix} = \begin{pmatrix} 0 \\ T(0) \end{pmatrix} = 0.$$

Thus the minimum distance of this code is 4.

(b) Below I will calculate the rank of H, and the dimension of the code is $n - \text{rank}(H)$.

Lemma: Given any 6 different vectors $x_1, x_2, \ldots, x_6 \in \{1, 2, \ldots, F\}$, we can always find a combination of an even number (not 0) of vectors with sum 0.

Proof: Look at the $\binom{6}{2} = 15$ sum vectors of combinations of two vectors, which are in the form $x_i + x_j$ where $i \neq j$. They are non-zero since $x_i \neq x_j$ when $i \neq j$.

- If any two of those 15 sum vectors are same, say, $x_i + x_j = x_{i'} + x_{j'}$, then these 4 vectors are distinct from each other[1] and the sum of them are 0.

[1] If not so, without loss of generality, assume $x_i = x_{i'}$, or $i = i'$. Then we get $x_j = x_{j'}$, or $j = j'$. Thus these are not two different combinations.

- Otherwise, those sums are 15 distinct non-zero vectors, i.e. the set of all non-zero vectors of length 4. Then for any combination of 4 different vectors x_i, x_j, x_m, and x_n, the sum $x_i + x_j + x_m + x_n$ is the sum of two distinct sum vectors thus is not zero, and it must be same with some sum vector, i.e.,

  $$x_i + x_j + x_m + x_n = x_{i'} + x_{j'}.$$

  Then we have

  $$x_i + x_j + x_m + x_n + x_{i'} + x_{j'} = 0. \tag{1}$$

  This time we don't necessarily have 6 distinct vectors. However, if there are two identical vectors between x_i, x_j, x_m, x_n and $x_{i'}$, $x_{j'}$, we can just remove them from (1). Since the sum of two identical vectors is 0, the sum of the remainders is still 0. We can repeat this until there are no identical vectors. Since every time we remove 2 vectors, the number of remaining vectors should be 0, 2, 4, or 6. However, x_i, x_j, x_m and x_n are different from each other, thus we will not end with 0 vectors.[2] Thus this lemma holds. □

Theorem: Every 6 different columns of H are linearly dependent.

Proof: For any 6 different columns of H:

$$\begin{pmatrix} x_i \\ f(x_i) \end{pmatrix}, i = 1..6,$$

The Lemma says that there's a combination of x_i's such that $x_{i_1} + \cdots + x_{i_k} = 0$, where k is a positive even number, and $i_1, \ldots, i_k$ are different numbers from 1..6. Thus

$$\begin{pmatrix} x_{i_1} \\ f(x_{i_1}) \end{pmatrix} + \cdots + \begin{pmatrix} x_{i_k} \\ f(x_{i_k}) \end{pmatrix} = \begin{pmatrix} x_{i_1} + \cdots + x_{i_k} \\ T(x_{i_1} + \cdots + x_{i_k}) \end{pmatrix} = 0,$$

which means these 6 columns are linearly dependent. □

From the Theorem we know that the rank of H is less than 6. And we can find 5 columns of H that are linearly independent:

$$\begin{pmatrix} 1 \\ f(1) \end{pmatrix}, \begin{pmatrix} 2 \\ f(2) \end{pmatrix}, \begin{pmatrix} 4 \\ f(4) \end{pmatrix}, \begin{pmatrix} 8 \\ f(8) \end{pmatrix}, \begin{pmatrix} F \\ f(F) \end{pmatrix}.$$

It is easy to see that any four vectors from them are linearly independent since the first four bits of these vectors are

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

And, the sum of them is

$$\begin{pmatrix} 1 \\ f(1) \end{pmatrix} + \begin{pmatrix} 2 \\ f(2) \end{pmatrix} + \begin{pmatrix} 4 \\ f(4) \end{pmatrix} + \begin{pmatrix} 8 \\ f(8) \end{pmatrix} + \begin{pmatrix} F \\ f(F) \end{pmatrix} = \begin{pmatrix} 0 \\ y \end{pmatrix} \neq 0.$$

Thus they are linearly independent. So the rank of H is 5, and the dimension of the code is $n - 5 = 10$.

[2] In fact, the sum of two distinct vectors is non-zero. And since we have proved that no 4 distinct vectors can have a zero sum, the number of remaining vectors can't be 2 or 4. Thus it has to be 6, i.e., there are no identical vectors in x_i, x_j, x_m, x_n and $x_{i'}$, $x_{j'}$.