EE/Ma 127a Error-Correcting Codes - Homework Assignment 7

Ling Li, ling@cs.caltech.edu

November 29, 2000

7.1 *BCH decoding.* For any syndrome $\binom{s_1}{s_3}$, if there are no more than 2 errors, we can suppose it is the sum of two vectors $\binom{\alpha}{\alpha^3}$ and $\binom{\beta}{\beta^3}$ which if not zero is a column of H, i.e. $\alpha+\beta = s_1, \alpha^3+\beta^3 = s_3$. If s_1 is not zero, then s_1^{-1} exists and we have

$$\begin{aligned}\sigma_1 &= \alpha+\beta = s_1,\\ \sigma_2 &= \alpha\beta = (\alpha^2+\beta^2)+(\alpha^2+\alpha\beta+\beta^2) = s_1^2 + s_1^{-1}s_3.\end{aligned}$$

So α and β are two roots of the equation

$$x^2 + \sigma_1 x + \sigma_2 = 0 \tag{1}$$

which is computed in the HexField.

- 101011000010000. The syndrome is $\binom{A}{9}$. Thus $s_1 = A$, $s_3 = 9$. From the multiplication table of the HexField, $s_1^{-1} = C$, and $\sigma_2 = A^2 + C\cdot 9 = 8+6 = E$. So equation (1) here is $x^2+Ax+E = 0$. Testing x over $0, 1, \ldots, F$ (remember α and β here may be zero) we get $x = 6$ or C. So the syndrome is the sum of columns #6 and #12 of H, i.e., $\binom{A}{9} = \binom{6}{1} + \binom{C}{8}$, and the decoded codeword is 101010000011000.
- 101011000110000. The syndrome is $\binom{0}{6}$. It can not be a sum of two columns of H since when $\alpha+\beta = 0$, we also have $\alpha^3+\beta^3 = (\alpha+\beta)(\alpha^2+\alpha\beta+\beta^2) = 0$, which contradicts with $s_3 = 6$. Obviously it is neither one column of H nor zero. So there must be more than 2 errors and the received vector can not be decoded.
- 111111100001100. The syndrome is $\binom{1}{2}$. Thus $s_1 = 1$, $s_3 = 2$, $s_1^{-1} = 1$, and $\sigma_2 = 1^2+1\cdot 2 = 3$. So equation (1) here is $x^2+x+3 = 0$. Testing x over $0, 1, \ldots, F$ we get $x = C$ or D. So the syndrome is the sum of columns #12 and #13 of H, i.e., $\binom{1}{2} = \binom{C}{8} + \binom{D}{A}$, and the decoded codeword is 111111100000000.
- 000000110110010. The syndrome is $\mathbf{0}$ and this is a valid codeword.
- 001010000000011. The syndrome is $\binom{7}{1}$, which is column #7 of H. So the decoded codeword is 001010100000011.

  We can still use equation (1) to solve it. Here $s_1 = 7$, $s_3 = 1$, $s_1^{-1} = 6$, and $\sigma_2 = 7^2+6\cdot 1 = 6+6 = 0$. Thus the equation is $x^2+7x = 0$ which hints $x = 0$ or 7.

7.2 *Cyclic BCH code.* Let $\mathcal{C}$ denote the $(15, 7)$ code defined by H'.

(a) Use the powers of 2 to rewrite H' (note that $2^{15} = 1$):

$$H' = \begin{bmatrix} 1 & 2 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 & 2^9 & 2^{10} & 2^{11} & 2^{12} & 2^{13} & 2^{14} \\ 1 & 2^3 & 2^6 & 2^9 & 2^{12} & 2^{15} & 2^{18} & 2^{21} & 2^{24} & 2^{27} & 2^{30} & 2^{33} & 2^{36} & 2^{39} & 2^{42} \end{bmatrix}.$$

For any codeword $\mathbf{C} = (C_0, C_1, \ldots, C_{14})$ in the code $\mathcal{C}$, we have $H'\mathbf{C}^T = 0$, i.e.,

$$\sum_{i=0}^{14} 2^i C_i = 0 \text{ and } \sum_{i=0}^{14} 2^{3i} C_i = 0.$$

Thus for the right cyclic shift of $\mathbf{C}$, i.e., $\mathbf{C}^R = (C_{14}, C_0, \ldots, C_{13})$, we also have

$$C_{14} + \sum_{i=0}^{13} 2^{i+1} C_i = 2^{15} C_{14} + 2 \sum_{i=0}^{13} 2^i C_i = 2 \sum_{i=0}^{14} 2^i C_i = 0,$$

and

$$C_{14} + \sum_{i=0}^{13} 2^{3(i+1)} C_i = 2^{45} C_{14} + 2^3 \sum_{i=0}^{13} 2^{3i} C_i = 2^3 \sum_{i=0}^{14} 2^{3i} C_i = 0.$$

So $H' \left(\mathbf{C}^R\right)^T = 0$, $\mathbf{C}^R$ is also a codeword of $\mathcal{C}$. Thus $\mathcal{C}$ is cyclic.

(b) Since $\mathcal{C}$ is cyclic, its generator polynomial $g(x)$ should be a divisor of $x^{15} - 1$. Note that the degree of $g(x)$ is $r = \text{rank}(H') = 8$. Thus $g(x)$ is the multiplication of two of $1+x+x^4$, $1 + x^3 + x^4$, and $1 + x + x^2 + x^3 + x^4$. We can verify $g(x)$ by calculating the syndrome of the vector that has $g(x)$ as the generating function. Among those 3 multiplications, only $g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$ turns out to have zero syndrome. Thus the generator polynomial for $\mathcal{C}$ is $g(x) = (1+x+x^4)(1+x+x^2+x^3+x^4) = 1+x^4+x^6+x^7+x^8$.

7.3 *HexField and* $x^4 + x + 1$.

(a) Consider

$$\begin{aligned}
&(a_0 + a_1 x + a_2 x^2 + a_3 x^3)(b_0 + b_1 x + b_2 x^2 + b_3 x^3) \bmod (x^4 + x + 1) = \\
&\quad (a_0 b_0 + a_1 b_3 + a_2 b_2 + a_3 b_1) + (a_0 b_1 + a_1 b_0 + a_1 b_3 + a_2 b_2 + a_2 b_3 + a_3 b_1 + a_3 b_2)x + \\
&\quad (a_0 b_2 + a_1 b_1 + a_2 b_0 + a_2 b_3 + a_3 b_2 + a_3 b_3)x^2 + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 + a_3 b_3)x^3.
\end{aligned}$$

Thus we get

$$[a_0, a_1, a_2, a_3] \cdot [b_0, b_1, b_2, b_3] = [c_0, c_1, c_2, c_3],$$

where

$$\begin{aligned}
c_0 &= a_0 b_0 + a_1 b_3 + a_2 b_2 + a_3 b_1, \\
c_1 &= a_0 b_1 + a_1 b_0 + a_1 b_3 + a_2 b_2 + a_2 b_3 + a_3 b_1 + a_3 b_2, \\
c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 + a_2 b_3 + a_3 b_2 + a_3 b_3, \\
c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 + a_3 b_3.
\end{aligned}$$

This is the rule for multiplication in the HexField.

(b) D is represented as $[1, 0, 1, 1]$ and 4 is $[0, 0, 1, 0]$. Using the rule in (a), we have $D \cdot 4$ is $[1, 0, 0, 0]$, i.e., $D \cdot 4 = 1$.

7.4 F is associated with $1 + x + x^2 + x^3$. Using the extended Euclidean algorithm

i	s_i	t_i	r_i	q_i
-1	1	0	$1+x+x^4$	-
0	0	1	$1+x+x^2+x^3$	-
1	1	$1+x$	x	$1+x$
2	$1+x+x^2$	x^3	1	$1+x+x^2$

So

$$x^3(1+x+x^2+x^3) \equiv 1 \pmod{1+x+x^4}.$$

Thus $F^{-1} = 8$ (which is x^3) in the HexField.