EE/Ma 127b Error-Correcting Codes - Homework Assignment 1

Ling Li, ling@cs.caltech.edu

January 14, 2001

1.1 Consider the field $GF(16)$ defined by polynomial $x^4+x^3+x^2+x+1$:

(a) By the table below, we know that the order of [0100] is 5.

i	0	1	2	3	4	5
$[0100]^i$	[1000]	[0100]	[0010]	[0001]	[1111]	[1000]

(b) We can *try* some non-zero elements other than $[0100]^i$. For example, [1100]. ord([1100]) is a divisor of 15, i.e., one of 1, 3, 5 or 15. Since none of [1100], $[1100]^3 = [1111]$, and $[1100]^5 = [1011]$ is equal to [1000], ord([1100]) must be 15.

1.2 $GF(49)$ *generated by* $x^2-3 \pmod 7$.

(a) From the table below, we know that the order of α $(= x)$ is 12.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^i \bmod (x^2-3)$	1	x	3	$3x$	2	$2x$	6	$6x$	4	$4x$	5	$5x$	1

(b) *Try* the element corresponding to the equivalence class of $x+1$, denoted by β. Let $d = \mathrm{ord}(\beta)$. From the table below,

i	0	1	2	3	4	$\cdots$
$(x+1)^i \bmod (x^2-3)$	1	$x+1$	$2x+4$	$6x+3$	$2x$	$\cdots$

we get $\beta^4 = \alpha^5$. Thus

$$\frac{d}{\gcd(d,4)} = \mathrm{ord}(\beta^4) = \mathrm{ord}(\alpha^5) = \frac{12}{\gcd(12,5)} = 12.$$

So $d = 12\gcd(d,4)$. Since $\gcd(d,4) = \gcd(12\gcd(d,4),4) = 4$, we get $d = 48$. Thus β is a primitive root. By the extended Euclidean algorithm,

$$(-2)\times 12 + 5\times 5 = 1.$$

Thus $\alpha = \alpha^{25} = \left(\alpha^5\right)^5 = \left(\beta^4\right)^5 = \beta^{20}$.

(c) From the table in (b), we know 1 and β are linear independent, and $\beta^2 - 2\beta - 2 = 0$. So the minimal polynomial of β is $f(x) = x^2 - 2x - 2 = x^2 + 5x + 5$.

1.3 *Minimal polynomials over $GF(2^4)$ defined by x^4+x+1.*

i	α^i	$\mathrm{ord}(\alpha^i)$	$\deg(\alpha^i)$	minimal polynomial	comment
0	0001	1	1	$x+1$	
1	0010	15	4	x^4+x+1	
2	0100	15	4	x^4+x+1	
3	1000	5	4	$x^4+x^3+x^2+x+1$	
4	0011	15	4	x^4+x+1	
5	0110	3	2	x^2+x+1	
6	1100	5	4	$x^4+x^3+x^2+x+1$	
7	1011	15	4	x^4+x^3+1	see note below
8	0101	15	4	x^4+x+1	same as $i=1,2,4$
9	1010	5	4	$x^4+x^3+x^2+x+1$	same as $i=3,6$
10	0111	3	2	x^2+x+1	same as $i=5$
11	1110	15	4	x^4+x^3+1	same as $i=7$
12	1111	5	4	$x^4+x^3+x^2+x+1$	same as $i=3,6$
13	1101	15	4	x^4+x^3+1	same as $i=7$
14	1001	15	4	x^4+x^3+1	same as $i=7$
15	0001	1	1	$x+1$	

Note that $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ are all conjugates. Thus their minimal polynomial is of degree 4, which appears to be x^4+x^3+1, the only irreducible polynomial with degree 4 over F_2 that is not the minimal polynomial of α^i for $1 \le i \le 6$.

1.4 *BCH codes with $n=15$.* The conjugates of α are $(\alpha, \alpha^2, \alpha^4, \alpha^8)$; of α^3: $(\alpha^3, \alpha^6, \alpha^{12}, \alpha^9)$; of α^5: (α^5, α^{10}); of α^7: $(\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11})$. And the minimal polynomials are: of α is $m_1(x) = x^4+x+1$ (by definition); of α^3 is $m_3(x) = x^4+x^3+x^2+x+1$; $m_5(x) = x^2+x+1$; $m_7(x) = (x^{15}-1)/[(x-1)m_1(x)m_3(x)m_5(x)] = x^4+x^3+1$. Thus we can list the table below: (the dimension of the code is $k = n - \deg g(x)$)

t	k	$g(x)$	comment
1	11	x^4+x+1	$m_1(x)$
2	7	$x^8+x^7+x^6+x^4+1$	$m_1(x)m_3(x)$
3	5	$x^{10}+x^8+x^5+x^4+x^2+x+1$	$m_1(x)m_3(x)m_5(x)$
4–7	1	$x^{14}+x^{13}+\cdots+x+1$	$m_1(x)m_3(x)m_5(x)m_7(x) = \frac{x^{15}-1}{x-1}$

1.5 For any odd number n, let β be one element of order n, and $t = \deg(\beta)$, i.e., the degree of the minimal polynomial of β. Since t is the smallest (positive) number such that $\beta^{2^t} = \beta$, or, $n|(2^t-1)$, and m is defined as the smallest (positive) number such that $n|(2^m-1)$, we get $t=m$. Thus the dimension of the code is $k = n-t = n-m$. In Table 1, I listed the minimum distance d and code dimension k for each code. Below is some explanations:

- $n=7$. The smallest m such that $n|2^m-1$ is $m=3$. Thus $k=4$. The code is the $(7,4)$ cyclic Hamming code, so the minimum distance of the code is $d=3$. Similar situations happen with $n=15$ and $n=31$.
- $n=9$. $m=6$, $k=3$. The set of conjugates of β is $\{\beta^1, \beta^2, \beta^4, \beta^8, \beta^7, \beta^5\}$. So the generator polynomial is

$$\frac{\prod_{i=1}^{8}(x-\beta^i)}{\prod_{i=1}^{2}(x-\beta^{3i})} = \frac{\prod_{i=0}^{8}(x-\beta^i)}{\prod_{i=0}^{2}(x-\beta^{3i})} = \frac{x^9-1}{x^3-1} = x^6+x^3+1.$$

n	m	k	d	comment
7	3	4	3	$(7,4)$ cyclic Hamming code
9	6	3	3	depth-3 interleaving of the $(3,1)$ code
11	10	1	11	$(11,1)$ repetition code
13	12	1	13	$(13,1)$ repetition code
15	4	11	3	$(15,11)$ cyclic Hamming code
17	8	9	3, 4, 5, or 6	
19	18	1	19	$(19,1)$ repetition code
21	6	15	3 or 4	
23	11	12	7	*told in the class*
25	20	5	5	depth-5 interleaving of the $(5,1)$ code
27	18	9	3	depth-9 interleaving of the $(3,1)$ code
29	28	1	29	$(29,1)$ repetition code
31	5	26	3	$(31,26)$ cyclic Hamming code

Table 1: Minimum distance d and code dimension k for some BCH codes of $t=1$.

So this code is a depth-3 interleaving of the $(3,1)$ repetition code, and $d=3$.

- $n = 11, 13, 19, 29$. Obviously they are repetition codes and thus $d = n$.
- $n = 17$. $m = 8$, $k = 9$. Since $2^m = 256 < 834 = 1 + \binom{17}{1} + \binom{17}{2} + \binom{17}{3}$, $d < 7$. However, $t = 1$ assures that $d \geq 3$. So d is 3, 4, 5, or 6.
- $n = 21$. $m = 6$, $k = 15$. Since $2^m = 64 < 232 = 1 + \binom{21}{1} + \binom{21}{2}$, $d < 5$. However, $t = 1$ assures that $d \geq 3$. So d is 3 or 4.
- $n = 25$. $m = 20$, $k = 5$. The set of conjugates of β is

$$\left\{\beta^1, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^7, \beta^{14}, \beta^3, \beta^6, \beta^{12}, \beta^{24}, \beta^{23}, \beta^{21}, \beta^{17}, \beta^9, \beta^{18}, \beta^{11}, \beta^{22}, \beta^{19}, \beta^{13}\right\}.$$

Thus the generator polynomial is

$$\frac{\prod_{i=1}^{24}(x-\beta^i)}{\prod_{i=1}^{4}(x-\beta^{5i})} = \frac{\prod_{i=0}^{24}(x-\beta^i)}{\prod_{i=0}^{4}(x-\beta^{5i})} = \frac{x^{25}-1}{x^5-1} = x^{20} + x^{15} + x^{10} + x^5 + 1.$$

So, this is a depth-5 interleaving of the $(5,1)$ repetition code. Thus $d = 5$.

- $n = 27$. $m = 18$, $k = 9$. Also an interleaving code. The set of conjugates of β is

$$\left\{\beta^1, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^5, \beta^{10}, \beta^{20}, \beta^{13}, \beta^{26}, \beta^{25}, \beta^{23}, \beta^{19}, \beta^{11}, \beta^{22}, \beta^{17}, \beta^7, \beta^{14}\right\}.$$

Thus the generator polynomial is

$$\frac{\prod_{i=1}^{26}(x-\beta^i)}{\prod_{i=1}^{8}(x-\beta^{3i})} = \frac{\prod_{i=0}^{26}(x-\beta^i)}{\prod_{i=0}^{8}(x-\beta^{3i})} = \frac{x^{27}-1}{x^9-1} = x^{18} + x^9 + 1.$$

Thus this code is a depth-9 interleaving of the $(3,1)$ repetition code, and $d = 3$.