Viewing A Code From An Extension Field

(一)

$C = [c_0, c_1, \ldots, c_{n-1}]$

Hamming (7, 4) code

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{matrix} Z^0 \\ Z^1 \\ Z^2 \end{matrix}$$

$CH^T = [0, 0, 0]$ – over GF(2)
$CH^T = 0$ – in $GF(2^3)$

$$c_0\begin{bmatrix}1\\0\\0\end{bmatrix} + c_1\begin{bmatrix}0\\1\\0\end{bmatrix} + \ldots + c_{n-1}\begin{bmatrix}1\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

$HC^T = [0,0,0]^T$

$$GF(8) \cong GF(2)[Z] / Z^3 + Z + 1$$

$\alpha = Z$
$\alpha^2 = Z^2$
$\alpha^3 = Z + 1$
$\alpha^4 = Z^2 + Z$
$\alpha^5 = Z^2 + Z + 1$
$\alpha^6 = Z^2 + 1$
$\alpha^7 = 1$

take the primitive element $\alpha = z$

$$\Rightarrow H = \left[\alpha^0\ \alpha^1\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\right]$$

$$\Rightarrow \sum_{i=0}^{6} c_i \alpha^i = 0 \leftrightarrow c(x) = \sum_{i=0}^{n-1} c_i x^i$$

e.g. $c(x)=1+x+x^3$

$\Rightarrow$ A binary polynomial c(x) is a codeword polynomial iff α (in GF(8)) is a zero of c(x)

※ $r(x) = c(x) + e(x)$

$$e(x) = e_0 + e_1 x + \ldots + e_{n-1} x^{n-1}$$

$$s_j \equiv r(v_j) = \sum_{i=0}^{n-1} e_j v_j^i \quad j = 1,2,\ldots r. \quad -(*)$$

how to choose v_j st. (*)有解

(二)

$$H = \begin{bmatrix} v_1^0 & v_1^1 & & v_1^{n-1} \\ v_2^0 & v_2^1 & & v_1^{n-1} \\ & & & \\ & & & \\ v_r^0 & v_r^1 & & v_r^{n-1} \end{bmatrix} \quad \text{where } v_j \in \mathrm{GF}(q^m)\ 1 \le j \le r$$

$$n = q^m\text{-}1 \quad r = (n\text{-}k)/m$$

$$CH^T = 0 \Rightarrow \sum_{i=0}^{n-1} c_i v_j^i = 0 \quad j = 1,\ldots,r$$

$\Rightarrow$ codeword polynomial c(x) has zeros at $v_1, \ldots, v_r$

EX: **H**(15, 7, 5)

$$H = \begin{bmatrix} 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ 1&0&0&0&1&1&0&0&0&1&1&0&0&0&1 \\ 0&0&0&1&1&0&0&0&1&1&0&0&0&1&1 \\ 0&0&1&0&1&0&0&1&0&1&0&0&1&0&1 \\ 0&1&1&1&1&0&1&1&1&1&0&1&1&1&1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ (\alpha^3)^0 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} & \alpha^{24} & \alpha^{27} & \alpha^{30} & \alpha^{33} & \alpha^{36} & \alpha^{39} & \alpha^{42} \end{bmatrix}$$

$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

α, α^3 in GF(2^4)
$\alpha^{15} = 1$

$\Rightarrow c(\alpha)=0$
$c(\alpha^3)=0$

取 $g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8 + x^7 + x^6 + x^4 + 1$

(i) $n - k = 8 \Rightarrow k = 7$

(ii) $d^* \le 9$ (= singleton bound)

≤ 5 ($\because$ w(g(x)) = 5)

$\because d^* \ge 2t + 1 = 5$ (BCH bound)

$\therefore d^* = 5$

Thm: F[x]/p(x) is a field iff p(x) is a prime polynomial

Prime polynomials over GF(2)

Degree	Primitive Polynomial
2	$x^2 + x + 1 \Rightarrow x^2+x+1 \mid x^3+1$
3	$x^3 + x + 1 \Rightarrow x^3+x+1 \mid x^7+1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x^3 + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$
9	$x^9 + x^4 + 1$
10	$x^{10} + x^3 + 1$
11	$x^{11} + x^2 + 1$
12	$x^{12} + x^6 + x^4 + x + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^{10} + x^6 + x + 1$
15	$x^5 + x + 1$
16	$x^{16} + x^{12} + x^3 + x + 1$

Def: Let GF(q) be a field and let GF(Q) be an extension field of GF(q). Let β be in GF(Q). The prime polynomial f(x) of smallest degree over GF(q) with f(β) = 0 is called the minimal polynomial of β over GF(q).

$GF(2^4) \doteq GF(2)[Z] / Z^4+Z+1$

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	0000	0	x
α^0	1	0001	1	x + 1
α^1	Z	0010	2	$x^4 + x + 1$ ◦
α^2	Z^2	0100	4	$x^4 + x + 1$ ◦
α^3	Z^3	1000	8	$x^4 + x^3 + x^2 + x + 1$
α^4	Z + 1	0011	3	$x^4 + x + 1$ ◦
α^5	$Z^2 + Z$	0110	6	$x^2 + x + 1$
α^6	$Z^3 + Z^2$	1100	12	$x^4 + x^3 + x^2 + x + 1$
α^7	$Z^3 + Z + 1$	1011	11	$x^4 + x^3 + 1$
α^8	$Z^2 + 1$	0101	5	$x^4 + x + 1$ ◦
α^9	$Z^3 + Z$	1010	10	$x^4 + x^3 + x^2 + x + 1$
α^{10}	$Z^2 + Z + 1$	0111	7	$x^2 + x + 1$
α^{11}	$Z^3 + Z^2 + Z$	1110	14	$x^4 + x^3 + 1$
α^{12}	$Z^3 + Z^2 + Z + 1$	1111	15	$x^4 + x^3 + x^2 + x + 1$
α^{13}	$Z^3 + Z^2 + 1$	1101	13	$x^4 + x^3 + 1$
α^{14}	$Z^3 + 1$	1001	9	$x^4 + x^3 + 1$

$\alpha = Z$

$x^{15} = 1$

Minimal Polynomials and Conjugates

Q: How to find g(x)

GF(q) ----------$GF(q^m)$ $n = q^m - 1$: primitive block length

$x^n - 1 = f_1(x)f_2(x)\ldots f_s(x)$ $f_i(x)$: prime polynomials over GF(q)

- $g(x) | x^n - 1 \Rightarrow g(x) = \prod f_i(x)$ $2^s - 2$ different nontrivial cyclic code

  $g(x) = 1$, $x^n - 1$ trivial cases

- Choosing desirable zeros in an extension field so as to ensure a good code

$$x^n - 1 = \prod_j (x - \beta_j)$$ β_j is a nonzero element of $GF(q^m)$

$$\beta_j \quad \frac{\text{minimal}}{\text{polynomial}} \quad f_l(x)$$

Thm: Suppose that f(x) is the minimal polynomial over GF(q) of β, an element of GF(q^m). Then f(x) is also the minimal polynomial of β^q.

Def: Two element of GF(q^m) that share the same minimal polynomial over GF(q) are called conjugates (with respect to GF(q))

GF(16) < GF(2^4), GF(4^2)

$\{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{r-1}}\}$ $\beta^{q^r} = \beta$

e.g.

q = 2 r = 4 m = 4

$\alpha^7 \ (\alpha^7)^2 \ (\alpha^7)^{2^2} \ (\alpha^7)^{2^3}$

$n = 2^m - 1 = 2^4 - 1 = 15$

ie. $\beta^{2^4} = \beta$

ie. $\beta^{15} = 1$

Thm: The minimal polynomial of β is $f(x) = (x- \beta)(x- \beta^q)\ldots(x- \beta^{q^{r-1}})$

Cor: ∵ $\beta^{q^m} = \beta(\beta^{q^m-1} = \beta^n = 1) \rightarrow r < m$

∴ deg(minimal polynomial) ≤ m

Thm1: Let g(x), the generator polynomial of a primitive code, have zeros $\beta_1, \beta_2 \ldots \beta_r$ in GF(q^m). A polynomial c(x) over GF(q) is a codeword polynomial iff $c(\beta_1) = c(\beta_2) = \ldots = c(\beta_r) = 0$, where $c(\beta_j)$ is evaluated in GF(q^m).

- Suppose we wish to construct a g(x) that has $\beta_1, \beta_2 \ldots \beta_r$ as zeros. Find the minimal polynomials of these field elements, denoting them as $f_1(x), f_2(x), \ldots, f_r(x)$, Then
  $g(x) = LCM[f_1(x), f_2(x), \ldots, f_r(x)]$
- How to find $f_l(x)$
- Cyclic codes in one field can be constructed by working with zeros in a larger field.

pf:

Thm1:

$\Rightarrow$ $c(x) = a(x)g(x)$ $\quad \because c(\beta_j) = 0$

$\Leftarrow$ Suppose $c(\beta_j) = 0$

$c(x) = Q(x)f_j(x) + s(x)$ where

$\deg s(x) < \deg f_j(x)$

$f_j(x)$ is the minimal polynomial of β_j

but $0 = Q(\beta_j)f_j(\beta_j) + s(\beta_j) = s(\beta_j)$ (if $s(x) \neq 0$ $\rightarrow\leftarrow$)

$\therefore s(x) = 0$

$\therefore f_j(x) | c(x) \quad \Rightarrow \quad \underline{g(x)} | c(x)$

$=\text{LCM}[f_1(x)f_2(x)\ldots f_r(x)]$

e.g.

$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(\underline{x^4+x^3+1})(x^4+x^3+x^2+x+1)$

In GF(2^4) $= (x-\alpha^0)(x-\alpha^5)(x-\alpha^{10})(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$

$\alpha^{15} = 1$ $\qquad \underline{(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})}$

$(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$

take $g(x) = (x^4+x^3+1)(x^4+x^3+x^2+x+1) = x^8 + x^4 + x^2 + x + 1$

has zeros $\alpha^3\ \alpha^6\ \alpha^7\ \alpha^9\ \alpha^{11}\ \alpha^{12}\ \alpha^{13}\ \alpha^{14}$

$*$ α^5, α^{10} : order = 3 $\qquad \deg[x^2 + x + 1] \mid 4$

$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$: order = 5 $\qquad \deg[x^4+x^3+x^2+x+1] \mid 4$