Non binary BCH codes

Note Title

Ex: $n = 10$, $q = 9$

$GF(9) = \{a + b\alpha : a, b \in GF(3)\}$

$\alpha^2 + \alpha + 2 = 0$

$\beta \in GF(81)$, primitive

$n = 10 \mid ord(\beta) = 80$

$\Rightarrow ord(\beta^8) = n = 10$

$\{0\}, \{5\}, \{1,9\}, \{2,8\}, \{3,7\}, \{4,6\}$

$x^{10} - 1 = (x-1)(x+1)(x-\beta^8)(x-\beta^{-2}) \cdots$

Ex: $q = 4$, $n = 15$

$\alpha \in GF(16)$, primitive, $\alpha^4 + \alpha + 1 = 0$

$\{0\}, \{1,4\}, \{2,8\}, \{3,12\}, \{5\}, \{6,9\}, \{10\}$

$\{7,13\}, \{11,14\}$

$m_\alpha(x) = x^2 + x + \alpha^5$

$x^{15} + 1 = (x+1)(x+\alpha^5)(x+\alpha^{10})(x+\alpha)(x+\alpha^4)(x+\alpha^2)(x+\alpha^8)(x+\alpha^3)(x+\alpha^{12})(x+\alpha^6)(x+\alpha^9)$

$m_{\alpha^3}(x) = x^2 + x + \alpha^{10}$, $x^2 + \alpha^{10}x + 1$, $x^2 + \alpha^5 x + 1$

$$\underbrace{(x+\alpha^7)(x+\alpha^{13})}_{x^2+\alpha^5 x+\alpha^5} \quad \underbrace{(x+\alpha^{11})(x+\alpha^{19})}_{x^2+\alpha^{10}x+\alpha^{10}}$$

Possible $g(x)$: $(x^2+x+\alpha^5)(x^2+x+\alpha^{10})$

BCH codes over GF(4) with $n=15$

$t=1$ $g(x)=\text{lcm}(M_\alpha(x), M_{\alpha^2}(x)) = x^4+x+1$, $k=11$

$t=2$ $g(x)=\text{lcm}(M_\alpha(x), M_{\alpha^2}(x), M_{\alpha^3}(x), M_{\alpha^4}(x))$

$= (x^2+x+\alpha^5)(x^2+x+\alpha^{10})(x^2+\alpha^{10}x+1)$

$k = 9$

Ex: $q=4$, $n=21$

Find m s.t. $21 \mid 4^m-1$ $\quad m=3$ ✓

$\beta \in GF(64)$, primitive

$\alpha = \beta^3 \Rightarrow \text{ord}(\alpha) = n = 21$

$x+1$ $\{0\}, \{1,4,16\}, \{2,8,11\}, \{3,12,6\}, \{5,20,17\}$,

$\{7\}, \{9,15,18\}, \{10,19,13\}, \{14\}$

$x+\beta^{21}$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $x+\beta^{42}$

BCH codes over GF(q), n = 21

$t=1$ $\quad g(x) = M_\alpha(x)\, M_{\alpha^2}(x)$ $\quad \deg = 6,\ k = 15$

$t=2$ $\quad g(x) = M_\alpha(x)\, M_{\alpha^2}(x)\, M_{\alpha^3}(x)$ $\quad k = 12$

$t=3$ $\quad g(x) = M_\alpha M_{\alpha^2} M_{\alpha^3} M_{\alpha^5}$ $\quad k = 9$

Reed-Solomon Codes

q: prime power $\quad n = q-1$

$\alpha \in GF(q)$, primitive

$ord(\alpha) = n$

$\{0\}, \{1\}, \{2\}, \ldots, \{q-2\}$

$x^{q-1} - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{q-2})$

$iq \bmod (q-1) = i$

MDS

$t=1$ $\quad g(x) = (x-\alpha)(x-\alpha^2)$ $\quad k = n-2t$

$\vdots$

t $\quad g(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t})$

Polynomial Evaluation Construction of Reed-Solomon Codes

n : blocklength

$\alpha \in GF(q)$, $ord(\alpha) \geq n$

$$f(x) = f_0 + f_1 x + \cdots + f_{k-1} x^{k-1}$$

message $= [f_0 f_1 \cdots f_{k-1}]$ $f_i \in GF(q)$ $\quad$ $f_i = (q^k)$

$$\text{Codeword} = [f(\alpha)\ f(\alpha^2)\ f(\alpha^3) \cdots f(\alpha^n)]$$

length $= n$

$$\Rightarrow wt(\text{codeword}) \geq n - (k-1) = n - k + 1$$