Nonbinary BCH codes over $GF(q)$

Let $q = p^s$, p - prime. Consider $GF(q^m)$, generated by $P(x) = P_0 + P_1 x + P_2 x^2 + \dots + P_{m-1} x^{m-1} + x^m$ (primitive)
$(P_i \in GF(q))$. Let $P(\alpha) = 0$; $\alpha^i \neq \alpha^j$ $(i,j = 0 \dots, q^m - 2)$
$\alpha^{q^m - 1} = 1$.

Let $n = q^m - 1$
q-ary cyclic BCH code $\mathbb{C}$ has the check matrix
$(q^m - 1, q^{q^m - (d-1)m - 1}, d)$

$$H = \left.\underbrace{\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^3 & \dots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ 1 & \alpha^{d-2} & \alpha^{2(d-2)} & \dots & \alpha^{(d-2)(n-1)} \end{bmatrix}}_{n}\right\} (d-1)m$$

$\mathbb{C}$ consists of polynomials
$v(x) = v_0 + v_1 x + \dots + v_{n-1} x^{n-1}$ $v_i \in \{GF(q)\}$
such that
$v(1) = v(\alpha) = v(\alpha^2) = \dots = v(\alpha^{d-2}) = 0$ thus $\mathbb{C}$ is cyclic

<u>Example 1</u> $q=3 \quad (p=3, s=1)$

$GF(3) = \{0,1,2\}$ $\quad \boxed{\cancel{\alpha=2 \quad \{\alpha^0=1, \alpha^1=2, \alpha^2=1\}}}$

Take $m=2$ and $P(x)=x^2+x+2$, $P(\alpha)=0$

GF(9):

0 0	
0 1	α
0 2	α^5
1 0	1
1 1	α^7
1 2	α^2
2 0	α^4
2 1	α^6
2 2	α^3
1 α	

$\alpha^2 = -\alpha - 2 = 2\alpha+1$

$\alpha^3 = 2\alpha^2+\alpha = (2\alpha+1)2+\alpha =$
$= 2\alpha+2$ $\quad$ (mod 3)

$\alpha^4 = (2\alpha+1)^2 = 4\alpha^2+4\alpha+1$
$= 2\alpha+1+4\alpha+1 = 2$

$\alpha^5 = 2\alpha$

$\alpha^6 = 2\alpha^2 = 4\alpha+2 = \alpha+2$

$\alpha^7 = \alpha^2+2\alpha = 2\alpha+1+2\alpha = \alpha+1$

$\alpha^8 = 1$

Construct a check matrix for
$(8, 3^4, 3) = (3^2-1,\ 3^{3^2-2\cdot 2-1}, 3)$ single error correcting code over GF(3)

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \end{bmatrix} \Big\} 2\cdot 2=4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \end{bmatrix}$$

not needed

For single error $\quad e = (0, \dots, 0, e_i, 0, \dots, 0) \quad e_i \in \{0,1,2\}$

The syndrome: $\quad H e = \begin{pmatrix} e_i \\ \alpha^i e_i \end{pmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$

Decoding:

Thus iff $s_2 = s_1 \cdot \alpha^i \Leftrightarrow$ then error is in the digit i

and $e_i = s_1 \quad (i=0, \dots, n-1)$

In general for single error correction by q-ary BCH codes

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \end{bmatrix}$$

$n = q^m - 1$, $k = q^m - 2m - 1$, $d = 3$, $r = 2m$

Thus we constructed $(q^m - 1, q^{q^m - 2m - 1}, 3)$ q-ary codes

(Before we constructed $\left(\frac{q^m - 1}{q-1}, q^{q^m - m - 1}, 3\right)$ <u>perfect</u> single error correcting codes

with check matrix $H = [1\ \alpha\ \alpha^2 \ldots \alpha^{n-1}]$, $n = \frac{q^m - 1}{q-1}$)

<u>Example 2</u> $q = 4$ $(p = 2, s = 2)$

$GF(4) =$

00	0
01	α
10	1
11	α^2

Take $m = 2$ Construct $GF(16)$ by $P(x) = x^2 + x + \alpha$

Let $\beta \in GF(16)$ $P(\beta) = 0$ β primitive $\beta^{15} = 1$

Construct a cyclic code of length 15 over $GF(4)$ correcting $\ell = 2$ errors $(d = 5)$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 & \beta^{10} & \beta^{11} & \beta^{12} & \beta^{13} & \beta^{14} \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} & \beta^{12} & \beta^{14} & \beta^{16} & \beta^{18} & \beta^{20} & \beta^{22} & \beta^{24} & \beta^{26} & \beta^{28} \\ 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & \beta^{15} & \beta^{18} & \beta^{21} & \beta^{24} & \beta^{27} & \beta^{30} & \beta^{33} & \beta^{36} & \beta^{39} & \beta^{42} \end{bmatrix}$$

$\beta^i = (v_0, v_1)$ $(v_0, v_1 \in \{0, 1, \alpha, \alpha^2\})$

This is $(15, 4^7, 5)$ code correcting 2 errors over $GF(4)$

The code consists of all polynomials

$$v(x) = v_0 + v_1 x + v_2 x^2 + \dots + v_{n-1} x^{n-1} \quad ; \quad v_i \in \{0, 1, \alpha, \alpha^2\}$$

such that $v(1) = v(\beta) = v(\beta^2) = v(\beta^3) = 0$.

Let us prove that the code has distance 5.

Suppose we have errors with magnitudes $e_{i_1}, e_{i_2}, e_{i_3}, e_{i_4}$ $\left(e_{i_j} \in \{0,1,\alpha,\alpha^2\}\right)$ at the positions $i_1, i_2; i_3, i_4$.

Then we have for the syndrome $S = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix}$ $(s_i \in \{0,1,\alpha,\alpha^2\})$

$$S_1 = e_{i_1} + e_{i_2} + e_{i_3} + e_{i_4}$$

$$S_2 = e_{i_1}\beta^{i_1} + e_{i_2}\beta^{i_2} + e_{i_3}\beta^{i_3} + e_{i_4}\beta^{i_4}$$

$$S_3 = e_{i_1}\beta^{2i_1} + e_{i_2}\beta^{2i_2} + e_{i_3}\beta^{2i_3} + e_{i_4}\beta^{2i_4}$$

$$S_4 = e_{i_1}\beta^{3i_1} + e_{i_2}\beta^{3i_2} + e_{i_3}\beta^{3i_3} + e_{i_4}\beta^{3i_4}$$

dende $\beta^{i_1} = X_1$, $\beta^{i_2} = X_2$, $\beta^{i_3} = X_3$, $\beta^{i_4} = X_4$

consider determinant

$$\Delta = \begin{vmatrix} 1 & 1 & 1 & 1 \\ X_1 & X_2 & X_3 & X_4 \\ X_1^2 & X_2^2 & X_3^2 & X_4^2 \\ X_1^3 & X_2^3 & X_3^3 & X_4^4 \end{vmatrix}$$

Δ is known as Van der Mond determinant

$\Delta \neq 0$ since $X_i \neq X_j$ $\quad (\beta^{i_1} \neq \beta^{i_2})$

$S_1 = S_2 = S_3 = S_4 = 0 \iff e_{i_1} = e_{i_2} = e_{i_3} = e_{i_4} = 0 \iff$

any error with multiplicity at most 4 produce

nonzero syndrome $\iff d = 5$.

Reed Solomon Codes (RS-codes)

Special case of $(q^m - 1, q^{q^m - (d-1)m - 1}, d)$ BCH

q-ary cyclic codes with $m = 1$

For RS codes we have $n = q-1$, $k = n - d + 1$, $r = d-1$
$k = q - d$

(T). RS are the best codes providing min r

Proof Since for any linear code G can be

written as

$$G = \Big[\underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{k} \Big| \underbrace{\; P \;}_{r} \Big] k \qquad r \geq d-1 \text{ — (Singleton bound}$$

and for q-ary RS codes $r = d-1$.