EC500

Design of Secure and Reliable Hardware

Lecture 11

Mark Karpovsky

1 Non-binary BCH Codes over $GF(q)$

Let $q = p^s$ where p is prime and consider $GF(q^m)$ which is generated by $p(x) = p_0 + p_1x + p_2x^2 + \cdots + p_{m-1}x^{m-1} + x^m$ (primitive, $p_i \in GF(q)$). Let $p(\alpha) = 0$ and $\alpha^i \neq \alpha^j$ for i, $j = 0, \cdots, q^m - 2$ and $i \neq j$ and $\alpha^{q^m-1} = 1$. Let $n = q^m - 1$ and **a q-ary cyclic BCH code $C\left(q^m - 1, q^{q^m-(d-1)m-1}, d\right)$** has a check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{d-2} & \alpha^{2(d-2)} & \cdots & \alpha^{(d-2)(n-1)} \end{bmatrix}_{(d-1)m \times n}$$

C consists of polynomials $v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}$ where $v_i \in \{GF(q)\}$ such that $v(1) = v(\alpha) = v(\alpha^2) = \cdots = v(\alpha^{d-2}) = 0$, thus C is cyclic.

Example 1

$q = 3$ ($p = 3$, $s = 1$), $GF(3) = \{0,1,2\}$

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

$GF(9)$:

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

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

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

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

$\alpha^5 = 2\alpha$

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

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

$\alpha^8 = 1$

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

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \end{bmatrix}_{4\times 8} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \end{bmatrix}$$ → not needed.

For a single error $e = (0, \cdots, 0, e_i, 0, \cdots, 0)$ where $e_i \in \{0,1,2\}$, the syndrome $S = He = \begin{bmatrix} e_i \\ \alpha^i e_i \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \end{bmatrix}$. To decode this, the error is in the digit i and $e_i = S_1$ iff $S_2 = S_1 \cdot \alpha^i$ ($i = 0, \cdots, n-1$).

In general for single error correction by q-ary BCH codes, $H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \end{bmatrix}$ and $n = q^m - 1$, $k = q^m - 2m - 1$, $d = 3$, $r = 2m$ for a q-ary BCH code constructed in the form $\left(q^m - 1, q^{q^m-2m-1}, 3\right)$. (Earlier we constructed $\left(\frac{q^m-1}{q-1}, q^{q^m-m-1}, 3\right)$ perfect single error correcting codes with the check matrix $H = [1 \quad \alpha \quad \alpha^2 \quad \cdots \quad \alpha^{n-1}]$.)

Example 2

$q = 4$ $(p = 2,\ s = 2)$

$$GF(4) = \begin{matrix} 0 & 0 & & 0 \\ 0 & 1 & & \alpha \\ 1 & 0 & & 1 \\ 1 & 1 & & \alpha^2 \end{matrix}$$

Take $m = 2$ and construct $GF(16)$ using $p(x) = x^2 + x + \alpha$. Let $\beta \in GF(16)$ and $p(\beta) = 0 \rightarrow \beta$ is primitive and $\beta^{15} = 0$. Construct a cyclic code of length 15 over $GF(4)$ correcting $l = 2$ errors. $(d = 5)$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 & \beta^{10} & \beta^{11} & \beta^{12} & \beta^{13} & \beta^{14} \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} & \beta^{12} & \beta^{14} & \beta^{16} & \beta^{18} & \beta^{20} & \beta^{22} & \beta^{24} & \beta^{26} & \beta^{28} \\ 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & \beta^{15} & \beta^{18} & \beta^{21} & \beta^{24} & \beta^{27} & \beta^{30} & \beta^{33} & \beta^{36} & \beta^{39} & \beta^{42} \end{bmatrix}, \quad \beta^i = (v_0, v_1),$$

$(v_0, v_1 \in \{0,1,\alpha,\alpha^2\})$.

This is a $(15, 4^7, 5)$ code correcting two errors over $GF(4)$. The code consists of all polynomials $v(x) = v_0 + v_1x + v_2x^2 + \cdots + v_{n-1}x^{n-1}$ for $v_i \in \{0,1,\alpha,\alpha^2\}$ 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 $e_{i_1}, e_{i_2}, e_{i_3}, e_{i_4}$ $(e_{i_j} \in \{0,1,\alpha,\alpha^2\})$ at the positions i_1, i_2, i_3, i_4. Then we have for the syndrome $S = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix}$ for $(S_i \in \{0,1,\alpha,\alpha^2\})$.

$$S_1 = e_{i_1} + e_{i_2} + e_{i_3} + e_{i_4}$$
$$S_2 = e_{i_1}\beta^{i_1} + e_{i_2}\beta^{i_2} + e_{i_3}\beta^{i_3} + e_{i_4}\beta^{i_4}$$
$$S_3 = e_{i_1}\beta^{2i_1} + e_{i_2}\beta^{2i_2} + e_{i_3}\beta^{2i_3} + e_{i_4}\beta^{2i_4}$$
$$S_4 = e_{i_1}\beta^{3i_1} + e_{i_2}\beta^{3i_2} + e_{i_3}\beta^{3i_3} + e_{i_4}\beta^{3i_4}$$

Denote $\beta^{i_1} = X_1$, $\beta^{i_2} = X_2$, $\beta^{i_3} = X_3$, and $\beta^{i_4} = X_4$ and consider the determinant $\Delta = \begin{bmatrix} 1 & 1 & 1 & 1 \\ X_1 & X_2 & X_3 & X_4 \\ {X_1}^2 & {X_2}^2 & {X_3}^2 & {X_4}^2 \\ {X_1}^3 & {X_2}^3 & {X_3}^3 & {X_4}^3 \end{bmatrix}$. Δ is known as the Vandermonde determinant and $\Delta \neq 0$ since $X_i \neq X_j$ $(\beta^{i_1} \neq \beta^{i_2})$. $S_1 = S_2 = S_3 = S_4 = 0 \leftrightarrow e_{i_1} = e_{i_2} = e_{i_3} = e_{i_4} = 0 \leftrightarrow$ any error with multiplicity at most 4 produces a non-zero syndrome, which means the distance of the code is 5.