EC500

Design of Secure and Reliable Hardware

Lecture 13

Mark Karpovsky

1 Reed Solomon (RS) Codes

(Non-binary (q-ary) BCH codes)

Let $q = p^s$, where p is prime. Consider the field $GF(p^s)$ generated by a polynomial $p(x) = \sum_{j=0}^{s} c_j x^j$, $c_j \in \{0,1,\cdots,p-1\}$ and $c_s = 1$. $p(x)$ is primitive and $\deg p(x) = s$. Let $\alpha \in GF(p^s)$ be primitive in $GF(p^s)$, where $\alpha^t \neq \alpha^\gamma$ for $t \neq \gamma$ and $t, \gamma = 0,1,\cdots,p^s - 2$.

RS codes are q-ary codes with the following parameters:

length $n = q - 1 = p^s - 1$

number of information digits $k = n - d + 1$

redundant digits $r = d - 1$

where d is the distance.

For these codes, $H = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{d-2} & \alpha^{2(d-2)} & \alpha^{3(d-2)} & \cdots & \alpha^{(d-2)(n-1)} \end{bmatrix}_{(d-1)\times(q-1)}$ **(*)**.

Example

$q = 11$ ($p = 11$, $s = 1$)

$GF(11) = \{0,1,2,3,4,5,6,7,8,9,10\}$

Take $\alpha = 2$ and construct the field

t	0	1	2	3	4	5	6	7	8	9
2^t	1	2	4	8	5	10	9	7	3	6

Thus 2 is primitive in $GF(11)$. We have for a check matrix of a single-error correcting RS code over $GF(11) \to H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \end{bmatrix}$. This is a $(10, 11^8, 3)$ RS code over $GF(11)$.

A codeword $v = (v_0, v_1, \cdots, v_9) \in V(RS) \leftrightarrow Hv = 0 \leftrightarrow \begin{cases} v_0 + v_1 + v_2 + \cdots + v_9 = 0 \\ v_0 + 2v_1 + 2^2 v_2 + \cdots + 2^9 v_9 = 0 \end{cases} \bmod 11$. Let $v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_9 x^9$, then $v \in V \leftrightarrow \begin{cases} v(1) = 0 \\ v(2) = 0 \end{cases}$.

For the general case of RS codes with $n = q - 1$, $k = n - d + 1$ with H defined by **(*)**. $v \in V \leftrightarrow v(1) = v(\alpha) = v(\alpha^2) = v(\alpha^3) = \cdots = v(\alpha^{d-2}) = 0$. Thus if $v \in v$ and $w(x) = v(x)\mathrm{a}(x) \to w \in V$ for any $\mathrm{a}(x) \to$ RS codes are cyclic codes (since cyclic shift is equivalent to multiplication by x or x^{-1} depending on the direction of the shift).

Example

$p = 2,\ s = 3$

RS codes of length $n = q - 1 = p^s - 1 = 7$ over $GF(2^3)$ and $d = 3$

Construct the field using $p(x) = x^3 + x + 1$

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

Take $\alpha = (010)$, then for a $(7, 8^5, 3)$ RS code, we have $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}$. $v \in V \leftrightarrow \begin{cases} v(1) = 0 \\ v(\alpha) = 0 \end{cases}$.

Let us prove that this code has distance $3 \leftrightarrow$ able to detect double errors. Suppose we have a double error $e = (0, \cdots, 0, e_i, 0, \cdots, 0, e_j, 0, \cdots, 0)$ where $e_i, e_j \in GF(2^3)$ and $e_i, e_j \neq (000)$. Then e is masked iff $He = 0 \leftrightarrow \begin{cases} e_i + e_j = 0 \\ e_i\alpha^i + e_j\alpha^j = 0 \end{cases} \leftrightarrow \begin{vmatrix} 1 & 1 \\ \alpha^i & \alpha^j \end{vmatrix} = 0$. But, $\begin{vmatrix} 1 & 1 \\ \alpha^i & \alpha^j \end{vmatrix} = \alpha^j - \alpha^i \neq 0$.

Q.E.D.

For the general case when H is defined by **(*)**, $\|e\| = d - 1$, $e_i \neq 0$ for $i = i_1, i_2, \cdots i_{d-1}$, $He = 0 \leftrightarrow$

$$\begin{cases} e_{i_1} + e_{i_2} + e_{i_3} + \cdots + e_{i_{d-1}} = 0 \\ e_{i_1}\alpha^{i_1} + e_{i_2}\alpha^{i_2} + \cdots + e_{i_{d-1}}\alpha^{i_{d-1}} = 0 \\ e_{i_1}\alpha^{2i_1} + e_{i_2}\alpha^{2i_2} + \cdots + e_{i_{d-1}}\alpha^{2i_{d-1}} = 0 \\ \vdots \\ e_{i_1}\alpha^{(d-2)i_1} + e_{i_2}\alpha^{(d-2)i_2} + \cdots + e_{i_{d-1}}\alpha^{(d-2)i_{d-1}} = 0 \end{cases} \quad (**).$$

Consider the determinant $\Delta = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{d-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \cdots & \alpha^{2i_{d-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{(d-2)i_1} & \alpha^{(d-2)i_2} & \cdots & \alpha^{(d-2)i_{d-1}} \end{vmatrix} = 0$. Δ is known as the Vandermonde determinant and $\Delta \neq 0 \leftrightarrow \Delta = \prod_{s \neq t}(\alpha^{i_s} - \alpha^{i_t})$. Thus **(**)** does <u>not</u> have a non-zero solution.

Q.E.D.

2 Single Error Correcting RS Codes

$(q-1, q^{q-3}, 3)$, $q = p^s$

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

Let $e = (0, \cdots, 0, e_i, 0, \cdots, 0)$, then $S = \begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = He = \begin{bmatrix} e_i \\ \alpha^i e_i \end{bmatrix}$. $S_1 = e_i$, $S_2 = \alpha^i e_i$, thus $\alpha^i = S_2 \cdot {S_1}^{-1}$ = the error location and $e_i = S_1$ = the magnitude of the error.

3 Extended RS Codes Over $GF(q)$

RS codes $(q-1, q^{q-d}, d)$ defined by **(*)** can be extended to $(q+1, q^{q-d+2}, d)$ codes by adding to H two columns $\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$. However, extended codes are <u>not</u> cyclic.

Theorem.

RS codes are optimal and have max k

Proof.

First, we note that for any code, $d \leq n-k+1 = r+1$ **(***)**. Since every code contains vector $v = (1,0,\cdots,0,v_{x+1},\cdots,v_{x+r})$ and $d(v,0) \leq r+1$. **(***)** is known as the **Singleton bound**. For RS codes and for extended RS codes, $d = r+1 = n-k+1$.

Q.E.D.

4 Binary Coded RS Codes (Over $GF(2^s)$) to Detect Burst Errors

Consider $(q+1, q^{q-d+2}, d)$ extended RS code V over $GF(2^s)$ with $q = 2^s$. Let $v = (v_0, v_1, \cdots, v_{n-1}) \in V$, $n = q+1$, $v_i \in GF(2^s)$. Let us substitute for every v_i its binary equivalent <u>BRS</u>, then we have a binary coded RS code of length $n \cdot s = (q+1) \cdot s = (2^s+1)s$ with a number of codewords as in the original RS code, i.e. $q^{q-d+2} = (2^s)^{(2^s-d+2)} = 2^{s(2^s-d+2)}$. This BRS code detects all binary bursts of length at most $(d-2)s+1$. Note that BRS is <u>not</u> cyclic.

<u>Example</u>

$p = 2$, $s = 3$, $d = 4 \rightarrow$ For extended RS code: $n = p^s + 1 = 9$, $r = 3$, $k = 6$, $d = 4$, $q = 8$.
$|V| = 8^6 = 2^{18}$

For BRS, $n = 9 \cdot 3 = 27$, $|V| = 2^{18} \rightarrow k = 18$. All bursts of length at most 7 are detected (since these bursts distort at most 3 bytes over 8-ary digits in the original RS code).