REED SOLOMON (RS) CODES

(NONBINARY (q-ary) BCH codes)

Let $q = p^{s}$ where p is prime

CONSIDER FIELD Z_p^s generated by a polynomial $P(x) = \sum_{j=0}^{s} c_j x^j$

$c_j \in \{0, 1, \dots, p-1\}$ $\quad c_s = 1$.

$P(x)$ is primitive $\quad \deg P(x) = s$

Let $\alpha \in Z_p^s$ is primitive in Z_p^s

$\alpha^t \neq \alpha^r \quad (t \neq r;\ t, r = 0, 1, \dots, p^s - 2)$

RS codes have following parameters:

These are q-ary codes with

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

number of INFORMATION DIGITS:

$$k = n - d + 1 \qquad r = d - 1$$

where d is a distance.

FOR THESE CODES

$$H = \underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \cdots & \alpha^{3(n-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \alpha^{d-2} & \alpha^{2(d-2)} & & \cdots & \alpha^{(d-2)(n-1)} \end{bmatrix}}_{n=q-1} \; r = d-1 \qquad (*)$$

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

$\mathbb{Z}_{11}^1 = \{0,1,2,3,4,5,6,7,8,9,10\}$

Take $\alpha=2$ Then mod 11

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

Thus 2 is primitive in $\mathbb{Z}_{11}$

We have for a check matrix of a single-error correcting RS code over $\mathbb{Z}_{11}$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 & 2^9 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \end{bmatrix} \quad [\text{mod } 11]$$

This is $(10, 11^8, 3)$ RS code over $\mathbb{Z}_{11}$

$v = (v_0, v_1, \dots, v_9) \in V$ - RS code $\Leftrightarrow$

$Hv = 0 \Leftrightarrow$

$$\begin{cases} v_0 + v_1 + v_2 + \dots + v_9 = 0 \\ v_0 + 2v_1 + 4v_2 + \dots + 2^9 v_9 = 0 \end{cases} \mod 11$$

Let $v(x) = v_0 + v_1 x + v_2 x^2 + \dots + v_9 x^9$

Then $v \in V \Longleftrightarrow$

$$\begin{cases} v(1) = 0 \\ v(2) = 0 \end{cases}$$

FOR THE GENERAL CASE OF RS codes WITH $n = q-1$ $k = n-d+1$ with H defined by $(*)$

$v \in V \Longleftrightarrow v(1) = v(\alpha) = v(\alpha^2) = v(\alpha^3) = \dots =$
$= v(\alpha^{d-2}) = 0$

thus:

$v \in V \quad w(x) = v(x)\,a(x) \Rightarrow$

$w \in V$ for any $a(x) \Rightarrow$

RS codes are cyclic codes

(SINCE cyclic shift is equivalent to multiplication by x or x^{-1}) depending on a direction of the shift)

<u>EXAMPLE 2</u> $p=2 \quad s=3$

RS codes of length $n = q-1 = p^3 - 1 = 7$ over $\mathbb{Z}_2^3$ $d=3$

0 0 0	0		
0 0 1	1		
0 1 0	x		
0 1 1	x^3		
1 0 0	x^2	$\mathbb{Z}_2^3$	
1 0 1	x^6		
1 1 0	x^4		
1 1 1	x^5		
x^2 x 1			

$P(x) = x^3 + x + 1$

primitive

$x^3 = x + 1$

$x^4 = x^2 + x$

$x^5 = x^3 + x^2$

$\quad = x^2 + x + 1$

$x^6 = x^2 + x$

$x^7 = 1$

TAKE $\alpha = x = 010$

THEN FOR $(7, 8^5, 3)$ RS code

we have

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{bmatrix}$$

$$v \in V \Longleftrightarrow \begin{cases} v(1) = 0 \\ v(x) = 0 \end{cases}$$

Let us prove that this code has distance 3 $\Leftrightarrow$ detects 2 errors

SUPPOSE we have a double error

$$e = (0 \ldots 0 \overset{i}{e_i} 0 \ldots 0 \overset{j}{e_j} 0 \ldots 0)$$

$$e_i, e_j \in \mathbb{Z}_2^3 - 000$$

Then e is masked $\Leftrightarrow$

$$He = 0$$

$$\Leftrightarrow \begin{cases} e_i + e_j = 0 \\ e_i x^i + e_j x^j = 0 \end{cases} \Leftrightarrow$$

$$\begin{vmatrix} 1 & 1 \\ x^i & x^j \end{vmatrix} = 0$$

but $\begin{vmatrix} 1 & 1 \\ x^i & x^j \end{vmatrix} = x^j - x^i \neq 0.$ Q.E.D.

FOR THE GENERAL CASE

When H is defined by $(*)$

$\|e\| = d-1$

$e_i \neq 0 \quad i = i_1, i_2, \ldots, i_{d-1}$

$$He = 0 \Leftrightarrow (**) \begin{cases} e_{i_1} + e_{i_2} + e_{i_3} + \ldots + e_{i_{d-1}} = 0 \\ e_{i_1}\alpha^{i_1} + e_{i_2}\alpha^{i_2} + \ldots + e_{i_{d-1}}\alpha^{i_{d-1}} = 0 \\ e_{i_1}\alpha^{2i_1} + e_{i_2}\alpha^{2i_2} + \ldots + e_{i_{d-1}}\alpha^{2i_{d-1}} = 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ e_{i_1}\alpha^{(d-2)i_1} + e_{i_2}\alpha^{(d-2)i_2} + \ldots + e_{i_{d-1}}\alpha^{(d-2)i_{d-1}} = 0 \end{cases}$$

CONSIDER the determinant

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{d-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \cdots & \alpha^{2i_{d-1}} \\ \alpha^{3i_1} & \alpha^{3i_2} & \cdots & \alpha^{3i_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-2)i_1} & \alpha^{(d-2)i_2} & \cdots & \alpha^{(d-2)i_{d-1}} \end{vmatrix} = \Delta$$

Δ is known as Van der Mond determinant

$$\Delta \neq 0 \Leftrightarrow \Delta = \prod_{s \neq t} (\alpha^{i_s} - \alpha^{i_t}).$$

Thus (**) does <u>not</u> have a nonzero solution QED.

SINGLE ERROR CORRECTING

RS codes

$$(q-1,\ q^{q-3},\ 3)$$

$$q = p^s$$

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

Let $e = (0 \ldots 0\ \underset{\substack{\uparrow \\ i}}{e_i}\ 0 \ldots 0)$

Then $S = \begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = He = \begin{bmatrix} e_i \\ \alpha^i e_i \end{bmatrix}$

$S_1 = e_i \quad S_2 = \alpha^i e_i$ Thus

$\alpha^i = S_2 \cdot S_1^{-1}$ – error location

$e_i = S_1$ – magnitude of the error

EXTENDED RS codes over $\mathbb{Z}_q$

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

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

extended codes are <u>not</u> cyclic

T: RS codes are optimal

have max K

<u>PROOF.</u> FIRST we note that

for any code

$d \le n-K+1 = r+1$ (***)

Since any code contains vector

$(\underbrace{1\,0 \ldots 0}_{K}\, v_{K+1}, \ldots, v_{K+r}) = v$ and

$d(v, 0) \le r+1$

(***) is known as Singleton bound

FOR RS codes and for extended RS codes $d = r+1 = n-K+1$

QED.

BINARY coded RS codes (over Z_2^S)

DETECTION OF BURST ERRORS

Consider

$(q+1, q^{q-d+2}, d)$ extended

RS code V over Z_2^S with $q=2^S$

Let $v = (v_0, v_1, \dots, v_{n-1}) \in V$

$(n = q+1)$ $\quad v_i \in Z_2^S$

Let us substitute for every v_i

it's binary equivalent BRS

Then we have 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 $(d-2)s+1$

BRS is <u>not</u> cyclic

<u>EXAMPLE 3</u> $p=2$, $s=3$, $d=4$. $\Rightarrow$

FOR RS code:

$n=p^{s}+1=9$, $r=3$, $k=6$, $d=4$, $q=8$

$|V| = 8^{6} = 2^{18}$

FOR BRS

$n = 9\cdot 3 = 27$ $\quad |V| = 2^{18} \Rightarrow k=18$

ALL BURSTS OF LENGTHS AT MOST 7 are detected (SINCE THESE bursts distort at most 3 bytes or 8-ary digits in the originae RS code)