Reed Solomon Codes

Reed Solomon code over $GF(2^m)$

$RS(n,k)$ $\quad n=2^m-1$ $\quad n-k=r$

$n-k=r$ → degree of $g(x)$ → generator polynomial degree

Reed Solomon Codes are non-binary cyclic codes

The generator polynomial of a Reed Solomon code is (t-error correcting)

$$g(x)=(x+\beta)(x+\beta^2)\cdots(x+\beta^{2t})$$

where $\beta \in GF(2^m)$

Ex: $GF(2^4)=\{0,1,\alpha,\alpha^2,\alpha^3,\ldots\alpha^{14}\}$

Let $\beta=\alpha$

The generator polynomial of double-error ($t=2$) correcting Reed-Solomon code over $GF(2^4)$ is

$$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$$

The code blocklength $n=2^4-1 \rightarrow n=15$

$r=4 \rightarrow$ degree of $g(x)$ $\quad k=n-r$ $\quad k=11$

(149) Hence we have RS(15,11) block code whose generator polynomial is

$$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$$

which can be expanded as

$$g(x) = x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}$$

Ex°: Construct RS(7,k) → n, t=1 → single error correcting code

Sln:

$GF(2^m)$ $m=3$ $n=2^m-1$ $n=7$

$\alpha \in GF(2^m)$

$g(x)=(x+\alpha)(x+\alpha^2)$

$= x^2 + \alpha^2 x + \alpha x + \alpha^3$

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

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

α^3

$= x^2 + \alpha^4 x + \alpha^3$ → $g(x)= x^2+\alpha^4 x+\alpha^3$

Let $p(x)=x^3+x+1$

$\alpha^3=\alpha+1$

$r=2 \rightarrow k=n-r \rightarrow k=7-2=5$

RS(7,5) code

(150)

Ex 3 $g(x) = x^2 + \alpha^4 x + \alpha^3$ $\quad \alpha^3 = \alpha + 1$

Encode $d = (1\ 0\ \alpha\ \alpha^5\ \alpha^2)$ using systematic & non-systematic approach

Sln:

RS(7,5) code

$c(x) = d(x)\, g(x) \qquad d(x) = x^4 + \alpha x^2 + \alpha^5 x + \alpha^2$

$$c(x) = (x^4 + \alpha x^2 + \alpha^5 x + \alpha^2)(x^2 + \alpha^4 x + \alpha^3)$$

$$= x^6 + \alpha^4 x^5 + \alpha^3 x^4 + \alpha x^4 + \alpha^5 x^3 + \alpha^4 x^2 + \alpha^5 x^3 + \alpha^9 x^2 + \alpha^8 x + \alpha^2 x^2 + \alpha^6 x + \alpha^5$$

$$= x^6 + \alpha^4 x^5 + (\alpha^3 + \alpha) x^4 + (\alpha^5 + \alpha^5) x^3 + (\alpha^4 + \alpha^3 + \alpha^2) x^2 + (\alpha^8 + \alpha^6) x + \alpha^5$$

The above encoding is non-systematic

Systematic encoding

$$x^2 \cdot d(x) \longrightarrow x^2 d(x) = x^6 + \alpha x^4 + \alpha^5 x^3 + \alpha^2 x^2$$

Divide $x^2 d(x)$ by $g(x)$ and keep the remainder

$$\begin{array}{r} x^4 + \alpha^4 x^3 + \alpha^3 x^2 + \alpha^5 x + \alpha^6 \\ x^2 + \alpha^4 x + \alpha^3 \;\big|\; x^6 + \alpha x^4 + \alpha^5 x^3 + \alpha^2 x^2 \\ -x^6 + \alpha^4 x^5 + \alpha^3 x^4 \\ \hline \alpha^4 x^5 + x^4 + \alpha^5 x^3 + \alpha^2 x^2 \\ \alpha^4 x^5 + \alpha x^4 + x^3 \\ \hline \alpha^3 x^4 + \alpha^4 x^3 + \alpha^2 x^2 \\ \alpha^3 x^4 + x^3 + \alpha^6 x^2 \\ \hline \alpha^5 x^3 + x^2 \end{array}$$

$$\begin{array}{r} \downarrow \\ -\alpha^5 x^3 + \alpha^2 x^2 + \alpha x \\ \hline \alpha^6 x^2 + \alpha x \\ \alpha^6 x^2 + \alpha^3 x + \alpha^2 \\ = \hline x + \alpha^2 \end{array}$$

151

$r(x) = x + \alpha^2$ → remainder

$c(x) = x^2 d(x) + r(x)$

$c(x) = x^6 + \alpha x^4 + \alpha^5 x^3 + \alpha^2 x^2 + x + \alpha^2$

which gives the codeword

$$c = (1\ 0\ \alpha\ \alpha^5\ \alpha^2\ 1\ \alpha^2)$$

$1 \rightarrow 001$
$0 \rightarrow 000$
$\alpha \rightarrow 010$
$\alpha^5 \rightarrow 111$
$\alpha^2 \rightarrow 100$

$GF(2^3)$ is used
$m = 3$

$\alpha^3 = \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha + 1$

α^i → represented by m-bits
$m = 3$
$GF(2^m)$ is used

$d = (1\ 0\ \alpha\ \alpha^5\ \alpha^2)$

$d = (001\ 000\ 010\ 111\ 100)$

$c = (1\ 0\ \alpha\ \alpha^5\ \alpha^2\ 1\ \alpha^2)$

$c = (001\ 000\ 010\ 111\ 100\ 001\ 100)$

Exercise: Construct RS(15, 13) over $GF(2^4)$

$t = 1$ → single error correcting code

Encode $d = (0\ 0\ \alpha\ 001\ \alpha^7\ \alpha^2\ 0\ 0\ 1\ \alpha\ \alpha^2)$

where α is a primitive element of $GF(2^4)$

(systematic encoding)

Decoding of RS codes

In binary code an error pattern of t errors can be represented by the error polynomial

$$e(x) = x^{p_1} + x^{p_2} + \cdots + x^{p_t}$$

where $p_1, p_2, \ldots p_t$ are the error positions.

For RS codes error pattern is

$$e(x) = y_{p_1} x^{p_1} + y_{p_2} x^{p_2} + \cdots y_{p_t} x^{p_t}$$

where y_{p_i} is the error magnitude at the position p_i.

Remarks: $c(x) = \cdots \alpha^5 x^4 + \alpha^2 x^3 + \cdots$

(α^5: codeword, x^4: magnitude, x^3: magnitude)

- Decoding Reed-Solomon codes is achieved by first determining the error positions and then error magnitudes.
- The methods used for locating errors in binary codes can be used in Reed-Solomon codes, the only additional method is for finding the error magnitudes.

Syndrome Decoding of RS codes

$$e(x) = y_{p_1} x^{p_1} + y_{p_2} x^{p_2} + \cdots y_{p_t} x^{p_t}$$

$$r(x) = c(x) + e(x)$$

$S_i = r(\alpha^i)$ → syndrome.

$S_i = r(\alpha^i) = e(\alpha^i)$ $\quad c(\alpha^i) = 0$

So giving

$$S_1 = y_{p_1} \alpha^{p_1} + y_{p_2} \alpha^{p_2} + \cdots + y_{p_t} \alpha^{p_t}$$

$$S_2 = y_{p_1} \alpha^{2p_1} + y_{p_2} \alpha^{2p_2} + \cdots + y_{p_t} \alpha^{2p_t}$$

$$\vdots$$

$$S_{2t} = y_{p_1} \alpha^{2tp_1} + y_{p_2} \alpha^{2tp_2} + \cdots + y_{p_t} \alpha^{2tp_t}$$

Let $X_i = \alpha^{p_i}$ and $y_i = y_{p_i}$

$$S_1 = y_1 X_1 + y_2 X_2 + \cdots + y_t X_t$$

$$S_2 = y_1 X_1^2 + y_2 X_2^2 + \cdots + y_t X_t^2$$

$$\vdots$$

$$S_{2t} = y_1 X_1^{2t} + y_2 X_2^{2t} + \cdots + y_t X_t^{2t}$$

For non-binary RS code $S_2 \neq S_1^2$

or in general $S_{2i} \neq S_i^2$

Ex 3 Let $t=2$

Syndrome eqn becomes as

$$\left.\begin{aligned} S_1 &= Y_1 X_1 \\ S_2 &= Y_1 X_1^2 \end{aligned}\right\} \rightarrow \text{solve for } X_1 \text{ \& } Y_2$$

$$\frac{S_1}{S_2} = \frac{X_1}{X_1^2} \longrightarrow X_1 = \frac{S_2}{S_2}$$

$$S_1 = Y_1 X_2 \rightarrow Y_1 = \frac{S_1}{X_2} \rightarrow Y_1 = \frac{S_1}{S_2/S_1}$$

$$Y_1 = \frac{S_1^2}{S_2}$$

$S_1 = r(\alpha)$

$S_2 = r(\alpha^2)$

$r(x)$ → received word polynomial.

Ex 5 $t=2$ $RS(7,5)$ $r = (0\ 1\ \alpha^5\ \alpha^2\ 1\ \alpha^6\ \alpha^3)$

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

Decode r

Soln $r(x) = x^5 + \alpha^5 x^4 + \alpha^2 x^3 + x^2 + \alpha^6 + \alpha^3$

155

$S_1 = r(\alpha) \rightarrow S_1 = \alpha^5 + \alpha^5\alpha^4 + \alpha^2\alpha^3 + \alpha^2 + \alpha^6 + \alpha^3$

$= \alpha$ use $\alpha^3 = \alpha + 1$

$S_2 = r(\alpha^2) \longrightarrow S_2 = \alpha^3$

$S_1 = y_1 X_1 \longrightarrow \alpha = y_1 X_1$

$S_2 = y_2 X_1^2 \longrightarrow \alpha^3 = y_2 X_1^2$ $\Big\} \rightarrow X_1 = \alpha^{(2)}$ ← p_2

$\alpha = y_1 \cdot \alpha^2$

$\rightarrow y_1 = \frac{1}{\alpha}$

$y_1 = \frac{\alpha^7}{\alpha}$

$= \alpha^6$ ← y_{p_1}

$e(x) = y_{p_1} x^{p_1} + y_{p_2} x^{p_2}$ ($p_1 = 0$, $p_2 = 0$)

single error

$e(x) = \alpha^6 x^2$

$c(x) = r(x) + e(x)$

$= x^5 + \alpha^5 x^4 + \alpha^2 x^3 + \alpha^2 x^2 + \alpha^6 x + \alpha^3$

$c = (0\ 1\ \alpha^5\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^6\ \alpha^3)$

PGZ algorithm can be used in decoding of RS codes:

Consider syndrome equations and let

$S = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ \vdots \\ S_{2t} \end{bmatrix}$ $\quad y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{bmatrix}$

and the matrix X as

$$X = \begin{bmatrix} X_1 & X_2 & \cdots & X_t \\ X_1^2 & X_2^2 & \cdots & X_t^2 \\ \vdots & & & \\ X_1^t & X_2^t & \cdots & X_t^t \end{bmatrix}$$

then $S = Xy$

The matrix X & column vector S are known terms, and so y can be found by inverting

$S = Xy$ to give $y = X^{-1}S$

Therefore the error magnitudes are given by

$$y = X^{-1}S$$

Summary (Decoding RS codes)

1) Find the number of errors t and error location numbers $X_1, X_2, \ldots X_t$ by using any technique suitable to binary BCH codes

2) From the error-location numbers construct the matrix X and determine its inverse X^{-1}

3) The error magnitudes $Y_1, Y_2, \ldots Y_t$ are then given by $y = X^{-1}S$ where S is the column vector constructed from error syndromes $S_1, S_2 \ldots S_t$

Examples

RS(15, 9) code.

triple error correcting code

$t = 3$

$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$

$r = 6 \quad k = n - r \rightarrow k = 15 - 6 = 9$ //

Assume that $c(x)$ is a codeword polynomial for RS(15, 9) code

$$r(x) = \alpha^3 x^{12} + x^8 + \alpha^{10} x^7 + \alpha^2 x^5 + \alpha^8 x^4 + \alpha^{14} x^3 + \alpha^5$$

is the received word polynomial incurring 3 errors.

Decode $r(x)$

Sln:

$GF(2^4) \rightarrow p(x) = x^4 + x + 1 \rightarrow \alpha^4 = \alpha + 1 \quad \alpha^{15} = 1$

$\overline{S} = \overline{x}\,\overline{y}$

The error syndromes are

$S_1 = r(\alpha) = \alpha^{15} + \alpha^8 + \alpha^{13} + \alpha^7 + \alpha^{12} + \alpha^{11} + \alpha^6 = \alpha^6$

$S_2 = r(\alpha^2) = 0$

$S_3 = r(\alpha^3) = \alpha^{14}$

$S_4 = r(\alpha^4) = \alpha^{11}$

$S_5 = r(\alpha^5) = \alpha^{14}$

$S_6 = r(\alpha^6) = \alpha^9$

$$S_1 = y_1 X_1 + y_2 X_2 + y_3 X_3$$
$$S_2 = y_1 X_1^2 + y_2 X_2^2 + y_3 X_3^2$$
$$S_3 = y_1 X_1^3 + y_2 X_2^3 + y_3 X_3^3$$
$$S_4 = y_1 X_1^4 + y_2 X_2^4 + y_3 X_3^4$$
$$S_5 = y_1 X_1^5 + y_2 X_2^5 + y_3 X_3^5$$
$$S_6 = y_1 X_1^6 + y_2 X_2^6 + y_3 X_3^6$$

↓ known

to find X_i's use PGZ algorithm

once X_i's are found using $S = XY$

$\rightarrow Y = X^{-1} S$

find y_i's

(At decoder side)

Assume that the maximum number of correctable errors 3, occurred.

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^6 & 0 & \alpha^{14} \\ 0 & \alpha^{14} & \alpha^{11} \\ \alpha^{14} & \alpha^{11} & \alpha^{14} \end{bmatrix}$$

$$\det(M) = \alpha^6 \begin{vmatrix} \alpha^{14} & \alpha^{11} \\ \alpha^{11} & \alpha^{14} \end{vmatrix} + 0 \begin{vmatrix} 0 & \alpha^{11} \\ \alpha^{14} & \alpha^{14} \end{vmatrix} + \alpha^{14} \begin{vmatrix} 0 & \alpha^{14} \\ \alpha^{14} & \alpha^{11} \end{vmatrix}$$

$$= 1$$

$\det(M) \neq 0$ and so the decoder assumes that 3 errors have occurred (which we know is correct)

The inverse of M is

$$M^{-1} = \frac{adj(M)}{det(M)} = \begin{bmatrix} \alpha^5 & \alpha^{10} & \alpha^{13} \\ \alpha^{10} & \alpha^7 & \alpha^2 \\ \alpha^{13} & \alpha^2 & \alpha^5 \end{bmatrix}$$

The coefficients of the error location polynomial are given by

$$\begin{bmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^5 & \alpha^{10} & \alpha^{13} \\ \alpha^{10} & \alpha^7 & \alpha^2 \\ \alpha^{13} & \alpha^2 & \alpha^5 \end{bmatrix} \begin{bmatrix} \alpha^{11} \\ \alpha^{13} \\ \alpha^9 \end{bmatrix} = \begin{bmatrix} \alpha^{16}+\alpha^{24}+\alpha^{22} \\ \alpha^{21}+\alpha^{21}+\alpha^{11} \\ \alpha^{21}+\alpha^{16}+\alpha^{14} \end{bmatrix} = \begin{bmatrix} \alpha^4 \\ \alpha^{11} \\ 1 \end{bmatrix}$$

$$\sigma = M^{-1} \cdot S$$

So $\sigma_1 = 1 \quad \sigma_2 = \alpha^{11} \quad \sigma_3 = \alpha^4$

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3$$
$$= 1 + x + \alpha^{11} x^2 + \alpha^4 x^3$$

The roots of $\sigma(x)$ are found using trial approach of $x = \alpha^3, \alpha^8, \alpha^{14}$. The reciprocal of the roots gives the error-location numbers $X_1 = \alpha^{12}$, $X_2 = \alpha^5$, and $X_3 = \alpha$ respectively

160

To find the error magnitudes we construct

$$X = \begin{bmatrix} X_1 & X_2 & X_3 \\ X_1^2 & X_2^2 & X_3^2 \\ X_1^3 & X_2^2 & X_3^3 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^6 & \alpha \\ \alpha^3 & \alpha^{12} & \alpha^2 \\ \alpha^6 & \alpha^3 & \alpha^3 \end{bmatrix}$$

$$\det(X) = \alpha^2 \qquad X^{-1} = \begin{bmatrix} \alpha^8 & \alpha^{12} & \alpha \\ \alpha^7 & \alpha^7 & \alpha^3 \\ \alpha^8 & \alpha^3 & \alpha^5 \end{bmatrix}$$

Using $y = X^{-1} S$

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} \alpha^8 & \alpha^{12} & \alpha \\ \alpha^7 & \alpha^7 & \alpha^3 \\ \alpha^8 & \alpha^3 & \alpha^5 \end{bmatrix} \begin{bmatrix} \alpha^6 \\ 0 \\ \alpha^{14} \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^{14} + \alpha^{15} \\ \alpha^{13} + \alpha^{23} \\ \alpha^{14} + \alpha^{13} \end{bmatrix} = \begin{bmatrix} \alpha^3 \\ \alpha^3 \\ \alpha^9 \end{bmatrix}$$

$y_1 = \alpha^3$ $y_2 = \alpha^3$ and $y_3 = \alpha^9$

The error location numbers $X_1 = \alpha^{12}$, $X_2 = \alpha^6$, and $X_3 = \alpha$ correspond to errors in positions x^{12}, x^6 and x respectively, the error pattern is therefore $e(x) = \alpha^3 x^{12} + \alpha^3 x^6 + \alpha^9 x$

decoder output is $c(x) = r(x) + e(x)$

$$c(x) = x^8 + \alpha^{10} x^7 + \alpha^3 x^6 + \alpha^2 x^5 + \alpha^8 x^4 + \alpha^{14} x^3 + \alpha^9 x + \alpha^6$$

(161) Exercise

RS(15,9) Code over GF(2^4)

$t=3$ → triple error correcting code

$r(x)$ → received word polynomial

$r(x) = x^{10} + \alpha^3 x^8 + \alpha^{11} x^7 + \alpha^8 x^6 + \alpha^6 x^5 + \alpha^4 x^4 + \alpha^5 x^2 + \alpha^9 x + \alpha^6$

Decode $r(x)$. (i.e, find $e(x)$ that calculate $c(x) = r(x) + e(x)$)

Sln: $p(x) = x^4 + x + 1$

Follow the same steps as in the previous example

answer is $e(x) = x^{10} + \alpha^4 x^7 + \alpha^6 x^3$

The Berlekamp Algorithm

The Berlekamp Algorithm:

- PGZ algorithm is used to find error locations for BCH and RS codes. However PGZ algorithm involves matrix inversion which requires excessive computation, especially for large matrices.
- In particular for non-binary codes for which a second matrix inversion is required to obtain the error magnitudes.

For these reasons PGZ is quite inefficient

The Berlekamp algorithm is a fast and efficient algorithm to find the error location polynomial. The algorithm uses an iterative technique to find an error location polynomial whose coefficients satisfy the Newton's identities given below

$$\begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_t \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ S_1 & 2 & \cdots & 0 \\ S_2 & S_1 & 3 & \cdots & 0 \\ \vdots & & & & \\ S_{t-1} & \cdots & S_1 & t \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

and

$$\begin{bmatrix} S_{p+1} \\ S_{t+2} \\ \vdots \\ S_{2t} \end{bmatrix} = \begin{bmatrix} S_t & S_{t-1} & \cdots & S_1 \\ S_{t+1} & \cdots & & S_2 \\ \vdots & & & \\ S_{2t-1} & \cdots & \cdots & S_t \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

In Berlekamp algorithm we first compute $\sigma^{(1)}(x)$, then $\sigma^{(2)}(x)$, then $\sigma^{(3)}(x)$ .... upto $\sigma^{(2t)}(x)$ which is the final polynomial and it is the error location polynomial

i.e, $\sigma(x) = \sigma^{(2t)}(x)$

let $\sigma^{(i)}(x)$ be the polynomial for the i^{th} iteration

$$\sigma^{(i)}(x) = 1 + \sigma_1^{(i)}(x) + \sigma_2^{(i)} x^2 + \cdots + \sigma_{r_i}^{(i)} x^{r_i}$$

r_i is the degree of $\sigma^{(i)}(x)$

To test whether the coefficients satisfy the Newtons equations, test

$$\hat{S}_{i+1} = \sigma_1^{(i)} S_i + \sigma_2^{(i)} S_{i-1} + \cdots + \sigma_{r_i}^{(i)} S_{i+1-r_i}$$

which is the estimated $(i+1)$th syndrome,

Adding $\hat{S}_{i+1}$ to the correct syndrome S_{i+1} gives $d_i = S_{i+1} + \hat{S}_{i+1}$ where d_i is known as the ith discrepancy (baskalilik, fark)

if $d_i = 0$ then

$$\sigma^{(i+1)}(x) = \sigma^{(i)}(x)$$

$r_{i+1} = r_i$ → degree of $\sigma^{(i)}(x)$

↓

degree of $\sigma^{(i+1)}(x)$

if $d_i \neq 0$ then

$$\sigma^{(i+1)}(x) = \sigma^{(i)}(x) + \left(\frac{x^i d_i}{x^k d_k}\right)\sigma^{k}(x)$$

where $d_i = S_{i+1} + \hat{S}_{i+1}$

and $\sigma^k(x)$ is one of the previous polynomials

r_k → degree of $\sigma^{(k)}(x)$

and $\sigma^k(x)$ is selected such that

$n_k = k - r_k$ has the largest value

↓ same k

$d_k = S_{k+1} + \hat{S}_{k+1}$

In equation $\sigma^{(i+1)}(x) = \sigma^{(i)}(x) + \left(\frac{x^i d_i}{x^k d_k}\right)\sigma^{k}(x)$

Correction term whose degree is $i - k + r_k = i - n_k$

So the degree of $\sigma^{(i+1)}(x)$

it $r_{i+1} = \max(i - n_k, r_i)$

Once $\sigma^{(i+1)}(x)$ and r_{i+1} are found, the coefficients of $\sigma^{(i+1)}(x)$ are used to estimate the next error syndrome

$$\hat{S}_{i+2} = \sigma_1^{(i+2)} S_{i+1} + \sigma_2^{(i+1)} S_i + \cdots + \sigma_{r_{i+1}}^{(i+1)} S_{i+2-r_{i+1}}$$

along with the discrepancy

$$d_{i+1} = S_{i+2} + \hat{S}_{i+2}$$

A note of d_{i+2} is made in a table, along with the value of $\Lambda_{i+1} = (i+1) - r_{i+2}$

The initial conditions for Berlekamp algorithm is chosen as in the following table

Initial conditions for Berlekamp Algorithm

i	$\sigma^{(i)}(x)$	r_i	Λ_i	d_i
-1	1	0	-1	1
0	1	0	0	S_1

Summary of Berlekamp Algorithm

Given initial conditions of in the previous table

$i = 0, 2 \ldots 2t$ $\quad$ t = error correction capability of the code

Step 1 Assume that $\sigma^{(i)}(x)$ and d_i are known then at the $(i+1)$th iteration

If $d_i = 0$

Take $\sigma^{(i)}(x)$ as the next polynomial, and so $\sigma^{(i+1)}(x) = \sigma^{(i)}(x)$

$$r_{i+1} = r_i$$

Go to Step 3

Step 2 If $d_i \neq 0$

Find a previous polynomial $\sigma^{(k)}(x)$ such that $n_k = k - r_k$ has the largest value and $d_k \neq 0$. Then

$$\sigma^{(i+1)}(x) = \sigma^{(i)}(x) + \left(\frac{x^i d_i}{x^k d_k}\right)\sigma^{k}(x)$$

$$r_{i+1} = \text{degree of } \left(\sigma^{(i+1)}(x)\right)$$

Step3

The polynomial $\sigma^{(i+1)}(x)$ is checked to see if its coefficients are consistent with the next Newton's equations, so determine

$$\hat{S}_{i+2} = \sigma_1^{(i+1)} S_{i+1} + \sigma_2^{(i+1)} S_i + \cdots + \sigma_{r_{i+1}}^{(i+1)} S_{i+2-r_{i+1}}$$

$$d_{i+1} = S_{i+2} + \hat{S}_{i+2}$$

and $\quad n_{i+1} = i+1 - r_{i+1}$

Make a note of $\sigma^{(i+1)}(x)$, r_{i+1}, n_{i+1}, d_{i+1}

and goto step4 such that repeat iterations until $\sigma^{(2t)}(x)$ is obtained.

Once $\sigma^{(2t)}(x)$ is obtained find the reprocal of the roots of $\sigma^{(2t)}(x)$ and determine the error pattern polynomial

Example: BCH(15,5) code over $GF(2^4)$

is a three error correcting code. $p(x) = x^4 + x + 1$

$\alpha \in GF(2^4)$. The syndromes for the received word $r(x) = x^3 + x^{10} + x^8 + x^2 + x + 1$

are given by $(S_i = r(\alpha^i))$

(168) $S_1 = \alpha^{12}$, $S_2 = \alpha^{9}$, $S_3 = \alpha^{10}$, $S_4 = \alpha^{3}$, $S_5 = \alpha^{5}$, $S_6 = \alpha^{5}$

Find the error location polynomial $\sigma(x)$ using Berlekamp algorithm.

Sln: The initial conditions for the Berlekamp algorithm is as follows

i	$\sigma^{(i)}(x)$	r_i	n_i	d_i
-1	1	0	-1	1
0	1	0	0	S_1

$S_1 = \alpha^{12}$

$i=0$ $\quad d_0 = S_1 \quad \sigma^{(0)}(x) = 1 \quad r_0 = 0$

Since $d_0 = S_1 \neq 0$

$$\sigma^{(1)}(x) = \sigma^{(0)}(x) + \left(\frac{x^0 d_0}{x^k d_k}\right)\sigma^{k}(x)$$

$\sigma^{k}(x)$ is a polynomial such that $n_k = k - r_k$ is largest $\quad k<0$ ↓ previous polynomials

there is only one polynomial which is $\sigma^{(-1)}(x) = 1$ $\quad d_{-1} = 1$ → from initial table

So $\sigma^{(1)}(x) = \underbrace{\sigma^{(0)}(x)}_{=1} + \frac{1 \cdot S_1}{x^{-1} \cdot 1} \cdot 1$

$\sigma^{(1)}(x) = 1 + xS_1 \longrightarrow \boxed{\sigma^{(1)}(x) = 1 + \alpha^{12}x}$

168

$$\sigma^{(1)}(x) = 1 + \alpha^{12} x$$

For $\sigma^{(1)}(x)$ calculate r_1, n_2, and d_1 values

r_1 = degree of $\sigma^{(1)}(x) \longrightarrow r_1 = 1$

Since $n_i = i - r_i \longrightarrow n_1 = 1 - r_2$

$n_1 = 1 - 1$

$= 0$

$d_1 = S_2 + \hat{S}_2$

α^9 ← we will calculate it using $\sigma^{(1)}(x)$

$$\sigma^{(1)}(x) = 1 + \alpha^{12} x$$

$$\hat{S}_2 = \alpha^{12} S_1 \longrightarrow \hat{S}_2 = \sigma_1^{(1)} S_1$$

$$= \alpha^{12} \alpha^{12}$$

$$= \alpha^9$$

then $d_1 = \alpha^9 + \alpha^9$

$= 0$

So, $r_1 = 1$, $n_1 = 0$, $d_1 = 0$, $\sigma^{(1)}(x) = 1 + \alpha^{12} x$

Now $i = 1$ Since $d_1 = 0$

$\sigma^{(2)}(x) = \sigma^{(1)}(x)$

$\sigma^{(2)}(x) = 1 + \alpha^{12} x$ $r_2 = 1$ → degree of $\sigma^{(2)}(x)$

170

$n_2 = 2 - r_2 \longrightarrow n_2 = 2 - 1 \longrightarrow n_2 = 1$

$d_2 = S_3 + \tilde{S}_3$

$S_3 \rightarrow \alpha^{10}$; $\tilde{S}_3$ will be computed

$\tilde{S}_3 = \sigma_1^{(2)} S_2 + \sigma_2^{(2)} S_1$

Remark: if $\sigma^{(i)}(x) = 1 + \sigma_1^{(i)}(x) + \sigma_2^{(i)} x^2 + \cdots \sigma_{r_i}^{(i)} x^{r_i}$

then $\tilde{S}_{i+1} = \sigma_1^{(i)} S_i + \sigma_2^{(i)} S_{i-1} + \cdots + \sigma_{r_i}^{(i)} S_{i+1-r_i}$

So $\tilde{S}_3 = \sigma_1^{(2)} S_2 + \sigma_2^{(2)} S_1$

$\sigma_1^{(2)} \rightarrow \alpha^{12}$; $S_2 \rightarrow \alpha^9$; $\sigma_2^{(2)} \rightarrow 0$

$= \alpha^{12} \alpha^9$

$= \alpha^6$ $\qquad \alpha^{15} = 1$

Then $d_2 = S_3 + \tilde{S}_3$

$= \alpha^{10} + \alpha^6$ $\qquad \alpha^{i+1} = \alpha \cdot \alpha^i$

$= \alpha^7$

$\underline{\underline{l = 2}}$

Since $d_2 = \alpha^7 \neq 0$

$\sigma^{(3)}(x) = \sigma^{(2)}(x) + \left(\frac{x^2 d_2}{x^k d_k} \right) \sigma^{(k)}(x)$

171

$$\sigma^{(3)}(x) = \sigma^{(2)}(x) + \left(\frac{x^2 \, d_2}{x^k \, d_k}\right) \sigma^{(k)}(x) \qquad k<2$$

$d_2 \to \alpha^7$

Choose $\sigma^{(k)}(x)$ such that $n_k = k - r_k$ is maximum

$k=1 \quad n_1=0 \quad d_1=0$ → makes denominator 0

$k=0 \quad n_0=0 \quad d_0=\alpha^{12}$

So choose $k=0 \; n_0=0 \; d_0=\alpha^{12}$

$$\sigma^{(3)}(x) = \sigma^{(2)}(x) + \frac{x^2 \cdot \alpha^7}{x^0 \cdot \alpha^{12}} \underbrace{\sigma^{(0)}(x)}_{=1}$$

$$\sigma^{(3)}(x) = \sigma^{(2)}(x) + x^2 \alpha^{-5} 1$$

$\alpha^{-5} \to \alpha^{-5} \cdot \underbrace{\alpha^{15}}_{=1}$

$$\sigma^{(3)}(x) = \sigma^{(2)}(x) + \alpha^{10} x^2 \qquad = \alpha^{10}$$

$\sigma^{(2)}(x) \to 1 + \alpha^{12} x$

$\hat{S}_4 = \alpha^{12} S_2 + \alpha^{10} S_1$

$\hat{S}_4 = \alpha^3$

$d_3 = S_4 + \hat{S}_4 = \alpha^3 + \alpha^3 = 0$

then $\sigma^{(3)}(x) = 1 + \alpha^{12} x + \alpha^{10} x^2$

$i=3$

proceeding in a similar manner

$\sigma^{(4)}(x) = 1 + \alpha^{12} x + \alpha^{10} x^2 \qquad r_4=2 \; n_4=2 \; d_4=1$

$l=4$ $\quad \sigma^{(5)}(x) = 1 + \alpha^{12}x + \alpha x^2 + \alpha^5 x^3$

$r_5 = 3 \quad n_5 = 2 \quad d_5 = 0$

$l=5$ $\quad \sigma^{(6)}(x) = 1 + \alpha^{12}x + \alpha x^2 + \alpha^5 x^3$

$\downarrow$

$2t$

Stop here

$\sigma(x) = \sigma^{(2t)}(x)$

$\sigma(x) = 1 + \alpha^{12}x + \alpha x^2 + \alpha^5 x^3$

Find the roots of $\sigma(x)$ in $GF(2^4)$

Take their reciprocals and determine error location polynomial

Remarks If the number of errors τ is less than t, then not all $2t$ iterations are required. If the discrepancy d_i and the following discrepancies are zero, then $\sigma^{(i)}(x)$ is the required error location polynomial.

Exercise:

The following codeword belongs to the BCH(15,5) triple-error-correcting code.

$$c(x) = x^{12} + x^{11} + x^9 + x^8 + x^7 + x^2 + 1$$

Introducing the single error $e(x) = x^{11}$ gives

$$r(x) = c(x) + e(x) = x^{12} + x^9 + x^8 + x^7 + x^2 + 1.$$

Decode $r(x)$ using Berlekamp algorithm

Soln: $p(x) = x^4 + x + 1 \longrightarrow GF(2^4)$

complete the solution.

The error-evaluator Polynomial's

Berlekamp algorithm is used to find error location polynomial.

For RS codes wee need to find also error magnitudes.

Let error location polynomial be as

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_t x^t$$

To find the error magnitudes we first define the error-evaluator polynomial as

$$\omega(x) = 1 + \omega_1 x + \omega_2 x^2 + \cdots + \omega_t x^t$$

where $\omega_1 = S_1 + \sigma_1 \quad \omega_2 = S_2 + \sigma_1 S_1 + \sigma_2$

$$\cdots\cdots \omega_t = S_t + \sigma_1 S_{t-1} + \sigma_2 S_{t-2} + \cdots + \sigma_t$$

Once the error-evaluator polynomial is determined, the magnitude Y_j corresponding to the error-location number X_j is given by

$$Y_j = \frac{\omega(X_j^{-1})}{(1+X_j^{-1}X_1)(1+X_j^{-1}X_2)\cdots(1+X_j^{-1}X_t)}$$

Ex: RS(15, 8) code is given ($p(x) = x^4 + x + 1$)

$$r(x) = \alpha^3 x^{12} + x^8 + \alpha^{10} x^7 + \alpha^2 x^5 + \alpha^8 x^4 + \alpha^{14} x^3 + \alpha^6$$

$S_i = r(\alpha^i)$ Syndromes are given as

$$S_1 = \alpha^6,\ S_2 = 0,\ S_3 = \alpha^{14},\ S_4 = \alpha^{11},\ S_5 = \alpha^{14},\ S_6 = \alpha^9$$

The error location polynomial was found to be $\sigma(x) = 1 + x + \alpha^{11}x^2 + \alpha^4 x^3$

which gives $t = 3$ errors with error-location numbers $X_1 = \alpha^{12}$, $X_2 = \alpha^5$, and $X_3 = \alpha$

For $t = 3$ the error-evaluator polynomial is given by $\omega(x) = 1 + \omega_1 x + \omega_2 x^2 + \omega_3 x^3$

where $\omega_1 = S_1 + \sigma_1$

$\omega_2 = S_2 + \sigma_1 S_1 + \sigma_2$

$\omega_3 = S_3 + \sigma_1 S_2 + \sigma_2 S_1 + \sigma_3$

which gives $w(x)$ as

$$w(x) = 1 + \alpha^{13}x + \alpha x^2 + \alpha^{11}x^3$$

which is the required error-evaluator polynomial.

To determine the error magnitudes

$$w(X_1^{-1}) = w(\alpha^{-12}) = 1 + \alpha^{13}\alpha^{-12} + \alpha\alpha^{-24} + \alpha^{11}\alpha^{-36} = \alpha^{11}$$

$$w(X_2^{-1}) = w(\alpha^{-5}) = \alpha^5$$

$$w(X_3^{-1}) = w(\alpha^{-1}) = \alpha$$

The error magnitudes are

$$y_1 = \frac{w(X_1^{-1})}{(1+X_1^{-1}X_2)(1+X_1^{-1}X_3)} = \frac{\alpha^{11}}{(1+\alpha^{-12}\alpha^5)(1+\alpha^{-12}\alpha)}$$

$$= \alpha^3$$

$$y_2 = \frac{w(X_2^{-1})}{(1+X_2^{-1}X_1)(1+X_2^{-1}X_3)} = \frac{\alpha^5}{(1+\alpha^{-5}\alpha^{12})(1+\alpha^{-5}\alpha)} = \alpha^3$$

$$y_3 = \frac{w(X_3^{-1})}{(1+X_3^{-1}X_1)(1+X_3^{-1}X_2)} = \frac{\alpha}{(1+\alpha^{-1}\alpha^{12})(1+\alpha^{-1}\alpha^5)}$$

$$= \alpha^9$$

Exercise

RS(15,9) → triple error correcting code

$S_1 = \alpha^4 \quad S_2 = 1 \quad S_3 = \alpha^{10} \quad S_4 = \alpha^7 \quad S_5 = 0$

$S_6 = \alpha^{14} \qquad \sigma(x) = 1 + \alpha^2 x + \alpha^{11}x^2 + \alpha^5 x^3$

Determine error magnitudes

Problems

1) Construct a single-error-correcting binary BCH code over $GF(2^3)$

2) Determine the generator polynomials of the double-error-correcting (15,11) and triple-error correcting (15,5) Reed Solomon codes

3) A decoder for the double-error correcting (15,11) Reed Solomon code uses the PGZ decoder to determine the position and magnitude of errors. Given that the input to the decoder is $r = (1\ \alpha^{13}\ \alpha^{13}\ \alpha^{8}\ \alpha^{7}\ \alpha^{3}\ \alpha^{10}\ 0\ 0\ 0\ \alpha\ 0\ 0\ 0)$

a) determine the decoding decision

b) Repeat the problem for a decoder that uses the Berlekamp algorithm for determining the error locating and the error evaluator polynomial to determine the error magnitudes

Supplementary Informations

$GF(q)$, q . $q = p^m$ $p \rightarrow$ prime number

$\alpha \in GF(q)$ $G(p^m)$ $p \neq 2$

Conjugates of α are given as

$$\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots\ldots$$

The minimal polynomial of α is given as

$$M_1(x) = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\ldots\ldots$$

Property: $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ $q = p^n$

Defn: An element α in a finite field $GF(q)$ is called a primitive element of $GF(q)$ if $GF(q) = \{0, \alpha, \alpha^2, \ldots \alpha^{q-1}\}$ ($p \rightarrow$ prime number)

& pay attention! i is not written

Ex°

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

$GF(3^2) = \{0, \alpha, \alpha^2, \alpha^3, \dots \alpha^8\}$ $\alpha^9 = 1$

α is a root of a polynomial (prime) such that $p(\alpha) = 0$

Ex° $p(x) = x^2 + x + 2$ $p(x) = x^2 + 1$

Extend $GF(3)$ to $GF(3^2)$

PROJECT WORK

RS(255, 223) is NASA standard code for satellite and space communications

$m = 8$, $t = 16$ $n = 255$ $k = n - 2t \rightarrow k = 223$

$d_{min} = 33$

Find $g(x)$ → generator polynomial of RS(255, 223)

Simulation

1) Generator random data frames whose lengths are $k = 223$ symbols

178

2) Encode data frames using RS(255, 223)

3) BPSK modulate the encoded frames

4) Add some noise

5) Decode received frames (noise added signal) and note error rate repeat this procedure for a sufficient number of frames

Finally obtain BER versus SNR plot with and without coding