REEDSOLOMON CODES

1. **Introduction**
2. **Encoding of RS Codes**
3. **Properties of RS Codes**
4. **RS Codes for Binary Data**
5. **Decoding of RS Codes**
6. **Modified RS Codes**
7. **Error Correcting Performance**
8. **References**

1. Introduction

- They are nonbinary cyclic codes with code symbols from a Galois field.
- Discovered in 1960 by I. Reed and G. Solomon.
- The most important Reed–Solomon (RS) codes are codes with symbols from GF(2^m). They are widely used in data communications and storage systems for error control.

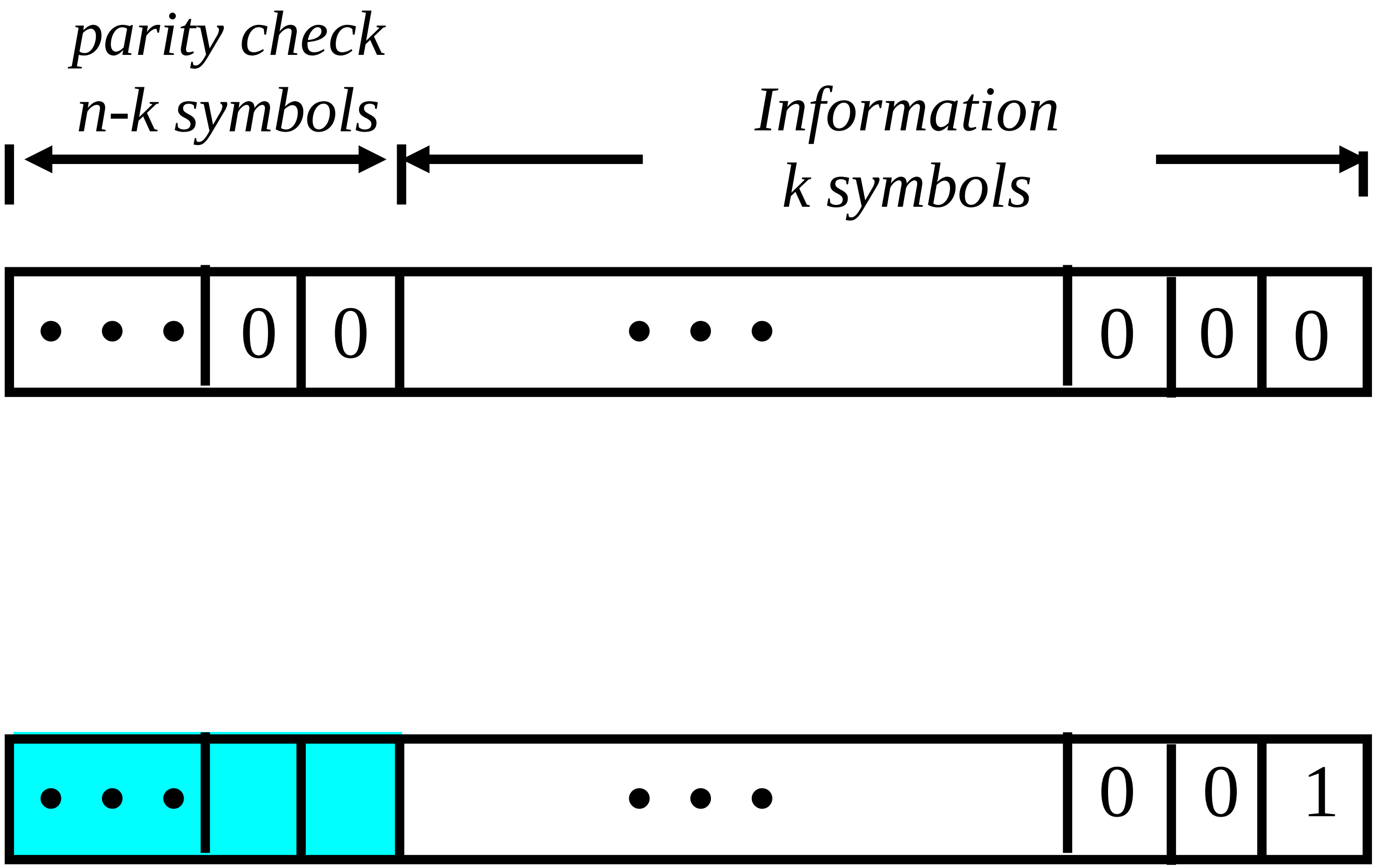
- Singleton bound

$$d_{min} \le n - k + 1.$$

- One of the most important features of RS codes is that the minimum distance of a RS code is one greater than its number of parity-check symbols. That is, the minimum distance of an (n, k) RS code is $n - k + 1$, i.e.,

$$d_{min} = n - k + 1$$

Codes of this kind are called **maximum-distance-separable (MDS) codes** .



$$d_{min} = n - k + 1$$

2 . Encoding of RS codes

- Let α be a primitive element in GF(2^m).
- For any positive integer $t \le 2^m - 1$, there exists a t-symbol-error-correcting RS code with symbols from GF(2^m) and the following parameters:

$$n = 2^m - 1$$

$$n - k = 2t$$

$$k = 2^m - 1 - 2t$$

$$d_{min} = 2t + 1.$$

- The generator polynomial is

$$g(X) = (X + \alpha)(X + \alpha^2)...(X + \alpha^{2t})$$
$$= g_0 + g_1 X + g_2 X^2 + ... + g_{2t-1} X^{2t-1} + X^{2t}$$

where $g_i \in GF(2^m)$.

- Note that $g(X)$ has α , α^2 , ... , α^{2t} as roots.
- Each code polynomial

$$v(X) = v_0 + v_1 X + v_2 X^2 + ... + v_{n-1} X^{n-1}$$

has coefficients from GF(2^m) and is a multiple of the generator polynomial $g(X)$.

- Let $c(X) = c_0 + c_1 X + c_2 X^2 + \ldots + c_{k-1} X^{k-1}$ be the message to be encoded where $c_i \in GF(2^m)$ and $k = n - 2t$.
- Dividing $X^{2t} c(X)$ by $g(X)$, we have

$$X^{2t} c(X) = a(X) \cdot g(X) + b(X)$$

where $b(X) = b_0 + b_1 X + \ldots + b_{2t-1} X^{2t-1}$ is the remainder.

- Then

$$v(X) = b(X) + X^{2t}c(X)$$

is the codeword for message $c(X)$.

- The encoding circuit is shown in Figure 1.

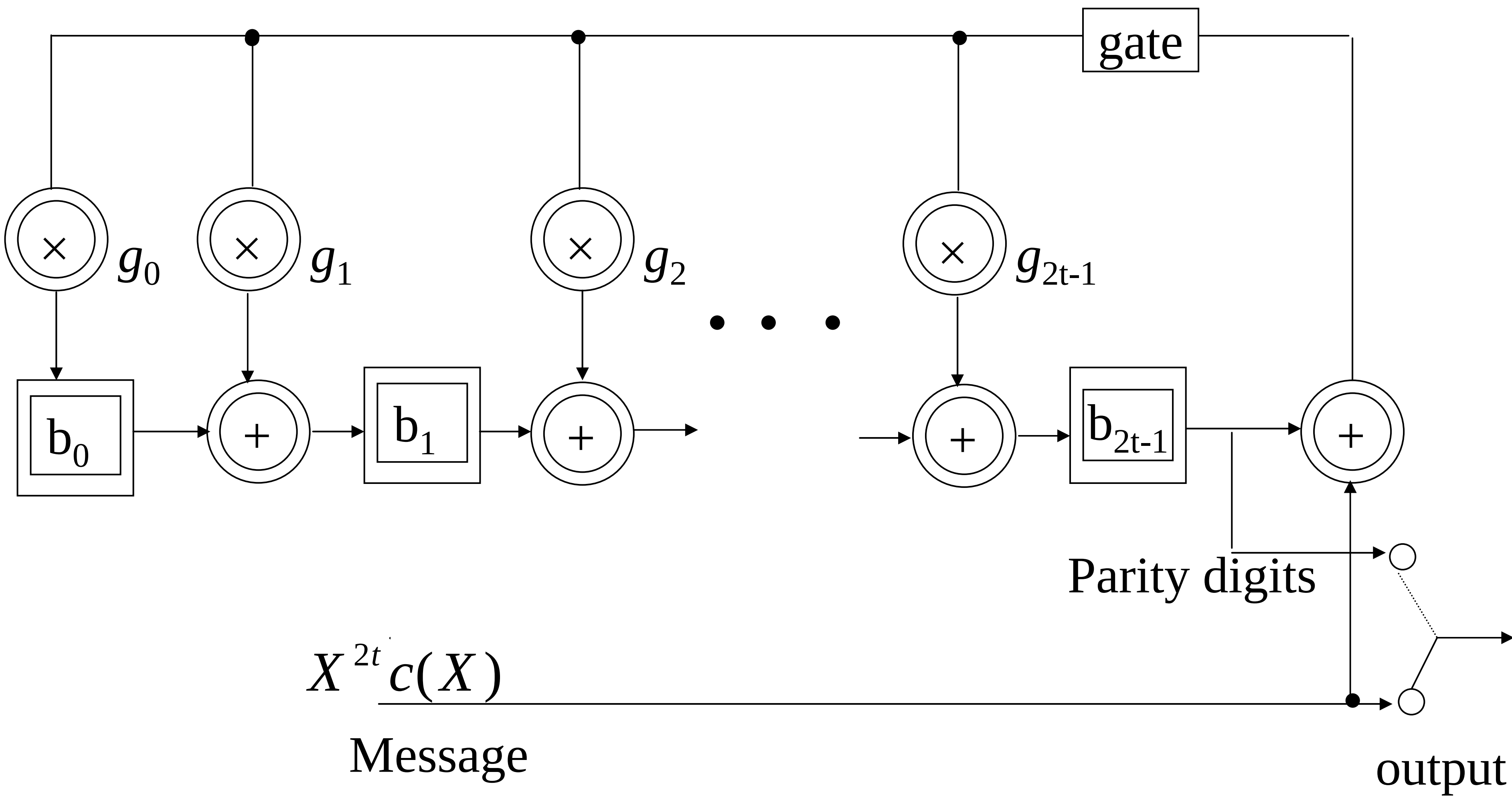


Figure 1: Encoding circuit for a nonbinary cyclic code

- Let

$$c(X) = 1, X, \cdots, X^{k-1}$$

the corresponding remainder polynomials $b_i(X)$ are denoted by

$$b_i(X) = b_{i,0} + b_{i,1}X + \cdots b_{i,2t-1}X^{2t-1}$$

for

$$0 \le i \le k-1$$

The corresponding generator matrix in systematic form is

$$G=\begin{bmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,2t-1} & 1 & 0 & \cdots & 0 \\ b_{1,0} & b_{1,1} & \cdots & b_{1,2t-1} & 0 & 1 & \cdots & 0 \\ \cdots & & & & & & & \\ b_{k-1,0} & b_{k-1,1} & \cdots & b_{k-1,2t-1} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

- Since (n, k, d_{min}) RS code is a cyclic code, the generator matrix in nonsystematic form is in the following

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{2t-1} & 1 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{2t-2} & g_{2t-1} & 1 & \cdots & 0 \\ & & \cdots & & & & & \\ 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_{2t-1} & 1 \end{bmatrix}$$

Example 1: Consider an (7, 5, 3) RS code over GF(2^3) generated by $\alpha^3+\alpha+1=0$, where α is primitive element.

power	polynomial	vector
0	0	(0,0,0)
1	1	(1,0,0)
α	α	(0,1,0)
α^2	α^2	(0,0,1)
α^3	$1+\alpha$	(1,1,0)
α^4	$\alpha+\alpha^2$	(0,1,1)
α^5	$1+\alpha+\alpha^2$	(1,1,1)
α^6	$1+\alpha^2$	(1,0,1)

The generator polynomial of (7, 5, 3) RS code is

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

And the generator matrix in nonsystematic form is

$$G = \begin{bmatrix} \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 \end{bmatrix}$$

Since

$$1 \cdot X^2 = 1 \cdot g(X) + \alpha^4 X + \alpha^3$$

$$X \cdot X^2 = (X + \alpha^4) \cdot g(X) + X + 1$$

$$X^2 \cdot X^2 = (X^2 + \alpha^4 X + 1) \cdot g(X) + \alpha^5 X + \alpha^3$$

$$X^3 \cdot X^2 = (X^3 + \alpha^4 X^2 + X + \alpha^5) \cdot g(X) + \alpha^5 X + \alpha$$

$$X^4 \cdot X^2 = (X^4 + \alpha^4 X^3 + X^2 + \alpha^5 X + \alpha^5) \cdot g(X) + \alpha^4 X + \alpha$$

therefore, the generator matrix in systematic form is

$$G = \begin{bmatrix} \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ \alpha^3 & \alpha^5 & 0 & 0 & 1 & 0 & 0 \\ \alpha & \alpha^5 & 0 & 0 & 0 & 1 & 0 \\ \alpha & \alpha^4 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= [P, I_5]$$

3. Properties of RS Codes

Theorem 1:

- Let a code polynomial be

$$v(X) = v_0 + v_1 X + \dots + v_{n-1} X^{n-1}$$

which has $\alpha, \alpha^2, \dots, \alpha^{2t}$ as roots.

- Since α^i is a root of $v(X)$, then

$$v(\alpha^i) = v_0 + v_1 \alpha^i + \dots + v_{n-1} \alpha^{i(n-1)} = 0$$

This equality can be written as a matrix product as follows:

$$(v_0, v_1, \cdots, v_{n-1}) \cdot \begin{bmatrix} 1 \\ \alpha^{i} \\ \alpha^{2i} \\ \vdots \\ \alpha^{(n-1)i} \end{bmatrix} = 0$$

If $\bar{v} = (v_0, v_1, \cdots, v_{n-1})$, then the parity check matrix H is

$$\bar{v} \cdot H^T = \underbrace{(0,0,\cdots 0)}_{(n-k)'s}$$

and

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^{2\times 2} & \alpha^{2\times 3} & \cdots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^{3\times 2} & \alpha^{3\times 3} & \cdots & \alpha^{3(n-1)} \\ \vdots & & & & \cdots & \vdots \\ 1 & \alpha^{2t} & \alpha^{2t\times 2} & \alpha^{2t\times 3} & \cdots & \alpha^{2t(n-1)} \end{bmatrix} \quad (4.1)$$

Example 2: Consider an (7, 5, 3) RS code mentioned in Example 1, the parity check matrix is

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

$$\downarrow$$

$$H=\begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 0 & \alpha^4 & \alpha & \alpha^4 & \alpha^2 & \alpha^2 & \alpha \end{bmatrix} \leftarrow \times\alpha^3$$

$$\downarrow$$

$$H=\begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 0 & 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 \end{bmatrix} \quad + \quad \times\alpha$$

$$\downarrow$$

$$H=\begin{bmatrix} 1 & 0 & \alpha^3 & 1 & \alpha^3 & \alpha & \alpha \\ 0 & 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 \end{bmatrix} = [I_2, P^T]$$

Theorem 2:

The dual code of an (n, k, d_{min}) RS code is still a **maximum-distance-separable (MDS) code,** whose code length is n, and information length is $n - k$, and minimum Hamming distance is $n - (n - k) + 1 = k + 1$.

Theorem 3[2]:

Any combination of k symbols in a codeword in an MDS code may be used as message symbols in a systematic representation. In other words, we use these k symbols to recovery the whole codeword.

Example 3: Let a codeword generated is shown in the following.

$$\bar{v} = (\alpha \;\; 1 \;\; 1 \;\; 0 \;\; 0) \cdot \begin{bmatrix} \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ \alpha^3 & \alpha^5 & 0 & 0 & 1 & 0 & 0 \\ \alpha & \alpha^5 & 0 & 0 & 0 & 1 & 0 \\ \alpha & \alpha^4 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= (\alpha^2 \;\; 1 \;\; \alpha \;\; 1 \;\; 1 \;\; 0 \;\; 0)$$

Assume there are some misses in transmission, we only get

$$\bar{r} = (\alpha^2 \quad 1 \quad \alpha \quad X \quad X \quad 0 \quad 0\ )$$

Misses

permutation

$$\bar{r}' = (\underbrace{\alpha^2 \quad 1 \quad \alpha \quad 0 \quad 0}_{} \quad X \quad X\ )$$

We use these 5 symbols as a message symbols

From above, we use the portion of data to obtain the whole codeword. Based on the data positions, we permute the generator matrix as the following form.

$$G = \begin{bmatrix} \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ \alpha^3 & \alpha^5 & 0 & 0 & 0 & 0 & 1 \\ \alpha & \alpha^5 & 0 & 1 & 0 & 0 & 0 \\ \alpha & \alpha^4 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

In the following steps, we show the raw operations to obtain a new systematic form

$$1 \quad \alpha \quad \alpha^4$$

$$\begin{bmatrix} \cancel{\alpha^3} & \cancel{\alpha^4} & \cancel{1} & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ \alpha^3 & \alpha^5 & 0 & 0 & 0 & 0 & 1 \\ \alpha & \alpha^5 & 0 & 1 & 0 & 0 & 0 \\ \alpha & \alpha^4 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{matrix} \leftarrow \times\alpha^4 \\ \leftarrow 1 \\ \leftarrow \alpha^3 \\ \leftarrow \alpha \\ \leftarrow \alpha \end{matrix}$$

$$\Downarrow$$

$$\begin{matrix} \\ \alpha^4\times \rightarrow \\ \\ \\ \\ \end{matrix} \begin{bmatrix} 1 & \alpha & \alpha^4 & 0 & 0 & 0 & 0 \\ 0 & \overset{1}{\cancel{\alpha^3}} & \overset{\alpha}{\cancel{\alpha^4}} & 0 & 0 & \overset{\alpha^4}{\cancel{1}} & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & \alpha^3 & \alpha^5 & 1 & 0 & 0 & 0 \\ 0 & \alpha & \alpha^5 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{matrix} \leftarrow \alpha \\ \\ \leftarrow 1 \\ \leftarrow \alpha^3 \\ \leftarrow \alpha \end{matrix}$$

$$
\alpha^{4}\times \rightarrow
\begin{bmatrix}
1 & 0 & \alpha & 0 & 0 & \alpha^{5} & 0 \\
0 & 1 & \alpha & 0 & 0 & \alpha^{4} & 0 \\
0 & 0 & \cancel{\alpha^{3}}\ 1 & 0 & 0 & \cancel{\alpha^{4}}\ \alpha & \cancel{1}\ \alpha^{4} \\
0 & 0 & 1 & 1 & 0 & \alpha^{3} & 0 \\
0 & 0 & \alpha^{3} & 0 & 1 & \alpha^{5} & 0
\end{bmatrix}
\begin{matrix}
\leftarrow \alpha \\
\leftarrow \alpha \\
\\
\leftarrow 1 \\
\leftarrow \alpha^{3}
\end{matrix}
$$

$$\downarrow$$

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & \alpha^{3} & \alpha^{5} \\
0 & 1 & 0 & 0 & 0 & \alpha & \alpha^{5} \\
0 & 0 & 1 & 0 & 0 & \alpha & \alpha^{4} \\
0 & 0 & 0 & 1 & 0 & 1 & \alpha^{4} \\
0 & 0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix}
$$

$$\bar{v}' = (\alpha^2 \quad 1 \quad \alpha \quad 0 \quad 0) \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \alpha^3 & \alpha^5 \\ 0 & 1 & 0 & 0 & 0 & \alpha & \alpha^5 \\ 0 & 0 & 1 & 0 & 0 & \alpha & \alpha^4 \\ 0 & 0 & 0 & 1 & 0 & 1 & \alpha^4 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$= (\alpha^2 \quad 1 \quad \alpha \quad 0 \quad 0 \quad 1 \quad 1)$$

↓ Inverse permutation

$$\bar{v} = (\alpha^2 \quad 1 \quad \alpha \quad 1 \quad 1 \quad 0 \quad 0)$$

4 . RS Codes for Binary Data

- Every element in GF(2^m) can be represented uniquely by a binary m-tuple, called a m-bit byte.
- Suppose an (n, k, d_{min}) RS code with symbols from GF(2^m) is used for encoding binary data.
- A message of $k \times m$ bits is first divided into k m-bit bytes.
- Each m-bit byte is regarded as a symbol in GF(2^m).
- The k-byte message is then encoded into an n-byte codeword based on the RS code.

- By doing this, we actually expand a RS code with symbols from GF(2^m) into a binary (nm, km) linear code, called a binary RS code.
- To decode, the binary received vector at the channel output is first divided into n m-bit bytes. Each m-bit bytes is transformed back into a symbol in GF(2^m).
- The resultant vector over GF(2^m) is then decoded based on the RS code.
- As a result, the binary RS code is capable of correcting any error pattern that affects t (or fewer) m-bit bytes. It is immaterial whether a byte has one error or m errors, it is counted as one byte (or symbol) error.

- Binary RS codes are very effective in correcting bursts of errors as long as no more t bytes are affected.

5. Decoding of RS Codes

1. Syndrome-based decoding
   - Peterson-Gorenstein-Zierler Algorithm[2]
   - Berlekamp-Massey Algorithm[1][2]
   - Euclidean Algorithm[1][2]
   - Frequency Domain Algorithm[1][2]
   - Step-by-Step Algorithm[3]-[6]

2. Interpolation-based decoding
   - Welch-Berlekamp algorithm[7][8]
   - List decoding[9]

Syndrome-based decoding

Decoding Procedure:

(1) Compute syndrome vector $\overline{S} = (S_1, S_2, ..., S_{2t})$.

(2) Determine error-location polynomial $\sigma(X)$.

(3) Determine error-value evaluator polynomial $Z(X)$

(4) Evaluate error-location numbers (find roots of $\sigma(X)$)and error values and perform error correction.

- RS codes are actually a special subclass of nonbinary BCH codes.
- Decoding of a RS code is similar to the decoding of a BCH code except an additional step is needed.
- Let

$$v(X) = v_0 + v_1 X + \ldots + v_{n-1} X^{n-1}$$

and

$$r(X) = r_0 + r_1 X + ... + r_{n-1} X^{n-1} = v(X) + e(X)$$

be the transmitted code polynomial and received polynomial respectively.

- Then the error polynomial is

$$e(X) = r(X) - v(X)$$

$$= e_0 + e_1 X + ... + e_{n-1} X^{n-1}$$

where $e_i = r_i - v_i$ is a symbol in GF(2^m) .

Syndrome Computation

- The syndrome of a received polynomial $r(X)$ is

$$\overline{S} = (S_1, S_2, ..., S_{2t})$$

where $S_i = r(\alpha^i)$.

- To find S_i, we divide $r(X)$ by $X+\alpha^i$. This gives us

$$r(X) = a(X)\cdot(X + \alpha^i) + b_i$$

where $b_i \in GF(2^m)$.

- Then

$$\begin{aligned} S_i &= r(\alpha^i) = b_i \\ &= e_{j_1}\alpha^{i\times j_1} + e_{j_2}\alpha^{i\times j_2} + \cdots e_{j_v}\alpha^{i\times j_v} \\ &= e_{j_1}\beta_1^i + e_{j_2}\beta_2^i + \cdots e_{j_v}\beta_v^i \end{aligned}$$

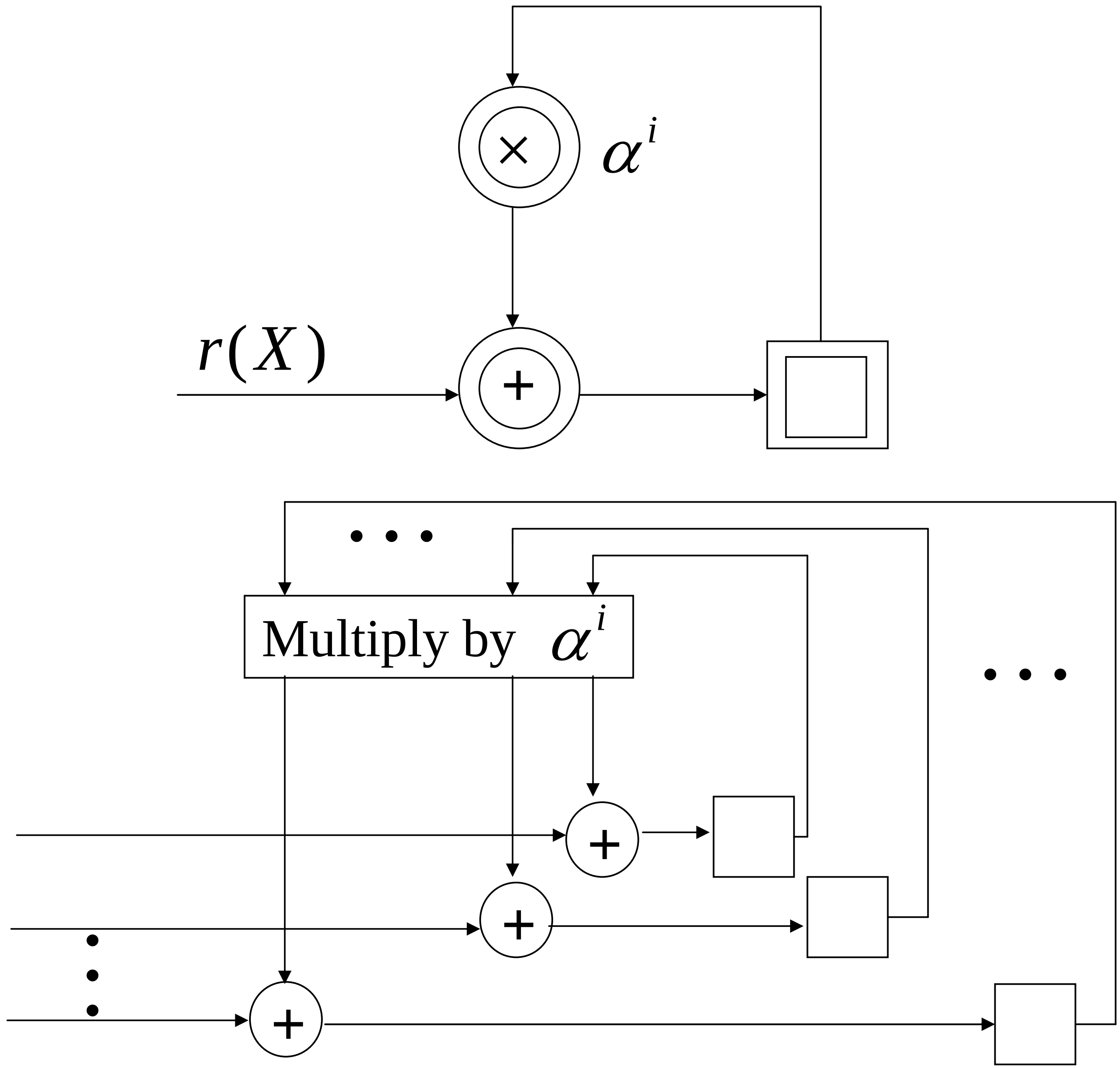


Figure 2: A syndrome computation circuit

- Suppose $e(X)$ has v errors at the locations $X^{j_1}, X^{j_2}, \cdots, X^{j_v}$. Then

$$e(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} + \cdots e_{j_v} X^{j_v}$$

- The syndromes are computed as follows:

$$\begin{aligned} S_1 &= e_{j_1}\beta_1 + e_{j_2}\beta_2 + \cdots e_{j_v}\beta_v \\ S_2 &= e_{j_1}\beta_1^2 + e_{j_2}\beta_2^2 + \cdots e_{j_v}\beta_v^2 \\ &\vdots \\ S_{2t} &= e_{j_1}\beta_1^{2t} + e_{j_2}\beta_2^{2t} + \cdots e_{j_v}\beta_v^{2t} \end{aligned} \qquad (1)$$

$$\boxed{S_l = \sum_{i=1}^{v} e_{j_i}\beta_i^{\,l}}$$

error-location polynomial

- And error-location numbers are given by

$$\begin{aligned} \beta_{j_1} &= \alpha^{j_1}, & & \beta_{j_1} = \beta_1 \\ \beta_{j_2} &= \alpha^{j_2}, & \xrightarrow{\text{for convenience}} \quad & \beta_{j_2} = \beta_2 \\ &\vdots & & \vdots \\ \beta_{j_v} &= \alpha^{j_v}. & & \beta_{j_v} = \beta_v \end{aligned}$$

- The error-location polynomial is defined by

$$\begin{aligned} \sigma(X) &\triangleq (1-\beta_1 X)(1-\beta_2 X^2)\cdots(1-\beta_v X^v) \\ &= 1+\sigma_1 X + \cdots + \sigma_v X^v \end{aligned} \tag{2}$$

- The error locator numbers are the reciprocals of the roots of the error-locator polynomial $\sigma(X)$.
- Let $X = \beta_i^{-1}$ in (2), and we obtain the following equation

$$\sigma(\beta_i^{-1}) = 1 + \sigma_1 \beta_i^{-1} + \cdots + \sigma_v \beta_i^{-v} = 0$$

- Since the expression sums to zero, we cam multiply through by a constant $e_{j_i} \beta_i^{l}$.

$$\begin{aligned} & e_{j_i} \beta_i^{l} (1 + \sigma_1 \beta_i^{-1} + \cdots + \sigma_v \beta_i^{-v}) \\ & = e_{j_i} (\beta_i^{l} + \sigma_1 \beta_i^{l-1} + \cdots + \sigma_v \beta_i^{l-v}) = 0 \end{aligned} \qquad (3)$$

- Sum (3) over all indices i, obtaining an following expression which is called "Newton's identities"

$$\sum_{i=1}^{v} e_{j_i}(\beta_i^l + \sigma_1\beta_i^{l-1} + \cdots + \sigma_v\beta_i^{l-v})$$

$$= \sum_{i=1}^{v} e_{j_i}\beta_i^l + \sigma_1\sum_{i=1}^{v} e_{j_i}\beta_i^{l-1} + \cdots + \sigma_v\sum_{i=1}^{v} e_{j_i}\beta_i^{l-v}$$

$$= S_l + \sigma_1 S_{l-1} + \cdots + \sigma_v S_{l-v}$$

$$= 0$$

$$\boxed{\sigma_1 S_{l-1} + \cdots + \sigma_v S_{l-v} = -S_l} \qquad (4)$$

Peterson-Gorenstein-Zierler Decoding Algorithm

- **Matrix method: there are *v* errors**

$$A\overline{\sigma} = \overline{S} \longrightarrow \overline{\sigma} = A^{-1}\overline{S}$$

$$\sigma(X) = 1 + \sigma_1 X + \cdots + \sigma_v X^v$$

$$\overline{\sigma} = [\sigma_1, \cdots, \sigma_v]^T$$

$$\overline{S} = [S_{v+1}, \cdots, S_{2v}]^T$$

$$B\bar{e} = \bar{S} \longrightarrow \bar{e} = B^{-1}\bar{S}$$

$$\bar{e} = [e_1, \cdots, e_v]^T$$

$$\bar{S} = [S_1, \cdots, S_v]^T$$

Peterson-Gorenstein-Zierler Decoding Algorithm

- In (4), if we assume $v = t$ and $t+1 \le l \le 2t$, then

$$
\begin{aligned}
\sigma_1 S_t + \sigma_2 S_{t-1} \cdots + \sigma_t S_1 &= -S_{t+1} \\
\sigma_1 S_{t+1} + \sigma_2 S_t \cdots + \sigma_t S_2 &= -S_{t+2} \\
&\vdots \\
\sigma_1 S_{2t-1} + \sigma_2 S_{2t-2} \cdots + \sigma_t S_t &= -S_{2t}
\end{aligned} \qquad (5)
$$

$$
A\overline{\sigma} = \begin{bmatrix} S_1 & S_2 & \cdots & S_t \\ S_2 & S_3 & \cdots & S_{t+1} \\ & \vdots & & \\ S_t & S_{t+1} & \cdots & S_{2t-1} \end{bmatrix} \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_{t+1} \\ S_{t+2} \\ \vdots \\ S_{2t} \end{bmatrix} \quad (6)
$$

- It can be shown that the matrix A is nonsingular if the received sequence contains t errors.
- It can also be shown that the matrix A is singular if fewer than t errors have occurred.

- If the matrix A is singular, the rightmost column and bottom row are removed and the determinant of the resulting matrix computed.
- This process is repeated until the resulting matrix is nonsingular.
- The coefficients of the error locator polynomial $\sigma(X)$ can be calculated by "Gaussian elimination" or the inverse matrix method over $GF(2^m)$.

- Once the error locator polynomial $\sigma(X)$ is determined, and the roots of $\sigma(X)$ are then computed.
- The error locator numbers β_i , $1 \le i \le v$, are the reciprocals of the roots of the error-locator polynomial $\sigma(X)$.
- From (1),

$$\begin{bmatrix} \beta_1 & \beta_2 & \cdots & \beta_v \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_v^2 \\ & \vdots & & \\ \beta_1^v & \beta_2^v & \cdots & \beta_v^v \end{bmatrix} \begin{bmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_v} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_v \end{bmatrix} \qquad (7)$$

- Decoding is completed by solving for the $\{e_{i_j}\}$
- If roots of $\sigma(X)$ are not distinct or roots do not exist, then declare a decoding failure.

Example 4: Consider an (7, 3, 5) RS code, its generator polynomial is

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

Assume the received sequence is

$$r(X) = X^4 + X^2 + \alpha X + \alpha^3$$

The syndromes are

$$S_1 = r(\alpha) = \alpha^6, \quad S_2 = r(\alpha^2) = \alpha^2$$
$$S_3 = r(\alpha^3) = \alpha^5, \quad S_4 = r(\alpha^4) = \alpha^2$$

The matrix A in (6) is given by

$$A = \begin{bmatrix} \alpha^6 & \alpha^2 \\ \alpha^2 & \alpha^5 \end{bmatrix}$$

Since

$$\det(A) = 0$$

We remove the rightmost column and bottom row from A, then

$$\alpha^6 \sigma_1 = \alpha^2 \longrightarrow \sigma_1 = \alpha^3$$

$$\longrightarrow \beta_1 = \alpha^3$$

From (7), we obtain the following

$$\alpha^3 e_3 = \alpha^6$$

which gives the error magnitude α^3. The error polynomial is thus

$$e(X) = \alpha^3 X^3$$

The coded sequence is

$$\begin{aligned} v(X) &= r(X) - e(X) \\ &= \alpha^3 + \alpha X + X^2 + \alpha^3 X^3 + X^4 \end{aligned}$$

Berlekamp-Massey Decoding Algorithm

- **Iterative method: at *u*-th step**

$$\sigma^{(u)}(X) = 1 + \sigma_1^{(u)} X + \sigma_2^{(u)} X^2 + \cdots \sigma_{l_u}^{(u)} X^{l_u}$$

$$\downarrow$$

$$\sigma(X) = \sigma^{(2t)}(X) = 1 + \sigma_1 X + \cdots + \sigma_v X^v$$

- **Initially,** $\sigma^{(1)}(X) = 1 + S_1 X$

- **At *u*+1-th step:**

$$\sigma^{(u+1)}(X) = \sigma^{(u)}(X) + \Delta$$

- **At final step (*u* = 2*t*):**

$$\sigma(X) = \sigma^{(2t)}(X) = 1 + \sigma_1 X + \cdots + \sigma_v X^v$$

Berlekamp-Massey Decoding Algorithm

- $\sigma(X)$ can be computed iteratively .
- The iteration process consists of $2t$ steps .
- At the u-th step, we determine a minimum-degree polynomial

$$\sigma^{(u)}(X) = 1 + \sigma_1^{(u)} X + \sigma_2^{(u)} X^2 + \cdots \sigma_{l_u}^{(u)} X^{l_u}$$

such that its coefficients satisfy the following $u - l_u$ Newton's identities:

$$
\begin{aligned}
&S_{l_u+1} + \sigma_1^{(u)} S_{l_u} + \cdots + \sigma_{l_u}^{(u)} S_1 = 0 \\
&S_{l_u+2} + \sigma_1^{(u)} S_{l_u+1} + \cdots + \sigma_{l_u}^{(u)} S_2 = 0 \\
&\qquad \vdots \\
&S_u + \sigma_1^{(u)} S_{u-1} + \cdots + \sigma_{l_u}^{(u)} S_{u-l_u} = 0
\end{aligned}
$$

- The next step is to find a new polynomial of minimum degree

$$
\sigma^{(u+1)}(X) = 1 + \sigma_1^{(u+1)} X + \cdots + \sigma_{l_{u+1}}^{(u+1)} X^{l_{u+1}}
$$

whose coefficients satisfy the following $u+1-l_{u+1}$ Newton's identities:

$$S_{l_{u+1}+1}+\sigma_1^{(u+1)}S_{l_{u+1}}+\cdots+\sigma_{l_{u+1}}^{(u+1)}S_1=0$$

$$S_{l_{u+1}+2}+\sigma_1^{(u+1)}S_{l_{u+1}+1}+\cdots+\sigma_{l_{u+1}}^{(u+1)}S_2=0$$

$$\vdots$$

$$S_{u+1}+\sigma_1^{(u+1)}S_u+\cdots+\sigma_{l_{u+1}}^{(u+1)}S_{u+1-l_{u+1}}=0$$

- We continue the foregoing process until $2t$ steps have been completed. At the $2t$-th, we have

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

- In u+1-th iteration, $\sigma^{(u+1)}(X)$ is found by testing the discrepancy:

$$d_u = S_{u+1} + \sigma_1^{(u)} S_u + \sigma_2^{(u)} S_{u-1} + \ldots. + \sigma_{l_u}^{(u)} S_{u+1-l_u}$$

- If $d_u = 0$, then the coefficients of $\sigma^{(u)}(X)$ satisfies the (u + 1)-th Newton's identity

$$\sigma^{(u+1)}(X) = \sigma^{(u)}(X)$$

$l_{\text{u+1}} = l_{\text{u}}$ (actually, l_{u} is the degree of $\sigma^{(u)}(X)$)

- If $d_u \neq 0$, $\sigma^{(u)}(X)$ needs to be adjusted to satisfy the $(u + 1)$-th Newton's identity

- Correction: we go back to the steps prior to the u-th step and determine a polynomial $\sigma^{(p)}(X)$ such that $d_p \neq 0$ and $p - l_p$ has the largest value, where l_p is the degree of $\sigma^{(p)}(X)$. Then

$$\sigma^{(u+1)}(X) = \sigma^{(u)}(X) + d_u d_p^{-1} X^{(u-p)} \sigma^{(p)}(X)$$

- $\sigma^{(u+1)}(X)$ is the solution at the $(u+1)$-th step of the iteration process.

Error-Value Evaluator Polynomial

- Once $\sigma(X) = \sigma_1 + \sigma_2 X + \ldots. + \sigma_v X^v$ has been found, we form

$$Z(X) = 1 + (S_1 + \sigma_1)X + (S_2 + \sigma_1 S_1 + \sigma_2)X^2 + \cdots + (S_v + \sigma_1 S_{v-1} + \cdots \sigma_{v-1} S_1 + \sigma_v)X^v \quad (8)$$

- Let $\sigma'(X) = \dfrac{d\sigma(X)}{dX}$

- Then the error value at location $\beta_l = \alpha^{j_l}$ is

$$e_{j_l} = \frac{Z(\beta_l^{-1})}{\beta_l^{-1}\sigma'(\beta_l^{-1})} = \frac{Z(\beta_l^{-1})}{\prod_{\substack{i=1 \\ i \neq l}}^{v} (1+\beta_i \beta_l^{-1})} \qquad (9)$$

Execution of the Iteration Process

- Note that $\sigma^{(1)}(X) = 1 + S_1 X$ satisfies the first Newton's identity.
- To carry out the iteration, we set up a table as below and fill out the table:

u	$\sigma^{(u)}(X)$	d_u	l_u	$u - l_u$
-1	1	1	0	-1
0	1	S_1	0	0
1	$1+S_1X$			
⋮				
$2t$				

Example 5: Consider (15, 9, 7) RS code with symbols from GF(2^4). The generator polynomial of this code is

$$g(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)$$
$$= \alpha^6 + \alpha^9 X + \alpha^6 X^2 + \alpha^4 X^3 + \alpha^{14} X^4 + \alpha^{10} X^5 + X^6$$

Let the all zero-vector be the transmitted code vector and let

$$\bar{r} = (0\ 0\ 0\ \alpha^7\ 0\ 0\ \alpha^3\ 0\ 0\ 0\ 0\ 0\ \alpha^4\ 0\ 0)$$

Thus,

$$r(X) = \alpha^7 X^3 + \alpha^3 X^6 + \alpha^4 X^{12}$$

Step 1. The syndrome components are computed as follows

$$S_1 = r(\alpha) = \alpha^{10} + \alpha^{9} + \alpha = \alpha^{12}$$

$$S_2 = r(\alpha^2) = \alpha^{13} + 1 + \alpha^{13} = 1$$

$$S_3 = r(\alpha^3) = \alpha + \alpha^{6} + \alpha^{10} = \alpha^{14}$$

$$S_4 = r(\alpha^4) = \alpha^{4} + \alpha^{12} + \alpha^{7} = \alpha^{10}$$

$$S_5 = r(\alpha^5) = \alpha^{7} + \alpha^{3} + \alpha^{4} = 0$$

$$S_6 = r(\alpha^6) = \alpha^{10} + \alpha^{9} + \alpha = \alpha^{12}$$

Step 2. To find the error-location polynomial $\sigma(X)$, we fill out the following table (mentioned in the BCH lecture), and $\sigma(X) = 1+\alpha^7X+\alpha^4X^2+\alpha^6X^3$

u	$\sigma^{(u)}(X)$	d_u	l_u	$u - l_u$
-1	1	1	0	-1
0	1	α^{12}	0	0 (take p = -1)
1	$1+ \alpha^{12} X$	α^7	1	0 (take p = 0)
2	$1+ \alpha^3X$	1	1	1 (take p = 0)
3	$1+ \alpha^3X+\alpha^3X^2$	α^7	2	1 (take p = 2)
4	$1+\alpha^4X+\alpha^{12}X^2$	α^{10}	2	2 (take p = 3)
5	$1+\alpha^4X+\alpha^3X^2+\alpha^{13}X^3$	α^{13}	3	2(take p = 4)
6	$1+\alpha^7X+\alpha^4X^2+\alpha^6X^3$	-	-	-

Step 3.

$$\sigma(\alpha^{3}) = 0 \qquad (\alpha^{3})^{-1} = \alpha^{12} = \beta_1$$

$$\sigma(\alpha^{9}) = 0 \quad \longrightarrow \quad (\alpha^{9})^{-1} = \alpha^{6} = \beta_2$$

$$\sigma(\alpha^{12}) = 0 \qquad (\alpha^{12})^{-1} = \alpha^{3} = \beta_3$$

errors occur at positions X^3, X^6, X^{12}.

Step 4. From (8) we find that

$$Z(X) = 1 + \alpha^{2} X + X^{2} + \alpha^{6} X^{3}$$

Using (9), we obtain the error values at locations X^3, X^6 and X^{12}:

$$e_3 = \frac{1+\alpha^2\alpha^{-3}+\alpha^{-6}+\alpha^6\alpha^{-9}}{(1+\alpha^6\alpha^{-3})(1+\alpha^{12}\alpha^{-3})} = \frac{\alpha^{13}}{\alpha^6} = \alpha^7$$

$$e_6 = \frac{1+\alpha^2\alpha^{-6}+\alpha^{-12}+\alpha^6\alpha^{-18}}{(1+\alpha^3\alpha^{-6})(1+\alpha^{12}\alpha^{-6})} = \frac{\alpha^{12}}{\alpha^9} = \alpha^3$$

$$e_{12} = \frac{1+\alpha^2\alpha^{-12}+\alpha^{-24}+\alpha^6\alpha^{-36}}{(1+\alpha^3\alpha^{-12})(1+\alpha^6\alpha^{-12})} = \frac{\alpha^9}{\alpha^5} = \alpha^4$$

Thus, the error pattern is

$$e(X) = \alpha^7 X^3 + \alpha^3 X^6 + \alpha^4 X^{12}$$

The decoding is completed by taking

$$v(X) = r(X) - e(X) = 0$$

Euclidean Decoding Algorithm

- Great Common Division (GCD):

$$Z_0(X) = \sigma(X)S(X) \bmod X^{2t}$$

where

$Z_0(X)$: error-value evaluator polynomial

$\sigma(X)$: error-location polynomial

$S(X)$: syndrome polynomial

Euclidean Decoding Algorithm

- Consider the product $\sigma(X)S(X)$,

$$\sigma(X)S(X) = (1+\sigma_1 X + \cdots + \sigma_v X^v)\cdot(S_1 + S_2 X + S_3 X^2 + \cdots)$$

$$= S_1 + (S_2 + \sigma_1 S_1)X + (S_3 + \sigma_1 S_2 + \sigma_2 S_1)X^2 + \cdots +$$

$$(S_{2t} + \sigma_1 S_{2t-1} + \cdots + \sigma_v S_{2t-v})X^{2t-1} + \cdots$$

- We define the other error-value evaluator polynomial $Z_0(X)$

$$Z_0(X) \triangleq \sigma(X)S(X) \bmod X^{2t}$$

$$\begin{aligned} Z_0(X) = {} & S_1 + (S_2 + \sigma_1 S_1)X + \\ & (S_3 + \sigma_1 S_2 + \sigma_2 S_1)X^2 + \cdots \\ & + (S_v + \sigma_1 S_{v-1} + \cdots + \sigma_{v-1} S_1)X^{v-1} \end{aligned} \quad (10)$$

- Why does the degree of $Z_0(X)$ be v-1 ?

- We know that the syndrome polynomial $S(X)$ is

$$S(X) \triangleq S_1 + S_2 X + \cdots + S_{2t} X^{2t-1} + \cdots$$

$$= \sum_{l=1}^{\infty} S_l X^{l-1} \qquad (11)$$

- Note that only the coefficients of the first 2t are known.

- Combining (1) and (11), we can put $S(X)$ in the following form:

$$
\begin{aligned}
S(X) &= \sum_{l=1}^{\infty} X^{l-1} \sum_{i=1}^{v} e_{j_i} \beta_i^l \\
&= \sum_{i=1}^{v} e_{j_i} \beta_i \sum_{l=1}^{\infty} (\beta_i X)^{l-1} \qquad (12) \\
&= \sum_{i=1}^{v} \frac{e_{j_i} \beta_i}{1 - \beta_i X}
\end{aligned}
$$

- From the definition of $Z_0(X)$, using (2) and (12), we obtain the following equation:

$$\begin{aligned}\sigma(X)S(X) &= \left\{\prod_{j=1}^{v}(1-\beta_j X)\right\}\cdot\left\{\sum_{i=1}^{v}\frac{e_{j_i}\beta_i}{1-\beta_i X}\right\} \\ &= \sum_{i=1}^{v} e_{j_i}\beta_i \prod_{j=1,\, j\neq i}^{v}(1-\beta_j X) \qquad (13) \\ &= Z_0(X)\end{aligned}$$

- Since for every i, there are exactly v-1 productions, therefore the degree of $Z_0(X)$ is v-1.

- The coefficients of the degree v to $2t$-1 in $Z_0(X)$ are zeros, which satisfy (5) and are call "Newton's identities".
- The error value e_{j_i} at location β_i is determined by

$$e_{j_i} = \frac{-Z_0(\beta_i^{-1})}{\sigma'(\beta_i^{-1})} \tag{14}$$

- A slightly different error-value evaluator shown in (8) is

$$Z(X) = \sigma(X) + XZ_0(X)$$

- We can express the definition of $Z_0(X)$, which is called the key equation in the following form:

$$\sigma(X)S(X) = Q(X)X^{2t} + Z_0(X)$$

- Rearrange the above equation, we have

$$Z_0(X) = -Q(X)X^{2t} + \sigma(X)S(X) \qquad (15)$$

- We see that (15) is exactly in the following form

$$\begin{aligned} Z_0(X) &= \mathrm{GCD}(X^{2t}, S(X)) \\ &= -Q(X)X^{2t} + \sigma(X)S(X) \end{aligned} \tag{16}$$

where GCD denotes the greatest common divisor.

- For example,

4 = GCD(112, 100)

4 = 100 – 8 × 12

= 100 – 8 × (112 – 100)

= -8 × 112 + 9 × 100

For example, $1 = \text{GCD}(X^6, X^3+1)$

$$= X^3 + X^3+1$$

$$= X^6 + X^3(X^3+1) +(X^3+1)$$

$$= X^6 + (X^3+1)(X^3+1)$$

- This decoding method is based on the Euclidean algorithm for finding the GCD. This suggests that $\sigma(X)$ and $Z_0(X)$ can be found by Euclidean iterative division algorithm in following form:

- At *i*-th step, we have

$$Z_0^{(i)}(X) = \gamma^{(i)}(X)X^{2t} + \sigma^{(i)}(X)S(X) \qquad (17)$$

and

$$Z_0^{(i)}(X) = Z_0^{(i-2)}(X) - q_i(X)Z_0^{(i-1)}(X)$$

$$\sigma^{(i)}(X) = \sigma^{(i-2)}(X) - q_i(X)\sigma^{(i-1)}(X)$$

$$\gamma^{(i)}(X) = \gamma^{(i-2)}(X) - q_i(X)\gamma^{(i-1)}(X)$$

With

$$Z_0^{(-1)}(X) = X^{2t}$$

$$Z_0^{(0)}(X) = S(X)$$

$$\gamma^{(-1)}(X) = \sigma^{(0)}(X) = 1$$

$$\gamma^{(0)}(X) = \sigma^{(-1)}(X) = 0$$

- To find $\sigma(X)$ and $Z_0(X)$, we carry out the iteration process given by (17) as follows: at the *i*-th step

1. We divided $Z_0^{(i-2)}(X)$ by $Z_0^{(i-1)}(X)$ to obtain the quotient $q_i(X)$ and the remainder $Z_0^{(i)}(X)$.
2. We find $\sigma^{(i)}(X)$ from

$$\sigma^{(i)}(X) = \sigma^{(i-2)}(X) - q_i(X)\sigma^{(i-1)}(X)$$

3. Iteration stops when we reach a step ρ for which

$$\deg(Z_0^{(\rho)}(X)) < \deg(\sigma^{(\rho)}(X)) \le t$$

4. Then $Z_0(X) = Z_0^{(\rho)}(X)$ and $\sigma(X) = \sigma_0^{(\rho)}(X)$

Execution of the Iteration Process

- The iteration process for finding $\sigma(X)$ and $Z_0(X)$ can be carried out by setting up filling the below table

i	$Z_0^{(i)}(X)$	$q_i(X)$	$\sigma_i(X)$
-1	X^{2t}	-	0
0	$S(X)$	-	1
1			
⋮			
ρ			

Example 6: Consider (15, 9, 7) RS code with symbols from GF(2^4). The generator polynomial of this code is

$$g(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)$$
$$= \alpha^6 + \alpha^9 X + \alpha^6 X^2 + \alpha^4 X^3 + \alpha^{14} X^4 + \alpha^{10} X^5 + X^6$$

Let the all zero-vector be the transmitted code vector and let

$$\bar{r} = (0\ 0\ 0\ \alpha^7\ 0\ 0\ 0\ 0\ 0\ 0\ \alpha^{11}\ 0\ 0\ 0\ 0)$$

Thus,

$$r(X) = \alpha^7 X^3 + \alpha^{11} X^{10}$$

The syndrome components are computed as follows

$$S_1 = r(\alpha) = \alpha^{10} + \alpha^{21} = \alpha^{7}$$

$$S_2 = r(\alpha^2) = \alpha^{13} + \alpha^{31} = \alpha^{12}$$

$$S_3 = r(\alpha^3) = \alpha^{16} + \alpha^{41} = \alpha^{6}$$

$$S_4 = r(\alpha^4) = \alpha^{19} + \alpha^{51} = \alpha^{12}$$

$$S_5 = r(\alpha^5) = \alpha^{7} + \alpha = \alpha^{14}$$

$$S_6 = r(\alpha^6) = \alpha^{10} + \alpha^{11} = \alpha^{14}$$

The syndrome polynomial is

$$S(X) = \alpha^7 + \alpha^{12} X + \alpha^6 X^2 + \alpha^{12} X^3 + \alpha^{14} X^4 + \alpha^{14} X^5$$

Using the Euclidean algorithm, we find

$$\sigma(X) = \alpha^{11} + \alpha^8 X + \alpha^9 X^2 = \alpha^{11}(1 + \alpha^{12} X + \alpha^{13} X^2)$$

and

$$Z_0(X) = \alpha^3 + \alpha^2 X$$

To find the error-location polynomial $\sigma(X)$, we fill out the following table

i	$Z_0^{(i)}(X)$	$q_i(X)$	$\sigma^{(i)}(X)$
-1	X^6	-	0
0	$S(X) = \alpha^7 + \alpha^{12} X + \alpha^6 X^2 + \alpha^{12} X^3 + \alpha^{14} X^4 + \alpha^{14} X^5$	-	1
1	$\alpha^8 + \alpha^3 X + \alpha^5 X^2 + \alpha^5 X^3 + \alpha^6 X^4$	$\alpha + \alpha \ X$	$\alpha + \alpha \ X$
2	$\alpha^3 + \alpha^2 X$	$\alpha^{11} + \alpha^8 X$	$\alpha^{11} + \alpha^8 X + \alpha^9 X^2$

$$Z_0^{(i)}(X) = Z_0^{(i-2)}(X) - q_i(X) Z_0^{(i-1)}(X)$$

$$\sigma^{(i)}(X) = \sigma^{(i-2)}(X) - q_i(X) \sigma^{(i-1)}(X)$$

- Step 1 (i = 1):

$$Z_0^{(-1)}(X) = q_1(X) Z_0^{(0)}(X) + Z_0^{(1)}(X)$$

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

$$\sigma^{(1)}(X) = \sigma^{(-1)}(X) - q_1(X)\sigma^{(0)}(X)$$

$$\sigma^{(1)}(X) = 0 - (\alpha + \alpha X)\cdot 1 = \alpha + \alpha X$$

- Step 2:

$$Z_0^{(0)}(X) = q_2(X)Z_0^{(1)}(X) + Z_0^{(2)}(X)$$

$$\alpha^7 + \alpha^{12}X + \alpha^6X^2 + \alpha^{12}X^3 + \alpha^{14}X^4 + \alpha^{14}X^5 =$$

$$(\alpha^{11} + \alpha^8X)(\alpha^8 + \alpha^3X + \alpha^5X^2 + \alpha^5X^3 + \alpha^6X^4)$$

$$+\alpha^3 + \alpha^2X$$

$\longrightarrow$ $$Z_0(X) = \alpha^3 + \alpha^2X$$

$$\sigma^{(2)}(X) = \sigma^{(0)}(X) - q_2(X)\sigma^{(1)}(X)$$

$$\sigma^{(1)}(X) = 1 - (\alpha + \alpha X)\cdot(\alpha^{11} + \alpha^{8} X)$$
$$= 1 + \alpha^{12} + (\alpha^{9} + \alpha^{12})X + \alpha^{9} X^{2}$$
$$= \alpha^{11} + \alpha^{8} X + \alpha^{9} X^{2}$$
$$= \sigma(X)$$

$$\longrightarrow \quad \sigma(X) = \alpha^{11} + \alpha^{8} X + \alpha^{9} X^{2}$$

$$\sigma'(X) = \frac{d\sigma(X)}{dX}$$
$$= \alpha^{8}$$

From $\sigma(X)$, we find that the roots are α^5 and α^{12}.
Hence, the error location number are α^{10} and α^3.
The error values at these locations are

$$e_3 = \frac{-Z_0(\alpha^{-3})}{\sigma'(\alpha^{-3})} = \frac{\alpha^3 + \alpha^2\alpha^{-3}}{\alpha^8} = \frac{1}{\alpha^8} = \alpha^7$$

$$e_{10} = \frac{-Z_0(\alpha^{-10})}{\sigma'(\alpha^{-10})} = \frac{\alpha^3 + \alpha^2\alpha^{-10}}{\alpha^8} = \frac{\alpha^4}{\alpha^8} = \alpha^{11}$$

Therefore, the error polynomial is

$$e(X) = \alpha^7 X^3 + \alpha^{11} X^{10}$$

And the decoded codeword $v(X)$ is given by

$$v(X) = r(X) - e(X) = 0$$

Frequency-Domain Decoding Algorithm

- $$r(X) = v(X) + e(X)$$

  $\big\downarrow$ **DFT**

  $$R(X) = V(X) + E(X)$$

  $$\overline{E} = (E_0, E_1, \cdots E_{n-1})$$

  $$S_j = r(\alpha^j) = E_j = R_j \quad \text{for } 0 \le j \le 2t$$

For t+1 ≤ *l* ≤ n - 1 - t

$$E_{l+t} = -(\sigma_1 E_{l+t-1} + \cdots + \sigma_v E_{l+t-v})$$

$$E_0 = -\frac{1}{\sigma_v}(E_v + \cdots + \sigma_{v-1} E_1)$$

- **Once we obtain**

$$E(X) \xrightarrow{\textbf{IDFT}} e(X)$$

Frequency-Domain Decoding Algorithm

- Let $V(X) = V_0 + V_1X + \dots + V_{n-1}X^{n-1}$ over GF(2^m) be the Galois field Fourier transform of $v(X) = v_0 + v_1X + \dots + v_{n-1}X^{n-1}$. Then

$$V_j = v(\alpha_j) = \sum_{i=0}^{n-1} v_i \alpha^{ij} \qquad (18)$$

$$v_i = V(\alpha^{-i}) = \sum_{j=0}^{n-1} V_j \alpha^{-ij} \qquad (19)$$

- The product of $a(X)$ and $b(X)$ is defined as follows

$$a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

$$b(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}$$

$$\begin{aligned} C(X) &\overset{\Delta}{=} a(X)b(X) \\ &= a_0 b_0 + a_1 b_1 X + a_2 b_2 X^2 + \cdots + a_{n-1} b_{n-1} X^{n-1} \\ &= c_0 + c_1 X + c_2 X_2 + \cdots + c_{n-1} X^{n-1} \end{aligned}$$

- Let the Fourier transform of a(X) and b(X) are given by

$$A(X) = A_0 + A_1 X + \cdots + A_{n-1} X^{n-1}$$

$$B(X) = B_0 + B_1 X + \cdots + B_{n-1} X^{n-1}$$

- The Fourier transform of c(*X*) is given by

$$C(X) = C_0 + C_1 X + \cdots + C_{n-1} X^{n-1}$$

where

$$C_j = \sum_{k=0}^{n-1} A_k B_{j-k} \qquad (20)$$

- Let v(X) and e(X) be the transmitted code polynomial and the error polynomial, and the received sequence $r(X)$ is denoted as follows

$$r(X) = v(X) + e(X)$$

- The Fourier transform of $r(X)$ is given by

$$R(X) = V(X) + E(X) \qquad (21)$$

where $V(X)$ and $E(X)$ are the Fourier transform of v(X) and r(X), respectively.

- Because $v(X)$ is a code polynomial that has α, α^2, … α^{2t} as roots, then

$$V_j = 0, \quad \text{for } 0 \le j \le 2t$$

- From (21), we find that for $0 \le j \le 2t$

$$R_j = E_j$$

- Let $S = (S_1, S_2, \ldots, S_{2t})$ be the syndrome of $r(X)$. Then for $0 < j \le 2t$,

$$S_j = r(\alpha^j) = E_j = R_j$$

- Suppose there are $v \le t$ errors, and

$$e(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} + \cdots e_{j_v} X^{j_v}$$

the error-location numbers are then $\alpha^{j_1}, \alpha^{j_2}, \cdots, \alpha^{j_v}$

- The error-location polynomial over GF(2^m) is

$$\sigma(X) = (1-\alpha^{j_1} X)(1-\alpha^{j_2} X)\cdots(1-\alpha^{j_v} X)$$

$$= 1 + \sigma_1 X + \cdots \sigma_v X^v$$

which has $\alpha^{-j_1}, \alpha^{-j_2}, \cdots, \alpha^{-j_v}$ as roots. Hence,

$$\sigma(\alpha^{-j_i}) = 0, \quad \text{for } 1 \le i \le v \qquad (22)$$

- We may regard $\sigma(X)$ as the Fourier transform of a polynomial over GF(2)

$$\lambda(X) = \lambda_0 + \lambda_1 X + \cdots + \lambda_{n-1} X^{n-1}$$

where

$$\lambda_j = \sigma(\alpha^{-j}), \quad \text{for } 0 \le j \le n\text{-}1 \qquad (23)$$

- From (22) and (23), we readily see that

$$\lambda(X)e(X) = 0 \qquad (24)$$

- That is,

$$\lambda_j \cdot e_j = 0, \quad \text{for} \;\; 0 \le j \le n-1 \qquad (25)$$

- Taking the Fourier transform of $\lambda(X)e(X)$ and using (20), we have

$$\sum_{k=0}^{n-1} \sigma_k E_{j-k} = 0, \quad \text{for} \;\; 0 \le j \le n-1 \quad (26)$$

- Since the degree of $\sigma(X)$ is v, that is $\sigma_k = 0$ for $k > v$.
- Then

$$E_j + \sigma_1 E_{j-1} + \cdots + \sigma_v E_{j-v} = 0 \qquad (27)$$

- The preceding equation can be put in the following form: for $0 \le j \le n$-1

$$E_j = -(\sigma_1 E_{j-1} + \cdots + \sigma_v E_{j-v}) \qquad (28)$$

- Since E_1, E_2,… E_{2t} are already known, it follows from (28) that for $t+1 \le l \le n-1-t$, we obtain the following recursive equation for computing E_0 and E_{2t+1} to E_{n-1}.

$$E_{l+t} = -(\sigma_1 E_{l+t-1} + \cdots + \sigma_v E_{l+t-v})$$
$$E_0 = -\frac{1}{\sigma_v}(E_v + \cdots + \sigma_{v-1} E_1) \qquad (29)$$

- The decoding consists of the following steps:

  1) Take the Fourier transform $R(X)$ of $r(X)$.

  2) Find $\sigma(X)$ (use the Berlekamp-Massy algorithm)

  3) Compute $E(X)$.

  4) Take the inverse transform $v(X)$ of $V(\mathrm{X}) = R(X) - E(X)$.

Example 7: Consider (15, 9, 7) RS code with symbols from GF(2^4). $r(X) = \alpha^7 X^3 + \alpha^3 X^6 + \alpha^4 X^{12}$ is received. The Fourier transform of $r(X)$ is

$$R(X) = \alpha^{12} X + X^2 + \alpha^{14} X^3 + \alpha^{10} X^4 + \alpha^{12} X^6 + X^7 + \alpha^{14} X^8 + \alpha^{10} X^9 + \alpha^{12} X^{11} + X^{12} + \alpha^{14} X^{13} + \alpha^{10} X^{14}$$

The syndrome components: $S_1 = \alpha^{12}$, $S_2 = 1$, $S_3 = \alpha^{14}$, $S_4 = \alpha^{10}$, $S_5 = 0$, $S_6 = \alpha^{12}$. They are also the spectral components E_1 to E_6.

Using the Berlekamp-Massy algorithm based on the syndrome (S_1, S_2, …, S_6), we find the error-location polynomial

$$\sigma(X) = 1 + \alpha^7 X + \alpha^4 X^2 + \alpha^6 X^3$$

From (29), for $4 \le l \le 11$, we obtain the following recursion equation for computing E_7 to E_{14} and E_0:

$$\begin{aligned} E_{l+3} &= \sigma_1 E_{l+2} + \sigma_2 E_{l+1} + \sigma_3 E_l \\ &= \alpha^7 E_{l+2} + \alpha^4 E_{l+1} + \alpha^6 E_l \end{aligned}$$

$$E_0 = \frac{1}{\sigma_3}(E_3 + \sigma_1 E_2 + \sigma_2 E_1)$$
$$= \alpha^{-6}(E_3 + \alpha^7 E_2 + \alpha^4 E_1)$$
$$= 0$$

The resultant error spectral polynomial is

$$E(X) = \alpha^{12} X + X^2 + \alpha^{14} X^3 + \alpha^{10} X^4 + \alpha^{12} X^6$$
$$+ X^7 + \alpha^{14} X^8 + \alpha^{10} X^9 + \alpha^{12} X^{11} + X^{12}$$
$$+ \alpha^{14} X^{13} + \alpha^{10} X^{14}$$

We find that $R(X) = E(X)$, and $V(X) = 0$. Therefore, the decoded codeword is that all-zero codeword. The inverse transform of $E(X)$ is $e(X) = \alpha^7 X^3 + \alpha^3 X^6 + \alpha^4 X^{12}$.

The Step-By-Step Decoding

- Trial and Error:

$$\bar{r} = (r_0, r_1, r_2, \cdots, r_{n-1})$$

↑ *test it error*

$$+\beta$$

$$\beta \in \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$$

$$|M_v^{(0)}| = \det\begin{bmatrix} S_1 & S_2 & \cdots & S_v \\ S_2 & S_3 & \cdots & S_{v+1} \\ & \vdots & & \\ S_v & S_{v+1} & \cdots & S_{2v-1} \end{bmatrix} \neq 0$$

$$|M_v^{'}| = \det\begin{bmatrix} S_1^{'} & S_2^{'} & \cdots & S_v^{'} \\ S_2^{'} & S_3^{'} & \cdots & S_v^{'} \\ & \vdots & & \\ S_v^{'} & S_{v+1}^{'} & \cdots & S_{2v-1}^{'} \end{bmatrix} = 0 \quad \textbf{?}$$

The Step-By-Step Decoding

- In this decoding, we do not find the error-location polynomial. Instead, we use the concept of the error-trapping decoding.
- From (6), we define the syndrome matrix as following:

$$M_v^{(0)} = \begin{bmatrix} S_1 & S_2 & \cdots & S_v \\ S_2 & S_3 & \cdots & S_{v+1} \\ & \vdots & & \\ S_v & S_{v+1} & \cdots & S_{2v-1} \end{bmatrix} \qquad (30)$$

and $\overline{S} = (S_1, S_2, \cdots, S_{2t})$

- Theorem 4: For any binary BCH (n, k, t) code, and any v such that $1 \le v \le t$, the v by v syndrome matrix is singular if the number of errors is at most v-1, and is nonsingular if the number of errors is at least v .
- The decision vector is defined

$$\overline{m} = (m_1, m_2, \cdots, m_t)$$

where decision bit m_v is calculated as

$$m_v = 0 \qquad \text{if } \det(M_v) = 0$$
$$m_v = 1 \qquad \text{if } \det(M_v) \neq 0$$

- The decision vector of a general *t*-error-correcting RS code can be determined as follows:

(1)if there are no errors, then

$$\overline{m} = (0,0,\cdots,0) = (0^t)$$

(2)if there is one error, then

$$\overline{m} = (1,0,\cdots,0) = (1,0^{t-1})$$

(3)if there are *v* errors, then

$$\overline{m} \in \{(X^{v-2},1,1,0^{t-v})\}$$

where the symbol *X* can be 0 or 1.

(4)if there are no less than *t* errors, then

$$\overline{m} \in \{(X^{v-2},1,1)\}$$

- For example, 2-error-correcting RS codes, the decision vector could be (0, 0) for no errors, (1, 0) for single error, and (1, 1) for two errors.
- Let $\bar{v}$ be codeword of a RS code, and $\bar{v}^{(p)}$ is also a codeword, which denotes the cyclically shifting p places to the right of $\bar{v}$. That is

$$\bar{v} = (v_0, v_1, \cdots, v_{n-1})$$

$$\bar{v}^{(p)} = (v_{n-p}, v_{n-p+1}, \cdots v_{n-1}, v_0, \cdots, v_{n-p-1})$$

- For $p > 0$, $\bar{r}^{(p)}$ is obtained by cyclically shifting p places to the right of $\bar{r}$.
- The syndrome matrix for $\bar{r}^{(p)} + \beta$ is defined as follows:

$$M_v^{(p)} = \begin{bmatrix} S_1^{(p)} + \beta & S_2^{(p)} + \beta & \cdots & S_v^{(p)} + \beta \\ S_2^{(p)} + \beta & S_3^{(p)} + \beta & \cdots & S_{v+1}^{(p)} + \beta \\ & \vdots & & \\ S_v^{(p)} + \beta & S_{v+1}^{(p)} + \beta & \cdots & S_{2v-1}^{(p)} + \beta \end{bmatrix} \quad (31)$$

- The step-by-step decoding is iterative, which contains the follow steps

(1) calculate syndrome vector, and find v such that

$\det(M_v^{(0)}) = 1$, and set $j = 0$.

(2) cyclically shift $\bar{r}$ one symbol one time, and find its corresponding syndrome vector.

(3) let $\beta = \alpha^j$, and check whether $\det(M_v^{(p)}) = 0$.

(4) If $\det(M_v^{(p)}) = 0$, then $r^{(p)}(X) = r^{(p)}(X) + \beta$.

(5) Otherwise, $j = j+1$, do Step (2) again.

Example 8: Consider 2-error-correcting (7,3) RS code over GF(2^3) The generator polynomial is

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

Suppose the all-zero vector is transmitted. And the received sequence is

$$\bar{r} = (0\,0\,0\,0\,0\,\alpha\,\alpha^5)$$

$$r(X) = \alpha X^5 + \alpha^5 X^6$$

$$S_1^{(0)} = r(\alpha) = \alpha\alpha^5 + \alpha^5\alpha^6 = \alpha^3$$

$$S_2^{(0)} = r(\alpha^2) = \alpha(\alpha^2)^5 + \alpha^5(\alpha^2)^6 = \alpha^6$$

$$S_3^{(0)} = r(\alpha^3) = \alpha(\alpha^3)^5 + \alpha^5(\alpha^3)^6 = 0$$

$$S_4^{(0)} = r(\alpha^4) = \alpha(\alpha^4)^5 + \alpha^5(\alpha^4)^6 = \alpha^3$$

$$\det(M_2^{(0)}) = \det\left(\begin{bmatrix} S_1^{(0)} & S_2^{(0)} \\ S_2^{(0)} & S_3^{(0)} \end{bmatrix}\right) = \det\left(\begin{bmatrix} \alpha^3 & \alpha^6 \\ \alpha^6 & 0 \end{bmatrix}\right)$$

$$= \alpha^5$$

which implies there are at least two errors in the received sequence

Cyclically shift $r(X)$ one time, $r^{(1)}(X)=\alpha^5+\alpha X^6$ is obtain. And the corresponding syndrome is given by

$$S_1^{(1)}=r^{(1)}(\alpha)=\alpha^5+\alpha\alpha^6=\alpha^5+1=\alpha^4$$

$$S_2^{(1)}=r^{(1)}(\alpha^2)=\alpha$$

$$S_3^{(1)}=r^{(1)}(\alpha^3)=0$$

$$\det(M_2^{(1)})=\det(\begin{bmatrix} S_1^{(1)}+\beta & S_2^{(1)}+\beta \\ S_2^{(1)}+\beta & S_3^{(1)}+\beta \end{bmatrix})$$

$$=\det(\begin{bmatrix} \alpha^4+\beta & \alpha+\beta \\ \alpha+\beta & \beta \end{bmatrix})$$

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

As $\beta = \alpha^5$, then $\det(M_2^{(1)}) = 0$. The modified cyclical received polynomial is

$$r^{(1)}(X) = r^{(1)}(X) + \beta = \alpha X^6$$

After the 2nd time cyclical shift, $r^{(2)}(X) = \alpha$ is obtained. The syndrome is given by

$$\begin{aligned} S_1^{(2)} &= r^{(2)}(\alpha) = \alpha \\ &= S_2^{(2)} \\ &= S_3^{(2)} \end{aligned}$$

$$\det(M_2^{(2)}) = \det\left(\begin{bmatrix} S_1^{(2)}+\beta & S_2^{(2)}+\beta \\ S_2^{(2)}+\beta & S_3^{(2)}+\beta \end{bmatrix}\right)$$

$$= \det\left(\begin{bmatrix} \alpha+\beta & \alpha+\beta \\ \alpha+\beta & \alpha+\beta \end{bmatrix}\right)$$

$$= 0 \qquad \text{(at most 1 error)}$$

$$\det(M_1^{(2)}) = S_1^{(2)} + \beta = \alpha + \beta \text{ (at least 1 error)}$$

From two preceding equation, there is still one error in the received sequence.

As β = α, then $\det(M_1^{(2)}) = 0$. The modified cyclical polynomial is given by

$$r^{(2)}(X) = r^{(2)}(X) + \beta = 0$$

Therefore, the corrected received polynomial is

$$r(X) = 0.$$

- In fact, the step-by-step decoding can be easily modified as a parallel decoding.
- Without cyclical shift, the received symbols r_{n-1}, r_{n-2}, … ,r_{n-k} are checked in parallel. That is, only one received symbols is changed in a corresponding decoding procedure by checking if $\det(M_v) = 0$.
- For RS codes with a few error-correcting capability, this parallel decoding is feasible.

6. Modified RS Codes

- Punctured Reed-Solomon codes:

In Theorem 3, it was shown that any combination of k symbols in an (n, k) RS code can be treated as message positions in a systematic representation.

An (n, k) RS code is thus punctured by deleting any one of its parity check symbols. The resulting $(n\text{-}1, k)$ code is, in general, no longer cyclic, but it is MDS.

- Shortened RS codes:

A code is shortened by deleting a message symbol from the encoding process. This resulting $(n\text{-}1, k\text{-}1)$ code is a shortened RS code, which is not cyclic, but it is MDS.

Example 9: These two (32, 28, 5) and (28, 24, 5) RS codes are employed in the audio CD system. Since each symbol is 8 bits, therefore these two RS codes are shorten from the (255, 251, 5) by deleting 223 and 227 information symbols.

(255, 251, 5) RS code → delete 223 info. symbols → (32, 28, 5) RS code

(255, 251, 5) RS code → delete 227 info. symbols → (28, 24, 5) RS code

• Extended RS codes: Any code can be extended multiple times through the addition of parity check symbols.

(1) Singly-extended RS code codes:

An (n, k) RS code can be extended to form a noncyclic (n+1, k) MDS code by adding a parity check. Each codeword $(c_0, c_1, \cdots, c_{n-1})$ thus becomes $(c'_0, c'_1, \cdots, c'_n)$, where

$$c'_j = c_j, \quad \text{for } 0 \le j \le n\text{-}1$$

$$c'_n = -\sum_{j=0}^{n-1} c_j$$

The corresponding parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} & 0 \\ 1 & \alpha^2 & \alpha^{2\times 2} & \alpha^{2\times 3} & \cdots & \alpha^{2(n-1)} & 0 \\ 1 & \alpha^3 & \alpha^{3\times 2} & \alpha^{3\times 3} & \cdots & \alpha^{3(n-1)} & 0 \\ \vdots & & & & \cdots & \vdots & 0 \\ 1 & \alpha^{2t} & \alpha^{2t\times 2} & \alpha^{2t\times 3} & \cdots & \alpha^{2t(n-1)} & 0 \end{bmatrix}$$

(2) Doubly-extended RS code codes:

An (n, k) RS code can be extended to form a no cyclic (n+2, k) MDS code by adding two parity checks. Each codeword $(c_0, c_1, \cdots, c_{n-1})$ thus becomes $(c'_0, c'_1, \cdots, c'_{n+1})$, where

$$c'_j = c_j, \quad \text{for } 0 \le j \le n\text{-}1$$

$$c'_n = -\sum_{j=0}^{n-1} c_j$$

$$c'_{n+1} = -\sum_{j=0}^{n-1} c_j \alpha^{j(2t+1)}$$

The corresponding parity check matrix is

$$H=\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} & 0 & 0 \\ 1 & \alpha^2 & \alpha^{2\times 2} & \alpha^{2\times 3} & \cdots & \alpha^{2(n-1)} & 0 & 0 \\ 1 & \alpha^3 & \alpha^{3\times 2} & \alpha^{3\times 3} & \cdots & \alpha^{3(n-1)} & 0 & 0 \\ \vdots & & & & \cdots & \vdots & 0 & 0 \\ 1 & \alpha^{2t} & \alpha^{2t\times 2} & \alpha^{2t\times 3} & \cdots & \alpha^{2t(n-1)} & 0 & 0 \\ 1 & \alpha^{2t+1} & \alpha^{(2t+1)\times 2} & \alpha^{(2t+1)\times 3} & \cdots & \alpha^{(2t+1)(n-1)} & 0 & 1 \end{bmatrix}$$

7. Error Correcting Performance

- There are 3 figures shown in the following for comparison of error correcting performance of Reed-Solomon codes.
- In generally, the error performance of a shorten RS code is better than that of a corresponding RS code, which results from that at the same signal-to-noise ratio and error correcting capability, the number of errors in a shorter code is less than in a longer code.

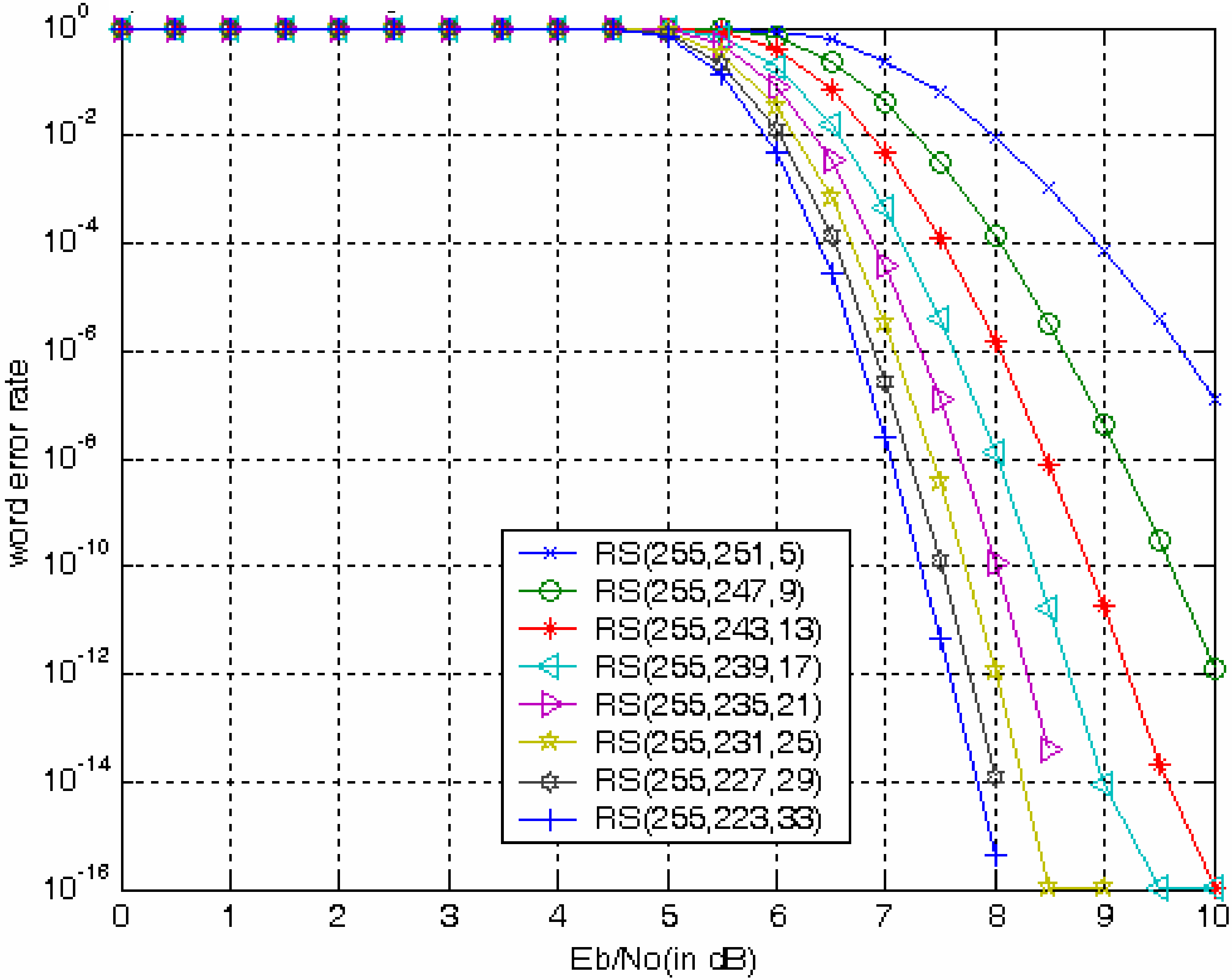


Figure 3: Comparison of error correcting for RS codes

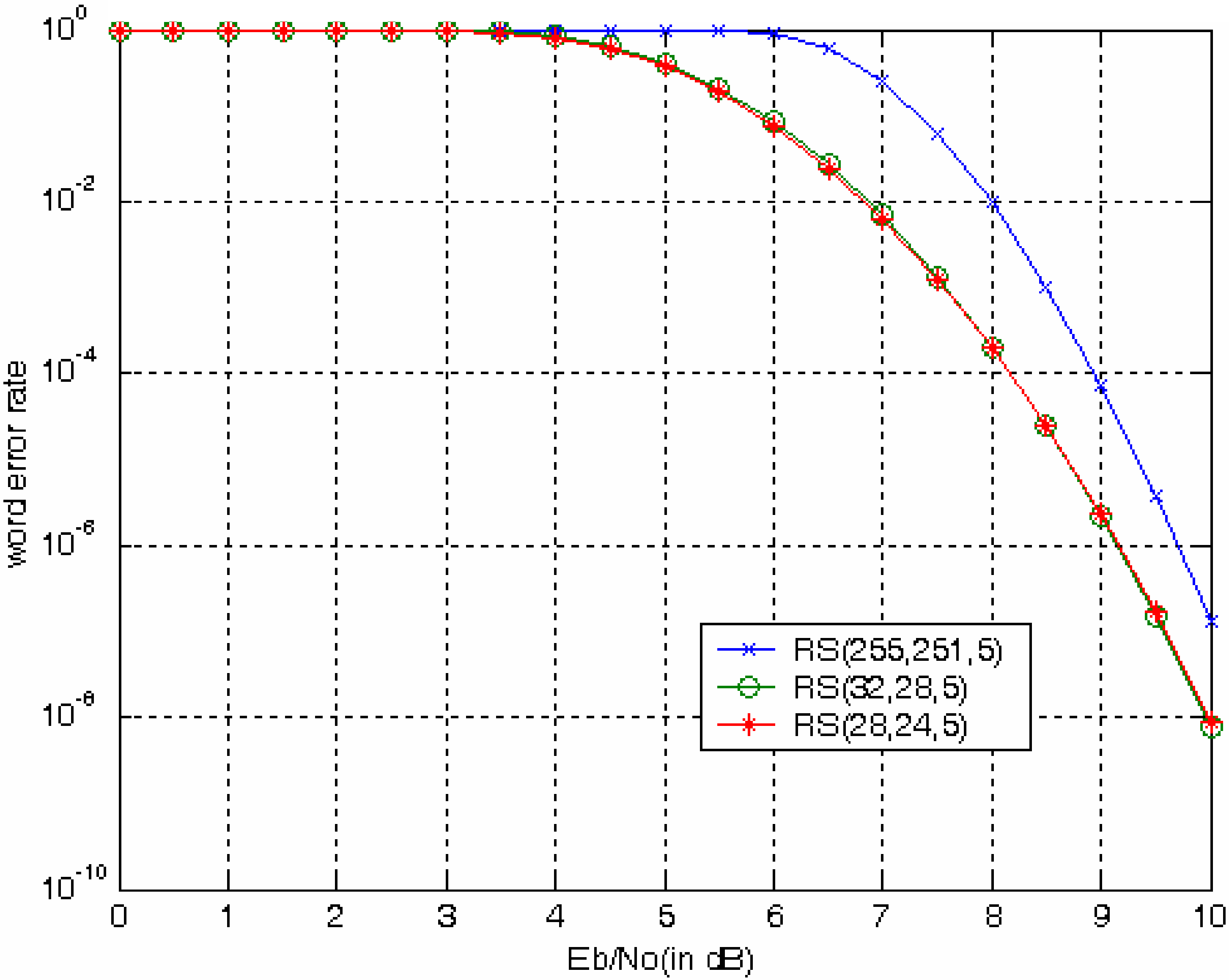


Figure 4: Comparison of error correcting for RS codes

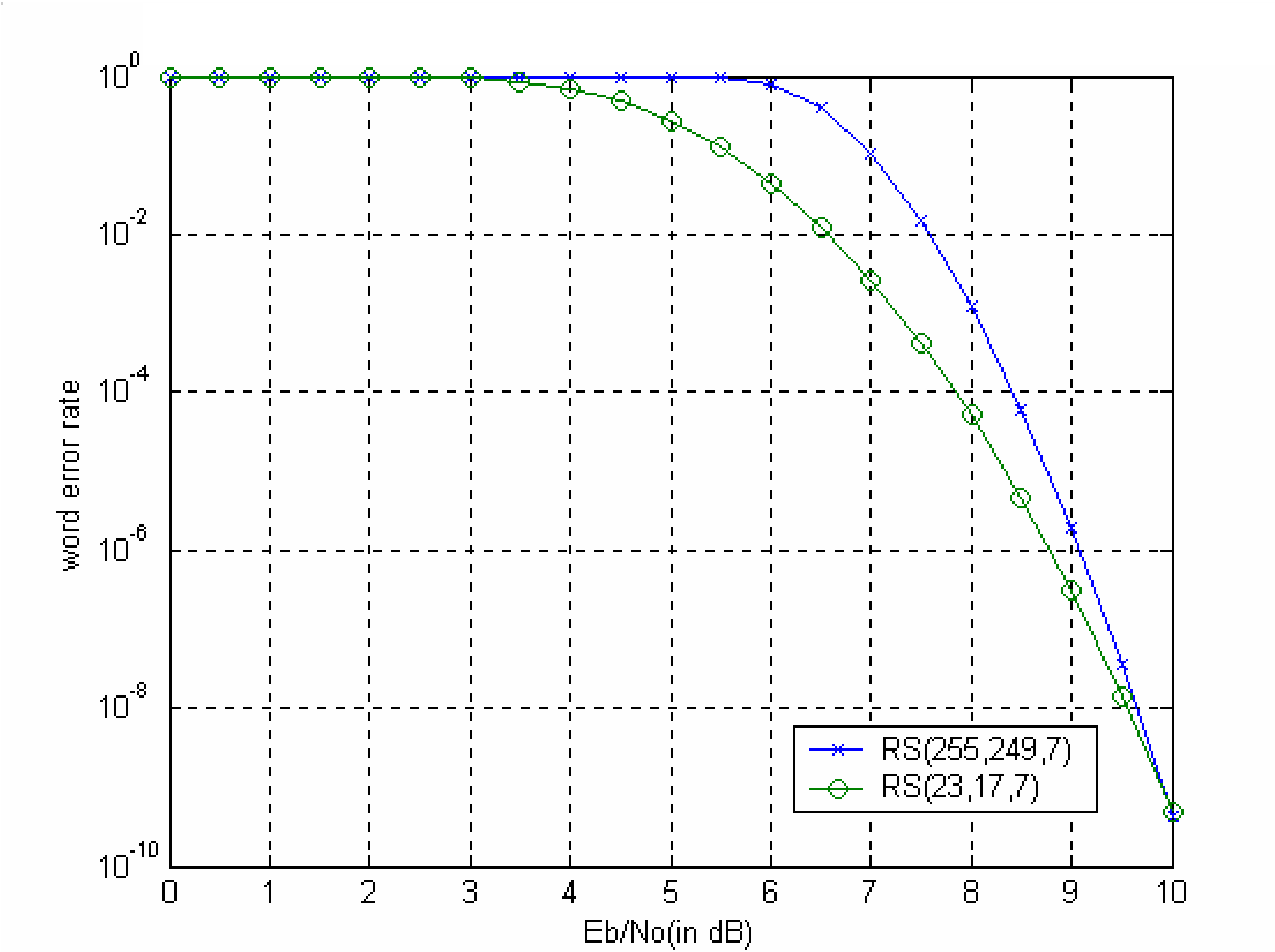


Figure 5: Comparison of error correcting for RS codes

8. Reference

[1]Shu Lin, and Daniel J Costello, Jr., Error Control Coding, Prentice hall, 2nd edition, 2004.

[2]Stephen B. Wicker, Error Control Systems for Digital Communication and Storage, Prentice hall, 1995.

[3]Peterson, W. W. and Weldon, E. J., Error-Control Codes, MIT press, Cambridge, 2nd edition, 1972.

[4]Massy, J. L, “Step-by-Step Decoding of Bose-Chauhuri-Hocquenghem codes,” IEEE Trans. Inf. Theory, IT-11, No. 4, pp.580-585, Nov., 1965.

[5]S.-W. Wei. and C-H. Wei, “High-Speed Decoder of Reed-Solomon Codes,” IEEE Trans. Comm, Vol. 41, No.11, Nov. 1993.

[6]T.-C. Chen; C.-H. Wei and S.-W. Wei, “Step-by-step decoding algorithm for Reed-Solomon codes,” IEE Proc.-Commun., Vol. 147, No.1, Feb. 2000.

[7]Masakatu Morii, and Masao Kasahara, “Generalized key-equation of remainder decoding algorithm for Reed-Solomon codes,” IEEE Trans. Inf. Theory, Vol. 38, No.6, pp. 1801-1807, Nov. 1992, .

[8]S. V. Fedorenko, “A simple algorithm for decoding Reed-Solomon codes and its relation to the Welch-Berlekamp algorithm,” IEEE Trans. Inf. Theory, Vol. 51, No.3, pp. 1196-1198, March. 2005.

[9]R. Koetter, and A. Vardy, “Algebraic Soft-Decision Decoding of Reed–Solomon Codes,” IEEE Trans. Inf. Theory, Vol. 49, No.11, pp.2809-2825, Nov. 2003.