Lecture 7

Reed-Solomon Codes

The most important and most widely used class of q-ary codes is the class of Reed-Solomon (RS) codes. RS codes were discovered in 1960, the same year as the discovery of binary BCH codes. In their original form, RS codes are not cyclic. When put in cyclic form, they form a very special subclass of q-ary BCH codes. For an RS code, the symbol field and construction field are the same. RS codes are effective for combating mixed types of noise and interferences. They are widely used in both communication and storage systems. In this lecture, we present RS codes in cyclic form and commonly used decoding algorithms.

7.1 Introduction

- For any q that is a power of a prime and any t with $1 \leq t < q$, there exists an RS code over GF(q) with the following parameters:

Length:	$q - 1,$
Dimension:	$q - 2t - 1,$
Number of parity-check symbols:	$n - k = 2t,$
Minimum distance:	$d_{\min} = 2t + 1.$

- Such an RS code called a $(q-1, q-2t-1, 2t+1)$ RS code over GF(q) (or a q-ay $(q-1, q-2t-1, 2t+1)$ RS code). This RS code is capable of correcting any error pattern with t or fewer random symbol errors. It can also correct random bursts of symbol errors or erasures.
- **Special characteristics:**
  1. The code length $q-1$ is one less than the size q of the code alphabet GF(q).
  2. The minimum distance $2t+1$ is equal to the number $2t$ of parity-check symbols plus one. Codes with this distance property are referred to as maximum distance separable (MDS) codes.
- **Example 7.1:** Two widely used RS codes are the $(255, 239,$

17) and (255, 223, 33) RS codes with symbols from GF(2^8). The first code is capable of correcting any combination of 8 or fewer random symbol errors. It is a standard code for optical communications, data storage and hard-disc drives. The second code is the NASA standard code for deep space, satellite communications and other missions. The code is capable of correcting 16 and fewer random symbol errors. The symbol and block (or word) error performances of these two codes are shown in Figure 7.1.

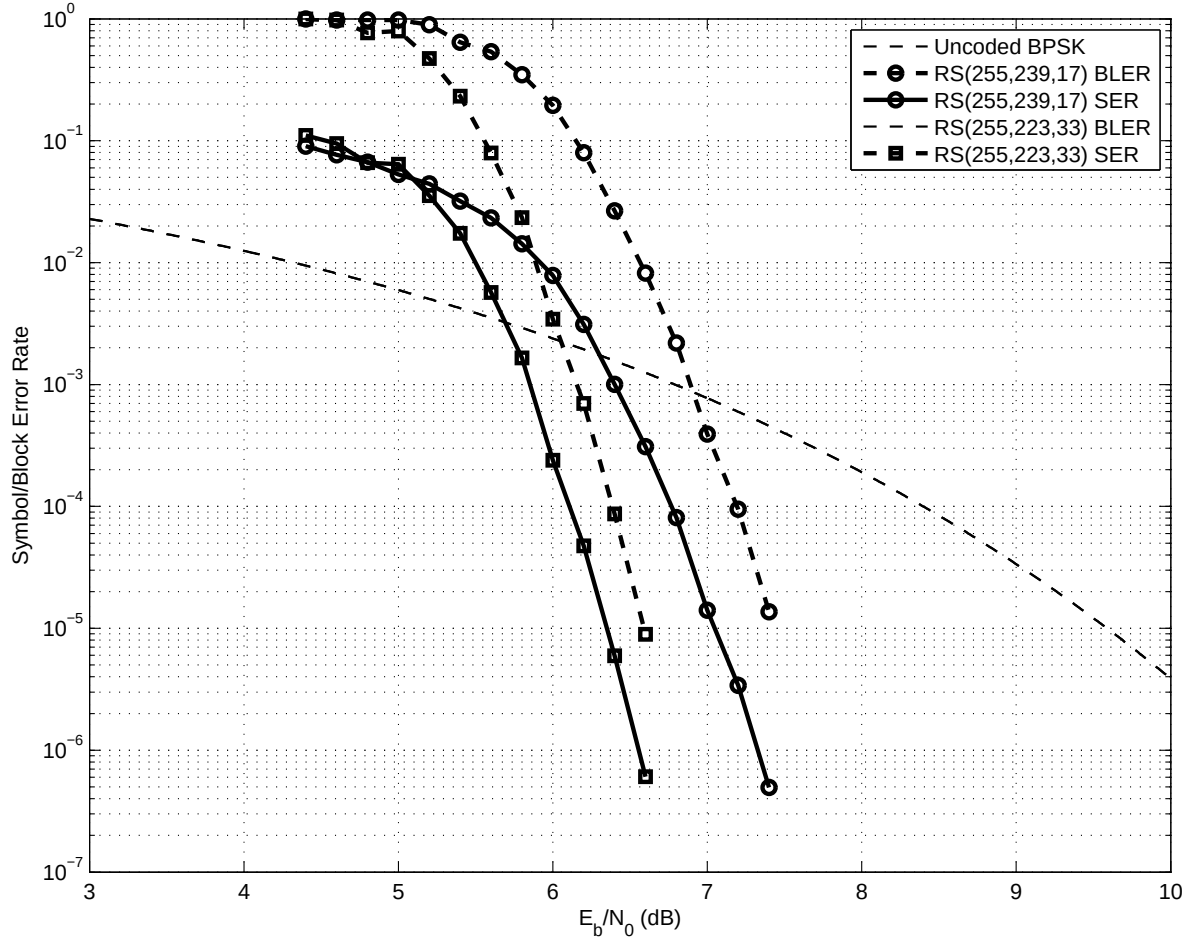

Figure 7.1: Error performances of the (255, 239, 17) and (255, 223, 33) RS codes over GF(2^8).

7.2 Code Characterization

- Let α be a primitive element of GF(q).
- The generator polynomial $\mathbf{g}(X)$ of the t-symbol-error-correcting $(q-1, q-2t-1, 2t+1)$ cyclic RS code $\mathcal{C}_{rs,t}$ over GF(q) has

$$\alpha, \alpha^2, \ldots, \alpha^{2t}$$

as roots.

- Since $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are elements of GF(q), their minimal polynomials over GF(q) are simply $X-\alpha, X-\alpha^2, \ldots, X-\alpha^{2t}$, respectively. Hence

$$\begin{aligned} \mathbf{g}(X) &= (X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{2t}) \\ &= g_0 + g_1 X + \cdots + g_{2t-1}X^{2t-1} + X^{2t}, \end{aligned} \tag{7.1}$$

  with $g_i \in$GF(q) for $0 \leq i < 2t$ and $g_{2t} = 1$.

- Since $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are roots of $X^{q-1}-1$, $\mathbf{g}(X)$ divides $X^{q-1}-1$. Therefore, $\mathbf{g}(X)$ generates a cyclic RS code of length $q-1$ with $2t$ parity-check symbols.

- Actually, RS codes form a **special subclass** of q-ary BCH codes with $m = 1$. However, since they were discovered independently and before q-ary BCH codes and are much

more important than other q-ary BCH codes in practical applications, we consider them as an independent class of q-ary codes.

- The BCH bound gives the minimum distance (or minimum weight) of the q-ary RS code $\mathcal{C}_{rs,t}$ of length $q-1$ generated by the polynomial $\mathbf{g}(X)$ given by (7.1) at least $2t+1$. Every none zero code polynomial in $\mathcal{C}_{rs,t}$ has at least $2t+1$ **nonzero terms** (or weight at least $2t+1$).
- Note that the generator polynomial $\mathbf{g}(X)$ is a code polynomial with exactly $2t+1$ terms. None of these $2t+1$ terms can have zero coefficient, otherwise, $\mathbf{g}(X)$ would have weight less than $2t+1$ which contradicts the BCH bound. Hence, $\mathbf{g}(X)$ is a code polynomial with weight exactly

$2t + 1$. As a result, the minimum distance of the RS code $\mathcal{C}_{rs,t}$ is exactly $2t + 1$.

- In all practical applications of RS codes in digital communication or data storage systems, q is commonly chosen as a **power** of 2, say $q = 2^s$, and the code symbols are from GF(2^s). If each code symbol is represented by an s-tuple over GF(2), then an RS code can be transmitted using binary signaling, such as BPSK.
- In decoding, every s received bits are grouped into a received symbol over GF(2^s). This results in a received sequence of $2^s - 1$ symbols over GF(2^s). Then decoding is performed on this received symbol sequence.
- Since RS codes are special q-ary BCH codes, they can be

decoded with the Berlekamp-Massey algorithm as described in Sections 6.4 to 6.7. Euclidean algorithm is also commonly used for decoding RS codes, which will be presented in the next Section.

- **Example 7.2:** Let $q = 2^4$ and GF(2^4) be the field for code construction. Let α be a primitive element of GF(2^4). Suppose we want to construct a triple-symbol-error-correcting RS code $\mathcal{C}_{rs,3}$ of length $n = 2^4 - 1 = 15$ over GF(2^4). The generator polynomial

$\mathbf{g}(X)$ of this code is

$$\begin{aligned}&\mathbf{g}(X)\\&= (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)\\&= \alpha^6 + \alpha^9 X + \alpha^6 X^2 + \alpha^4 X^3 + \alpha^{14} X^4 + \alpha^{10} X^5 + X^6.\end{aligned}$$

- Suppose the zero code polynomial is transmitted and

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

is received.

- The syndrome of $\mathbf{r}(X)$ is

$$\mathbf{S} = (S_1, S_2, S_3, S_4, S_5, S_6)$$

where

$$S_1 = \mathbf{r}(\alpha) = \alpha^{12}, S_2 = \mathbf{r}(\alpha^2) = 1, S_3 = \mathbf{r}(\alpha^3) = \alpha^{14},$$
$$S_4 = \mathbf{r}(\alpha^4) = \alpha^{10}, S_5 = \mathbf{r}(\alpha^5) = 0, S_6 = \mathbf{r}(\alpha^6) = \alpha^{12}.$$

- Using the syndrome $\mathbf{S}$ and Berlekamp-Massey algorithm, we find that the error-location polynomial (see Table 7.1) is

$$\begin{aligned} \boldsymbol{\sigma}(X) &= 1 + \alpha^7 X + \alpha^4 X^2 + \alpha^6 X^3 \\ &= (1 + \alpha^{12} X)(1 + \alpha^6 X)(1 + \alpha^3 X). \end{aligned}$$

- We find the roots of the error-location polynomial $\boldsymbol{\sigma}(X)$ are α^3, α^9 and α^{12}. The inverses of the roots give the error-location numbers, α^{12}, α^6 and α^3. So the errors occur at position X^3, X^6 and X^{12}.

- Using (6.18), we find the error-value evaluator,

$$\begin{aligned}\mathbf{Z}_0(X) &= S_1 + (S_2 + \sigma_1 S_1)X + (S_3 + \sigma_1 S_2 + \sigma_2 S_1)X^2 \\ &= \alpha^{12} + \alpha X.\end{aligned}$$

- Using (6.21) to (6.23), we find the error-values at the location X^3, X^6 and X^{12},

$$\begin{aligned}e_3 &= -\mathbf{Z}_0(\alpha^{-3})/\boldsymbol{\sigma}'(\alpha^{-3}) = \alpha^7 \\ e_6 &= -\mathbf{Z}_0(\alpha^{-6})/\boldsymbol{\sigma}'(\alpha^{-6}) = \alpha^3 \\ e_{12} &= -\mathbf{Z}_0(\alpha^{-12})/\boldsymbol{\sigma}'(\alpha^{12}) = \alpha^4.\end{aligned}$$

- So the estimated error polynomial is

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

which is the true error polynomial.

7.3 Decoding RS Codes With Euclid's Algorithm

- Suppose a $(q-1, q-2t-1, 2t+1)$ RS code over GF(q) is used for error control over a noisy channel. Suppose a code polynomial

$$\mathbf{v}(X) = v_0 + v_1 X + \cdots + v_{q-2} X^{q-2}$$

is transmitted.

Let

$$\mathbf{r}(X) = r_0 + r_1 X + \cdots + r_{q-2} X^{q-2}$$

be the received polynomial and

$$\mathbf{e}(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} + \cdots + e_{j_\nu} X^{j_\nu}, \qquad (7.2)$$

be the error pattern, where $0 \leq j_1 < j_2 < \cdots < j_\nu < q-1$ are the locations of the errors in $\mathbf{e}(X)$ and $e_{j_1}, e_{j_2}, \ldots, e_{j_\nu}$ are the values of errors at the locations $j_1, j_2, \ldots, j_\nu$ which are elements in GF(q).

- The first step of decoding is to compute the syndrome of the received polynomial $\mathbf{r}(X)$,

$$\mathbf{S} = (S_1, S_2, \ldots, S_{2t}),$$

where $S_1 = \mathbf{r}(\alpha), S_2 = \mathbf{r}(\alpha^2), \ldots, S_{2t} = \mathbf{r}(\alpha^{2t})$.

- Let

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

be the error-location polynomial.

- Define the following two polynomials:

$$\mathbf{S}(X) = S_1 + S_2 X + \cdots + S_{2t} X^{2t-1}, \tag{7.3}$$

$$\begin{aligned}\mathbf{Z}_0(X) = {} & S_1 + (S_2 + \sigma_1 S_1)X + (S_3 + \sigma_1 S_2 + \sigma_2 S_1)X^2 + \cdots \\ & + (S_0 + \sigma_1 S_{\nu-1} + \cdots + \sigma_{\nu-1} S_1)X^{\nu-1}.\end{aligned} \tag{7.4}$$

- $\mathbf{S}(X)$ and $\mathbf{Z}_0(X)$ are called the **syndrome polynomial** and **error-value evaluator**, respectively. The error-value

evaluator was defined earlier in Section 6.6 of Lecture 6.

- Note the degree of $\mathbf{Z}_0(X)$ is at least one less than the degree of the error-location polynomial.
- The three polynomials $\boldsymbol{\sigma}(X)$, $\mathbf{S}(X)$ and $\mathbf{Z}_0(X)$ are related by the following equation

$$\boldsymbol{\sigma}(X)\mathbf{S}(X) \equiv \mathbf{Z}_0(X) \text{ modulo } X^{2t}, \tag{7.5}$$

  which is called the **Key-equation**.
- Any method of solving this Key-equation to find $\boldsymbol{\sigma}(X)$ and $\mathbf{Z}_0(X)$ is a decoding method for RS codes (or q-ary BCH codes).
- If the number of errors in $\mathbf{e}(X)$ is less than or equal to t (the error-correction capability of the code), then the

Key-equation has a unique pair of solutions, ($\boldsymbol{\sigma}(X)$ and $\mathbf{Z}_0(X)$) with

$$\deg \mathbf{Z}_0(X) < \deg \boldsymbol{\sigma}(X) \leq t. \tag{7.6}$$

- The Key-equation of (7.5) can be solved by using the **Euclid's iterative division algorithm** to find the **greatest common divisor** (GCD) of X^{2t} and $\mathbf{S}(X)$. The first step is to divide X^{2t} by $\mathbf{S}(X)$. This results in the following expression:

$$X^{2t} = \mathbf{q}_1(X)\mathbf{S}(X) + \mathbf{Z}_0^{(1)}(X), \tag{7.7}$$

where $\mathbf{q}_1(X)$ and $\mathbf{Z}_0^{(1)}(X)$ are the quotient and remainder, respectively.

- Then, we divide $\mathbf{S}(X)$ by $\mathbf{Z}_0^{(1)}(X)$. Let $\mathbf{q}_2(X)$ and $\mathbf{Z}_0^{(2)}(X)$ be the resultant quotient and remainder, respectively.
- Then, we divide $\mathbf{Z}_0^{(1)}(X)$ by $\mathbf{Z}_0^{(2)}(X)$. We repeat above division process.
- Let $\mathbf{Z}_0^{(i-2)}(X)$ and $\mathbf{Z}_0^{(i-1)}(X)$ be the remainders at the $(i-2)$th and $(i-1)$th division steps, respectively.
- **Euclid's Algorithm:** The Euclid's algorithm for finding $\boldsymbol{\sigma}(X)$ and $\mathbf{Z}_0(X)$ is to carry out the following two computations iteratively: At the ith division step with $i = 1, 2, \ldots,$
  1. Divide $\mathbf{Z}_0^{(i-2)}(X)$ by $\mathbf{Z}_0^{(i-1)}(X)$ to obtain the quotient $\mathbf{q}_i(X)$ and remainder $\mathbf{Z}_0^{(i)}(X)$.

2. Find $\boldsymbol{\sigma}^{(i)}(X)$ from

$$\boldsymbol{\sigma}^{(i)}(X) = \boldsymbol{\sigma}^{(i-2)}(X) - \mathbf{q}_i(X)\boldsymbol{\sigma}^{(i-1)}(X). \tag{7.8}$$

- Iteration begins with the following initial conditions:

$$\begin{aligned} \mathbf{Z}^{(-1)}(X) &= X^{2t}, \quad \mathbf{Z}^{(0)}(X) = \mathbf{S}(X), \\ \boldsymbol{\sigma}^{(-1)}(X) &= 0, \qquad \boldsymbol{\sigma}^{(0)}(X) = 1. \end{aligned} \tag{7.9}$$

- Iteration stops when a step ρ is reached for which

$$\deg \mathbf{Z}_0^{(\rho)}(X) < \deg \boldsymbol{\sigma}^{(\rho)}(X) \leq t. \tag{7.10}$$

- Then the error-location polynomial $\boldsymbol{\sigma}(X)$ and error-value

evaluator are given by:

$$\boldsymbol{\sigma}(X) = \boldsymbol{\sigma}^{(\rho)}(X), \tag{7.11}$$

$$\mathbf{Z}_0(X) = \mathbf{Z}_0^{(\rho)}(X). \tag{7.12}$$

- If the number of errors in $\mathbf{e}(X)$ is t or less, there always exists a step ρ for which the condition given by (7.6) holds. It is easy to see that $\rho \leq 2t$.
- Once $\boldsymbol{\sigma}(X)$ and error-value evaluator have been found, the locations and values of errors in the error pattern $\mathbf{e}(X)$ can be determined as follows:
  1. Find the roots of $\boldsymbol{\sigma}(X)$ and take the reciprocal of the roots which give the error-location numbers $\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_\nu}$. Then the exponents of α, $j_1, j_2, \ldots, j_\nu$,

give the locations of errors in the error pattern $\mathbf{e}(X)$.

2. Let $\boldsymbol{\sigma}'(X)$ be the derivative of $\boldsymbol{\sigma}(X)$ (see (6.21) of Lecture 6). Then the error value at location j_i is given by

$$e_{j_i} = \frac{-\mathbf{Z}_0(\alpha^{-j_i})}{\boldsymbol{\sigma}'(\alpha^{-j_i})}. \tag{7.13}$$

- The above two steps completely determine the error pattern $\mathbf{e}(X)$. Then the estimated transmitted code polynomial is given by $\mathbf{v}^*(X) = \mathbf{r}(X) - \mathbf{e}(X)$.
- The iteration process for finding $\boldsymbol{\sigma}(X)$ and $\mathbf{Z}_0(X)$ can be carried out by setting up and filling the Table 7.2 as shown below:

Table 7.1: Steps of the Euclid's algorithm for finding error-location polynomial and Error-value evaluator.

Iteration step i	$\mathbf{Z}_0^{(i)}(X)$	$\mathbf{q}_i(X)$	$\boldsymbol{\sigma}^{(i)}(X)$
-1	X^{2t}	-	0
0	$\mathbf{S}(X)$	-	1
1			
2			
$\vdots$			
i			
$\vdots$			

- **Example 7.3:** Let GF(2^4) be the field constructed from the primitive polynomial $\mathbf{p}(X) = 1 + X + X^4$. Let α be a primitive element of GF(2^4). Consider the triple-error-correction $(15, 9, 7)$ RS code over GF(2^4) generated by

  $$\mathbf{g}(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6).$$

  Suppose a code polynomial $\mathbf{v}(X)$ is transmitted and the received polynomial is $\mathbf{r}(X) = \alpha^7 X^3 + \alpha^{11} X^{10}$. The

syndrome components of $\mathbf{r}(X)$ are:

$$S_1 = \mathbf{r}(\alpha) = \alpha^{10} + \alpha^{20} = \alpha^7,$$
$$S_2 = \mathbf{r}(\alpha^2) = \alpha^{13} + \alpha^{31} = \alpha^{12},$$
$$S_3 = \mathbf{r}(\alpha^3) = \alpha^{16} + \alpha^{41} = \alpha^6,$$
$$S_4 = \mathbf{r}(\alpha^4) = \alpha^{19} + \alpha^{51} = \alpha^{12},$$
$$S_5 = \mathbf{r}(\alpha^5) = \alpha^7 + \alpha = \alpha^{14},$$
$$S_6 = \mathbf{r}(\alpha^6) = \alpha^{10} + \alpha^{11} = \alpha^{14}.$$

- The syndrome polynomial is

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

- Carrying out the Euclid's algorithm by dividing X^6 by $\mathbf{S}(X)$, we construct the table below,

i	$\mathbf{Z}_0^{(i)}(X)$	$\mathbf{q}_i(X)$	$\boldsymbol{\sigma}^{(i)}(X)$
-1	X^6	-	0
0	$\mathbf{S}(X)$	-	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	$\alpha^3 + \alpha^2 X$	$\alpha^{11} + \alpha^8 X$	$\alpha^{11} + \alpha^8 X + \alpha^9 X^2$

- We find that at iteration step 2, the condition (7.6) holds. Hence

$$\begin{aligned}
&\boldsymbol{\sigma}(X) = \boldsymbol{\sigma}_2(X) \\
&= \alpha^{11} + \alpha^8 X + \alpha^9 X^2 = \alpha^{11}(1 + \alpha^{10} X)(1 + \alpha^3 X) \\
&\mathbf{Z}_0(X) = \alpha^3 + \alpha^2 X.
\end{aligned}$$

- The roots of $\boldsymbol{\sigma}(X)$ are α^5 and α^{12}. Their reciprocals are α^{10} and α^3 and hence there are two errors in the estimated error

pattern $\mathbf{e}(X)$ at the locations X^3 and X^{10}. The error values at the locations X^3 and X^{10} are:

$$\mathbf{e}_3 = \frac{-\mathbf{Z}_0(\alpha^{-3})}{\boldsymbol{\sigma}'(\alpha^{-3})} = \frac{\alpha^3+\alpha^2\alpha^{-3}}{\alpha^{11}\alpha^3(1+\alpha^{10}\alpha^{-3})} = \frac{1}{\alpha^8} = \alpha^7,$$
$$\mathbf{e}_{10} = \frac{-\mathbf{Z}_0(\alpha^{-10})}{\boldsymbol{\sigma}'(\alpha^{-10})} = \frac{\alpha^3+\alpha^2\alpha^{-10}}{\alpha^{11}\alpha^{10}(1+\alpha^3\alpha^{-10})} = \frac{\alpha^4}{\alpha^8} = \alpha^{11}.$$

- Therefore, the estimated error pattern is $\mathbf{e}^*(X) = \alpha^7 X^3 + \alpha^{11} X^{10}$ and the decoded code word $\mathbf{v}^*(X) = \mathbf{r}(X) - \mathbf{e}(X)$ is the all-zero code word.

Decoding with the Euclidean Algorithm

- Recall that the error-location polynomial $\sigma(X)$ and the error-value evaluator $Z_0(X)$ are related by the key-equation given by (32),

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

where $S(X)$ is the syndrome polynomial,

$$S(X) = S_1 + S_2X + S_3X^2 + \ldots + S_{2t}X^{2t-1}.$$

- Any method of solving the key-equation to find $\sigma(X)$ and $Z_0(X)$ is a decoding method for BCH codes. If the number of errors ν during the transmission of a code polynomial $v(X)$ is less than or equal to t, (i.e., $\nu \leq t$), then the key-equation has a unique pair of solutions, $(\sigma(X), Z_0(X))$ with

$$deg\ Z_0(X) < deg\ \sigma(X) \leq t. \qquad (7.40)$$

- We have already presented the Berlekamp-Massey algorithm for solving the key-equation which is a very effective method for practical implementation and has been widely used.

- There is another method for solving the key-equation which is much easier to understand. This method is based on the Euclidean algorithm for finding the greatest common divisor (GCD) of two polynomials.

6.1 Euclidean Algorithm for Polynomials

- Consider two polynomials, $a(X)$ and $b(X)$, over GF(q). Assume that

$$deg\ a(X) \geq deg\ b(X).$$

Let GCD $[a(X), b(X)]$ denote the greatest common divisor of $a(X)$ and $b(X)$.

Then GCD $[a(X), b(X)]$ can be found by an iterative application of the division algorithm as follows:

$$\begin{aligned}
a(X) &= q_1(X)b(X) + r_1(X) \\
b(X) &= q_2(X)r_1(X) + r_2(X) \\
r_1(X) &= q_3(X)r_2(X) + r_3(X) \\
&\vdots \\
r_{i-2}(X) &= q_i(X)r_{i-1}(X) + r_i(X) \\
&\vdots \\
r_{n-2}(X) &= q_n(X)r_{n-1}(X) + r_n(X) \\
r_{n-1}(X) &= q_{n+1}(X)r_n(X)
\end{aligned} \tag{7.41}$$

where $q_i(X)$ and $r_i(X)$ are the quotient and the remainder respectively at the i-th step of the iterative division. The iteration stops when the remainder is identical to zero. Then the last nonzero remainder $r_n(X)$ is the GCD of $a(X)$ and $b(X)$ (may be different by a constant scalar α),

i.e.

$$r_n(X) = \alpha \, \mathrm{GCD}[a(X), b(X)] \tag{7.42}$$

where $\alpha \in$ GF(q).

- Note that for $1 \leq i \leq n$,

$$deg\ r_{i-1}(X) > deg\ r_i(X) \tag{7.43}$$

- From (41), it is possible to show that

$$\mathrm{GCD}[a(X), b(X)] = f(X)a(X) + g(X)b(X) \tag{7.44}$$

where $f(X)$ and $g(X)$ are polynomials over GF(q).

- In fact, the remainder at each division step can be expressed as follows:

$$\begin{aligned} r_1(X) &= f_1(X)a(X) + g_1(X)b(X) \\ r_2(X) &= f_2(X)a(X) + g_2(X)b(X) \\ &\vdots \\ r_i(X) &= f_i(X)a(X) + g_i(X)b(X) \\ &\vdots \\ r_n(X) &= f_n(X)a(X) + g_n(X)b(X) \end{aligned} \tag{7.45}$$

- From (44) and (45), we have

$$\begin{aligned} f(X) &= \alpha^{-1} f_n(X) \\ g(X) &= \alpha^{-1} g_n(X) \end{aligned} \tag{7.46}$$

- From (41) and (45), we obtain the following recursive equations for finding $r_i(X)$ and $g_i(X)$:

$$\begin{aligned} r_i(X) &= r_{i-2}(X) - q_i(X)r_{i-1}(X) \\ f_i(X) &= f_{i-2}(X) - q_i(X)f_{i-1}(X) \\ g_i(X) &= g_{i-2}(X) - q_i(X)g_{i-1}(X) \end{aligned} \tag{7.47}$$

for $1 \leq i \leq n$. The initial conditions for the recursion are:

$$\begin{aligned} r_{-1}(X) &= a(X), \\ r_0(X) &= b(X), \\ f_{-1}(X) &= g_0(X) = 1, \\ f_0(X) &= g_{-1}(X) = 0. \end{aligned} \tag{7.48}$$

- An important property of the Euclid's algorithm is

$$deg\ a(X) = deg\ g_i(X) + deg\ r_{i-1}(X) \tag{7.49}$$

We see that as i increases, the degree of $r_{i-1}(X)$ decreases and the degree of $g_i(X)$ increases. This fact will be used for solving the key equation.

Example 7.1

Let $a(X) = X^3 + 1$ and $b(X) = X^2 + 1$ be two polynomials over GF(2). The Euclid's algorithm for finding the GCD $[X^3 + 1, X^2 + 1]$ is shown in Table 4.1. We see that last nonzero remainder is

$$r_1(X) = X + 1$$

which is the GCD of $X^3 + 1$ and $X^2 + 1$.

Table 7.1

i	$r_i(X)$	$q_i(X)$	$f_i(X)$	$g_i(X)$
-1	X^3+1	-	1	0
0	X^2+1	-	0	1
1	$X+1$	X	1	X
2	0	$X+1$	$X+1$	X^2+X+1

6.2 Solving the Key-Equation

- The key-equation can be expressed in the following form:

$$\sigma(X)S(X) = Q(X)X^{2t} + Z_0(X). \tag{7.50}$$

Rearranging (50), we have

$$Z_0(X) = -Q(X)X^{2t} + \sigma(X)S(X). \tag{7.51}$$

Setting $a(X) = X^{2t}$ and $b(X) = S(X)$, (51) is exactly in the form given by (45).

- This suggests that $\sigma(X)$ and $Z_0(X)$ can be found by the Euclidean iterative division algorithm for the two polynomials:

$$\begin{aligned} a(X) &= X^{2t} \\ b(X) &= S(X) \end{aligned} \tag{7.52}$$

- Let

$$\begin{aligned} Z_0^{(i)}(X) &= r_i(X) \\ \sigma^{(i)}(X) &= g_i(X) \\ \gamma^{(i)}(X) &= f_i(X) \end{aligned} \tag{7.53}$$

- Then it follows from (52) and (53) that (45), (47) and (48) can be put in the following forms:

$$Z_0^{(i)}(X) = \gamma^{(i)}(X)X^{2t} + \sigma^{(i)}(X)S(X), \tag{7.54}$$

and

$$\begin{aligned} Z_0^{(i)}(X) &= Z_0^{(i-2)}(X) - q_i(X)Z_0^{(i-1)}(X) \\ \sigma^{(i)}(X) &= \sigma^{(i-2)}(X) - q_i(X)\sigma^{(i-1)}(X) \\ \gamma^{(i)}(X) &= \gamma^{(i-2)}(X) - q_i(X)\gamma^{(i-1)}(X) \end{aligned} \tag{7.55}$$

with

$$\begin{aligned} Z_0^{(-1)}(X) &= X^{2t} \\ Z_0^{(0)}(X) &= S(X) \\ \gamma^{(-1)}(X) &= \sigma^{(0)}(X) = 1 \\ \gamma^{(0)}(X) &= \sigma^{(-1)}(X) = 0. \end{aligned} \tag{7.56}$$

- To find $\sigma(X)$ and $Z_0(X)$, we carry out the iteration process given by (55) as follows: At the i^{th} step,

  (1) Divide $Z_0^{(i-2)}(X)$ by $Z_0^{(i-1)}(X)$ to obtain the quotient $q_i(X)$ and the remainder $Z_0^{(i)}(X)$.

  (2) Find $\sigma^{(i)}(X)$ from

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

  Iteration stops when a step ρ is reached for which

$$\deg Z_0^{(\rho)}(X) < \deg \sigma^{(\rho)}(X) \leq t. \qquad (7.57)$$

  Then

$$\begin{aligned} Z_0(X) &= Z_0^{(\rho)}(X) \\ \sigma(X) &= \sigma^{(\rho)}(X). \end{aligned}$$

- If the number of errors is t or less, there always exists a step ρ for which the condition given by (57) holds. It is easy to see that

$$\rho \leq 2t.$$

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

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

- **Example7.2**Consider the triple-error-correcting RS code of length $n = 15$ over $GF(2^4)$ whose generator polynomial has α, α^2, α^3, α^4, α^5 and α^6 as roots, i.e.,

$$\bar{g}(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6).$$

Suppose the received polynomial is

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

The syndrome components are:

$$\begin{aligned}
S_1 &= \bar{r}(\alpha) = \alpha^{10} + \alpha^{21} = \alpha^7 \\
S_2 &= \bar{r}(\alpha^2) = \alpha^{13} + \alpha^{31} = \alpha^{12} \\
S_3 &= \bar{r}(\alpha^3) = \alpha^{16} + \alpha^{41} = \alpha^6 \\
S_4 &= \bar{r}(\alpha^4) = \alpha^{19} + \alpha^{51} = \alpha^{12} \\
S_5 &= \bar{r}(\alpha^5) = \alpha^7 + \alpha = \alpha^{14} \\
S_6 &= \bar{r}(\alpha^6) = \alpha^{10} + \alpha^{11} = \alpha^{14}
\end{aligned}$$

Hence 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

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

and

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

as shown in the table below:

i	$Z_0^{(i)}(X)$	$q_i(X)$	$\sigma_i(X)$
-1	X^6	-	0
0	$S(X)$	-	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	$\alpha^3 + \alpha^2 X$	$\alpha^{11} + \alpha^8 X$	$\alpha^{11} + \alpha^8 X + \alpha^9 X^2$

From $\sigma(X)$, we find that the roots are α^5 and α^{12}. Hence the error location numbers are: α^{10} and α^3.