https://doi.org/10.7840/kics.2022.47.11.1747

Decoding Process of RS Codes with Errors and Erasures: An Overview

Zhi Jing◆°, Hyojeong Choi*, Hong-Yeop Song*

ABSTRACT

This paper provides a comprehensive overview of the hard-decision decoding process of Reed-Solomon codes for error-and-erasure decoding. For an $[n, k]$ RS code, the decoder can correct simultaneously v errors and μ erasures in the received data if $2v+\mu \leq n-k$ (correctable range) and will fail otherwise (uncorrectable range). We give detailed reviews of both Berlekamp-Massy and Continued-Fraction algorithms for error-and-erasure decoding. Berlekamp-Massy algorithm has long been known but sometimes appeared incorrectly in some references. Continued-Fraction algorithm has been recently applied for error-and-erasure decoding. Finally, we verify by simulation that two algorithms work exactly the same even in the uncorrectable range.

Key Words : Reed-Solomon codes, Decoding process for both errors and erasures, Berlekamp-Massey algorithm, Continued-Fraction algorithm, Error-locator polynomials.

Ⅰ. Introduction

Reed-Solomon (RS) codes has been widely used in communications and storage systems[1-3] because of its Maximum-Distance-Separable (MDS) property and hence its strong fault-tolerant ability. The most time-consuming step of the hard-decision decoding process of RS codes is to find the error-locator polynomials. Most famous algorithms here are Berlekamp-Massey (BM) algorithm[4-7] and Continued-Fraction (CF) algorithm[8-11]. The BM algorithm is computationally efficient in terms of the number of operations in $\mathbb{F}_{2^m}$[7]. The BM algorithm is a popular choice to simulate the decoder of RS codes in software[7]. The well-known BM algorithm has been successfully applied to not only the error-only case but also the case with both errors and erasures[7].

For error-only decoding, the less well-known CF algorithm can be more simply implemented than the BM algorithm[8] and was verified theoretically that it works exactly the same as the BM algorithm when the received data is in the correctable range[9,10]. Recently, the CF algorithm has been successfully applied to the error-and-erasure case in the 2022 KICS Winter Conference[11]. It is the main purpose of this paper that clearly summarize the variations of these algorithms for both errors and erasures, which sometimes incorrectly appeared in their descriptions.

In this paper, we consider the hard-decision decoding of the narrow-sense q-ary $[n, k]$ RS codes with both errors and erasures when $q=2^m$. When the received data has no erasures, the decoding process reduces to the case for error-only decoding. The decoding process works with μ erasures (when $0 \leq \mu \leq n$-k) and successfully finds the correct

※ 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2020R1A2C2011969).
◆ First and Corresponding Author : Yonsei University School of Electrical and Electronic, z.jing@yonsei.ac.kr, 학생회원
* Yonsei University School of Electrical and Electronic, hysong@yonsei.ac.kr, 종신회원
논문번호 : KICS202206-114-A-RN, Received June 07, 2014; Revised August 30, 2022; Accepted September 06, 2022

codeword when the number of errors is not exceeding $(n-k-\mu)/2$ (correctable range).

The data in uncorrectable range is also another research point, which affects the decoding performance. When the received data belongs to uncorrectable range, it may result in incorrect decoding or be the data with undetected error. The probability of undetected error and the probability of incorrect decoding can be computed by the weigh distribution of the code in theory. Some researches of weight distribution were proposed[2,7]. In this paper, we also verify, by simulation, that the BM and CF algorithms work exactly the same even in the uncorrectable range.

Subsection 2.1 reviews the overall decoding process with both errors and erasures in general. As one step of the decoding process, BM and CF algorithms are reviewed in detail in subsection 2.2. Section Ⅲ discusses the decoding results when the received data belongs to uncorrectable range. Section Ⅳ is the conclusion.

Ⅱ. Decoding Process of RS Codes with Errors and Erasures

2.1 Overall decoding process

We first show the overall hard-decision decoding process[7] for RS codes with errors and erasures in Fig. 1. Let $g(z) = (z+\alpha)(z+\alpha^2)\cdots(z+\alpha^r)$ be the generator polynomial of a primitive narrow-sense $[n, k]$ RS code over $\mathbb{F}_{2^m}$, where $r = n-k$ and α is a primitive element of $\mathbb{F}_{2^m}$. Let $r(z) = r_0 + r_1 z + \cdots + r_{n-1}z^{n-1}$ be the received polynomial associated with a received data $r = (r_0, r_1, \cdots, r_{n-1})$.

The decoding will start with erasure detection. When the number of erasures is μ, their corresponding coordinates $i_1, i_2, \cdots, i_\mu$ are known to the decoder. The erasure-locators will be denoted by $Y_1 = \alpha^{i_1}, Y_2 = \alpha^{i_2}, \ldots, Y_\mu = \alpha^{i_\mu}$. When $\mu = 0$, the following steps become exactly the same as those for the error-only decoding. When $\mu > n-k$, the decoding will fail immediately.

Step A. When the received symbol is erased, its value is undefined and the syndromes cannot be calculated. Therefore, we may have to assign some values to all the erasures so that the syndromes are calculated and errors are processed. For simplicity, we set all the erasure values to be zero and the corresponding received polynomial is denoted by $r_f(z)$. This step will be omitted and $r_f(z)$ becomes the same as $r(z)$ if the received data does not have any erasure.

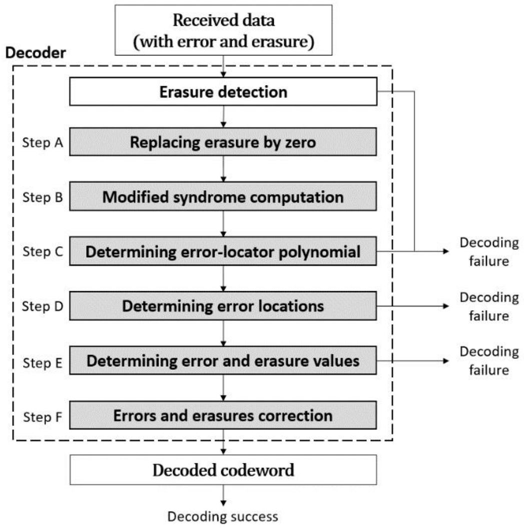

Fig. 1. The decoding process for RS code with both errors and erasures.

Step B. The syndrome $S_1, S_2, \ldots, S_r$ is calculated by r consecutive roots of the generator polynomial as $S_i = r_f(\alpha^i)$, for $i = 1, 2, \cdots, r$, and define the syndrome

$$S(z) = 1 + S_1 \cdot z + S_2 \cdot z^2 + \cdots S_r \cdot z^r,$$

If $S_1, S_2, \ldots, S_r$ are all zero, which means $r_f(z)$ is a codeword polynomial, then the decoding process succeeds; else, go on. The modified syndrome polynomial is given as

$$\begin{aligned} T(z) &\equiv S(z)\cdot\tau(z) \pmod{z^{r+1}} \\ &= 1 + T_1\cdot z + T_2\cdot z^2 + \cdots + T_r\cdot z^r, \end{aligned}$$

where

$$\tau(z) = \prod_{l=1}^{\mu} 1 + Y_l \cdot z$$

is the erasure-locator polynomial. Note that $\tau(z) = 1$ when there is no erasure.

Step C. Using modified syndromes $T_1, T_2, \cdots, T_r$, the error-locator polynomial $\sigma(z)$ of degree v will be obtained. The BM algorithm and the CF algorithm will be given in some detail in Subsection 2.2.

Step D. The error-locators will be determined by Chien search[12] after obtaining the error-locator polynomial $\sigma(z)$. Chien search is an algorithm that finds all the roots of the polynomial by substituting all elements of the field into the polynomial[12]. The error-locators $X_1, X_2, \ldots, X_v$ are the inverses of these roots.

Step E. The error and erasure values will be determined by the Forney algorithm[13]. The Forney algorithm obtains the error and erasure values at known error locations, which is based on Lagrange interpolation[13]. The error value e_{j_k} and erasure value f_{i_l} is computed as

$$e_{j_k} = F(X_k) \text{ and } f_{i_l} = F(Y_l) \ ,$$

for $1 \le k \le v$ and $1 \le l \le \mu$, where

$$F(z) = \frac{z \cdot \Omega(z^{-1})}{\Psi'(z^{-1})},$$
$$\Omega(z) \equiv \sigma(z)T(z) \pmod{x^{r+1}},$$
$$\Psi(z) = \sigma(z)\tau(z),$$

and $\Psi'(z)$ is the formal derivative of $\Psi'(z)$ with respect to z[13].

Step F. Correct the received data by e_{j_k} and f_{i_l}.

The decoding failure is caused by the following 3 reasons:

Step C cannot determine the appropriate error-locator polynomial $\sigma(z)$. It happens when $\mu > n - k$ or else the output $\sigma(z)$ of Step C has the degree exceeding $\left\lfloor \frac{n-k-\mu}{2} \right\rfloor$.

Step D cannot determine the error locations correctly. It happens when all the roots of $\sigma(z)$ are not in $\mathbb{F}_{2^m}$.

Step E cannot determine the values of errors and erasures. The Forney algorithm fails when $\Psi'(z^{-1}) = 0$.

2.2 Algorithm of determining the error-locator polynomial

As the most time-consuming step of the decoding process of RS codes, we will introduce two algorithms to determine the error-locator polynomial $\sigma(z)$: BM algorithm and CF algorithm.

2.2.1 Berlekamp-Massey algorithm

For an $[n, k]$ RS code, the number of the multiplication (and division) is almost $3r/2$ in each loop of BM algorithm, where $r = n - k$ is the redundancy of the code. So, the complexity of BM algorithm is $O(r^2)$.

Example 1. Consider a [7, 3] RS code over $\mathbb{F}_{2^3}$ with the generator polynomial

$$g(z) = \prod_{j=1}^{4} (z + \alpha^i)$$
$$= \alpha^3 + \alpha z + z^2 + \alpha^3 z^3 + z^4,$$

Algorithm 1. The process of determining $\sigma(z)$ based on BM algorithm with $T(z)$ and μ

1:	Input $T_1, T_2, \ldots, T_r, \mu$
2:	Initialize $k = 0, \sigma^{(0)}(z) = 1, L^{(0)} = 0,$ $\rho^{(0)} = z$, and $d^{(0)} = T_{\mu+1}$
3:	Increase k by 1. If $d^{(k-1)} \neq 0$, then $\sigma^{(k)}(z) = \sigma^{(k-1)}(z) + d^{(k-1)}\rho^{(k-1)}(z)$, Else, $\sigma^{(k)}(z) = \sigma^{(k-1)}(z)$ and go to Step 5.
4:	If $2L^{(k-1)} < k$, then $L^{(k)} = k - L^{(k-1)}$ and $\rho^{(k)}(z) = \frac{\sigma^{(k-1)}(z)}{d^{(k-1)}} z$ and go to Step 6; Else, go to Step 5.
5:	$L^{(k)} = L^{(k-1)}$ and $\rho^{(k)}(z) = \rho^{(k-1)}(z) \cdot z$.
6:	If $k < L^{(k)} + \frac{r-\mu}{2}$, then $d^{(k)} = T_{k+\mu+1} + \sum_{j=1}^{L^{(k)}} \sigma_j^{(k)} T_{k+\mu+1-j}$ and go to Step 3.
7:	Output the error-locator polynomial $\sigma(z) = \sigma^{(k)}(z)$ and stop.

where α is the root of the primitive polynomial $1 + z + z^3$. Let the transmitted codeword be

$$c = (\alpha^4, \alpha^3, \alpha^5, \alpha^4, \alpha^5, \alpha, \alpha).$$

Suppose that the received data r_1 contains two erasures:

$$r_1 = (\alpha^4, f, \alpha^5, \alpha^4, \alpha^4, \alpha, f).$$

where f indicates an erasure. The erasure-locators are $Y_1 = \alpha$ and $Y_2 = \alpha^6$, and $\tau(z) = (1+\alpha z)(1+\alpha^6 z) = 1 + \alpha^5 z + z^2$.

First, we get the modified syndromes

$$T_1 = \alpha^4, T_2 = \alpha^4, T_3 = \alpha^2, T_4 = \alpha^6$$

Then, the error-locator polynomial is $\sigma(z) = 1 + \alpha^4 z$ using BM algorithm as shown in Tab.1.

The error-locator is determined as $X_1 = (\alpha^3)^{-1} = \alpha^4$, where α^3 is the root of $\sigma(z)$. Then, the error value is

$$e_{j_1} = F(X_1) = \frac{X_1 \cdot \Omega(X_1^{-1})}{\Psi'(X_1^{-1})} = 1,$$

and the erasure values are

$$f_{i_1} = F(Y_1) = \alpha^3 \text{ and } f_{i_2} = F(Y_2) = \alpha.$$

So, the decoded codeword is

$$= (\alpha^4, 0, \alpha^5, \alpha^4, \alpha^4, \alpha, 0) + (0, \alpha^3, 0, 0, 1, 0, \alpha)$$
$$= (\alpha^4, \alpha^3, \alpha^5, \alpha^4, \alpha^5, \alpha, \alpha)$$

Table 1. The process of the BM algorithm of Example 1.

k	$\sigma^{(k)}(z)$	$L^{(k)}$	$\rho^{(k)}(z)$	$d^{(k)}$
0	1	0	z	α^2
1	$1+\alpha^2 z$	1	$\alpha^5 z$	α^3
2	$1+\alpha^4 z$	1	$\alpha^5 z^2$	–

2.2.2 Continued-Fraction algorithm

Here, we use X as an unknown value with corresponding operations of resulting in X when X is involved with any value in either addition or multiplication[9].

The most time-consuming step of CF algorithm is the polynomial division in step 4. For an $[n, k]$ RS code, the complexity of CF algorithm is $O(r^3)$, where $r = n - k$.

For Example 1, we determine the error-locator polynomial again using the continued fraction algorithm as shown in Tab.2. The error-locator polynomial $\sigma(z) = 1 + \alpha^4 z$ is the reciprocal polynomial of $P^{(1)}(z)$, which is the same as that of BM algorithm.

Algorithm 2. The process of determining $\sigma(z)$ based on BM algorithm with $T(z)$ and μ

1:	Input $T_1, T_2, \ldots, T_r, \mu$
2:	Initialize $k = 0, P^{(-1)}(z) = 1, P^{(0)} = 1,$ $R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$ $R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$
3:	Increase k by 1. $b^{(k)} = \frac{\text{coefficient of the highest degree term of } R^{(k-1)}(z)}{\text{coefficient of the highest degree term of } R^{(k-2)}(z)}$
4:	Obtain the quotient $a^{(k)}(z)$ and the remainder $R^{(k)}(z)$ such that $b^{(k)} \cdot R^{(k-2)}(z) = a^{(k)} \cdot R^{(k-1)}(z) + R^{(k)}(z),$ where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.
5:	Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)}(z) + b^{(k)}(z) \cdot P^{(k-2)}(z)$
6:	If the coefficient of the highest degree term of $R^{(k)}(z)$ is not X, go to Step 3.
7:	Output the error-locator polynomial $\sigma(z)$ as the reciprocal polynomial of $P^{(k)}(z)$ and stop.

Table 2. The process of the CF algorithm of Example 1.

k	$R^{(k)}(z)$	$b^{(k)}$	$a^{(k)}(z)$	$P^{(k)}(z)$
-1	$1+\alpha^2 z^{-1} + \alpha^6 z^{-2} + X \cdot z^{-3}$	–	–	1
0	$\alpha^2 z^{-1} + \alpha^6 z^{-2} + X \cdot z^{-3}$	–	–	1
1	$X \cdot z^{-2}$	α^2	$z+\alpha$	$z+\alpha^4$

Ⅲ. Uncorrectable Error and Undetected Error

After erasure detection and replacing erasure by zero, if all syndromes S_1, S_2, ⋯, S_r that are calculated by the polynomial $r_f(z)$ are all zero, then $r_f(z)$ is determined as the codeword polynomial and the decoding process succeeds; else, the received data has some errors in addition.

The received data can be decoded correctly when belongs to the correctable range; else the received data is in the uncorrectable range. These data are divided into two types:

- data with detected but uncorrectable error;
- data with undetected error.

3.1 Data with uncorrectable error

The received data is the data with detected but uncorrectable error when the decoding process fails that is discussed in subsection 2.1. We will show three examples of the failure of the decoding process, which happen in Step C, Step D, and Step E, respectively.

Example 2. In Example 1 we saw that the transmitted codeword is

$$c = (\alpha^4, \alpha^3, \alpha^5, \alpha^4, \alpha^5, \alpha, \alpha).$$

Suppose that the received data r_2 contains one erasure:

$$r_2 = (\alpha^4, \alpha^3, \alpha^5, \alpha^5, \alpha^4, \alpha^3, f).$$

where f indicates an erasure. The erasure-locator is $Y_1 = \alpha^6$, and $\tau(z) = 1 + \alpha^6 z$.

First, we get the modified syndromes $T_1 = \alpha^4, T_2 = \alpha^6, T_3 = \alpha^3, T_4 = \alpha^3$. Then, the error-locator polynomial can be obtained $\sigma(z) = 1 + \alpha^4 z + \alpha^2 z^2$ using CF algorithm as shown in Tab.3.

Now, the decoding fails since $deg(\sigma(z)) = 2 > \left\lfloor \frac{4-1}{2} \right\rfloor = 1$.

Comparing with the transmitted codeword c, the received data r_2 has 3 errors and 1 erasure, which is out of the correctable range.

Table 3. The process of the CF algorithm of Example 2.

k	$R^{(k)}(z)$	$b^{(k)}$	$a^{(k)}(z)$	$P^{(k)}(z)$
-1	$1 + \alpha^6 z^{-1} + \alpha^3 z^{-2} + \alpha^3 z^{-3} + X \cdot z^{-4}$	–	–	1
0	$\alpha^6 z^{-1} + \alpha^3 z^{-2} + \alpha^3 z^{-3} + X \cdot z^{-4}$	–	–	1
1	$\alpha z^{-2} + X \cdot z^{-3}$	α^6	$z + \alpha^3$	$z + \alpha^4$
2	$X \cdot z^{-2}$	α^2	z	$z^2 + \alpha^4 z + \alpha^2$

Example 3. In Example 1 we saw that the transmitted codeword is

$$c = (\alpha^4, \alpha^3, \alpha^5, \alpha^4, \alpha^5, \alpha, \alpha).$$

Suppose that the received data r_3 without erasure:

$$r_3 = (\alpha^5, \alpha, \alpha^4, \alpha^4, \alpha^5, \alpha, \alpha).$$

First, we get the modified syndromes $T_1 = S_1 = \alpha^5, T_2 = S_2 = \alpha^3, T_3 = S_3 = \alpha^5, T_4 = S_4 = \alpha^6$. Then, the error-locator polynomial can be obtained $\sigma(z) = 1 + \alpha^5 z + \alpha z^2$ using CF algorithm as shown in Tab.4.

Now, the decoding fails since $\sigma(x)$ has no root over $\mathbb{F}_{2^3}$.

Comparing with the transmitted codeword c, the received data r_3 has 3 errors, which is out of the correctable range.

Table 4. The process of the CF algorithm of Example 3.

k	$R^{(k)}(z)$	$b^{(k)}$	$a^{(k)}(z)$	$P^{(k)}(z)$
-1	$1 + \alpha^5 z^{-1} + \alpha^3 z^{-2} + \alpha^5 z^{-3} + \alpha^6 z^{-4} + X \cdot z^{-5}$	–	–	1
0	$\alpha^5 z^{-1} + \alpha^3 z^{-2} + \alpha^5 z^{-3} + \alpha^6 z^{-4} + X \cdot z^{-5}$	–	–	1
1	$\alpha^6 z^{-2} + \alpha^4 z^{-3} + X \cdot z^{-4}$	α^5	z	$z + \alpha^5$
2	$X \cdot z^{-2}$	α	z	$z^2 + \alpha^5 z + \alpha$

Example 4. In Example 1 we saw that the transmitted codeword is

$$c = (\alpha^4, \alpha^3, \alpha^5, \alpha^4, \alpha^5, \alpha, \alpha).$$

Suppose that the received data r_4 contains two erasures:

$r_4 = (f,\ \alpha,\ \alpha^4,\ \alpha^5,\ f,\ \alpha,\ \alpha)$,

where f indicates an erasure. The erasure-locators are $Y_1 = 1$ and $Y_2 = \alpha^4$, and $\tau(z) = (1+z)(1+\alpha^4 z)$.

First, we get the modified syndromes $T_1 = 0, T_2 = 1, T_3 = \alpha, T_4 = \alpha$ Then, the error-locator polynomial can be obtained $\sigma(z) = 1 + z$ using CF algorithm as shown in Tab.5.

The error-locator is determined as $X_1 = 1$. We can get $\Psi(X_1 = 1)' = 0$, where $\Psi(z) = \sigma(z)\tau(z) = (1+z)^2(1+\alpha^4)$. So, the decoding fails since the denominator of its error value is zero.

Comparing with the transmitted codeword c, the received data r_4 has 3 errors and 2 erasures, which is out of the correctable range.

Table 5. The process of the CF algorithm of Example 4.

k	$R^{(k)}(z)$	$b^{(k)}$	$a^{(k)}(z)$	$P^{(k)}(z)$
-1	$1+\alpha z^{-1}+\alpha z^{-2}+X\cdot z^{-3}$	−	−	1
0	$\alpha z^{-1}+\alpha z^{-2}+X\cdot z^{-3}$	−	−	1
1	$X\cdot z^{-2}$	α	α^3+z	$z+1$

3.2 Data with undetected error

Assume the codeword c is transmitted, and the data r is received. When the received data r contains many errors and erasures, it is not in the correctable range of c. However, r maybe more closed to another codeword $\acute{c}$, even in the correctable range of $\acute{c}$. That is to say, r is decoded to $\acute{c}$. The errors and erasures of r cannot be corrected correctly, and cannot be detected because the decoding process ends successfully. The received data r is the data with undetected errors.

Example 5. In Example 1 we saw that the transmitted codeword is

$$c = (\alpha^4,\ \alpha^3,\ \alpha^5,\ \alpha^4,\ \alpha^5,\ \alpha,\ \alpha)$$

Suppose that the received data r_5 contains two erasures:

$$r_5 = (f,\ f,\ \alpha^4,\ \alpha^5,\ \alpha^4,\ \alpha,\ \alpha),$$

where f indicates an erasure. The erasure-locators are $Y_1 = 1$ and $Y_2 = \alpha$, and $\tau(z) = (1+z)(1+\alpha z)$.

First, we get the modified syndromes $T_1 = \alpha, T_2 = 1, T_3 = \alpha^5, T_4 = \alpha$ Then, the error-locator polynomial can be obtained $\sigma(z) = 1 + \alpha^3 z$ using CF algorithm as shown in Tab.6.

The error-locator is determined as $X_1 = (\alpha^4)^{-1} = \alpha^3$. Then, the error value is $e_{j_1} = \alpha$, and the erasure values are $f_{i_1} = \alpha^6$ and $f_{i_1} = 1$. So, the decoded data is

$$\begin{aligned} &= (0,0,\alpha^4,\alpha^5,\alpha^4,\alpha,\alpha) + (\alpha^6,1,0,\alpha,0,0,0) \\ &= (\alpha^6,1,\alpha^4,\alpha^6,\alpha^4,\alpha,\alpha). \end{aligned}$$

The decoding process succeeds but the decoded data is not the codeword c. Comparing with the transmitted codeword c, the received data r_5 has 3 errors and 2 erasures, which is out of the correctable range.

Table 6. The process of the CF algorithm of Example 5.

k	$R^{(k)}(z)$	$b^{(k)}$	$a^{(k)}(z)$	$P^{(k)}(z)$
-1	$1+\alpha^5 z^{-1}+\alpha z^{-2}+X\cdot z^{-3}$	−	−	1
0	$\alpha^5 z^{-1}+\alpha z^{-2}+X\cdot z^{-3}$	−	−	1
1	$X\cdot z^{-2}$	α^5	$z+\alpha^2$	$z+\alpha^3$

Ⅳ. Simulation result

We also simulate the BM algorithm and the CF algorithm for a [7,3] RS code over $\mathbb{F}_{2^3}$ with any number of errors and erasures. In the correctable range, the CF algorithm was verified theoretically that it works exactly the same as the BM algorithm[9,10], and we also proved this by simulation. To the best of our knowledge, there is no theoretical result on the uncorrectable range.

Here, we only list some cases that are out of the correctable ranges. The simulation results for the

BM algorithm and the CF algorithm are shown in Tab.7 and Tab.8, respectively. In the uncorrectable range, the received data cannot be decoded successfully (uncorrectable error) or be decoded to other codewords (undetected error). For these received data, their error-locator polynomial $\sigma(z)$ cannot be obtained correctly. By simulation, we get that $\sigma(z)$ obtained by BMA and CFA are not always the same, which may lead to different flows in the decoding process. We count the number of failures that occurred in Step C, D, or E. The reasons why these steps fail to decode are given in subsection 2.1. We also count the number of undetected errors. Tab.7 and Tab.8 verify that the result of the decoding process is the same, although the obtained $\sigma(z)$ is different in Step C. Therefore, we can get that the BM algorithm and the CF algorithm also work exactly the same even in the uncorrectable range.

Table 7. The results of decoding algorithms using BMA for [7,3] RS codes in some uncorrectable ranges.

No. of erasure	No. of error	Total	Decoding failure in			Undetected error
			BMA (Step C)	Chien algorithm (Step D)	Foney algorithm (Step E)	
0	3	35	7	28	-	-
	4	35	7	28	-	-
1	2	105	105	-	-	-
	3	140	140	-	-	-
2	2	210	42	-	168	-
	3	210	112	-	50	48
3	1	140	140	-	-	-
	2	210	170	-	20	20
4	1	105	41	-	-	64
5	0	21	21	-	-	-

Table 8. The results of decoding algorithms using CFA for [7,3] RS codes in some uncorrectable ranges.

No. of erasure	No. of error	Total	Decoding failure in			Undetected error
			CFA (Step C)	Chien algorithm (Step D)	Foney algorithm (Step E)	
0	3	35	7	28	-	-
	4	35	7	28	-	-
1	2	105	105	-	-	-
	3	140	140	-	-	-
2	2	210	42	-	168	-
	3	210	112	-	50	48
3	1	140	140	-	-	-
	2	210	170	-	20	20
4	1	105	41	-	-	64
5	0	21	21	-	-	-

Ⅴ. Conclusion

We review the hard-decision decoding process of RS code with errors and erasures. As one step of the decoding process, BM and CF algorithms are discussed in detail, which is to find the error-locator polynomials. We also verify the BM and CF algorithms work exactly the same by simulation.

References

[1] S. Wicker, V. Bhargava, et al., *Reed-Solomon codes and their applications*, John Wiley & Sons, 1999. (https://doi.org/10.1109/9780470546345)

[2] S. Lin and D. J. Costello, *Error control coding*, Scarborough: Prentice hall, 2001.

[3] H. Cho, H.-Y. Song, J. M. Ahn, and D. W. Lim, "Some new RS-coded orthogonal modulation schemes for future GNSS," *ICT Express*, vol. 7, no. 4, pp. 530-534, Dec. 2021. (https://doi.org/10.1016/j.icte.2021.04.004)

[4] E. R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw-Hill, 1968; revised edition, 2015.

[5] J. Yu and H. Loeliger, "Partial inverses mod $m(x)$ and reverse Berlekamp–Massey decodi-ng," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 6737-6756, Dec. 2016. (https://doi.org/10.1109/ TIT.2016.2613559)

[6] I. Ilani, "Berlekamp-Massey algorithm: Euclid in disguise," in *Proc. 2018 IEEE Int. Conf.Sci. Electr. Eng.*, pp. 1-5, Eilat, Israel, Dec. 2018. (https://doi.org/10.1109/ICSEE.2018.8646027)

[7] R. H. Morelos-Zaragoza, *The art of error correcting coding*, Second Ed., John Wiley & Sons, 2006. (https://doi.org/10.1002/0470847824)

[8] I. Reed, R. Scholtz, T. Truong, and L. Welch, "The fast decoding of Reed-Solomon codes using Fermat theoretic transforms and continued fractions," *IEEE Trans. Inf. Theory*,

vol. 24, no. 1, pp. 100-106, Jan. 1978. (https://doi.org/10.11 09/TIT.1978.1055816)

[9] L. Welch and R. Scholtz, "Continued fractions and Berlekamp's algorithm," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 19-27, Jan. 1979. (https://doi.org/10.1109/TIT.1979.1055987)

[10] U. Cheng, "On the continued fraction and Ber-lekamp's algorithm," *IEEE Trans. Inf. Theory*, vol. 30, no. 3, pp. 541-544, May 1984. (https://doi.org/10.1109/TIT.1984.1056906)

[11] Z. Jing, G. Kim, H. Cho, and H.-Y. Song, "Decoding RS codes with errors and erasures by continued fractions," in *Proc. KICS Winter Conf. 2022*, pp. 1618-1619, Pyeongchang, Korea, Feb. 2022.

[12] R. Chien, "Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 4, pp. 357-363, Oct. 1964. (https://doi.org/10.1109/TIT.1964.1053699)

[13] G. Forney, "On decoding BCH codes," *IEEE Trans. Inf. Theory*, vol. 11, no. 4, pp. 549-557, Oct. 1965. (https://doi.org/10.1109/TIT.1965.1053825)

Zhi Jing

2014년 2월 : China University of Geosciences (Beijing) Dept. of Electronic Info-rmation Engineering 학사

2015년 11월 : Hong Kong Baptist University Dept. of Computer Science 석사

2016년 9월~현재 : 연세대학교 전기전자공학과 석박사통합과정

<관심분야> 통신공학, 정보이론, 부호이론

[ORCID:0000-0002-1444-3289]

최 효 정 (Hyojeong Choi)

2018년 2월 : 연세대학교 정보통신공학부 졸업

2021년 2월 : 연세대학교 전기전자공학과 석사

2021년 3월~현재 : 연세대학교 전기전자공학과 박사과정

<관심분야> 통신공학, 부호이론, 분산저장시스템

[ORCID:0000-0003-2305-5111]

송 홍 엽 (Hong-Yeop Song)

1984년 2월 : 연세대학교 전자공학과 졸업

1986년 5월 : University of Southern California Dept. of EE. System 석사

1991년 12월 : University of Southern California Dept. of EE. System 박사

1992년 1월~1993년 12월 : University of Southern California 박사 후 연구원

1994년 1월~1995년 8월 : Qualcomm, San Diego, Senior Engineer

1995년 9월~현재 : 연세대학교 전기전자공학과 전임교수

<관심분야> 통신공학, 정보이론, 부호이론

[ORCID:0000-0001-8764-9424]