Decoding RS codes with errors and erasures by continued fractions

Zhi Jing and Hong-Yeop Song

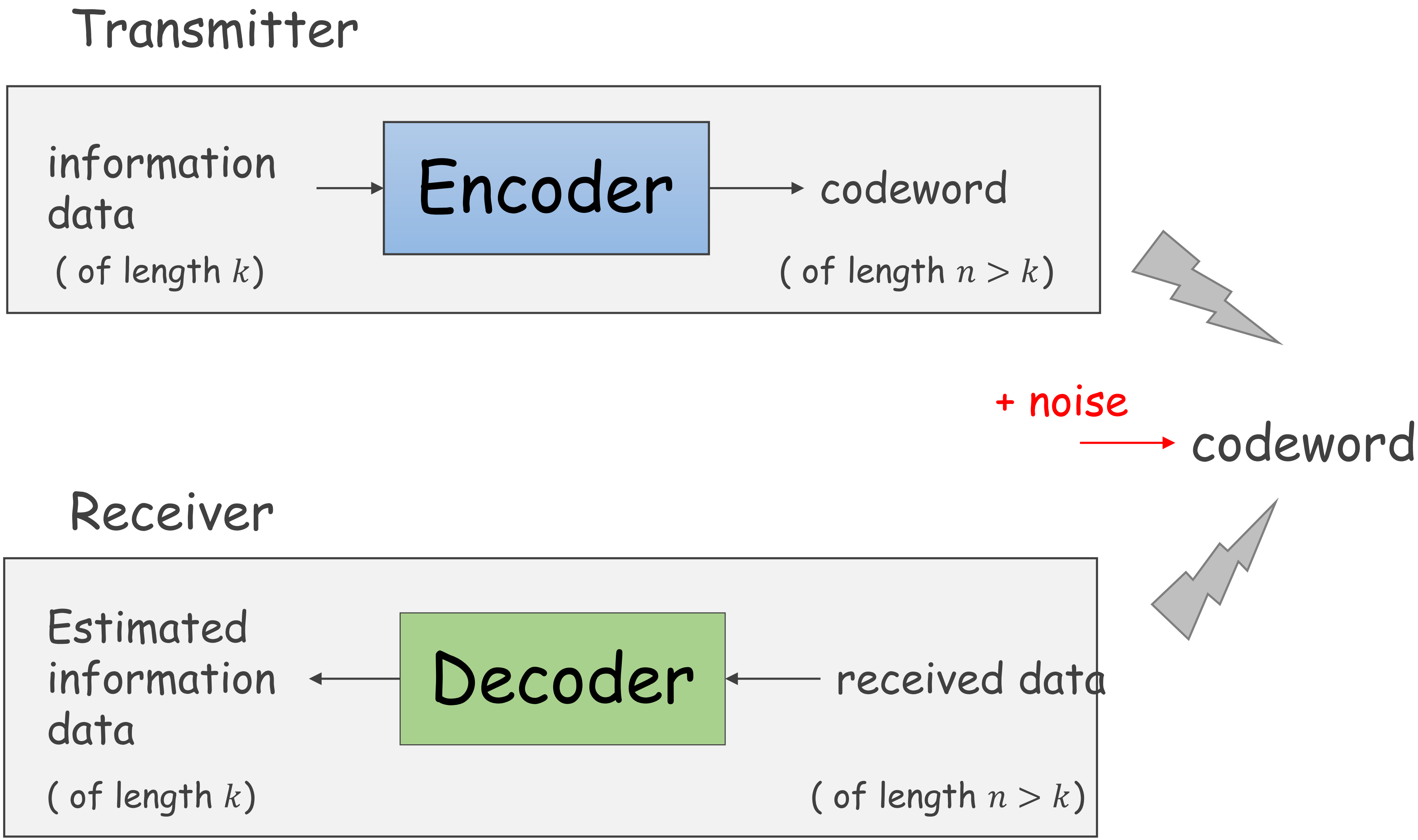
Yonsei University

2022.02.11

2022년 한국통신학회 동계종합학술발표회

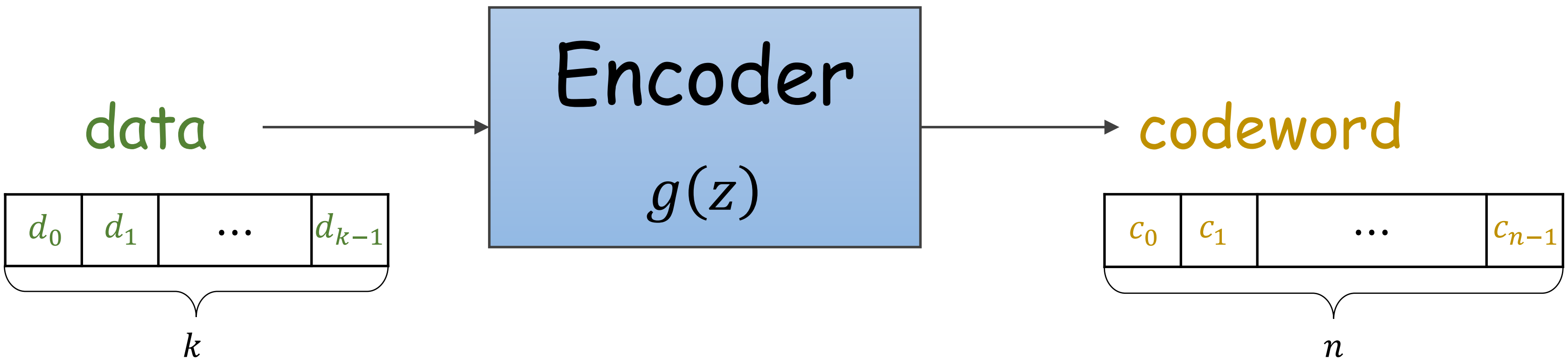
Contents

System model



RS code

- $[\boldsymbol{n}, \boldsymbol{k}]$ narrow-sense RS code over $\mathbb{F}_{2^m}$



$$d_0 + d_1 z + \cdots d_{k-1} z^{k-1} = d(z)$$

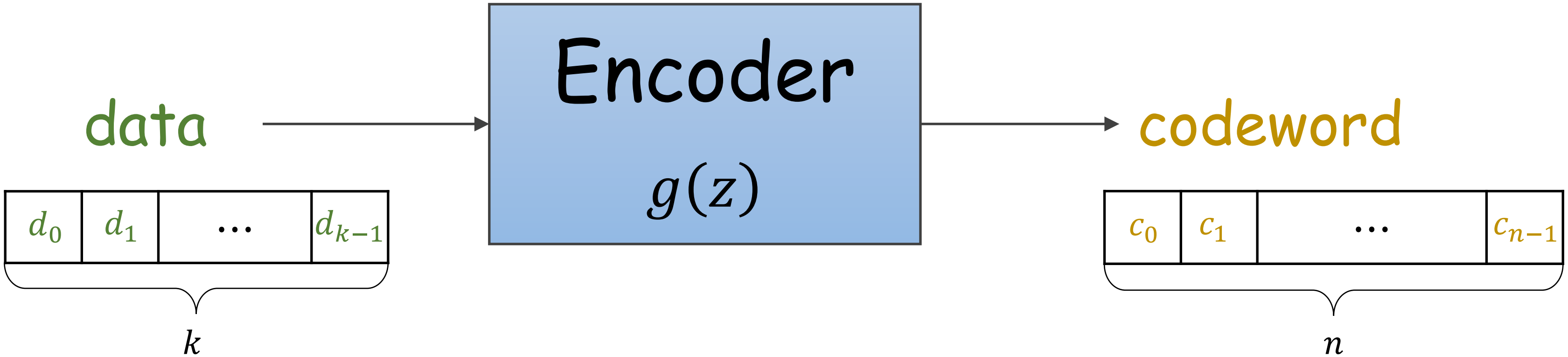
$$c_0 + c_1 z + \cdots c_{n-1} z^{n-1} = c(z)$$

RS code

- $[n, k]$ **narrow-sense** RS code over $\mathbb{F}_{2^m}$

$$g(z) = (z + \alpha)(z + \alpha^2) \cdots (z + \alpha^r),$$

where $r = n - k$



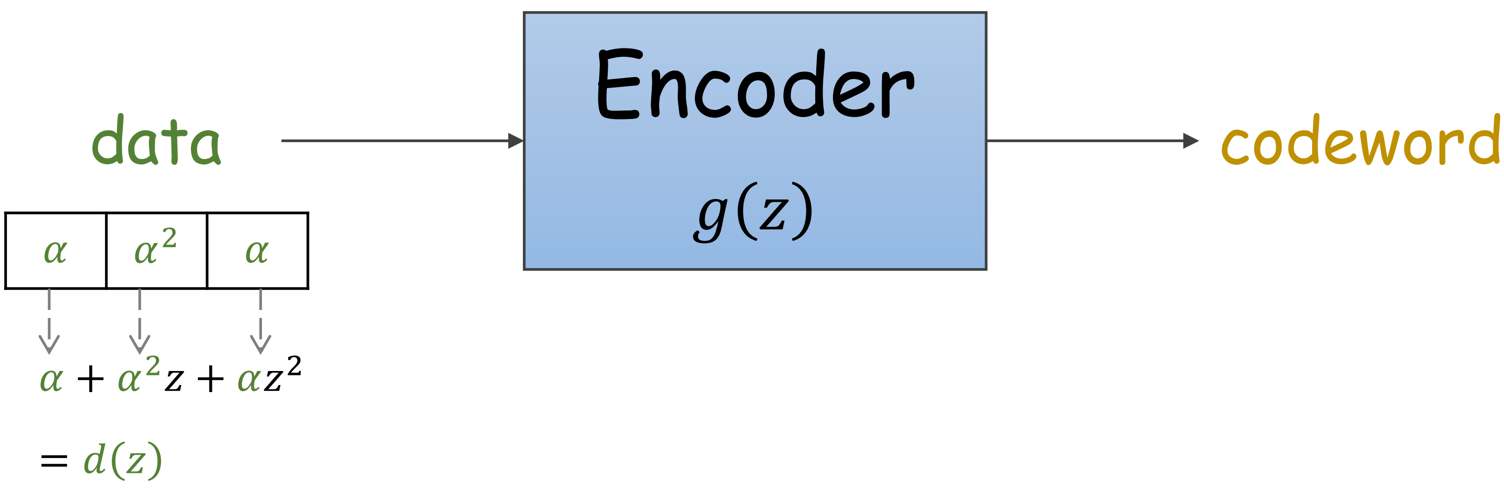
$$d_0 + d_1 z + \cdots d_{k-1} z^{k-1} = d(z)$$

$$c_0 + c_1 z + \cdots c_{n-1} z^{n-1} = c(z)$$

- α is the root of the primitive polynomial

Example: $[7,3]$ RS code over $\mathbb{F}_{2^3}$

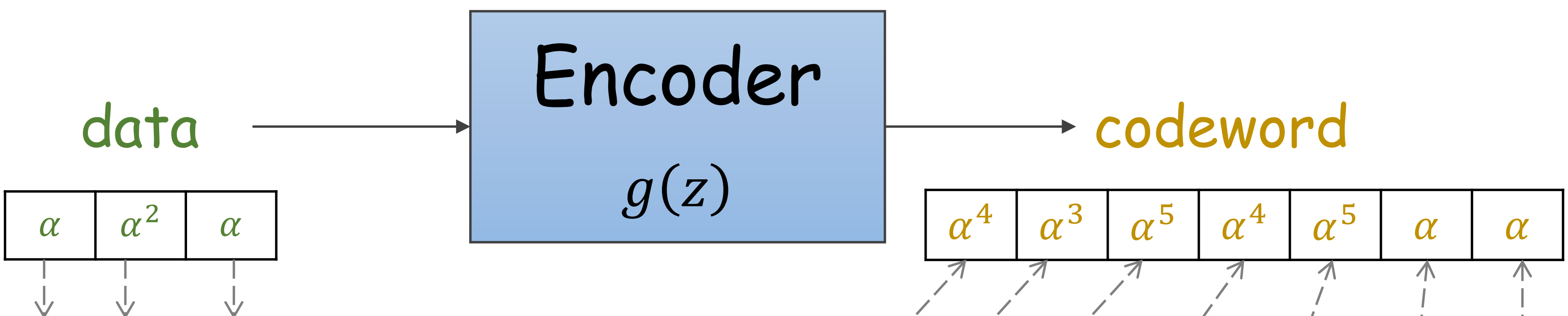
$$g(z) = (z+\alpha)(z+\alpha^2)(z+\alpha^3)(z+\alpha^4)$$
$$= \alpha^3 + \alpha z + z^2 + \alpha^3 z^3 + z^4$$



- α is the root of $z^3 + z + 1 = 0$

Example: $[7,3]$ RS code over $\mathbb{F}_{2^3}$

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



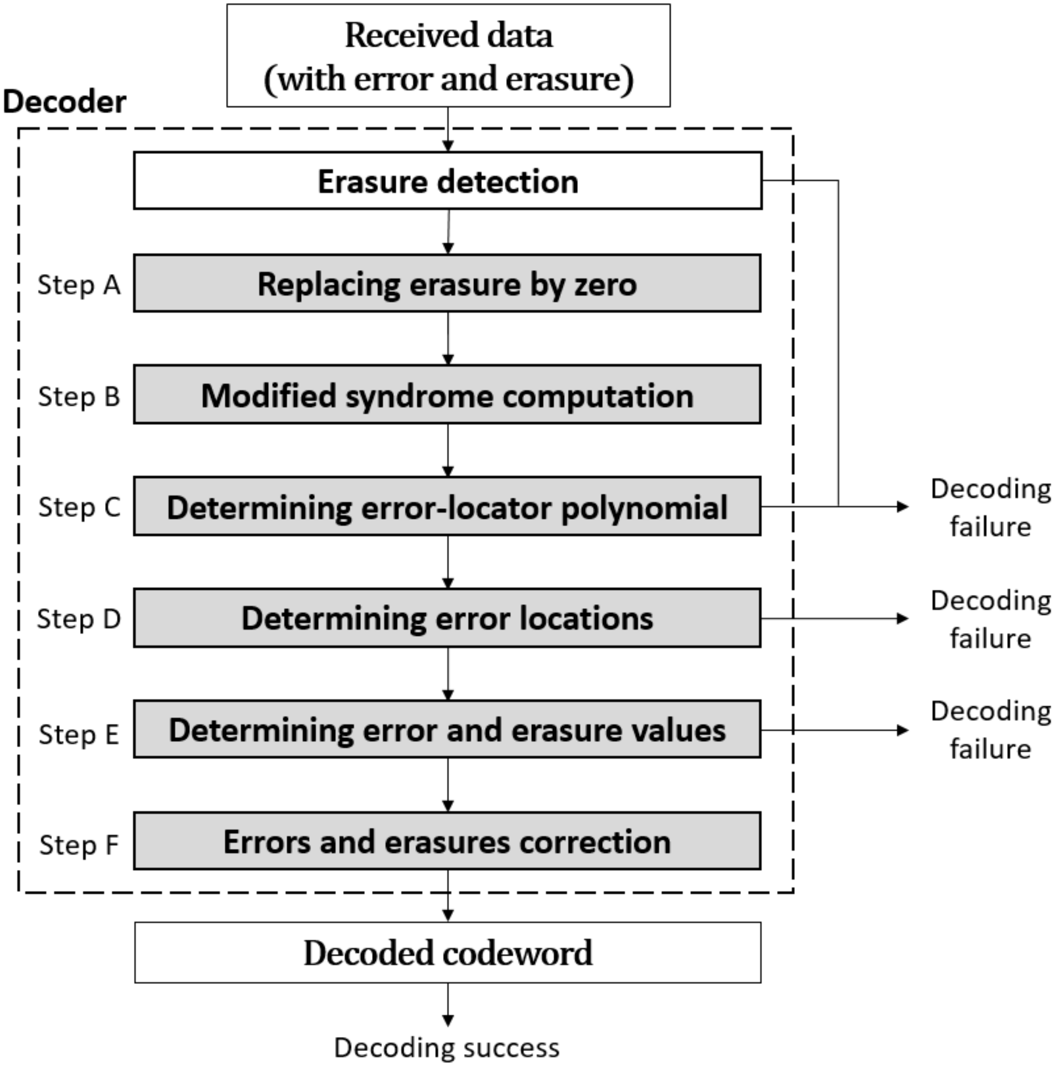
$\alpha + \alpha^2 z + \alpha z^2$

$= d(z)$

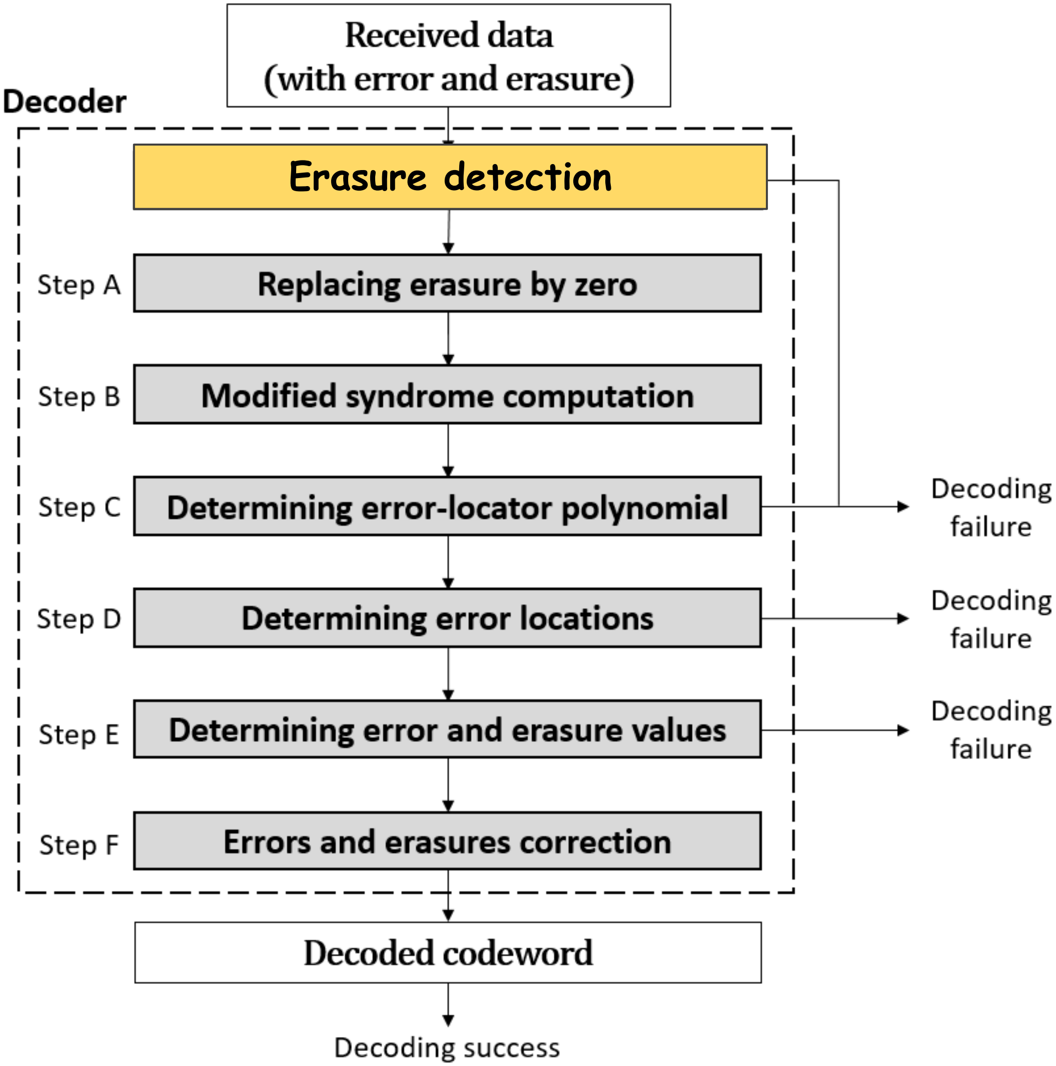
$d(z)g(z) = c(z) = \alpha^4 + \alpha^3 z + \alpha^5 z^2 + \alpha^4 z^3 + \alpha^5 z^4 + \alpha z^5 + \alpha z^6$

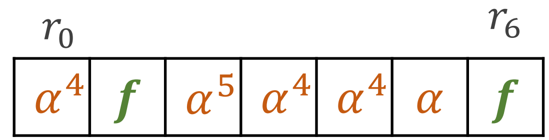
- α is the root of $z^3 + z + 1 = 0$

Decoding with errors and erasures

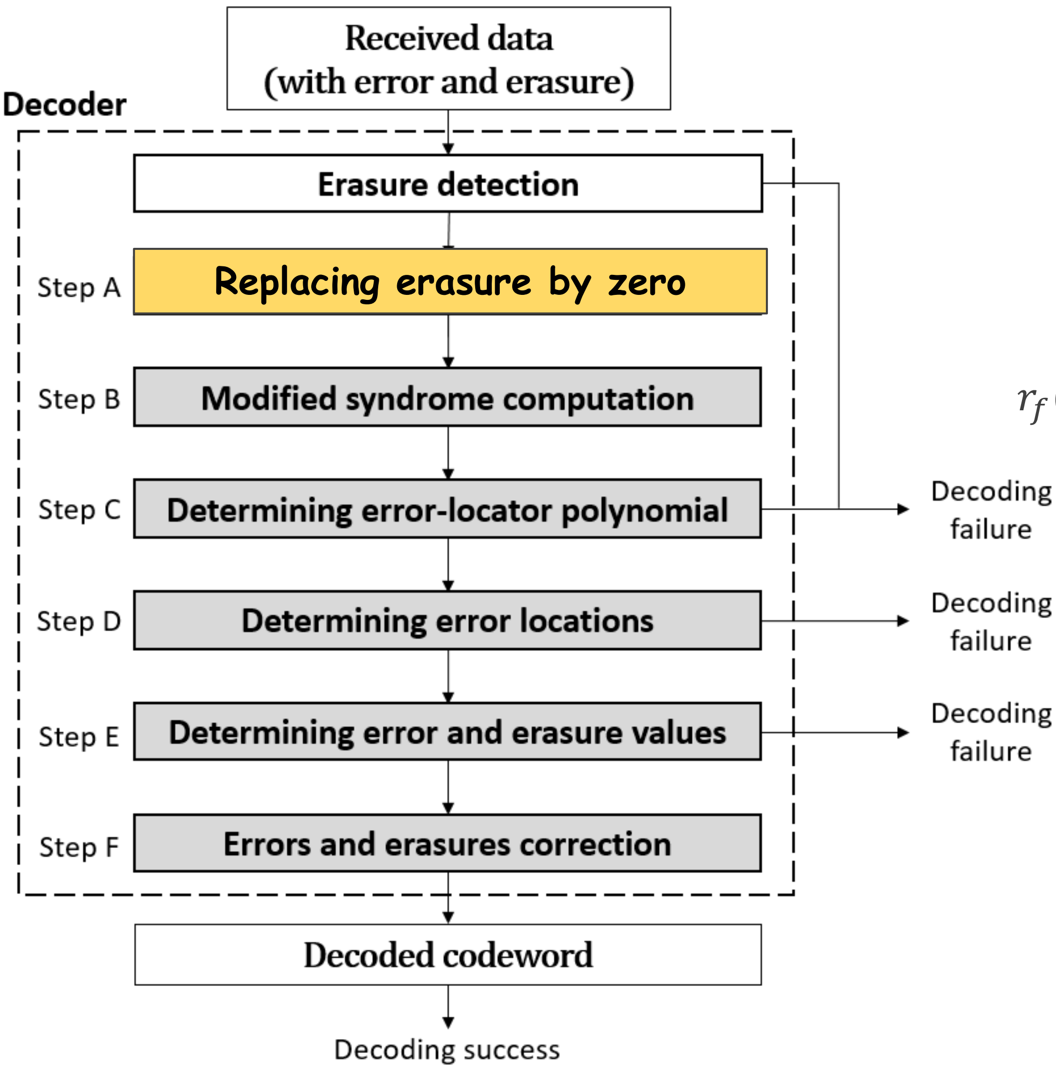


Decoding with errors and erasures





Decoding with errors and erasures



r_0	r_1					r_6
α^4	f	α^5	α^4	α^4	α	f

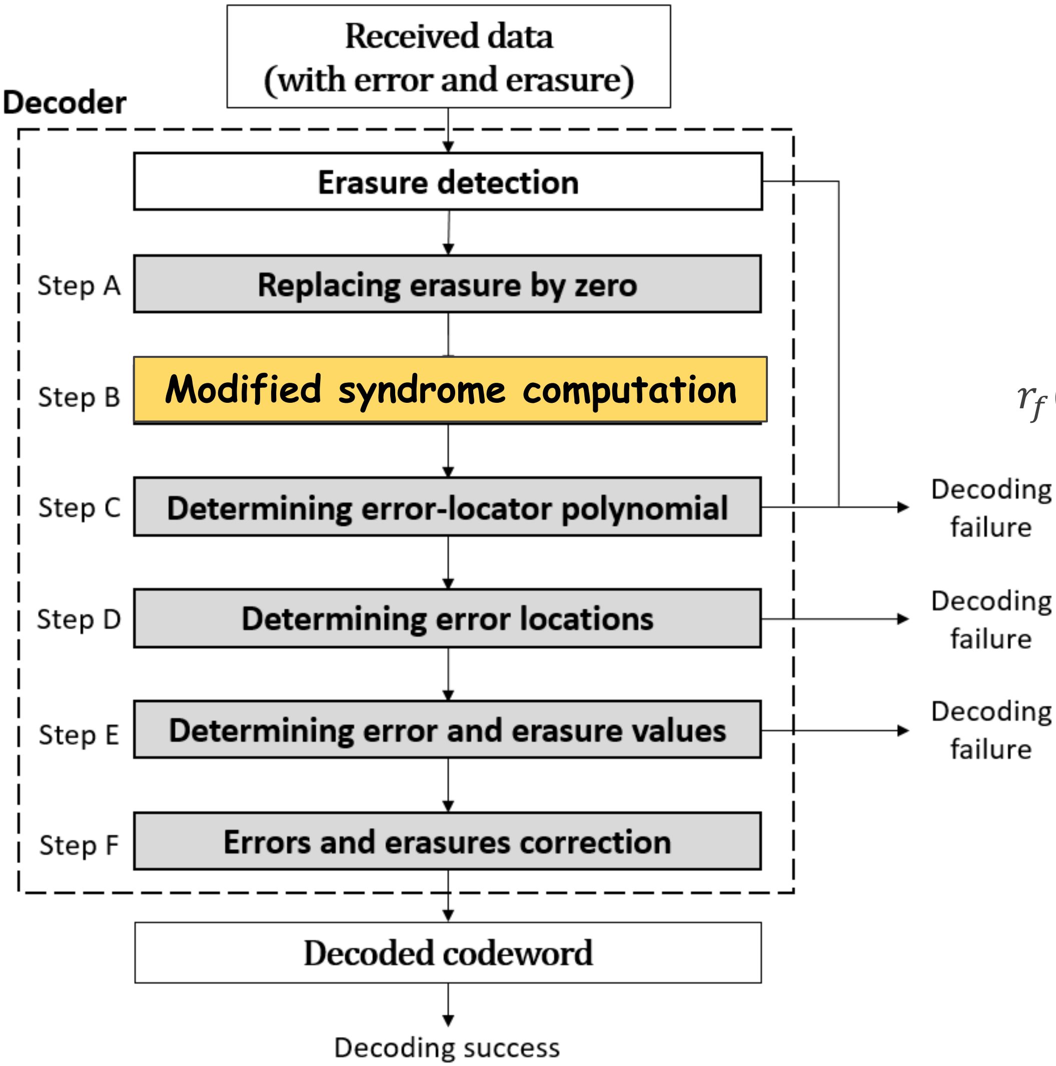
α^4	0	α^5	α^4	α^4	α	0

$$r_f(z) = \alpha^4 + \alpha^5 z^2 + \alpha^4 z^3 + \alpha^4 z^4 + \alpha z^5$$

Erasure-locator polynomial:

$$\tau(z) = (1 + \alpha^1 z)(1 + \alpha^6 z)$$

Decoding with errors and erasures



T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

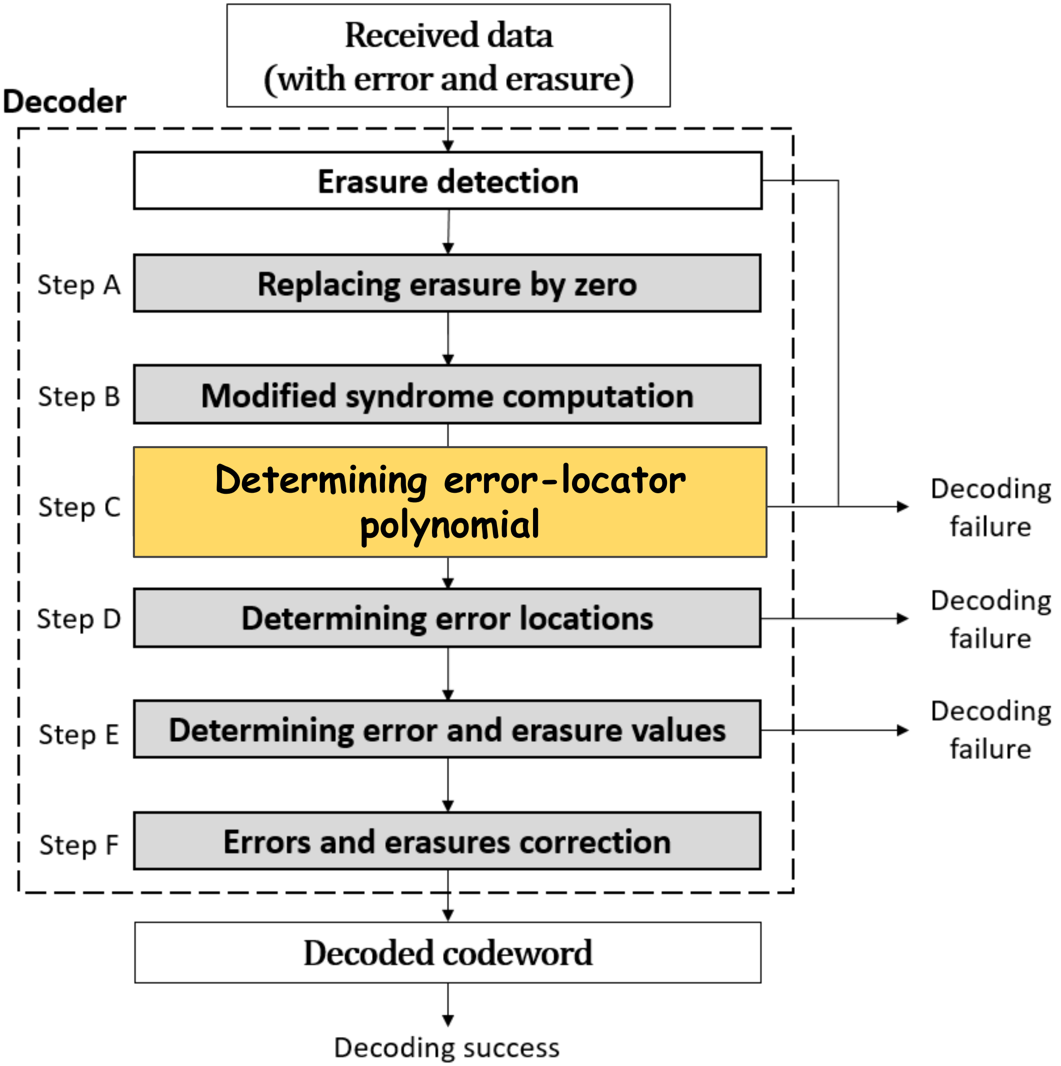
$\Uparrow$

$$r_f(z) = \alpha^4 + \alpha^5 z^2 + \alpha^4 z^3 + \alpha^4 z^4 + \alpha z^5$$

Erasure-locator polynomial:

$$\tau(z) = (1 + \alpha^1 z)(1 + \alpha^6 z)$$

Decoding with errors and erasures



the number of erasures: $\mu = 2$

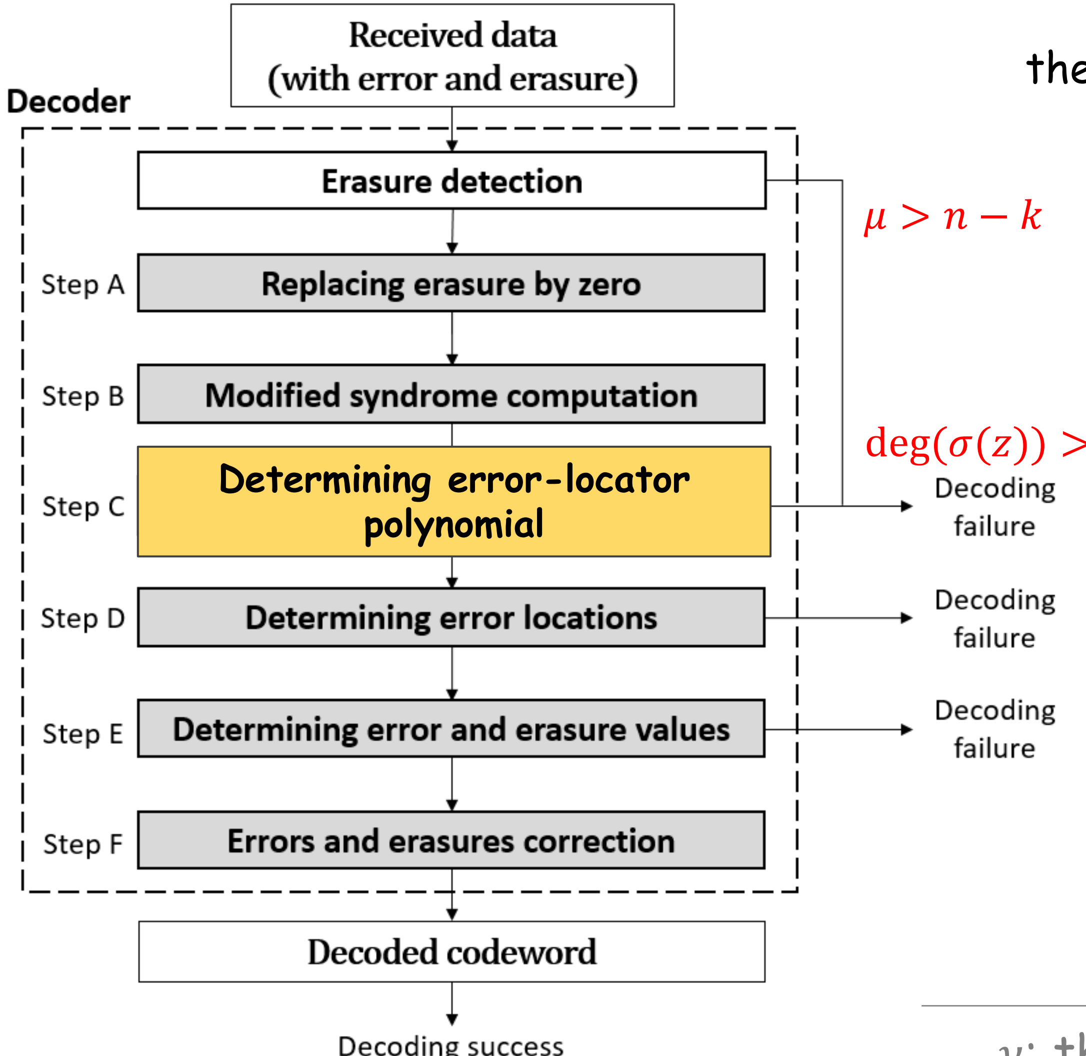
T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

$\Downarrow$

$\boldsymbol{\sigma(z)}$: error-locator polynomial

$$\sigma(z) = 1 + \alpha^4 z$$

Decoding with errors and erasures



the number of erasures: $\mu = 2$

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

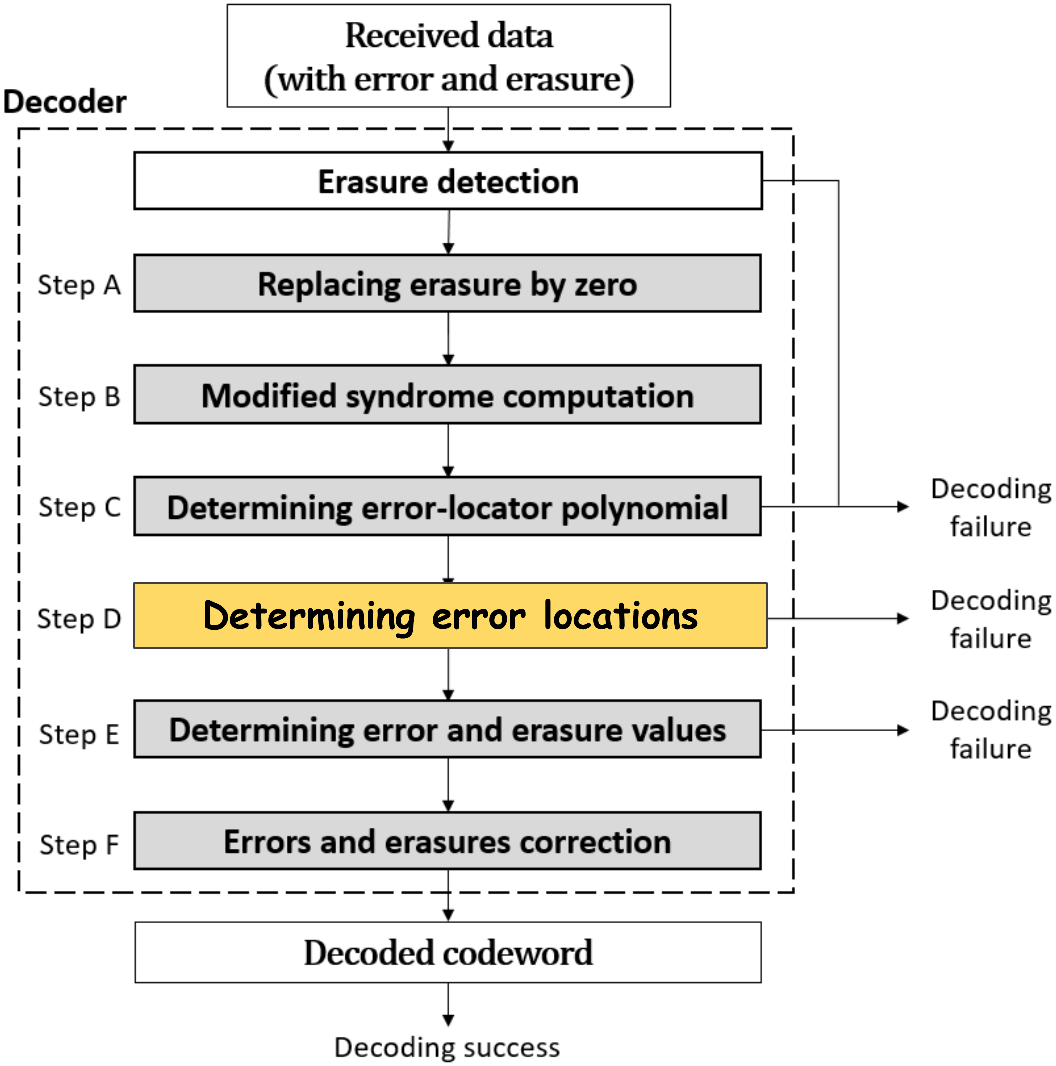
$\boldsymbol{\sigma(z)}$: error-locator polynomial

$\sigma(z) = 1 + \alpha^4 z$

Correctable range:
$2\nu + \mu \le n - k$

ν: the number of errors
μ: the number of erasures

Decoding with errors and erasures



$\boldsymbol{\sigma(z)}$: error-locator polynomial

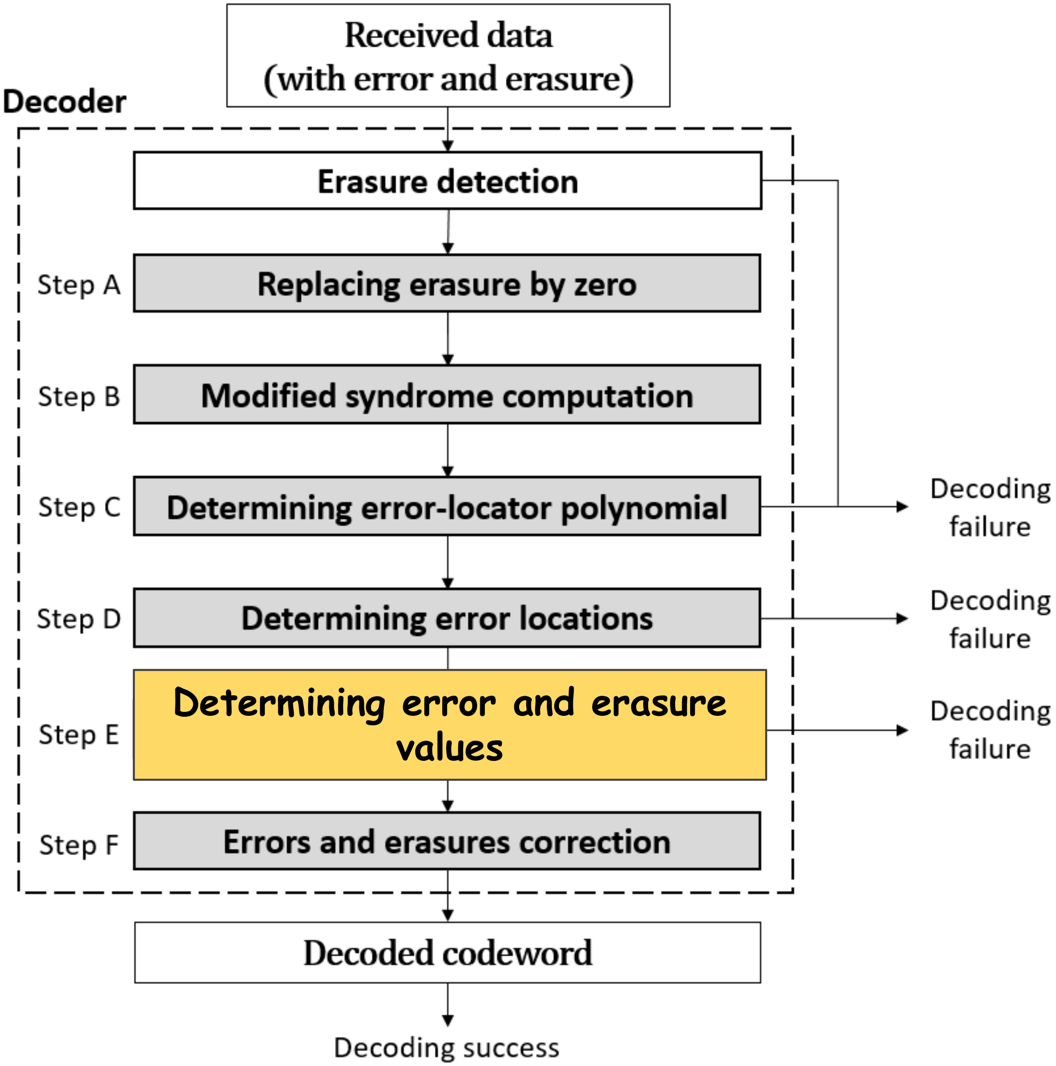
$$\sigma(z) = 1 + \alpha^4 z$$

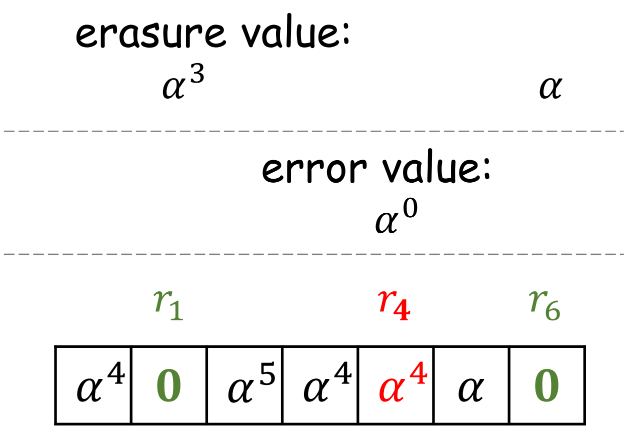
Root of $\sigma(z)$: α^3

The inverse of root: α^{4}

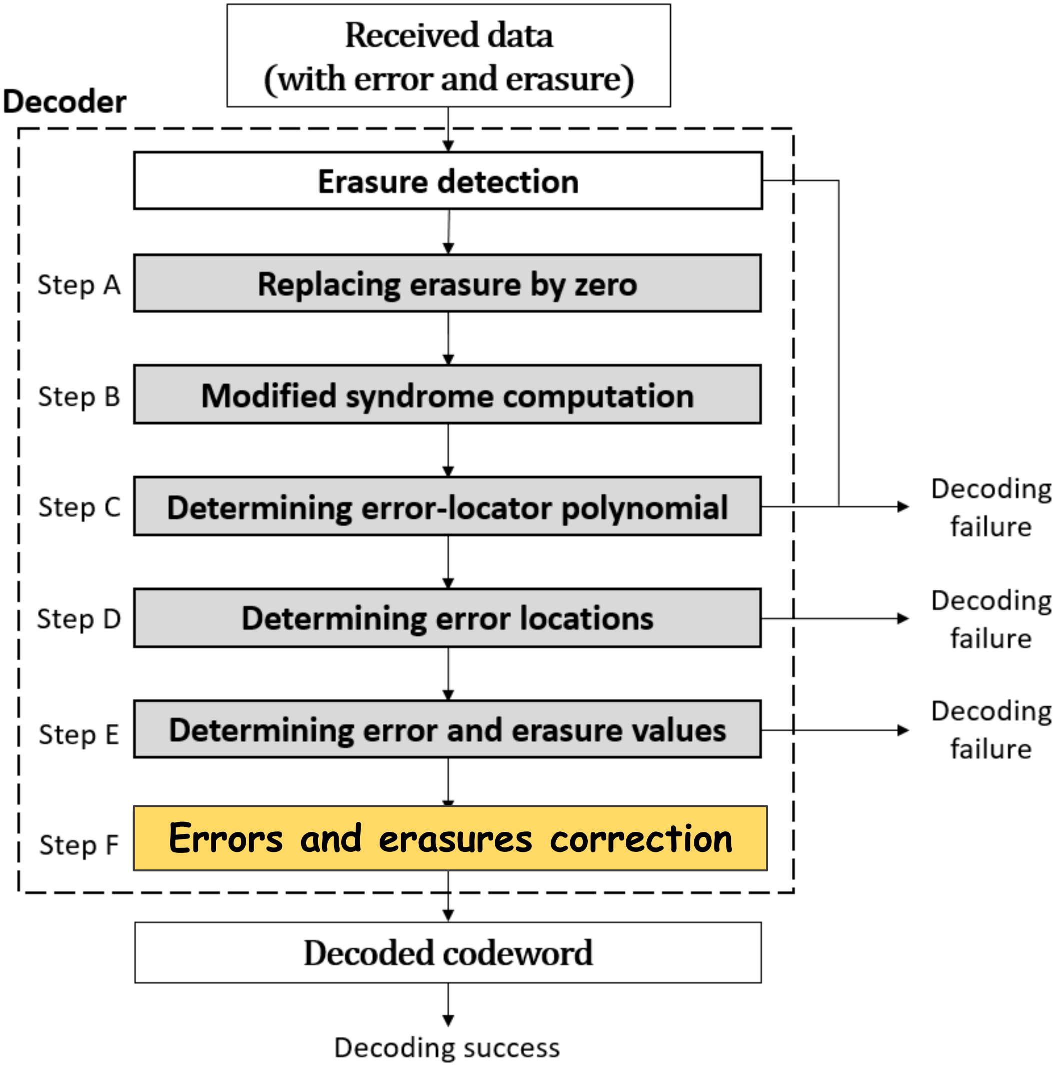
	r_1			r_4		r_6
α^4	**0**	α^5	α^4	α^4	α	**0**

Decoding with errors and erasures





Decoding with errors and erasures



erasure value:

α^3 α

---

error value:

α^0

---

	r_1			r_4		r_6
α^4	$\mathbf{0}$	α^5	α^4	α^4	α	$\mathbf{0}$

$\Downarrow$

α^4	α^3	α^5	α^4	α^5	α	α

Continued fractions

integer part fractional part

Field element

multiplication identity

$$s = a_0 + r_0$$

$$= a_0 + \cfrac{I}{a_1 + r_1}$$

$$= a_0 + \cfrac{I}{a_1 + \cfrac{I}{a_2 + r_2}}$$

$$\vdots$$

$$= a_0 + (a_1 + (a_2 + \cdots + (a_n + r_n)^{-1} \cdots)^{-1})^{-1}$$

$$= \frac{A_n(a_n + r_n) + B_n}{C_n(a_n + r_n) + D_n}$$

s_n: n^{th} approximation of s

$$s_n = \frac{A_n a_n + B_n}{C_n a_n + D_n} = \frac{P_n}{Q_n} \quad \Longrightarrow \quad \begin{aligned} P_{n+1} &= a_{n+1} P_n + P_{n-1} \\ Q_{n+1} &= a_{n+1} Q_n + Q_{n-1} \end{aligned}$$

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.

2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.

5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$

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**.

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.
2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.
5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$
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**.

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

the number of erasures: $\mu = 2$

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.

2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.

5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$

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**.

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

the number of erasures: $\mu = 2$

$$R^{(-1)}(z) = 1 + \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$R^{(0)}(z) = \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$X + any\ value = X$
$X \cdot any\ value = X$

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.

2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.

5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$

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**.

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

the number of erasures: $\mu = 2$

$$R^{(-1)}(z) = 1 + \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$R^{(0)}(z) = \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$b^{(1)} = \frac{\alpha^2}{1} = \alpha^2$$

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.
2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.
5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$
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**.

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

the number of erasures: $\mu = 2$

$$R^{(-1)}(z) = 1 + \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$R^{(0)}(z) = \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$b^{(1)} = \frac{\alpha^2}{1} = \alpha^2$$

$a^{(1)}(z)$: the quotient of $b^{(1)} R^{(-1)} \div R^{(0)}$
$= z + \alpha$

$R^{(1)}(z)$: the remainder of $b^{(1)} R^{(-1)} \div R^{(0)}$
$= X z^{-2}$

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.

2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.

5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$

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**.

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

the number of erasures: $\mu = 2$

$$R^{(-1)}(z) = 1 + \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$R^{(0)}(z) = \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$b^{(1)} = \frac{\alpha^2}{1} = \alpha^2$$

$a^{(1)}(z)$: the quotient of $b^{(1)} R^{(-1)} \div R^{(0)}$
$= z + \alpha$

$R^{(1)}(z)$: the remainder of $b^{(1)} R^{(-1)} \div R^{(0)}$
$= X z^{-2}$

$$P^{(1)}(z) = z + \alpha^4$$

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.

2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.

5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$

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**.

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

the number of erasures: $\mu = 2$

$$R^{(-1)}(z) = 1 + \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$R^{(0)}(z) = \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$b^{(1)} = \frac{\alpha^2}{1} = \alpha^2$$

$a^{(1)}(z)$: the quotient of $b^{(1)} R^{(-1)} \div R^{(0)}$ $= z + \alpha$

$R^1(z)$: the remainder of $b^{(1)} R^{(-1)} \div R^{(0)}$ $= Xz^{-2}$

$$P^{(1)}(z) = z + \alpha^4$$

Determining error-locator polynomial: Continued fractions-based algorithm

Algorithm 1 The process of determining $\sigma(z)$ based on the continued fractions with $T(z)$ and μ erasures

1: **Input** $T_1, T_2, \ldots, T_r, \mu$.

2: **Initialize** $k = 0$, $P^{(-1)}(z) = 1$, $P^{(0)}(z) = 1$,

$$R^{(-1)}(z) = 1 + \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)},$$

$$R^{(0)}(z) = \sum_{j=1}^{r-\mu} T_{\mu+j} \cdot z^{-j} + X \cdot z^{-(r-\mu+1)}.$$

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

$$b^{(k)} \cdot R^{(k-2)} = a^{(k)}(z) \cdot R^{(k-1)} + R^{(k)}(z),$$

where $a^{(k)}(z)$ must not contain negative powers of the indeterminate z.

5: Obtain $P^{(k)}(z) = a^{(k)}(z) \cdot P^{(k-1)} + b^{(k)} \cdot P^{(k-2)}$

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.**

T_1	T_2	T_3	T_4
α^4	α^4	α^2	α^6

the number of erasures: $\mu = 2$

$$R^{(-1)}(z) = 1 + \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$R^{(0)}(z) = \alpha^2 z^{-1} + \alpha^6 z^{-2} + X z^{-3}$$

$$b^{(1)} = \frac{\alpha^2}{1} = \alpha^2$$

$a^{(1)}(z)$: the quotient of $b^{(1)} R^{(-1)} \div R^{(0)}$ $= z + \alpha$

$R^1(z)$: the remainder of $b^{(1)} R^{(-1)} \div R^{(0)}$ $= X z^{-2}$

$$P^{(1)}(z) = z + \alpha^4$$

$$\sigma(z) = 1 + \alpha^4 z$$

Simulation result

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

No. of erasure	No. of error	Total	Decoding failure in			Undetected error
			CFA/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	-	-	-

Thank you !