(63, 51) BCH code example

1. Parameters

$m = 6,\ n = 63,\ k = 51,\ t = 2$. Primitive polynomial $p(X) = 1 + X + X^6$.

2. Encoding example

We use the generator polynomial

$g(X) = 1 + X^3 + X^4 + X^5 + X^8 + X^{10} + X^{12}$.

Suppose that the message is

$\boldsymbol{u} = (u_0, u_1, \ldots, u_{50})$

= (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0).

The remainder of $X^{63-51}u(X)$ divided by $g(X)$ is $b(X)$, which is

$\boldsymbol{b} = (b_0, b_1, \ldots, b_{11}) =$ (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1).

Therefore, the codeword is

$\boldsymbol{c} = (c_0, c_1, \ldots, c_{62})$

= (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0).

3. Decoding example

Let the error pattern be $e(X)$, where $e_6 = 1,\ e_{20} = 1$, and $e_i = 0$ for $i \neq 6, 20$.

Note that we do not know the error pattern in actual situation.

The received code is

$\boldsymbol{r} = (r_0, r_1, \ldots, r_{62})$

= (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0).

Step 1: Syndrome calculation

We need to calculate $\boldsymbol{S} = (S_1, S_2, S_3, S_4)$.

$S_1 = r(\alpha) = \alpha^{58},\ S_2 = r(\alpha^2) = \alpha^{53},\ S_3 = r(\alpha^3) = \alpha^{39},\ S_4 = r(\alpha^4) = \alpha^{43}$.

Step 2: Berlekamp's algorithm

Initialization

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$
-1	1	1	0	-1
0	1	α^{58}	0	0

We fill the row of $\mu = 1$.

$d_0 \neq 0$, so we choose $\rho = -1$.

$\sigma^{(1)}(X) = \sigma^{(0)}(X) + d_0 d_{-1}^{-1} X^1 \sigma^{(-1)}(X) = 1 + \alpha^{58} \cdot 1 \cdot X \cdot 1 = 1 + \alpha^{58} X.$

$l_1 = \max(l_0, l_{-1} + 1) = 1.$

$d_1 = S_2 + \sigma_1^{(1)} S_1 = \alpha^{53} + \alpha^{58}\alpha^{58} = 0.$

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$
-1	1	1	0	-1
0	1	α^{58}	0	0
1	$1 + \alpha^{58} X$	0	1	0

We fill the row of $\mu = 2$.

$d_1 = 0$, so $\sigma^{(2)}(X) = \sigma^{(1)}(X) = 1 + \alpha^{58} X$, and $l_2 = l_1 = 1$.

$d_2 = S_3 + \sigma_1^{(2)} S_2 = \alpha^{39} + \alpha^{58}\alpha^{53} = \alpha^{21}.$

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$
-1	1	1	0	-1
0	1	α^{58}	0	0
1	$1 + \alpha^{58} X$	0	1	0
2	$1 + \alpha^{58} X$	α^{21}	1	1

We fill the row of $\mu = 3$.

$d_2 \neq 0$, so we choose $\rho = 0$.

$\sigma^{(3)}(X) = \sigma^{(2)}(X) + d_2 d_0^{-1} X^2 \sigma^{(0)}(X) = 1 + \alpha^{58} X + \alpha^{21} \cdot \alpha^{-58} \cdot X^2 \cdot 1 = 1 + \alpha^{58} X + \alpha^{26} X^2.$

$l_3 = \max(l_2, l_0 + 2) = 2.$

$d_3 = S_4 + \sigma_1^{(3)} S_3 + \sigma_2^{(3)} S_2 = \alpha^{43} + \alpha^{58}\alpha^{39} + \alpha^{26}\alpha^{53} = 0.$

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$
-1	1	1	0	-1
0	1	α^{58}	0	0
1	$1+\alpha^{58}X$	0	1	0
2	$1+\alpha^{58}X$	α^{21}	1	1
3	$1+\alpha^{58}X+\alpha^{26}X^2$	0	2	1

We fill the row of $\mu = 4$.

$d_3 = 0$, so $\sigma^{(4)}(X) = \sigma^{(3)}(X) = 1 + \alpha^{58}X + \alpha^{26}X^2$.

We terminate the loop and obtain $\sigma(X) = 1 + \alpha^{58}X + \alpha^{26}X^2$.

Step 3: Finding the roots

We have $\sigma(\alpha^{-6}) = 1 + \alpha^{58}\alpha^{-6} + \alpha^{26}\alpha^{-12} = 0$ and $\sigma(\alpha^{-20}) = 1 + \alpha^{58}\alpha^{-20} + \alpha^{26}\alpha^{-40} = 0$.

So, the error location numbers are 6 and 20.

We perform the error correction.

$\hat{c}(X) = r(X) + e(X) = r(X) + X^6 + X^{20}$.

$\hat{\boldsymbol{c}} = (\hat{c}_0, \hat{c}_1, \dots, \hat{c}_{62})$

= (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)