

Bose-Chaudhuri-Hocquengham (BCH) Codes

An important class of multiple-error-correcting codes is the class of Bose-Chaudhuri-Hocquengham codes or \mathcal{BCH} codes. These codes are important for two reasons:

1. They admit a relatively easy decoding scheme.
2. The class of \mathcal{BCH} codes is quite extensive. Indeed, for any positive integers r and t with $t \leq 2^{r-1} - 1$, there is a \mathcal{BCH} code of length $n = 2^r - 1$ which is t -correcting and has dimension $k \geq n - rt$.

The class of \mathcal{BCH} codes is, in fact, a generalization of the Hamming codes for multiple-error correction. Binary \mathcal{BCH} codes were first discovered by A. Hocquenghem in 1959 and independently by R. C. Bose and D. K. Ray-Chaudhuri in 1960.

Example. Let b be a primitive element in $GF(2^r)$ ($r \geq 4$) generated by a primitive polynomial $h(x) = 1 + x + x^4$.

The 2 error-correcting \mathcal{BCH} code of length $2^r - 1$ is the cyclic linear code that is generated by $g(x) = m_b(x) * m_b^3(x)$, where $m_b(x)$ and $m_b^3(x)$ are minimal polynomials of b and b^3 .

Word	P(x) modulo h(x)	Power of b
0000	0	---
1000	1	$*b^0 = 1$
0100	x	b^1
0010	x^2	b^2
0001	x^3	$*b^3$
1100	$x^4 = 1 + x$	b^4
0110	$x^5 = x + x^2$	b^5
0011	$x^6 = x^2 + x^3$	$*b^6$
1101	$x^7 = 1 + x + x^3$	b^7
1010	$x^8 = 1 + x^2$	b^8
0101	$x^9 = x + x^3$	$*b^9$
1110	$x^{10} = 1 + x + x^2$	b^{10}
0111	$x^{11} = x + x^2 + x^3$	b^{11}
1111	$x^{12} = 1 + x + x^2 + x^3$	$*b^{12}$
1011	$x^{13} = 1 + x^2 + x^3$	b^{13}
1001	$x^{14} = 1 + x^3$	b^{14}

$$H = \begin{pmatrix} & \text{power of } b & & & \text{power of } b^3 & & & \\ & & & & & & & \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

♣ Algorithm for IMLD.

Enter your 15-digit received word:

$$[110111101011000]$$

STEP 1. Calculate the syndrome $wH = [s_1, s_3] = [w(b), w(b^3)]$:

$$\text{syndrome} = [01110110]$$

STEP 2.

$$s_1 = [0111] \quad s_3 = [0110]$$

If $s_1 = s_3$, conclude that no error occurred.

If $s_1 = 0$ and $s_3 \neq 0$, then ask for retransmission.

STEP 3.

$$s_1 = [0111] = b^{11} \quad s_3 = [0110] = b^5$$

If $s_1^3 = s_3$, then correct a single error at position i , where $s_1 = b^i$.

$$s_1^3 = (b^{11})^3 = b^{33} = b^3 = [0001]$$

$$s_3 = [0110] = b^5$$

STEP 4. If s_1^3 and s_3 are different, then form the quadratic equation:

$$\begin{aligned}
 x^2 + s_1x + (s_3/s_1 + s_1^2) &= 0. \\
 s_3/s_1 + s_1^2 &= b^5 * b^{(-11)} + (b^{11})^2 = b^9 + b^7 \\
 &= [0101] + [1101] = [1000] = b^0
 \end{aligned}$$

so

$$x^2 + (b^{11})x + b^0 = 0$$

STEP 5. If the quadratic equation has two distinct roots b^i and b^j , correct errors at positions i and j .

Trying the elements of $GF(2^4)$ in turn as possible roots, we come to $x = b^7$ and find

$$\begin{aligned}
 (b^7)^2 + b^{11} * b^7 + b^0 &= b^{14} + b^3 + b^0 \\
 &= [1001] + [0001] + [1000] \\
 &= [0000].
 \end{aligned}$$

Now $b^7 * b^j = 1 = b^{15}$, so $b^j = b^8$ is the other root. Therefore we correct errors at positions $i = 7$ and $j = 8$; that is

$$u = [000000110000000]$$

is the most likely error pattern. We decode

$$v = w + u = [110111110011000]$$

as the word sent.

STEP 6.

If the quadratic equation does not have two distinct roots in $GF(2^r)$, conclude that at least three errors occurred in transmission, and ask for a retransmission.