So it ($bch_7(5,5)$?) has only $7^1 = 7$ words

Since $d = 5$, can correct 2 errors.

$$|S(c,2)| = \binom{5}{0} + \binom{5}{1}(7-1) + \binom{5}{2}(7-1)^2 = 1 + 30 + 360 = 391$$

$\therefore \left|\bigcup_{c\in C} S(c,2)\right| = 7\cdot 391 = 2737$

But $\left|\mathbb{F}_7^5\right| = 7^5 = 16807$

So not perfect.

See handout for BCH decoding algorithm.

Note:

1) only applies when d is odd

(so $d - 1 = 2t$)

2) Not only for $bch_p(n, d)$

Top row of H need not be 1, 2,..., n

Example:

$bch_7(5,5)$

$d = 5$, so $t = 2$

Suppose we receive $y = (1, 0, 0, 6, 3)$

1) $S(y) = (1, 0, 0, 6, 3) H^t = (5, 4, 4, 3)$

2) so $\sigma(z) = 5z + 4z^2 + 4z^3 + 3z^4$

3) $B(z) = 1 + B_1(z) + B_2(z^2)$

So $\sigma(z) B(z) = \ldots + (5B_2 + 4B_1 + 4)z^3 + (4B_2 + 4B_1 + 3)z^4$

$5B_2 + 4B_1 + 4 = 0$

$4B_2 + 4B_1 + 3 = 0$

These two equations are linearly independent

$\therefore s = 2 = t$

So there are no B_i to set to zero and we solve for the others.

$$\begin{bmatrix} 5 & 4 & -4 \\ 4 & 4 & -3 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -1 \\ 4 & 4 & -3 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -1 \\ 0 & 4 & -6 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -12 \end{bmatrix}$$

$\therefore B_2 = -1 = 6,\ B_1 = -12 = 2$

$B(z) = 1 + 2z + 6z^2$

4) $A(z) = z$ and z^2 terms in $\sigma(z)B(z)$

$= z$ and z^2 terms in $(5z + 4z^2 + \ldots)(1 + 2z + \ldots)$

$= 5z + 14z^2 = 5z$

$B'(z) = 2 + 5z$

5) $B(z) = 1 + 2z + 6z^2 = (1 - 2z)(1 - 3z)$

α_j's are 2 and 3

So here j's are 2 and 3

$M = \{2, 3\}$

6) So we decode y as

$$y + \sum_{j \in \{2, 3\}} \alpha_j A\left(a_j^{-1}\right)\left(B'\left(\alpha_j^{-1}\right)\right)^{-1} e_j$$

$$= y + 2A(4)(B'(4))^{-1}e_2 + y + 3A(5)(B'(5))^{-1}e_3$$

$$= y + 2\cdot 6\cdot 1^{-1}e_2 + 3\cdot 4\cdot 6^{-1}e_3 = (1, 0, 0, 6, 3) + 5e_2 + 2e_3 = (1, 5, 2, 6, 3)$$