Before we get into BCH codes, we will need some basic results from Linear Algebra. Therefore, we will first get introduced with some Linear Algebra results (proofs will be omitted), and then define generalised version of a particular class of BCH codes, along with their decoding procedure.

0.1 Preliminary results from linear algebra

Theorem 0.1. Suppose $a_1, a_2, \ldots, a_r$ are distinct non-zero elements of a field. Then the determinant of the following matrix A (called *Vandermonde matrix*) is non-zero and is given by $\prod_{i>j}(a_i - a_j)$.

$$A = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_r \\ a_1^2 & a_2^2 & \cdots & a_r^2 \\ \vdots & \vdots & & \vdots \\ a_1^{r-1} & a_2^{r-1} & \cdots & a_r^{r-1} \end{bmatrix} \text{ and } det(A) = \prod_{i>j}(a_i - a_j)$$

Theorem 0.2. If A is an $r \times r$ matrix having a non-zero determinant, then the r columns of A are linearly independent (converse is also true).

0.2 A class of BCH codes

Now we will give construction for t-error-correcting code of length n over $GF(q)$, provided

$$2t + 1 \leq n \leq q - 1.$$

We will assume for simplicity that q is a prime, so that $GF(q) = \{0, 1, \ldots, q-1\}$, but this construction can be generalized for any prime-power by relabelling accordingly.
Let C be the code over $GF(q)$ defined to have the parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 3 & \cdots & n \\ 1 & 2^2 & 3^2 & \cdots & n^2 \\ \vdots & & & & \\ 1 & 2^{d-2} & 3^{d-2} & \cdots & n^{d-2} \end{bmatrix}$$

where $d \leq n \leq q - 1$, i.e.

$$C = \left\{ x_1 x_2 \cdots x_n \in V(n, q) \mid \sum_{i=1}^{n} i^i x_i = 0 \text{ for } j = 0, 1, \ldots, d-2 \right\}.$$

Theorem 0.3. If q is a prime-power and if $d \leq n \leq q - 1$, then

$$A_q(n, d) = q^{n-d+1}.$$

Proof. Any $d - 1$ columns of H (defined above) form a Vandermonde matrix and so are linearly independent, by Theorems 0.1 and 0.2. Also, any d columns of H corresponds to solving $d - 1$ linear equations in d variables, which implies the linear dependence of those d columns. Hence, by Theorem **??**, C has a minimum distance of d and so is a q-ary (n, q^{n-d+1}, d)-code and it meets the Singleton bound (Theorem **??**). □

Decoding algorithm:
Suppose the codeword $\mathbf{x} = x_1 x_2 \cdots x_n$ is transmitted and that the vector $\mathbf{y} = y_1 y_2 \cdots y_n$ is received in which we assume atmost t errors have occurred, at positions $X_1, X_2, \ldots, X_t$ with respective magnitudes $m_1, m_2, \ldots, m_t$ (if $e < t$ errors have occurred then we assume other magnitudes to be zero). From $\mathbf{y}$ we calculate the syndrome

$$(S_1, S_2, \ldots, S_{2t}) = \mathbf{y}H^T,$$

Thus, we must solve for X_i and m_i the following equations

$$\left.\begin{array}{lll} m_1 + m_2 & +\cdots+ m_t & = S_1 \\ m_1X_1 + m_2X_2 & +\cdots+ m_tX_t & = S_2 \\ m_1X_1^2 + m_2X_2^2 & +\cdots+ m_tX_t^2 & = S_3 \\ \vdots & & \\ m_1X_1^{2t-1} + m_2X_2^{2t-1} & +\cdots+ m_tX_t^{2t-1} & = S_2t. \end{array}\right\} \tag{1}$$

Now consider the expression

$$\phi(\theta) = \frac{m_1}{1 - X_1\theta} + \frac{m_2}{1 - X_2\theta} + \cdots + \frac{m_t}{1 - X_t\theta} \tag{2}$$

Now as $\dfrac{m_j}{1 - X_j\theta} = m_j(1 + X_j\theta + X_j^2\theta^2 + \cdots)$,
and therefore by combination of set of eqautions (1) and equation 2, we get

$$\phi(\theta) = S_1 + S_2\theta + S_3\theta^2 + \cdots + S_{2t}\theta^{2t-1} + \cdots \tag{3}$$

Reducing the fractions in (2), we have

$$\phi(\theta) = \frac{A_1 + A_2\theta + A_3\theta^2 + \cdots + A_t\theta^{t-1}}{1 + B_1\theta + B_2\theta^2 + \cdots + B_t\theta^t}. \tag{4}$$

Hence,

$$(S_1 + S_2\theta + S_3\theta^2 + \cdots)(1 + B_1\theta + B_2\theta^2 + \cdots + B_t\theta^t) = A_1 + A_2\theta + A_3\theta^2 + \cdots + A_t\theta^{t-1}.$$

Equationg coefficients of like powers of θ, we have

$$\left.\begin{array}{l} A_1 = S_1 \\ A_2 = S_2 + S_1B_1 \\ \quad\vdots \\ A_t = S_t + S_{t-1}B_1 + S_{t-2}B_2 + \cdots + S_tB_{t-1} \end{array}\right\} \tag{5}$$

$$\left.\begin{array}{l} 0 = S_{t+1} + S_tB_1 + S_{t-1}B_2 + \cdots + S_1B_t \\ 0 = S_{t+2} + S_{t+1}B_1 + S_tB_2 + \cdots + S_2B_t \\ \vdots \\ 0 = S_{2t} + S_{2t-1}B_1 + S_{2t-2}B_2 + \cdots + S_tB_t \end{array}\right\} \tag{6}$$

Since S_is are known, the t equations (6) gives us B_is, and then A_is can be found from equations in (5).
After this, we can split equation (4) into partial fractions and compare with equation (2) to get corresponding m_i and X_i.

Note: By directly looking at the syndrome vector, we cannot predict the number errors which have actually occured, but the number of actual errors e will be same as the maximum number of linearly independent equations in system (6). After finding e, we can substitute $B_{e+1}, B_{e+2}, \ldots, B_t$ all equal to zero, and the denominator in equation (4), becomes

$$1 + B_1\theta + B_2\theta^2 + \cdots + B_e\theta^e$$

which can be factorised to give the e errors and their location.