Linear Block Code

Andersen Ang

First created: 2013-Nov. Last update: 2017-Feb-1

Consider a message m with length k (k bits), an encoding scheme E (which tells how the parity bits p are generated), then the code can be expressed as

$$c = m + p = m + E(m)$$

When the parity bits are generated as linear combination of the message bits, so it is called *linear code*, and in this case

$$E\left(m\right) = Em$$

The encoding function $E(m)$ becomes a multiplication between the message m and the encoding scheme matrix E

For example, suppose the message m has 3 bits : $m = m_1 m_2 m_3$, and the parity bits are generated as

$$\begin{aligned} p_1 &= m_1 + m_3 \\ p_2 &= m_1 + m_2 \\ p_3 &= m_2 + m_3 \end{aligned}$$

Then the partiy bits p can be expressed as

$$\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}$$

And therefore

$$E = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

That is, the elements E_{ij} in E tells the relationship between the partiy bits p_i and the message bits m_j

By using such notation, thus the generator matrix G, which transform the message m into codeword c is

$$c = Gm$$

For example, using the encoding scheme as stated above, and put the parity bits before the message,

$$c = \begin{bmatrix} p \\ m \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ m_1 \\ m_2 \\ m_3 \end{bmatrix} = \begin{bmatrix} m_1 + m_3 \\ m_1 + m_2 \\ m_2 + m_3 \\ m_1 \\ m_2 \\ m_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = \begin{bmatrix} E \\ I_{3\times 3} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}$$

And thus

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{bmatrix} = \begin{bmatrix} E \\ I_{3\times 3} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}$$

And the matrix $\begin{bmatrix} E \\ I_{3\times 3} \end{bmatrix}$ is denoted as generator matrix G

Property of G

It can be observed that G has two submatrices, the encoding matrix E and the identity matrix I

The size of the matrix G is $n - by - k$ where n is the length of the codeword and k is the length of the message.

The order of the identity matrix is thus of order $k - by - k$.

The order of the encoding matrix is $k - by - (n - k)$

Parity Check Matrix H

A matrix H that the kernel (null space) is the set of all the codeword C is called parity check matrix H

Since the kernal of H is the entire set of the codeword C, therefore, therefore

$$Hc = 0$$

since $c = Gm$, so

$$HGm = 0$$

since $m \neq 0$ (message is not empty message), so

$$HG = 0$$

Since G has the structure $G = \begin{bmatrix} E \\ I \end{bmatrix}$, therefore inorder for the product HG to be zero, H can have the following structure

$$H = \begin{bmatrix} I & -E \end{bmatrix}$$

Symdrome Decoding

Assume we have a message m. After the message pass through the encoder E , we have the parity bits p. Combinding the parity bits and the message bits we have the codeword c. Now we send the codeword c to the receiver. Since there is noise in the communication channel, so the codeword received in the receiver , denoted as r , will have some error e

$$r = c + e$$

Then, we can indeed recover the orginal code word c by using the following scheme : computer Hr

$$Hr = H(c + e) = Hc + He = HGm + He$$

Since $HG = 0$, so it reduces to

$$Hr = He$$

Assume there is now only ONE error, so that the error vector e only have one position is 1, and other positions are all zero.

Since the multiplication of He means computing the linear combination of the columns of H weighted by the coefficients of e , therefore the result will be one column of the martrix H.

And therefore, by comparing the result of Hr to the columns of H, we can know which position has error.