Multiple Parity Bits - The Hamming (7,4) Code

September 29, 2013

Introduction

Recall that for a n bit code, if the last bit is the parity bit, then the first $n-1$ bits are the information bit

$$\underbrace{c_0 c_1 ... c_{n-2}}_{n-1 \text{ info bit}} \underbrace{c_{n-1}}_{parity}$$

For using even-parity method, the receiver only need to do the following operation for error detection

$$S = c_0 \oplus c_1 \oplus c_2 \oplus ... \oplus c_{n-2} \oplus c_{n-1} = \begin{cases} 0 & \text{no error} \\ 1 & \text{error occurred} \end{cases}$$

What if .... we use TWO parity bits?

The Two parity bits system

For a code with length n

$$\underbrace{c_0 c_1 ... c_{n-3} c_{n-2} c_{n-1}}_{\text{length n}}$$

The first $n-2$ bits are information bit, and the last 2 bits are parity bits

$$\underbrace{c_0 c_1 ... c_{n-3}}_{\text{information bits}} \quad \underbrace{c_{n-2} c_{n-1}}_{\text{parity}}$$

Then the error-detection operations performed by the receiver can be

$$S_1 = c_0 \oplus c_1 \oplus c_2 \oplus ... \oplus c_{n-3} \oplus c_{n-2}$$

$$S_2 = c_0 \oplus c_1 \oplus c_2 \oplus ... \oplus c_{n-3} \oplus c_{n-1}$$

Then we have $S_1 S_2$ as TWO bits that can be used to represent FOUR things , 00 for no-error and 01,10,11 for some type of error

The Hamming (7,4) Code

The Hamming (7,4) code can detect and correct all one-bit error.

For a code with length 7, 4 bits are information, 3 bits are parity bits

$$abcd\alpha\beta\gamma$$

We can have 3 chekcing equations for the receiver

$$S_1 = a \oplus b \oplus c \oplus \alpha$$

$$S_2 = a \oplus b \oplus d \oplus \beta$$

$$S_3 = a \oplus c \oplus d \oplus \gamma$$

Therefore α, β, γ actually is checking all the 4 information bits
α is checking a, b, c
β is checking a, b, d
γ is checking a, c, d

Then $S_1S_2S_3$ forms a 3bits message that can represent 8 information

$S_1S_2S_3$	Position of error
000	no error
001	γ
010	β
011	α
100	d
101	c
110	b
111	a

Some explanation

When $S_1S_2S_3 = 000$, that means all even-parity pit equations are showing that there is no error

When $S_1S_2S_3 = 001$, the means for $S_3 = a \oplus c \oplus d \oplus \gamma$ has one error
Then for a, c, d, γ , one of the bit has error. But since $S_1 = S_2 = 0$, it guarantee the a has no error (otherwise if a has error, $S_1 \neq 0$ and $S_2 \neq 0$), thus c, d, γ may have error.
For c, d, γ , S_1 has guarantee that c has no error (otherwise if c has error, then $S_1 \neq 0$), thus d, γ may have error

For d, γ , S_2 has guarantee that d has no error (otherwise if d has error, then $S_2 \neq 0$) , thus γ has error
Therefore for $S_1S_2S_3 = 001$, γ has error

The Hamming Weight and Hamming Distance

Condier 4 code examples $C_1 = 1101$, $C_2 = 1001$, $C_3 = 0000$, $C_4 = 1111$

The Hamming Weight of one code is the number of non-zero bit

$$w(C_1) = 3 \qquad w(C_2) = 2 \qquad w(C_3) = 0 \qquad w(C_4) = 4$$

The Hamming Distance between 2 codes is the number of bits that is different

$$d(C_1, C_2) = d(C_1, C_4) = 1 \qquad d(C_1, C_3) = 3 \qquad d(C_3, C_4) = 4$$

By applying the properties of modular 2 addition

$$d(C_i, C_j) = w(C_i \oplus C_j)$$

Thus, notice that the smallest Hamming Distance between 2 codes is the Hamming Weight

$$\min d = d(C_i \oplus C_i) = w(C_i)$$

Generator Matrix and Parity Check Matrix$P$

Consider the codes that have no-error

$$\begin{aligned} S_1 = 0 = a \oplus b \oplus c \oplus \alpha &= 1 \cdot a + 1 \cdot b + 1 \cdot c + 0 \cdot d + 1 \cdot \alpha + 0 \cdot \beta + 0 \cdot \gamma \\ S_2 = 0 = a \oplus b \oplus d \oplus \beta &= 1 \cdot a + 1 \cdot b + 0 \cdot c + 1 \cdot d + 0 \cdot \alpha + 1 \cdot \beta + 0 \cdot \gamma \\ S_3 = 0 = a \oplus c \oplus d \oplus \gamma &= 1 \cdot a + 0 \cdot b + 1 \cdot c + 1 \cdot d + 0 \cdot \alpha + 0 \cdot \beta + 1 \cdot \gamma \end{aligned}$$

Express these equations in matrix form

$$\underbrace{\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}}_{H} \underbrace{\begin{bmatrix} a \\ b \\ c \\ d \\ \alpha \\ \beta \\ \gamma \end{bmatrix}}_{C^T} = \underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}}_{0}$$

Express as Parity Check matrix H and codeword vector C

$$\mathbf{HC}^T = \mathbf{0}$$

Notice that

$$H = [P_{3\times4}\, I_3] \qquad P_{3\times4} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \qquad I_3 = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

About P matrix

Notice that P relate the parity bits and information bits

$$\begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} a+b+c \\ a+b+d \\ a+c+d \end{bmatrix}$$

$$\iff \begin{cases} a+b+c = \alpha \\ a+b+d = \beta \\ a+c+d = \gamma \end{cases} \iff \begin{cases} a+b+c-\alpha = 0 \\ a+b+d-\beta = 0 \\ a+c+d-\gamma = 0 \end{cases}$$

Recall that binary system is actually GaloisField(2) with the following property in modular 2 addition

$+$	0	1
0	0	1
1	1	0

Thus all the element in GF(2) fulfill following equations

$$x + x = 0 \quad \Rightarrow \quad x = -x$$

Thus

$$\begin{cases} a+b+c-\alpha=0 \\ a+b+d-\beta=0 \\ a+c+d-\gamma=0 \end{cases} \iff \begin{cases} a+b+c+\alpha=0 \\ a+b+d+\beta=0 \\ a+c+d+\gamma=0 \end{cases}$$

Which is the error-free conditions

Now consider the parity bit- information bit relation

$$\begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

This equations show that parity bits are the linear combination of the information bits, therefore, Hamming (7,4) code is a kind of *linearcode*.

Take the transpose

$$[\alpha\ \beta\ \gamma] = [a\ b\ c\ d] \underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}}_{Q} \qquad \left(\text{recall } (AB)^T = B^T A^T \right)$$

Form an augmented matrix by identity matrix, called generator matrix G

$$G = \begin{bmatrix} 1 & & & & 1 & 1 & 1 \\ & 1 & & & 1 & 1 & 0 \\ & & 1 & & 1 & 0 & 1 \\ & & & 1 & 0 & 1 & 1 \end{bmatrix} = [I_4\ Q_{4\times 3}]$$

Notice that the code C can be generated from information bits $M = [a, b, c, d]$ and generator matrix G

$$[a\,b\,c\,d\,\alpha\,\beta\,\gamma] = [a\,b\,c\,d] \begin{bmatrix} 1 & & & & 1 & 1 & 1 \\ & 1 & & & 1 & 1 & 0 \\ & & 1 & & 1 & 0 & 1 \\ & & & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$C = MG$$

This equations demonstrate the fundamental idea of channel coding / error-control coding : error-detection and error-correction abilit can be gauranteed by adding redundant bits (parity bits) after the information bits.

$$-END-$$