[Volume 1 issue 10 Nov 2013]
Page No.266-269 ISSN :2320-7167

INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH

# A Ternary BCH Code by Example

***Partha Pratim Dey***

Department of Electrical Engineering and Computer Science, North South University, Dhaka, Bangladesh

Email: ppd@northsouth.edu

**Abstract** Almost all undergraduate text books on error-correcting codes are found to focus on binary error-correcting codes hardly ever mentioning their ternary counterparts, though ternary codes are as interesting as binary ones and are in use from long time ago. In this context one might recall that Morse code is just a simple instance of a very useful ternary codes. In this document we discuss ternary BCH codes and use a simple example to illustrate how a ternary 2-error correcting BCH code could be created and how it can be used to correct the bit-errors that are likely to appear during the transmission of a message through a channel.

**Keywords** Ternary code, BCH code, generator matrix, decoding, elp.

## 1. Introduction

Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables reconstruction of the original data. The Bose, Chaudhuri, and Hocquenghem (BCH) codes form a large class of powerful random error-correcting codes. This class of codes is a remarkable generalization of the Hamming codes for multiple error correction. Binary BCH codes were invented by Hocquenghem in 1959 and independently by Bose and Chaudhury in 1960. Since then these codes are being used in applications such as satellite communications, compact disc players, DVDs, disk drives, two-dimensional bar codes etc. In this paper we show how a 2-error correcting ternary BCH could be constructed. We also discuss the theory of elp (error locator polynomial) and illustrate with an easy example how it can be used for error location and ultimate correction of errors.

## 2. CONSTRUCTION of a TERNARY BCH CODE

Throughout this paper $F_3$ will denote the Galois field of order $3$ and $F_3[x]$ will denote the ring of polynomials in $x$ with coefficients in $F_3$. Recall that $F_3[a]/(a^2+a+2)$ is the $GF(3^2)$, a Galois field of order $9$ and $a^2+a+1$ is a primitive polynomial as $a=a,\ a^2=2a+1,\ a^3=2a+2,\ a^4=2,\ a^5=2a,\ a^6=a+2,\ a^7=a+1$ and $a^8=1$. We factor the poly $f(x)=x^8-1$ in $F_3[x]$ to get

$$f(x)=(x^2+2x+2)(x^2+1)(x^2+x+2)(x+1)(x+2)$$

Since each nonzero member of $GF(3^2)$ satisfies $f(x)$, each factor of $f(x)$ is a minimal polynomial of some power of $a$ in $F_3[a]/(a^2+a+2)$. Thus $x^2+x+2$ is the minimal polynomial of $a$ and $a^3$, and $x^2+1$ and $x+1$ are the minimal polynomials

of $a^2$ and $a^4$ respectively. The interested reader is welcome to find the remaining minimal polynomials, but for our exercise which is to find a $2-$error correcting BCH code $C$, it is enough to find the $4$ minimal polynomials of $4$ powers of $a$, namely $a, a^2, a^3$ and $a^4$ as the generator polynomial $g(x)$ of a $2-$error correcting BCH code is given by the product of these $4$ minimal polynomials. Hence $g(x) = (x^2 + x + 2)(x^2 + 1)(x + 1) =$ $x^5 + 2x^4 + x^3 + x^2 + 2$ and the BCH code $C$ is the set of the multiples of $g(x)$ in $F_3[x]$ of degree less than $8$ (the degree of $f(x)$). Thus $C$ is a subspace over $F_3$ of dimension $= 8 -$ degree of $g(x) = 8 - 5 = 3$ with basis $g(x), xg(x)$ and $x^2 g(x)$ in $V =$ $F_3[x]/(x^8 - 1)$, the vector space of polynomials of degree less than 8 with coefficients in $F_3$. A generator matrix $G$ of $C$ is then given by:

$$G = \begin{bmatrix} 2 & 0 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 1 & 2 & 1 \end{bmatrix}.$$

For a background in coding theory, please see [1],[2] and [3].

## 3. DECODING with elp

Since $g(x)$ is the product of the minimal polynomials of $a, a^2, a^3$ and $a^4$ and a codeword $c(x)$ of $C$ is a multiple of $g(x)$, we have $c(a) = c(a^2) = c(a^3) = c(a^4) = 0$. Suppose now a codeword $c(x)$ is sent through a communication channel and a $r(x) \in V$ with at most 2-errors is received. Below we will explain how the transmitted codeword $c(x)$ can be recovered from $r(x)$.

Let $r(x) = c(x) + e(x)$. Then $r(a^i) = e(a^i)$ for , as $c(a^i) = 0$ as above. Let $e(x) = \alpha x^{m_1} + \beta x^{m_2}$ where $\alpha, \beta \in F_3$. Then

$$r_1 = r(a) = \alpha a^{m_1} + \beta a^{m_2}$$

$$r_2 = r(a^2) = \alpha (a^{m_1})^2 + \beta (a^{m_2})^2$$

$$r_3 = r(a^3) = \alpha (a^{m_1})^3 + \beta (a^{m_2})^3$$

$$r_4 = r(a^4) = \alpha (a^{m_1})^4 + \beta (a^{m_2})^4$$

Let $\text{elp}(z) = (z - a^{m_1})(z - a^{m_2}) = z^2 + \sigma_1 z + \sigma_2$ for some $\sigma_1, \sigma_2 \in F_3[a]/(a^2 + a + 2)$. Hence

$$\begin{cases} (a^{m_1})^2 + \sigma_1 a^{m_1} + \sigma_2 = 0 & (1) \\ (a^{m_2})^2 + \sigma_1 a^{m_2} + \sigma_2 = 0 & (2) \end{cases}$$

Multiplying equation (1) and equation (2) above by $\alpha a^{m_1}$ and $\beta a^{m_2}$ respectively, we obtain:

$$\begin{cases} \alpha (a^{m_1})^3 + \alpha \sigma_1 (a^{m_1})^2 + \alpha \sigma_2 a^{m_1} = 0 & (3) \\ \beta (a^{m_2})^3 + \beta \sigma_1 (a^{m_2})^2 + \beta \sigma_2 a^{m_2} = 0 & (4) \end{cases}$$

We now add $(3)$ and $(4)$ to get:

$$[\alpha (a^{m_1})^3 + \beta (a^{m_2})^3] + \sigma_1 [\alpha (a^{m_1})^2 + \beta (a^{m_2})^2] +$$

$$\sigma_2 [\alpha a^{m_1} + \beta a^{m_2}] = 0$$

or equivalently,

$$r_3 + \sigma_1 r_2 + \sigma_2 r_1 = 0 \qquad (5)$$

Now multiplying equation (1) and equation (2) above by $\alpha (a^{m_1})^2$ and $\beta (a^{m_2})^2$ respectively, and then adding them as above we obtain:

$$r_4 + \sigma_1 r_3 + \sigma_2 r_2 = 0 \qquad (6)$$

We now solve the system formed from equations $(5)$ and $(6)$ and obtain $\sigma_1$ and $\sigma_2$, which are the coefficients of the error locator polynomial $\text{elp}(z)$.

Solving $\text{elp}(z) = 0$, we now obtain $a^{m_1}$ and $a^{m_2}$.

Previously 4 of the parameters of $e(x) = \alpha x^{m_1} + \beta x^{m_2}$ were unknown. Now we know at least two, namely $m_1$ and $m_2$. The other two i.e. $\alpha$ and $\beta$ can be obtained by solving the following simultaneous equation:

$$\begin{cases} \alpha a^{m_1} + \beta a^{m_2} = r_1 \\ \alpha (a^{m_1})^2 + \beta (a^{m_2})^2 = r_2 \end{cases}$$

To recover $c(x)$, we subtract $e(x)$ from $r(x)$.

## 4. An EXAMPLE

Suppose a codeword $c(x)$ has been sent and we have received

$$r(x) = x^2 + x^3 + 2x^4 + 2x^6 + x^7$$

Let $\text{elp}(z) = z^2 + \sigma_1 z + \sigma_2$.

Evaluate

$$r_1 = r(a) = a$$

$$r_2 = r(a^2) = 2a$$

$$r_3 = r(a^3) = a^3 \text{ and}$$

$$r_4 = r(a^4) = 0$$

Let us now solve the system:

$$\begin{cases} r_3 + \sigma_1 r_2 + \sigma_2 r_1 = 0 \\ r_4 + \sigma_1 r_3 + \sigma_2 r_2 = 0 \end{cases}$$

In matrix form,

$$\begin{bmatrix} r_1 & r_2 \\ r_2 & r_3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} 2r_3 \\ 2r_4 \end{bmatrix}$$

$$\begin{bmatrix} a & a^5 \\ a^5 & a^3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} 2a^3 \\ 0 \end{bmatrix}$$

Hence $\sigma_2 = a^3$ and $\sigma_1 = a$.

Thus $\text{elp}(z) = z^2 + az + a^3$.

Notice that $\text{elp}(1) = 0$ and $\text{elp}(a^3) = 0$. Hence the error function $e(x)$ is given by:

$e(x) = \alpha + \beta x^3$ with $\alpha, \beta \in F_3$.

As $r(x) = c(x) + e(x)$, we have:

$r(a) = c(a) + e(a)$ i.e. $r_1 = 0 + \alpha + \beta a^3 = \alpha + \beta a^3$

$r(a^2) = c(a^2) + e(a^2)$ i.e. $r_2 = 0 + \alpha + \beta a^6 =$

$\alpha + \beta a^6$.

Since $r_1 = a$ and $r_2 = a^5$, we obtain from above:

$$\begin{cases} a = \alpha + \beta a^3 \\ a^5 = \alpha + \beta a^6 \end{cases}$$

We solve the system to get $\alpha = 2$ and $\beta = 2$. Hence

$e(x) = 2 + 2x^3$ and

$c(x)$

$= r(x) - e(x)$

$= x^2 + x^3 + 2x^4 + 2x^6 + x^7 - 2 - 2x^3$

$= 1 + x^2 + 2x^3 + 2x^4 + 2x^6 + x^7$

## REFERENCES

[1] Introduction to the Theory of Error Correcting Codes, Wiley Student Edition, John Wiley & Sons (Asia) Pte. Ltd., Singapore, 2003.

[2] Hill, R. (1986) A First Course in Coding Theory, The Oxford University Press, Oxford, UK,1986.

[3] van Lint, J. H. Introduction to Coding Theory, Graduate Texts in Mathematics, Springer-Verlag, New York, 1982