Research Article

Zero Set of Ternary 3- Error- Correcting BCH Type Codes

O.P Vinocha\(^a\) and Ajay Kumar\(^b\)\(^*\)

\(^a\)Department Mathematics, I.K.Gujral Punjab Technical University, Jalandhar, Address FCET, Ferozepur, Country India
\(^b\)I.K.Gujral Punjab Technical University, Jalandhar, Country India

Accepted 20 February 2014, Available online 25 February 2014, Vol.4, No.1 (February 2014)

Abstract

In 1970’s Kasami proposed an idea that triple error correcting codes can be constructed by using different zero than the BCH Code. Furthermore, Bracken and Helleseth [2009] discovered some new zero set leading to triple-error-correcting codes. Kasami and Bracken find these triples for the binary triple error correcting Code. In this work, we study on ternary triple error correcting BCH type Code and proposed some new triple error correcting code having zeros \(\{1, 3^m + 1, 3^{3m} + 1\}\) and \(\{1, 3^m + 1, 3^{3m} + 1\}\) where \(gcd (m, n) = 1\).

Keywords: Minimum distance, zeros, BCH code and parity check matrix, cyclic code

1. Introduction

In coding theory, the BCH codes form a class of cyclic error-correcting codes that are constructed using finite fields. BCH codes were invented in 1959 by French mathematician Alexis Hocquenghem, and independently in 1960 by Raj Bose and D. K. Ray-Chaudhuri. The acronym BCH comprises the initials of these inventors’ names.

One of the key features of BCH codes is that during code design, there is a precise control over the number of symbol errors correctable by the code. In particular, it is possible to design binary BCH codes that can correct multiple bit errors. Another advantage of BCH codes is the ease with which they can be decoded, namely, via an algebraic method known as syndrome decoding. This simplifies the design of the decoder for these codes, using small low-power electronic hardware.

The main advantage of the BCH Code is that it has control over the number of symbol errors correctable by these codes. BCH Code can be design for correcting multiple bit errors. BCH Codes are better considered as a subclass of cyclic code. The binary triple error correcting BCH Code is a cyclic code with minimum distance seven.

We will assume a finite field with \(3^n\) elements and \(g(X)\) be the generator polynomial of the above said codes having \(\theta\), \(\theta^3\) and \(\theta^5\) be its zeros. The set \(\{1, 3, 5\}\) are defined as zeros of the code. Bracken and Helleseth [2009] showed that one can construct similar triple error correcting Codes by using different zeros. In the proposed work we construct some new zero set of triple error correcting BCH type code in \(F_3\).

Let \(p_1=1, p_2=3\) and \(p_3=5\) then the parity check matrix \(H\) is

\[
\begin{bmatrix}
1 & \varepsilon^{\theta p_1} & \ldots & \varepsilon^{\theta^{(3^m-2)p_1}} \\
1 & \varepsilon^{\theta p_2} & \ldots & \varepsilon^{\theta^{(3^m-2)p_2}} \\
1 & \varepsilon^{\theta p_3} & \ldots & \varepsilon^{\theta^{(3^m-2)p_3}}
\end{bmatrix}
\]

The order of \(H\) is given \(3n\) by \(3^n - 1\). The code \(C = \{3^n - 1, 3^n - 3^n - 1, d\}\) is a code of dimension \(3^n - 3n - 1\) and minimum distance \(d = 7\) between any pair of code word.

**Argument-1:** An equation of the form \(x^{3^k+1} + bx^{3^k} + cx = d\) defined on GF \((3^n)\) has no more than four solutions in \(x\) when \(gcd (k, n) = 1\) for all \(b, c\) and \(d\) in GF \((3^n)\). [A.W. Bluh, 2004].

For calculating minimum\[4\] distance a famous result in coding theory is that if there are no sets of \(d - 1\) column in parity check matrix then the code has minimum distance at least \(d\). We will prove our results by contradicting the fact that \(H\) has six linear dependent columns. Which result the minimum distance is seven.

2. List of new zeros of 3-Error Correcting codes

<table>
<thead>
<tr>
<th>Zeros</th>
<th>Conditions</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>({1, 3^m + 1, 3^{2m} + 1})</td>
<td>(gcd(m,n)=1, n) is odd</td>
<td>Theorem-1</td>
</tr>
<tr>
<td>({1, 3^m + 1, 3^{3m} + 1})</td>
<td>(gcd(m,n)=1, n) is odd</td>
<td>Theorem-2</td>
</tr>
</tbody>
</table>

\*Corresponding author Ajay Kumar is PhD Scholar in Mathematics
Theorem 3.1: The set \( \{1, 3^m + 1, 3^{2m} + 1\} \) are the zero set of a triple \( - \) error-correcting code provided \( \text{gcd}(m, n) = 1 \), with an addition condition that \( x + x = 0 \) for all \( x \) in GF \((3^m)\).

Proof: The parity check matrix \( H \) has six or less dependent columns then there exist elements \( p, q, r, s, t, u \) in GF \((3^m)\) s.t.
\[
\begin{align*}
p + q + r + s + t + u &= 0 \\
p^{3^m+1} + q^{3^m+1} + r^{3^m+1} + s^{3^m+1} + t^{3^m+1} + u^{3^m+1} &= 0 \\
p^{2^{2m}+1} + q^{2^{2m}+1} + r^{2^{2m}+1} + s^{2^{2m}+1} + t^{2^{2m}+1} + u^{2^{2m}+1} &= 0
\end{align*}
\]
The code with zero set \( \{1, 3^m + 1\} \) with \( \text{gcd}(m, n) = 1 \) has minimum distance 5. It follows from first two equations that all elements \( p, q, r, s, t, u \) have to be different

We can write this as \( p + q + r = C_1 \)
\[
\begin{align*}
p^{3^m+1} + q^{3^m+1} + r^{3^m+1} &= C_2 \\
p^{2^{2m}+1} + q^{2^{2m}+1} + r^{2^{2m}+1} &= C_3
\end{align*}
\]
Replace \( p = p + C_1 \), \( q = q + C_1 \) and \( r = r + C_1 \)
\[
\begin{align*}
p + q + r &= 0 \\
p^{3^m+1} + q^{3^m+1} + r^{3^m+1} &= \omega \\
p^{2^{2m}+1} + q^{2^{2m}+1} + r^{2^{2m}+1} &= \mu
\end{align*}
\]
Where \( \omega = C_2 + C_1^{3^m+1} \) and \( \mu = C_3 + C_1^{3^{2m}+1} \)
From (3.1.1) substituting \( r = p + q \)

Therefore equations (3.1.2) & (3.1.3) becomes
\[
\begin{align*}
p^{3^m} q + q^{3^m} p &= \omega \\
p^{2^{2m}+1} q + q^{2^{2m}+1} p &= \mu
\end{align*}
\]
Replace \( q = pq \) and we get
\[
\begin{align*}
p^{3^m+1}(q + q^{3^m}) &= \omega \\
p^{2^{2m}+1}(q + q^{2^{2m}}) &= \mu
\end{align*}
\]
The equations (3.1.4) can be written as
\[
(q + q^{3^m}) = \omega p^{-3^m-1}
\]
Equation (3.1.4) implies
\[
q + q^{3^m} = \omega^{3^m} p^{-3^m-3^m} + \omega p^{-3^m-1}
\]
Using above equation (3.1.5) becomes
\[
p^{2^{2m}+1} [\omega^{3^m} p^{-3^m-3^m} + \omega p^{-3^m-1}] = \mu
\]
Put \( \lambda = p^{3^m-1} \)

Therefore the equation becomes
\[
\omega \lambda^{3^{2m}+1} + \mu \lambda + \omega^{3^m} = 0
\]
As we know \( \omega \neq 0 \) this implies by Argument-1 that the above equation has no more than four solutions in \( \lambda \) and we are done.

Theorem 3.2: The set \( \{1, 3^m + 1, 3^{2m} + 1\} \) are the zero set of a triple \( - \) error-correcting code provided \( \text{gcd}(m, n) = 1 \), for odd \( n \).

Proof: we use the same concept as we do in theorem 1 the systems of equations are
\[
\begin{align*}
p^{3^m+1}(q + q^{3^m}) &= \omega \\
p^{2^{2m}+1}(q + q^{2^{2m}}) &= \mu
\end{align*}
\]
Where \( \omega = C_2 + C_1^{3^m+1} \) & \( \mu = C_3 + C_1^{3^{2m}+1} \)

From equation (3.2.1) implies
\[
(q + q^{3^m}) = \omega p^{-3^m-1}
\]
\[
\Rightarrow q + q^{3^m} = \omega^{3^m} p^{-3^m-3^m} + \omega^{3^m} p^{-3^m-3^m} + \omega^{3^m} p^{-3^m-3^m} + \omega^{3^m} p^{-3^m-3^m} + \omega^{3^m} p^{-3^m-3^m}
\]
\[= p^{-3^m-1}
\]
Therefore equation (3.2.2) becomes
\[
\omega^{3^m} p^{-3^m-3^m} + \omega p^{-3^m-1} = \mu
\]
Put \( Y = p^{2^{2m}+1} \)
The equation is
\[
\omega Y^{3^m+1} + \omega^{3^m} Y^{3^m} - Y \mu + \omega^{3^m} = 0
\]
Hence by argument 1 the above equation has at most four solutions in \( Y \) and we are done.

Conclusion

In this work we discover some new zero set of ternary BCH type code. Finding further such type of triples in ternary case is an interesting and challenging research problem. In future we will work on 4 error correcting codes and try to find zero sets for this code different than the existing one.

References

R. Bose and D-Ray-Chaudari(1960), On a class of error correcting binary group codes Info.and Control, vol.3, pp-68-79
F.J. McWilliams and N.J.A.Sloane(1977),The Theory of Error-Correcting Codes’ North Holland Amsterdam.