Indian Journal of Advanced Mathematics (IJAM)
ISSN: 2582-8932 (Online), Volume-6 Issue-1, April 2026

An MDS Code Generated from a Three-Term Exponential Sum

Shikha Singh

Abstract: ***In this paper, I investigate the method for constructing Maximum Distance Separable (MDS) codes using exponential sums. By utilizing the properties of the trace function over finite fields, I explicitly calculate linear codes associated with certain three-term exponential sums. The parameters, weight distributions, and distance properties of these codes are analyzed in detail. Furthermore, we analyse the syndrome-decoding process for these codes.***

Keywords: Three-Term Exponential Sum, Linear Code, Syndrome Decoding, MDS Code. MSC: 11 LO5.

Nomenclature:
MDS: Maximum Distance Separable

I. INTRODUCTION

Let p be a prime, I, t be positive integers and χ a Dirichlet character $(\mathrm{mod} p)$. For integers m, s, n, the generalized three-term exponential sum $C(m; s; n; l; t; \chi; p)$ is defined by

$$C(m; s; n; l; t; \chi; p) = \int_{a=1}^{p-1} \chi(a) e \frac{ma^l + sa^t + na}{p}. \quad (1.1)$$

where $e(g) = e^{2i\pi g}$.

In this area, several researchers have made contributions. Z. Heng, Q. Yue [3]

Construct a class of linear codes whose Hamming weights are evaluated using Gauss sums. By employing additive and multiplicative characters over finite fields, they derive explicit expressions for the code weights and also demonstrate the effectiveness of Gauss sums in connecting finite field theory with coding-theoretic properties.

G.Jain, Z.Lin, R.Fena [4] use Weil sums to construct codes with exactly two or three nonzero weights. These codes are useful in combinatorial designs and have clear mathematical structures, linking finite field polynomials to code performance.

Zhao Hu, Nian Li, and Xi Zeng [5] use Kloosterman sums to define new families of linear codes. These codes have a small number of weights and near-optimal minimal distances. The study shows that Kloosterman sums can be effectively used to construct codes with strong error-correcting performance and well-defined combinatorial properties.

The primary aim of this study is to construct the Maximum Distance Separable (MDS) codes using exponential sums over finite fields, to calculate linear codes derived from certain three-term exponential sums via the trace function, and to analyse their properties, including weight distributions and syndrome decoding.

Manuscript received on 28 February 2026 | First Revised Manuscript received on 10 March 2026 | Second Revised Manuscript received on 25 March 2026 | Manuscript Accepted on 15 April 2026 | Manuscript published on 30 April 2026.

* Correspondence Author(s)
Dr. Shikha Singh*, Assistant Professor, Department of Mathematics, Central University of Jharkhand Building, Ranchi (Jharkhand), India. Email ID: shikhasingh2606@gmail.com, ORCID ID: 0009-0008-7936-1752

© The Authors. Published by Lattice Science Publication (LSP). This is an open-access article under the CC-BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

II. PRELIMINARY

This section introduces key concepts used in the paper, including the trace function over finite fields and the generator and parity-check matrices of linear codes. These preliminaries provide the foundation for code construction [1] [2].

Let p be a prime and $q = p^r$. We denote the finite field with q elements by F_q.

Definition 2.1 Trace function: - Let m be a positive integer and F_{pm} be the m-degree extension of the finite field F_p

$$\mathrm{Tr}_{F_{p^m}/F_p}: F_{p^m} \to F_p$$

given by

$$\mathrm{Tr}_{F_{p^m}/F_p}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} \ldots + \alpha^{p^{m-1}}, \forall \alpha \in F_{p^m}$$

Definition 2.2 Generator matrix: Let $\boldsymbol{C}$ be an $[n, k]_q$ code. A generator matrix for $\boldsymbol{C}$ is any $k \times n$ matrix G with entries in F_q such that the rows of G form a basis of $\boldsymbol{C}$. A generator matrix of the form $[I_k \mid A]$ is said to be in standard form.

Definition 2.3 Parity check matrix: Let $\boldsymbol{C}$ be an $[n, k]_q$ code. A parity check matrix for $\boldsymbol{C}$ is an $(n-k) \times n$ matrix H over F_q such that.

$$\boldsymbol{C} = \{c \in F_q^n : Hc^T = 0\}$$

If $G = [I_k \mid A]$ is a generator matrix for C, then

$$H = [-A^T \mid I_{n-k}]$$

is the parity check matrix for C.

Now, we incorporate the following notations: C = linear code, $\mathbf{n}$ = length of linear code, $\mathbf{k}$ = dimension of linear code, d = distance of code.

The following prepositions are from [2].

Preposition 1: (Singleton bound) For any $[\boldsymbol{n}, \boldsymbol{k}, \boldsymbol{d}]$ of a linear code over F_p, satisfy

$$k + d \leq n + 1$$

A code that attains this bound is known as an MDS code.

Preposition 2 A q-ary linear code $\boldsymbol{C}$ is MDS if and only if every set of $\boldsymbol{k}$ Columns of the generator matrix are linearly independent.

Preposition 3 A q-ary linear code $\boldsymbol{C}$ is MDS if and only if every set of ($\mathbf{n} - \mathbf{k}$) columns of the parity check matrix is linearly independent.

Thus, if C is an MDS code, then the dual of C is also an MDS code.

© Copyright: All rights reserved.

III. SYNDROME DECODING THROUGH A THREE-TERM EXPONENTIAL SUM

In this section, we discuss syndrome decoding using a three-term exponential sum. Let p be a prime and $q = p^r$, any $m, n, s \in F_q$ and $t, l \in \mathrm{Z}^+$. Then the three-term exponential sum is defined by,

$$C(m,s,n,l,t;q) = \sum_{a \in F_q^*} e(\mathrm{Tr}(m,s,n,l,t,a)),$$

where $e(\Omega) = e^{\frac{2i\pi\Omega}{p}}$ and $\mathrm{Tr}(m,s,n,l,t,a) = \mathrm{tr}(ma^l + sa^t + na)$.

We define a map $\psi: F_q^3 \to F_p^{q-1}$ by $\psi(m,s,n) = [\mathrm{Tr}(m,s,n,l,t,a)]_{a \in F^*}$. For a fixed $I, t \in Z^+$, let $\mathbf{C}(q) \subseteq F_p^{(q^{q-1})}$ be defined as the image of the map $\psi_0^p: F^3 \to {}_pF^{q-1}$, i.e.,

$$\mathbf{C}(q) = \{\psi(m,s,n): m,n,s \in F_q\}$$

As,

$$\psi(m,s,n) = \mathrm{tr}(ma_1^l + sa_1^t + na_1), \mathrm{tr}(ma_2^l + sa_2^t + na_2), \mathrm{tr}(ma_3^l + sa_3^t + na_3), \ldots \mathrm{tr}(ma_{q-1}^l + sa_{q-1}^t + na_{q-1})$$

Where g is a generator of F_q^*.

A. Computational Techniques

i. $r = 1$ *and* $I = t = 1$

For $r = 1$ and $I = t = 1$, we have some computational techniques, when we take the condition $m + s + n = 1$

$$\psi(1,0,0) = (\mathrm{tr}(1), \mathrm{tr}(2), \mathrm{tr}(3), \ldots \mathrm{tr}(p-1))$$
$$\psi(0,1,0) = (\mathrm{tr}(1), \mathrm{tr}(2), \mathrm{tr}(3), \ldots \mathrm{tr}(p-1))$$
$$\psi(0,0,1) = (\mathrm{tr}(1), \mathrm{tr}(2), \mathrm{tr}(3), \ldots \mathrm{tr}(p-1))$$

when we consider the condition: $m + s + n = 2$

$$\psi(1,1,0) = (\mathrm{tr}(2), \mathrm{tr}(4), \mathrm{tr}(6), \ldots \mathrm{tr}(2(p-1)))$$
$$\psi(0,1,1) = (\mathrm{tr}(2), \mathrm{tr}(4), \mathrm{tr}(6), \ldots \mathrm{tr}(2(p-1)))$$
$$\psi(1,0,1) = (\mathrm{tr}(2), \mathrm{tr}(4), \mathrm{tr}(6), \ldots \mathrm{tr}(2(p-1)))$$
$$\psi(2,0,0) = (\mathrm{tr}(2), \mathrm{tr}(4), \mathrm{tr}(6), \ldots \mathrm{tr}(2(p-1)))$$

when we take the condition: $m + s + n = 3$

$$\psi(1,1,1) = (\mathrm{tr}(3), \mathrm{tr}(6), \mathrm{tr}(9), \ldots \mathrm{tr}(3(p-1)))$$
$$\psi(2,1,0) = (\mathrm{tr}(3), \mathrm{tr}(6), \mathrm{tr}(9), \ldots \mathrm{tr}(3(p-1)))$$
$$\psi(3,0,0) = (\mathrm{tr}(3), \mathrm{tr}(6), \mathrm{tr}(9), \ldots \mathrm{tr}(3(p-1)))$$

when we take the condition: $m + s + n = 4$

$$\psi(4,0,0) = (\mathrm{tr}(4), \mathrm{tr}(8), \mathrm{tr}(12), \ldots \mathrm{tr}(4(p-1)))$$

when we take the condition: $m + s + n = 5$

$$\psi(0,5,0) = (\mathrm{tr}(5), \mathrm{tr}(10), \mathrm{tr}(15), \ldots \mathrm{tr}(5(p-1)))$$

similarly, $m + s + n = p$

$$\psi(p-1,1,0) = (\mathrm{tr}(p), \mathrm{tr}(2p), \mathrm{tr}(3p), \ldots \mathrm{tr}(p(p-1)))$$
$$\psi(p-2,1,1) = (\mathrm{tr}(p), \mathrm{tr}(2p), \mathrm{tr}(3p), \ldots \mathrm{tr}(p(p-1)))$$
$$\psi(p,0,0) = (\mathrm{tr}(p), \mathrm{tr}(2p), \mathrm{tr}(3p), \ldots \mathrm{tr}(p(p-1)))$$

Now, calculating the value of trace functions, we have the matrix of codewords as follows:

tr(1)	tr(2)	tr(3)	tr(4)	tr$(p-1)$
tr(2)	tr(4)	tr(6)	tr(8)	tr$(2(p-1))$
tr(3)	tr(6)	tr(9)	tr(12)	tr$(3(p-1))$
tr(4)	tr (8)	tr(12)	tr(16)	tr$(4(p-1))$
tr(5)	tr (10)	tr(15)	tr(20)	tr$(5(p-1))$
tr$(p-2)$	tr$(2(p-2))$	tr$(3(p-2))$	tr$(4(p-2))$	tr$((p-1)(p-2))$,
tr$(p-1)$	tr$(2(p-1))$	tr$(3(p-1))$	tr$(4(p-1))$	tr$((p-1)(p-1))'$
tr(p)	tr(2p)	tr(3p)	tr$(4p)$	tr$(p(p-1))$

where $m, s, n \in \mathrm{F}_q$. Here, we discuss the computational technique for these codewords for $l = t = 1$. When we take the condition: $m + s + n = 1$

1	2	3	4	.	.
2	4	6	8	.	..
3	6	9	12	..	$2(p-1)$
4	8	12	16	..	$3(p-1)$
.	.	.	.	.	$4(p-1)$
.	.	.	.	.	.
.	.	.	.	.	.
$(p-2)$	$2(p-2)$	$3(p-2)$	$4(p-2)$	..	$(p-1)(p-2)$
0	0	0	0	..	0

Now, by the row reduction method, we have

1	2	3	4	.	.
0	0	0	0	.	.
0	0	0	0	.	.
0	0	0	0	.	0
.	.	.	.	.	0
.	.	.	.	.	.
.	.	.	.	.	.
0	0	0	0	..	0

which looks like $\begin{matrix}\Delta \\ 0\end{matrix}$ with $\Delta = 1|_{1*1}\ 2\ 3\ \ldots p-1$ as the generator matrix of the code, so we find the parity-check matrix H of the linear code as follows.

H =.

-2	.	
.	-3	.
-4	.	$I_{(p-2)}$
.	.	.

Coding and Syndrome decoding using this generator and parity-check matrices can be performed as usual.

Similar computational techniques can be applied for $r > 1$, as discussed in the next subsubsection.

3.1.2 $r > 1$ **and** $I = t = 1$

For $r > 1$, If we enumerate the elements of F_q^* as $1, g, g^2, \cdots, g^{q-2}$, then the codewords of $C(q)$ are given by the functions.

$$\psi(m,s,n) = \mathrm{tr}(m+s+n), \mathrm{tr}(mg' + sg^t + ng), \mathrm{tr}\left(m(g^2)' + s(g^2)^t + n(g^2)\right), \ldots \mathrm{tr}\left(m\left(g^{(q-2)}\right)' + s\left(g^{(q-2)}\right)^t + n\left(g^{(q-2)}\right)\right)$$

© Copyright: All rights reserved.

$$\psi(1,0,0) = \left(\mathrm{tr}(1), \mathrm{tr}(g), \mathrm{tr}(g^2), \mathrm{tr}(g^3), \ldots \mathrm{tr}(g^{q-2})\right)$$
$$\psi(0,1,0) = \left(\mathrm{tr}(1), \mathrm{tr}(g), \mathrm{tr}(g^2), \mathrm{tr}(g^3), \ldots \mathrm{tr}(g^{q-2})\right)$$
$$\psi(0,0,1) = \left(\mathrm{tr}(1), \mathrm{tr}(g), \mathrm{tr}(g^2), \mathrm{tr}(g^3), \ldots \mathrm{tr}(g^{q-2})\right)$$

when we consider the condition: $m + s + n = g$

$$\psi(g,0,0) = \left(\mathrm{tr}(g), \mathrm{tr}(g^2), \mathrm{tr}(g^3), \ldots \mathrm{tr}(g \cdot g^{q-2})\right)$$
$$\psi(0,g,0) = \left(\mathrm{tr}(g), \mathrm{tr}(g^2), \mathrm{tr}(g^3), \ldots \mathrm{tr}(g \cdot g^{q-2})\right)$$
$$\psi(0,0,g) = \left(\mathrm{tr}(g), \mathrm{tr}(g^2), \mathrm{tr}(g^3), \ldots \mathrm{tr}(g \cdot g^{q-2})\right)$$

when we take the condition: $m + s + n = g^2$

$$\psi(g^2,0,0) = \left(\mathrm{tr}(g^2), \mathrm{tr}(g^3), \mathrm{tr}(g^4), \ldots \mathrm{tr}(g^2 \cdot g^{q-2})\right)$$
$$\psi(0,g^2,0) = \left(\mathrm{tr}(g^2), \mathrm{tr}(g^3), \mathrm{tr}(g^4), \ldots \mathrm{tr}(g^2 \cdot g^{q-2})\right)$$
$$\psi(0,0,g^2) = \left(\mathrm{tr}(g^2), \mathrm{tr}(g^3), \mathrm{tr}(g^4), \ldots \mathrm{tr}(g^2 \cdot g^{q-2})\right)$$

when we take the condition: $m + s + n = g^3$

$$\psi(g^3,0,0) = \left(\mathrm{tr}(g^3), \mathrm{tr}(g^4), \mathrm{tr}(g^4), \ldots \mathrm{tr}(g^3 \cdot g^{q-2})\right)$$

when we take the condition: $m + s + n = g^4$

$$\psi(0,g^4,0) = \left(\mathrm{tr}(g^4), \mathrm{tr}(g^5), \mathrm{tr}(g^6), \ldots \mathrm{tr}(g^4 \cdot g^{q-2})\right)$$

similarly, $m + s + n = g^{q-2}$

$$\psi(g^{q-2},0,0) = \left(\mathrm{tr}(g^{q-2}), \mathrm{tr}(g \cdot g^{q-2}), \mathrm{tr}(g^2 \cdot g^{q-2}), \ldots \mathrm{tr}(g^{q-2} \cdot g^{q-2})\right)$$

Now, calculating the value of trace functions, we have the matrix of codewords as follows:

$\mathrm{tr}(1)$	$\mathrm{tr}(g)$	$\mathrm{tr}(g^2)$	$\mathrm{tr}(g^3)$	$\mathrm{tr}(g^{q-2})$
$\mathrm{tr}(g)$	$\mathrm{tr}(g^2)$	$\mathrm{tr}(g^3)$	$\mathrm{tr}(g^4)$	$\mathrm{tr}(g.g^{q-2})$
$\mathrm{tr}(g^2)$	$\mathrm{tr}(g^2)$	$\mathrm{tr}(g^2)$	$\mathrm{tr}(g^2)$	$\mathrm{tr}(g^2 \cdot g^{q-2}))$
$\mathrm{tr}(g^3)$	$\mathrm{tr}(g^4)$	$\mathrm{tr}(g^5)$	$\mathrm{tr}(g^6)$	$\mathrm{tr}(g^3 \cdot g^{q-2})$
$\mathrm{tr}(g^{q-2})$	$\mathrm{tr}(g.g^{q-2})$	$\mathrm{tr}(g^2 \cdot g^{q-2})$	$\mathrm{tr}(g^3 \cdot g^{q-2})$	$\mathrm{tr}(g^{q-2} \cdot g^{q-2})$

Using the definition of the Trace function

$$\begin{matrix} 1 + 1^p + 1^{p^2} + \cdots 1^{p^{r-1}} & g + g^p + g^{p^2} + \cdots g^{p^{r-1}} & g^2 + (g^2)^p + \cdots (g^2)^{p^{r-1}} & \ldots & g^{q-2} + \cdots (g^{q-2})^{p^{r-1}} \\ g + g^p + g^{p^2} + \cdots g^{p^{r-1}} & g^2 + (g^2)^p + \cdots (g^2)^{p^{r-1}} & g^3 + (g^3)^p + \cdots (g^3)^{p^{r-1}} & \ldots & g \cdot g^{q-2} + \cdots (g \cdot g^{q-2})^{p^{r-1}} \\ g^2 + (g^2)^p + \cdots (g^2)^{p^{r-1}} & g^3 + (g^3)^p + \cdots (g^3)^{p^{r-1}} & g^4 + (g^4)^p + \cdots (g^4)^{p^{r-1}} & \ldots & \ldots \\ g^3 + (g^3)^p + \cdots (g^3)^{p^{r-1}} & g^4 + (g^4)^p + \cdots (g^4)^{p^{r-1}} & g^5 + (g^5)^p + \cdots (g^5)^{p^{r-1}} & \ldots & g^2 \cdot g^{q-2} + \cdots (g^2 \cdot g^{q-2})^{p^{r-1}} \\ & & & & g^3 \cdot g^{q-2} + \cdots (g^3 \cdot g^{q-2})^{p^{r-1}} \end{matrix}$$

$$g^{q-2} + \cdots (g^{q-2})^{p^{r-1}} \quad \because \quad (g^{q-2})^2 + \cdots [(g^{q-2})^2]^{p^{r-1}}$$

$$= \begin{bmatrix} 1 + 1 + 1 + \cdots 1 & g + g + g + \cdots g & g^2 + (g^2) + \cdots (g^2) & \ldots & g^{q-2} + \cdots (g^{q-2})^{p^{r-1}} \\ g + g + g + \cdots g & g^2 + (g^2) + \cdots (g^2) & g^3 + (g^3) + \cdots (g^3) & \cdot & \cdot \\ g^2 + (g^2) + \cdots (g^2) & g^3 + (g^3) + \cdots (g^3) & g^4 + (g^4) + \cdots (g^4) & \cdot & \cdot \\ g^3 + (g^3) + \cdots (g^3) & g^4 + (g^4) + \cdots (g^4) & g^5 + (g^5) + \cdots (g^5) & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & g^{3-2} \cdot g^{q-2} + \cdots (g^2 \cdot g^{q-2}) \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ g^{q-2} + \cdots (g^{3-2} \cdot g^{q-2}) & 0 & 0 & \ldots & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 \end{bmatrix}$$

$$\mathbf{H} = \begin{matrix} -g \\ \cdot \quad \cdot \quad -g^2. \\ - \quad -g^3 \end{matrix}$$

By using the row echelon method, it is equivalent to

$$\begin{matrix} 1 & g & g^2 & g^3 & . & . & \\ g & g^2 & g^3 & g^4 & . & . & g^{q-2} \\ .g^2 & g^3 & g^4 & g^5 & . & . & .g^{q-2} \\ g^3 & g^4 & g^5 & g^6 & . & . & . \\ k & .g^{3-2} & & & & & .g^{q-2} \\ . & . & . & . & . & & . \\ . & . & . & . & . & & . \\ g^{q-2} & g.g^{q-2} & . & . & . & . & (g^{q-2})^2 \end{matrix}$$

$$\begin{matrix} 1 & g & g^2 & g^3 & . & . & g^{q-2} \\ 0 & 0 & 0 & 0 & . & . & 0 \\ 0 & 0 & 0 & 0 & . & . & 0 \\ 0 & 0 & 0 & 0 & . & . & 0 \\ \sim & . & . & . & . & & . \\ . & . & . & . & . & & . \\ . & . & . & . & . & & . \\ 0 & 0 & . & . & . & . & 0 \end{matrix}$$

This looks like $\begin{matrix} \Delta \\ 0 \end{matrix}$ with $\Delta = 1|_{1*1}\ g\ g^2\ g^3\ \ldots\ g^{q-2}$ as the generator matrix of the code in standard form. So, we find the parity check matrix **H** of the linear code as below.

Example 3.1 Here, we establish the syndrome decoding in the case of $p = 5$; the corresponding linear code is $C = \{0000,1234,2413,3142,4321\}$.

The matrix of the codewords is

$$\boldsymbol{G} \sim \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12. \\ 4 & 8 & 12 & 16 \\ 0 & 0 & 0 & 0 \end{matrix}$$

Applying the row echelon method to the matrix G, we get

$$\boldsymbol{G} \sim \begin{matrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0. \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}$$

Here we see that the code is 1 - dimensional. According to [theorem 2.5.6] and [theorem 2.5.10] in [2], this

© Copyright: All rights reserved.

code is 3-error detecting and 1-error correcting. The generator matrix is

$$\Delta = 1|_{1\times 1}234.$$

Note:

If $G = [I_k \mid A]$ is a generator matrix for $\boldsymbol{C}$, then

$$\boldsymbol{H} = [-A^T \mid I_{n-k}]$$

is the parity check matrix for $\boldsymbol{C}$. So, we obtain a parity-check matrix for C as follows.

$$\boldsymbol{H} = \begin{matrix} -2 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0, \\ -4 & 0 & 0 & 1 \end{matrix}$$

$$= \begin{matrix} 3 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0. \\ 1 & 0 & 0 & 1 \end{matrix}$$

Next, we find the closet leaders and their syndrome.

The coset leader of a closet is a minimum-weight codeword in the closet, and it is chosen using the weight formula.

Table Syndrome

Coset leader	Syndrome	Coset leader	Syndrome
0000	000	1130	401
1000	321	0010	010
0100	100	0001	001
2000	142	0200	200
0020	020	0002	002
3010	423	0300	300
0003	003	0030	030
3000	411	0004	004
4000	234	0400	400
0040	040	1100	421
1010	331	1001	322
0011	011	1200	021
1020	341	1002	323
0102	102	0012	012
0021	021	0201	201
2001	143	1300	121
1030	301	1003	324
0103	103	0013	013
0031	031	3001	414
0130	130	0310	310

Table Coset Leader Syndrome

1400	221	1040	311
1004	320	0104	104
0140	140	0410	410
4100	334	0014	014
0041	041	1110	431
1120	441	1201	022
1021	342	1012	333
3110	023	1310	131
1103	424	1140	411
1104	420	4101	330
1410	231	0141	141
1111	432	1112	433
1113	434	1114	430
1211	032	1311	132
1411	232	1141	412
4111	340	1221	040
1212	033	1202	023
1203	024	1213	034
1222	043	1223	044
1224	040	1330	101
1340	111	1341	112
1342	113	1042	313
1343	114	1344	110
1440	211	1441	212
1442	213	1443	214
1444	210	1401	222
1402	223	1403	224
1043	314	2111	203
2311	403	2201	343
2202	344	2300	442
2210	302	2220	312
0444	444	0443	443
3221	134	1414	230
3440	303	2002	144
2240	332	2330	422
3330	243	3331	244
3332	240	3333	241

Table Coset Leader Syndrome

Coset leader	Syndrome	Coset Leader	Syndrome
3334	242	3330	233
4441	120	4440	124
4444	123	4443	122
2110	202		

Syndrome Decoding:

We take (i) $\boldsymbol{z} = 1102$. The syndrome is $S(\boldsymbol{z}) = \boldsymbol{z}\boldsymbol{H}^T = 423$. From the table, we see that the coset leader is 3010. So, here z gets decoded by $z - j = 1102 - 3010$

$$= 3142.$$

(ii) $z = 3234$,

The syndrome is $S(z) = \boldsymbol{z}\boldsymbol{H}^T = 142$

From the table, we see that the coset leader is 2000, so here. z gets decoded by $z - j = 3234 - 2000$

$$= 1234.$$

IV. MDS CODE FOR THREE-TERM EXPONENTIAL SUM

4. $1\ r = 1$ and $I = t = 1$

Here, $\mathbf{C} = C(p)$ is a $[p-1, 1, p-1]$ linear code over F_p. Let Δ and $\mathbf{H}$ be the generator and parity check matrices, respectively, for $\mathbf{C}$, which are given as follows:

$$\Delta = [\quad 1|_{1*1} \quad 2 \quad 3 \quad \ldots \quad (p-1)],$$

$$\mathbf{H} = \begin{matrix} -2 & \cdot & & \\ -3 & \cdot & & \cdot \\ \cdot -4 & \cdot & \cdot & l_{(p-2)} \\ \cdot & \cdot & \cdot & \\ \cdot & \cdot & & \end{matrix}$$

With reference to the calculations in the previous section, for the case of $r = 1$ we have $\mathbf{k} = 1, \mathbf{n} = p - 1$ and $\mathbf{d} = p - 1$. So, we have $k + d = n + 1 = p$. So, $\mathbf{C}$ is an MDS code. Similarly, for the case $\mathrm{r} > 1$, One can see that $\mathrm{d} = \mathrm{q} - 1, \mathrm{n} = \mathrm{q} - 1$, and $\mathrm{k} = 1$, so the corresponding code is MDS.

Thus, for $\mathrm{I} = \mathrm{t} = 1$, the code $\mathrm{C(q)}$ of the three-term exponential sum over F_q is an MDS code.

Remark 4.1 For $r \geq 1, I = t = 1, \boldsymbol{C}$ is an exact $(q-2)$-error detecting and exactly $\left[\frac{(q-2)}{2}\right]$-error correcting code.

Example 4.1 For $p = 5$, the linear code $\mathrm{C} = \{0000, 1234, 2413, 3142, 4321\}$ is an MDS (maximum distance separable) code.

The matrix

© Copyright: All rights reserved.

$$G \sim \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12 \\ 4 & 8 & 12 & 16 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Generator matrix (Δ) and parity check matrix $\boldsymbol{H}$ are,

$$\Delta = 1\,|_{1\times 1}\ 2\ 3\ 4$$

$$\boldsymbol{H} = \begin{matrix} -2 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0. \\ -4 & 0 & 0 & 1 \end{matrix}$$

According to S. Ling, C. Xing [2], we can say that,

1. $\boldsymbol{C}$ is MDS code if $\boldsymbol{d} = \boldsymbol{n} - \boldsymbol{k} + 1$.

Now find the minimum distance of the code $\boldsymbol{C} = \{0000,1234,2413,3142,4321\}$,

$$d(1234,2413) = 4$$
$$d(1234,4321) = 4$$
$$d(1234,0000) = 4$$
$$d(2413,4321) = 4$$
$$d(2413,1234) = 4$$
$$d(2413,0000) = 4$$
$$d(4321,1234) = 4$$
$$d(4321,2413) = 4$$
$$d(4321,0000) = 4$$

So, the minimum distance is 4. Here we see that the codeword matrix G has only one linearly independent row, i.e., the rank of the matrix G is 1, so we can say that C It is a 1 -dimensional code.

Now,

$$\Rightarrow n - k + 1$$
$$= 4 - 1 + 1$$
$$= 4$$

so $\boldsymbol{C}$ is the MDS code.

2. Every set of k columns of Δ is linearly independent.

$$\Delta = [1\,|_{1\times 1} \quad 2 \quad 3 \quad 4].$$

We know that $\boldsymbol{C}$ is 1 dimensional code. So, the value of $\boldsymbol{k}$ is 1. Here, we take any 1 column of the Δ matrix to be linearly independent.

3. Every set of $\boldsymbol{n} - \boldsymbol{k}$ columns of $\boldsymbol{H}$ is linearly independent.

We select any 3 columns of the parity-check matrix; we have 3 pivot elements. So, we can say that every set of 3 columns of the parity-check matrix is linearly independent.

V. CONCLUSION

In this article, we apply the hybrid power mean to three-term exponential sums in coding theory. First, we calculate a linear code of a three-term exponential sum. Afterwards, we construct a generator matrix and a parity-check matrix from the codewords. Also, we find the syndrome and construct syndrome decoding for a given linear code.

VI. ACKNOWLEDGMENT

The authors would like to thank Central University of Jharkhand for their support in the preparation of this research article.

DECLARATION STATEMENT

I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed solely by the author.

REFERENCES

1. W. C. Huffman, J.L. Kim, P. Sol, Concise Encyclopedia of Coding Theory, Chapman and Hall/CRC, Boca Raton (2021). DOI: https://doi.org/10.1201/9781315147901
2. J. Bierbrauer, Introduction to Coding Theory, Taylor and Francis. (2018) DOI: https://doi.org/10.1201/9781482296372
3. Z.Heng, Q.Yue, "Evaluation of the Hamming Weights of a class of linear codes based on Gauss sums. Designs, codes, cryptography. 83, 307-326 (2017). DOI: https://doi.org/10.1007/s10623-016-0222-7
4. G.Jain, Z.Lin, R.Fena, "Two Weight and Three Weight Linear Codes Based on Weil Sums", Finite Fields and Their Applications. 57, 92-107 (2019). DOI: https://doi.org/10.1016/j.ff9.2019.02.001
5. Zhao Hu,Nian Li, Xi. Zeng, "New linear codes with few weights derived from Kloostermann sum", Finite Fields and their Application. 62,101608 (2020). DOI: https://doi.org/10.1016/j.ffa.2019.101608

AUTHOR'S PROFILE

Dr. Shikha Singh is an Assistant Professor at Sidhhu Kanhu Murmu University (SKMU). She earned her PhD from Central University of Jharkhand (CUJ), specialising in Algebra and Number Theory. She has published papers in peer-reviewed journals and actively participates in academic conferences.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/journal and/or the editor(s). The Lattice Science Publication (LSP)/ journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

© Copyright: All rights reserved.