JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

On Weight Distribution of $\mathbb{Z}_{p^t}$-linear code

Saheb Navghare,
Research Student ,
School of Mathematical Sciences,
SRTM University, Nanded-431606, Maharashtra, India.

Abstract : In this research paper, we introduce a new type of $\mathbb{Z}_{p^t}$-linear code, where $p^t \geq 2$. Here, p represents a prime number, and t is a positive integer. We thoroughly investigate the parameters of these codes and determine their weight distribution for rank 2.

***Index Terms* - $\mathbb{Z}_{p^t}$-linear code, codes over finite rings, , rank, minimum Hamming distance.**

I. Introduction

A code C is a subset of $\mathbb{Z}_{p^t}^n$, where $\mathbb{Z}_{p^t}$ represents the set of integers modulo p^t, and n is a positive integer. For any two elements x and y in $\mathbb{Z}_{p^t}^n$, the Hamming distance between them, denoted as $d(x, y)$, is defined as the count of differing coordinates. In other words, it is the Hamming weight of the difference $x - y$, which represents the number of non-zero coordinates in $x - y$.

The minimum Hamming distance $d(C)$ of a code C is defined as follows:

$$\begin{aligned} d(C) &= \min\{d(x, y) \mid x, y \in C \text{ and } x \neq y\} \\ &= \min\{wt(x - y) \mid x, y \in C \text{ and } x \neq y\} \end{aligned}$$

Here, $wt(x - y)$ denotes the Hamming weight of $x - y$, representing the number of non-zero entries in the vector $x - y$.

Additionally, the minimum Hamming weight of C can be determined as $\min\{wt(c) \mid c \in C \text{ and } c \neq 0\}$. Therefore, the terms "minimum distance" and "minimum weight" refer to the minimum Hamming distance and minimum Hamming weight of a code, respectively. An $(n, M, d)\mathbb{Z}_{p^t}$-code denotes a code over $\mathbb{Z}_q$ with a length of n, a cardinality of M, and a minimum Hamming distance of d. For more in-depth information on coding theory, please refer to [1]. The group $\mathbb{Z}_{p^t}$ is well-known to be a group under addition modulo p^t. Consequently, the set $\mathbb{Z}_{p^t}^n$ forms a group under coordinate-wise addition modulo p^t, making it a $\mathbb{Z}_{p^t}$-module. A subset C of $\mathbb{Z}_{p^t}^n$ is considered a $\mathbb{Z}_{p^t}$-linear code if it functions as a submodule of $\mathbb{Z}_{p^t}^n$. Since $\mathbb{Z}_{p^t}^n$ is a finitely generated $\mathbb{Z}_{p^t}$-module, the code C represents a finitely generated submodule of $\mathbb{Z}_{p^t}^n$. The rank of the code C is defined as the cardinality of a minimal generating set for C [4].

A generator matrix of a linear code C is a matrix whose rows generate C. For any linear code C over $\mathbb{Z}_{p^t}$, it is possible to apply a permutation to obtain a code with a generator matrix G where the rows of G generate C. The generator matrix G takes the following form:

$$G = \begin{bmatrix} I_{k_0} & M_{01} & M_{02} & \cdots & M_{0s-1} & M_{0s} \\ 0 & z_1 I_{k_1} & z_1 M_{12} & \cdots & z_1 M_{1s-1} & z_1 M_{1s} \\ 0 & 0 & z_2 I_{k_2} & \cdots & z_2 M_{2s-1} & z_2 M_{2s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & z_{s-1} I_{k_{s-1}} & z_{s-1} M_{s-1s} \end{bmatrix}$$

In the matrix G, M_{ij} represents matrices over $\mathbb{Z}_{p^t}, \{z_1, z_2, \dots, z_{s-1}\}$ denotes the set of zero-divisors in $\mathbb{Z}_{p^t}$, and the columns are organized into blocks of sizes $k_0, k_1, \dots, k_{s-1}, k_s$, respectively.

The cardinality of C can be calculated as $|C| = p^{tk_0} \left(\frac{p^t}{z_1}\right)^{k_1} \left(\frac{p^t}{z_2}\right)^{k_2} \cdots \left(\frac{p^t}{z_{s-1}}\right)^{k_{s-1}}$.

We define an $[n, k, d]\mathbb{Z}_{p^t}$-linear code as a code of rank k, length n, and minimum Hamming distance d over the ring $\mathbb{Z}_{p^t}$. Extensive research has been conducted by several scholars on codes over finite rings, as documented in various works [2-4]. In the past two decades, significant attention has been given to codes over the specific ring $\mathbb{Z}_{2^2}$. In this study, we focus on investigating codes over $\mathbb{Z}_{p^t}$, where p is a prime number and t is a positive integer, with $p^t \geq 2$.

In the context of a $\mathbb{Z}_{p^t}$-linear code C, it has been established in references [5, 6] that the minimum Hamming distance of C is equal to its minimum Hamming weight.

Lemma 1: For a $\mathbb{Z}_{p^t}$-linear code C, the minimum Hamming distance is equivalent to the minimum Hamming weight.

In an $(n, M, d)\mathbb{Z}_q$-code denoted by C, where $0 \leq i \leq n$, the value A_i represents the number of codewords in C with a Hamming weight of i. The sequence $\{A_i\}_{i=0}^{n}$ is commonly known as the weight distribution of the code C.

Let us examine the properties of the element p^{t-1} in $\mathbb{Z}_{p^t}$. It has the smallest order among all elements, and the subgroup H generated by p^{t-1} is the smallest subgroup that contains more than one element. To further explore these concepts, we consider the following matrix:

$$G = \begin{bmatrix} 0 & 1 & 1 & 2 & \cdots & p^t - 1 \\ 1 & 0 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

The matrix provided generates a code C defined as $= \{\alpha x + \beta y \mid \alpha, \beta \in \mathbb{Z}_{p^t}\}$. Referring to Theorem 3.1 in [8], we conclude that the code C is a $[p^t + 1, 2, p^{t-1}(p-1) + 1]\mathbb{Z}_{p^t}$-linear code.

This kind of work, has been carried out by authors in [9] However, they did in the general set up, in the sense that, authors did it for any integer $q > 1$. This is our small attempt to tackle the particular case for $q = p^t$, for p prime. This research paper is dedicated to the comprehensive study of $\mathbb{Z}_{p^t}$-linear codes, covering a wide range of topics. In Section 2, we present a detailed introduction and analysis of a new class of $\mathbb{Z}_{p^t}$-linear codes, examining their specific parameters and properties. In Section 3, we focus on the weight distributions associated with these code, providing valuable insights and results to complement our investigations.

II. $\mathbb{Z}_{p^t}$-LINEAR CODE WITH THE GENERATOR MATRIX OVER ZERO-DIVISORS OF $\mathbb{Z}_{p^t}$

In this section, we proceed to construct an additional novel $\mathbb{Z}_{p^t}$-linear code and analyze its various parameters. Considering that $\mathbb{Z}_{p^t}$ consists of $p^t - p^{t-1}$ units, it follows that there exist $p^{t-1} - 1$ zero-divisors within this ring.

Let us define the matrix:

$$G = \begin{bmatrix} 1 & 0 & z_1 & z_2 & \cdots & z_s \\ 0 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

Here, $z_1, z_2, \ldots, z_s$ represent zero-divisors, with $s = p^{t-1} - 1$. The matrix G generates a $[p^{t-1} + 1, 2]\mathbb{Z}_{p^t}$-linear code denoted by C. The code C consists of all the vectors of the form $\alpha x + \beta y$, where $\alpha, \beta \in \mathbb{Z}_{p^t}$ and x and y are the first and second rows of G, respectively. The length of the code C is $p^{t-1} + 1$, and it has a rank of 2.

Theorem 1: Consider $p^t \geq 2$, and let

$$G = \begin{bmatrix} 1 & 0 & z_1 & z_2 & \cdots & z_s \\ 0 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

where $\{z_1, z_2, \ldots, z_s\}$ represents the set of zero-divisors in $\mathbb{Z}_{p^t}$. The code

C generated by G is a $\left[p^{t-1} + 1, 2, p^{t-1} + 1 - \frac{p^t}{o(\alpha)}\right] \mathbb{Z}_{p^t}$-linear code,

where α denotes the non-zero element in $\mathbb{Z}_{p^t}$ with the least order.

Proof:
let's consider the following cases:

Case (i): If $\alpha = 0$ and $\beta = 0$, then $wt(\alpha x + \beta y) = 0$.

Case (ii): If $\alpha = 0$ and $\beta \neq 0$, then $\min\{wt(\alpha x + \beta y)\} = p^{t-1} + 1 - 1 = p^{t-1}$. Case (iii): If $\alpha \neq 0$ and $\beta = 0$, let's proceed to the next part. Let α be a non-zero element in $\mathbb{Z}_{p^t}$ with order $r > 1$. In the sequence $\alpha(0,1,2, \ldots, p^t - 1)$, each element in the subgroup generated by α, denoted as $\langle\alpha\rangle$, appears $\frac{p^t}{r}$ times. Therefore, the element 0 appears $\frac{p^t}{r}$ times in this sequence.

Now, let's consider the case when u is a unit in $\mathbb{Z}_{p^t}$. Since $o(\alpha) = o(\alpha u)$, it implies that $\alpha u \neq 0$. Hence, all the zero coordinates in the sequence $\alpha(0,1,2,\dots,p^t - 1)$ are contributed by the terms in $\alpha(0, z_1, z_2, \dots, z_s)$. Therefore, we have $t(\alpha(0, z_1, z_2, \dots, z_s)) = s + 1 - \frac{p^t}{r}$.

Now, let's consider the sequence $\alpha(1,0, z_1, z_2, \dots, z_s)$. Here, the first coordinate is 1 , followed by the terms in $\alpha(0, z_1, z_2, \dots, z_s)$. The zero coordinates in this sequence are the same as in $\alpha(0, z_1, z_2, \dots, z_s)$. Therefore, we have $wt(\alpha(1,0, z_1, z_2, \dots, z_s)) = s + 1 - \frac{p^t}{r} + 1 = p^{t-1} - \frac{p^t}{r} + 1$. In fact, we can simplify this as $wt(\alpha(1,0, z_1, z_2, \dots, z_s)) = p^{t-1} - \frac{p^t}{o(\alpha)} + 1$.

Consider

$$\begin{aligned} & \min\{wt(\alpha(1,0, z_1, z_2, \dots, z_s) \mid \alpha \in \mathbb{Z}_{p^t}, \alpha \neq 0)\} \\ = \quad & \min\left\{p^{t-1} - \frac{p^t}{o(\alpha)} + 1 \mid \alpha \in \mathbb{Z}_{p^t} - \{0\}\right\} \\ = \quad & p^{t-1} + 1 - \max\left\{\frac{p^t}{o(\alpha)} \mid \alpha \in \mathbb{Z}_{p^t} - \{0\}\right\}. \end{aligned}$$

If $o(\alpha)$ is minimum, then $\frac{p^t}{o(\alpha)}$ is maximum.

Therefore,

$$\min\{wt(\alpha(1,0, z_1, z_2, \dots, z_s) \mid \alpha \neq 0, \alpha \in \mathbb{Z}_{p^t})\} = p^{t-1} + 1 - \frac{p^t}{o(\alpha)}$$

where α is the least order non-zero element in $\mathbb{Z}_t$.

Case (iv). Let $\alpha \neq 0$ and $\beta \neq 0$.

Let $\alpha \in \mathbb{Z}_{p^t}$, with $o(\alpha) = d \neq 1$. In $\alpha(0, z_1, z_2, \dots, z_s)$, each d order element in $\langle\alpha\rangle$ appears $\frac{p^t}{d} - \frac{p^t - p^{t-1}}{\phi(d)}$ times and each remaining element of order less than d in $\langle\alpha\rangle$ appears exactly $\frac{p^t}{d}$ times.

Let $\beta \in \mathbb{Z}_{p^t}, \beta \neq 0$. (i) If $\beta \in \langle\alpha\rangle$ with $o(\beta) = d$, then $wt(\alpha x + \beta y) = 2 + (p^{t-1} - 1) - \left[\frac{p^t}{d} - \frac{p^t - p^{t-1}}{\phi(d)}\right] = p^{t-1} + 1 - \left[\frac{p^t}{d} - \frac{p^t - p^{t-1}}{\phi(d)}\right] = 1 + p^{t-1} - \frac{p^t}{d} + \frac{p^t - p^{t-1}}{\phi(d)}$.

(ii) If $\beta \in \langle\alpha\rangle$ with $o(\beta) \neq d$ and $\beta \neq 0$, then $wt(\alpha x + \beta y) = 1 + q - p^t - p^{t-1} - \frac{p^t}{d}$ and

(iii) If $\beta \in \mathbb{Z}_{p^t}$ but $\beta \notin \langle\alpha\rangle$, then $wt(\alpha x + \beta y) = 1 + p^{t-1}$.

Therefore,

$$\begin{aligned} & \min\{wt(\alpha x + \beta y) \mid \alpha \neq 0 \neq \beta \text{ and } \alpha, \beta \in \mathbb{Z}_{p^t}\} \\ = \quad & \min\left\{1 + p^{t-1} - \frac{p^t}{d} + \frac{p^t - p^{t-1}}{\phi(d)}, 1 + p^{t-1} - \frac{p^t}{d}, 1 + p^{t-1}\right\} \\ = \quad & \min\left\{1 + p^{t-1} - \frac{p^t}{o(\alpha)}\right\}. \end{aligned}$$

If α is the least order element, then it reaches the minimum. Therefore, for the least order non-zero element $\alpha \neq 0$ in $\mathbb{Z}_{p^t}$,

$$\min\{wt(\alpha x + \beta y) \mid \alpha \neq 0 \neq \beta \text{ and } \alpha, \beta \in \mathbb{Z}_{p^t}\} = 1 + p^{t-1} - \frac{p^t}{o(\alpha)}$$

III. WEIGHT DISTRIBUTION OF THE $\mathbb{Z}_{p^t}$-LINEAR CODE C OF RANK 2

In this section, we consider a positive integer p^t where $p \geq 2$. According to Theorem 1, the matrix

$$G = \begin{bmatrix} 1 & 0 & z_1 & z_2 & \cdots & z_s \\ 0 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

generates a $\left[p^{t-1}+1,2,p^{t-1}+1-\frac{p^t}{o(\alpha)}\right]\mathbb{Z}_{p^t}$-linear code. Here, α represents the least order non-zero element in $\mathbb{Z}_{p^t}$, and s is equal to $p^{t-1}-1$. The resulting code has a rank of 2 .

Theorem 2: For any integer $p^t \geq 2$, the weight distribution of $\mathbb{Z}_{p^t}$-linear code of rank 2 generated by the Matrix

$$G=\begin{bmatrix}1 & 0 & z_1 & z_2 & \cdots & z_{p^{t-1}-1}\\ 0 & 1 & 1 & 1 & \cdots & 1\end{bmatrix}$$

is

$$\begin{aligned}&A_0=1,\\&A_{p^{t-1}}=p^t-1,\\&A_{p^{t-1}+1}=\phi(d)[p^t-d], d\neq p^t,\\&A_{p^{t-1}-\frac{p^t}{d}+1}=\phi(d)[d-\phi(d)] \text{ and}\\&A_{p^{t-1}-\left[\frac{p^t}{d}-\frac{p^t-p^{t-1}}{\phi(d)}\right]+1}=[\phi(d)]^2\end{aligned}$$

where d is a divisor of p^t and $d\neq 1$.

Proof:
Let x and y be the first and second rows of the above matrix. Then $=\{\alpha x+\beta y \mid \alpha,\beta \in \mathbb{Z}_{p^t}\}$.

Case (i). If $\alpha=0=\beta$, then $wt(\alpha x+\beta y)=0$. Therefore,

$$A_0=1$$

Case (ii). If $\alpha=0$ and $\beta\neq 0$, then $\beta 1\neq 0$ for all non-zero β in $\mathbb{Z}_{p^t}$ which implies $wt(\beta y)=p^{t-1}+1-1$ and hence $wt(\alpha x+\beta y)=p^{t-1}$ for all non-zero $\beta\in\mathbb{Z}_{p^t}$. In this way, we get p^t-1 codewords of weight p^{t-1}.

Case (iii). Let $\alpha,\beta\in\mathbb{Z}_{p^t}$ with $\alpha\neq 0$ and $\beta=0$. Let $o(\alpha)=d, d\neq 1$. Then $wt(\alpha x+\beta y)=p^{t-1}+1-\frac{p^t}{d}$. Thus, there are $\phi(d)$ codewords of weight $p^{t-1}+1-\frac{p^t}{d}$

Case (iv). Let $\alpha,\beta\in\mathbb{Z}_{p^t}$ with $\alpha\neq 0$ and $\beta\neq 0$. Let $o(\alpha)=d, d\neq 1$. In $\alpha(0,z_1,z_2,\ldots,z_s), s=p^{t-1}-1$, each d order element in $\langle\alpha\rangle$ appears $\frac{p^t}{d}-\frac{p^t-p^{t-1}}{\phi(d)}$ times and each remaining element in $\langle\alpha\rangle$ appears exactly $\frac{p^t}{d}$ times.

If $\beta\in\langle\alpha\rangle$ with $o(\beta)=d$, then $wt(\alpha x+\beta y)=1+p^{t-1}-\left[\frac{p^t}{d}-\frac{p^t-p^{t-1}}{\phi(d)}\right]$, for all $\alpha,\beta\in\mathbb{Z}_{p^t}$. Therefore, for $o(\alpha)=o(\beta)=d$, there are $\phi(d)$ such α 's and $\phi(d)$such β 's. This gives $\phi(d)\phi(d)$ codewords of weight $1+p^{t-1}-\left[\frac{p^t}{d}-\frac{p^t-p^{t-1}}{\phi(d)}\right]$

If $\beta\in\langle\alpha\rangle$ with $o(\beta)\neq d,\beta\neq 0$, then $wt(\alpha x+\beta y)=1+p^{t-1}-\frac{p^t}{d}$, for $o(\alpha)=d$ and $o(\beta)\neq d$. That is, for $o(\alpha)\neq o(\beta), wt(\alpha x+\beta y)=1+p^{t-1}-\frac{p^t}{d}$. Therefore, there are $\phi(d)[d-1-\phi(d)]$ codewords of weight $1+p^{t-1}-\frac{p^t}{d}$

If $\beta\notin\langle\alpha\rangle$, then $wt(\alpha x+\beta y)=1+p^{t-1}$. This implies that there are $\phi(d)[p^t-d]$ codewords of weight $1+p^{t-1}$, for $o(\alpha)=d,\beta\notin\langle\alpha\rangle$.

References

[1] Ling, San, and Chaoping Xing. Coding theory: a first course. Cambridge University Press, 2004.

[2] Eugene Spiegel, Codes over $\mathbb{Z}_m$, Information and Control 35 (1977), 48-51.

[3] Steven T. Dougherty, T. Aaron Gulliver, Young Ho Park and John N. C Wong, Optimal linear codes over $\mathbb{Z}_m$, J. Korean Math. Soc. 44(5) (2007), 11391162.

[4] Steven T. Dougherty, Manish K. Gupta and Keisuke Shiromoto, On generalised weights for codes over $\mathbb{Z}_k$, Australasian J. Combin. 31 (2005), 231-248.

[5] P. Chella Pandian and C. Durairajan, On the $\mathbb{Z}_q$-linear and $\mathbb{Z}_q$-Simplex codes and its related parameters for q is a prime power, J. Discrete Math. Sci. Crypto. (to appear).

[6] C. Durairajan, J. Mahalakshmi and P. Chella Pandian, On the $\mathbb{Z}_q$-Simplex codes and its weight distribution for dimension 2 (communicated).

[7] Joseph Rotman, Galois Theory, Springer-Verlag, Inc., New York, 1998.

[8] Mahalakshmi, J., and C. Durairajan. "On the Z_q-Macdonald code and its weight distribution of dimension 3." arXiv preprint arXiv:1505.05642 (2015). [9] Durairajan, C., and J. Mahalakshmi. "On codes over integers modulo q." Adv. Appl. Math 15 (2015): 125-143.