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 $\mathbb{Z}_{p^t}$ Simplex Code

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

Abstract : This research paper investigates the weight distribution of rank $2\mathbb{Z}_{p^t}$- Simplex codes, where $p^t \geq 2$, with p being a prime number and t a positive integer.

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

I. Introduction

A code C represents a subset of $\mathbb{Z}_{p^t}^n$, where $\mathbb{Z}_{p^t}$ denotes the set of integers modulo p^t and n is a positive integer. In this context, let x and y be elements of $\mathbb{Z}_{p^t}^n$. The Hamming distance between x and y is defined as the count of differing coordinates, denoted by $d(x,y)$. Specifically, $d(x,y)$ can be expressed as the Hamming weight of $x-y$, which represents the number of non-zero coordinates in $x-y$. The minimum Hamming distance $d(C)$ for code C is defined as follows:

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

Furthermore, the minimum Hamming weight of C is given by $\min\{wt(c) \mid c \in C \text{ and } c \neq 0\}$. Henceforth, the terms "minimum distance" and "minimum weight" refer to the minimum Hamming distance and the minimum Hamming weight, 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 further details on coding theory, please refer to [1].

It is well-known that $\mathbb{Z}_{p^t}$ forms a group under addition modulo p^t. Consequently, $\mathbb{Z}_{p^t}^n$ becomes a group under coordinate-wise addition modulo p^t, thus 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 serves as a submodule of $\mathbb{Z}_{p^t}^n$. Since $\mathbb{Z}_{p^t}^n$ is a finitely generated $\mathbb{Z}_{p^t}$-module, C represents a finitely generated submodule of $\mathbb{Z}_{p^t}^n$. The rank of the code C refers to the cardinality of a minimal generating set of C[7].

A generator matrix of C is a matrix whose rows generate C. Every linear code C over $\mathbb{Z}_{p^t}$ can be transformed via permutation to a code with a generator matrix G (where the rows of G generate), which takes the following form:

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

Here, M_{ij} represents matrices over $\mathbb{Z}_{p^t}, \{z_1, z_2, \ldots, z_{s-1}\}$ denotes the zerodivisors in $\mathbb{Z}_{p^t}$, and the columns are organized into blocks of sizes $k_0, k_1, \ldots, k_{s-1}, k_s$, respectively. The cardinality of C can be calculated as

$$|C| = p^{tk_0} \left(\frac{p^t}{z_1}\right)^{k_1} \left(\frac{p^t}{z_2}\right)^{k_2} \cdots \left(\frac{p^t}{z_{s-1}}\right)^{k_{s-1}}$$

An $[n,k,d]\mathbb{Z}_{p^t}$-linear code refers to a code with rank k, length n, and a minimum Hamming distance of d over $\mathbb{Z}_{p^t}$. Research on codes over finite rings has been extensively carried out by numerous researchers [2-4]. Over the past two decades, there has been a substantial amount of research focused on codes over $\mathbb{Z}_{2^2}$. In this paper, we specifically investigate codes over $\mathbb{Z}_{p^t}$, considering any positive integer $p^t \geq 2$, where p is a prime number and t is a positive integer.

When C represents a $\mathbb{Z}_{p^t}$-linear code, the following result holds true, as demonstrated in references [5,6] :

Lemma 1: The minimum Hamming distance of a $\mathbb{Z}_{p^t}$-linear code C is equal to its minimum Hamming weight.

For an $(n, M, d)\mathbb{Z}_q$-code denoted by C, where $0 \leq i \leq n$, the quantity A_i corresponds to the number of codewords with a Hamming weight of i. The sequence $\{A_i\}_{i=0}^n$ is referred to as the weight distribution of the code C.

In $\mathbb{Z}_{p^t}$, the element p^{t-1} has the smallest order, and the subgroup H generated by p^{t-1} is the smallest subgroup containing more than one element. Consider the matrix:

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

This matrix generates the code $C = \{\alpha x + \beta y \mid \alpha, \beta \in \mathbb{Z}_{p^t}\}$. According to Theorem 3.1 in [6], the code C is a $[p^t + 1, 2, p^{t-1}(p - 1) + 1]\mathbb{Z}_{p^t}$-linear code. This code is known as a $\mathbb{Z}_{p^t}$-Simplex code of rank 2 and is denoted by $S_2(p^t)$. Additionally, in [6], a generalization of the $\mathbb{Z}_{p^t}$-Simplex code to rank k is introduced and denoted as $S_k(p^t)$.

The authors in [9] have previously conducted similar research, but their focus was on a broader context, encompassing all integers $q > 1$. In contrast, our study specifically addresses the special case of $q = p^t$, where p is a prime number. This research paper focuses on various aspects of $\mathbb{Z}_{p^t}$-linear codes. In Section 2 , we analyze the weight distribution of $\mathbb{Z}_{p^t}$-Simplex codes with a rank of 2 , considering positive integers $p^t \geq 2$.

II. Main Result

In [5, 6], the parameters and properties of $\mathbb{Z}_{p^t}$ Simplex codes $S_k(p^t)$ with rank k were introduced for positive integers $p^t \geq 2$, focusing on the weight distribution of rank 2 for prime power p^t. In this section, we aim to determine the weight distribution of $S_2(p^t)$ for any positive integer $p^t \geq 2$.

Theorem 1: For any integer $p^t \geq 2$, the weight distribution of a $\mathbb{Z}_{p^t}$-Simplex code with rank 2 is given by:

$$\begin{aligned} &A_0 = 1, \\ &A_{p^t} = p^{2t} - p^{2t-1} + p^t - 1, \\ &A_{p^t - p^{t-e} + 1} = p^e(p^e - p^{e-1}), \text{ for } 0 < e < t, \\ &A_{p^t+1} = p^t(p^t - 1) - \sum_{0<e\leq t} p^e(p^e - p^{e-1}). \end{aligned}$$

Proof:
Consider the matrix (1.2):

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

Let x and y represent the first and second rows of the above matrix. Then $S_2(p^t) = \{\alpha x + \beta y \mid \alpha, \beta \in \mathbb{Z}_{p^t}\}$, where $\alpha x = \underbrace{x + x + \cdots + x}_{\alpha \text{ times}}$.

Case (i): If $\alpha = 0 = \beta$, then $wt(\alpha x + \beta y) = 0$. Consequently, we have $A_0 = 1$.

Case (ii): If $\alpha = 0$ and $\beta \neq 0$, then $\beta 1 \neq 0$ for all $\beta \neq 0$ in $\mathbb{Z}_{p^t}$. This implies $wt(\beta y) = p^t$, resulting in $wt(\alpha x + \beta y) = p^t$. In this scenario, there are $p^t - 1$ codewords of weight p^t.

Before proceeding to the next case, we apply the following theorem:

Theorem 2 [5]: Let G be a cyclic group of order n. For every divisor d of n, G has a unique subgroup of order d.

Consider elements $x, y \in \mathbb{Z}_{p^t}$. We define the relation $x \sim y$ if $\langle x \rangle = \langle y \rangle$ under addition. This relation is an equivalence relation. Let $H(x) = \{y \in \mathbb{Z}_{p^t} \mid x \sim y\}$. It follows that $H(x)$ contains only elements of order $o(x)$. According to Theorem 2 , we have $o(H(x)) = \phi(o(x))$. For every divisor d of p^t, there exists a subset $H(x)$ of $\mathbb{Z}_{p^t}$ that contains elements of order $o(x)$. Since $H(x)$ represents an equivalence class, we have either $H(x) = H(y)$ or $H(x) \cap H(y) = \phi$. Moreover, $\mathbb{Z}_{p^t} = \cup H(x)$, where the sum runs over one element from each equivalence class.

Case (iii): Let $\alpha \neq 0$ and $\beta = 0$. If $\alpha \in H(x)$ for $x \neq 0$, then $o(\alpha) = o(x) = p^e$ where $0 \leq e \leq t$, let's say. Since $o(\alpha) \mid o(\mathbb{Z}_{p^t})$, all elements in the subgroup generated by α appear an equal number of times in the set $\{\alpha 0, \alpha 1, \alpha 2, \dots, \alpha(p^t - 1)\}$. In other words, $\alpha(0,1,2,\dots,p^t - 1) = 0,1\alpha, 2\alpha, \dots, (p^e - 1)\alpha, 0,1\alpha, 2\alpha, \dots, (p^e - 1)\ \alpha, \dots, 0,1\alpha, 2\alpha, \dots, (p^e - 1)\alpha$. This implies that zero appears p^{t-e} times in the sequence $\alpha(0,1,2,\dots,p^t - 1)$. Therefore, $wt\big(\alpha(0,1,2,\dots,p^t - 1)\big) = p^t + 1 - p^{t-e}$, where $0 \leq e \leq t$. Since $H(x)$ has $p^e - p^{e-1}$ elements of order p^e, there are $p^e - p^{e-1}$ codewords of weight $p^t - p^{t-e} + 1$. Hence, for $0 < e \leq t$, there are $p^e - p^{e-1}$ codewords of weight $p^t - p^{t-e} + 1$.

Case (iv): Let $\alpha \neq 0$ and $\beta \neq 0$. If $o(\alpha) = p^e$, where $0 < e \leq t$, then all elements in $\langle \alpha \rangle$ appear an equal number of times in the sequence $\alpha(0,1,2,\dots,p^t - 1)$, specifically p^{t-e} times.

(1) If $\beta \in \langle \alpha \rangle \setminus \{0\}$, then $wt(\alpha x + \beta y) = p^t + 1 - p^{t-e}$. Consequently, the number of codewords with weight $p^t - p^{t-e} + 1$ is $(p^e - 1)(p^e - p^{e-1})$.

(2) If $\beta \notin \langle \alpha \rangle \setminus \{0\}$, then $wt(\alpha x + \beta y) = p^t + 1$. Hence, there are $(p^t - p^e)(p^e - p^{e-1})$ codewords with weight $p^t + 1$, where $1 < e < t$.

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] M. K. Gupta and C. Durairajan, On the covering radius of some modular codes, Adv. Math. Commun. 8(2) (2014), 129-137.

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

[9] Durairajan, C., and J. Mahalakshmi. "On codes over integers modulo q." Adv. Appl. Math 15 (2015): 125-143.