Filomat 30:2 (2016), 255–268
DOI 10.2298/FIL1602255O

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

On Codes over $\mathbb{Z}_{p^s}$ with the Extended Lee Weight

Zeynep Ödemiş Özger[a], Bahattin Yıldız[b], Steven T. Dougherty[c]

[a]*Department of Engineering Sciences, İzmir Kâtip Çelebi University, 35620 İzmir, Turkey*
[b]*Department of Mathematics, Fatih University, 34500 İstanbul, Turkey*
[c]*Department of Mathematics, University of Scranton, Scranton, PA 18510, USA*

Abstract. We consider codes over $\mathbb{Z}_{p^s}$ with the extended Lee weight. We find Singleton bounds with respect to this weight and define MLDS and MLDR codes accordingly. We also consider the kernels of these codes and the notion of independence of vectors in this space. We investigate the linearity and duality of the Gray images of codes over $\mathbb{Z}_{p^s}$.

1. Introduction

In the early history of coding theory, codes over finite fields were predominantly studied. The most common weight used for such codes was the Hamming weight, which is defined to be the number of nonzero coordinates. We will denote the Hamming weight by w_H. Many encoding and decoding schemes as well as error correction algorithms are based on the Hamming distance.

Codes over rings have been considered since the early seventies, however it was not until the beginning of the nineties that they became a widely popular research field in coding theory. In 1994, Hammons et al.([12]) solved a long standing problem in nonlinear binary codes by constructing the Kerdock and Preparata codes as the Gray images of linear codes over $\mathbb{Z}_4$. This work started an intense activity on codes over rings. The rich algebraic structure that rings bring together with some better than optimal nonlinear codes obtained from linear codes over rings have increased the popularity of this topic. What started with the ring $\mathbb{Z}_4$, later was extended to rings such as $\mathbb{Z}_{2^k}$, $\mathbb{Z}_{p^k}$, Galois rings, $\mathbb{F}_q + u\mathbb{F}_q$, and various other rings.

For codes over rings, weights other than the Hamming weight were considered. For example, in [12], the authors used the Lee weight on $\mathbb{Z}_4$, which we will denote by w_L and was defined as

$$w_L(x) := \begin{cases} 0 & \text{if } x = 0, \\ 2 & \text{if } x = 2, \\ 1 & \text{otherwise.} \end{cases}$$

The Gray map

$$\phi_L : \mathbb{Z}_4 \to \mathbb{Z}_2^2,$$

2010 *Mathematics Subject Classification*. Primary 94B05, 94B15
Keywords. extended Lee weight, Gray map, kernel, Singleton bound, MLDS codes, MLDR codes
Received: 17 April 2013; Accepted: 18 March 2016
Communicated by Miroslav Ćirić

Email addresses: zeynep.odemis.ozger@ikc.edu.tr (Zeynep Ödemiş Özger), byildiz@fatih.edu.tr (Bahattin Yıldız), prof.steven.dougherty@gmail.com (Steven T. Dougherty)

with

$$\phi_L(0) = (00), \phi_L(1) = (01), \phi_L(2) = (11), \phi_L(3) = (10)$$

turns out to be a nonlinear isometry from ($\mathbb{Z}_4^n$, Lee distance) to ($\mathbb{F}_2^{2n}$, Hamming distance), where the Lee distance on $\mathbb{Z}_4$ is defined as

$$d_L(x, y) := w_L(x - y), \quad x, y \in \mathbb{Z}_4,$$

and similarly, the Hamming distance on $\mathbb{Z}_4$ as

$$d_H(x, y) := w_H(x - y), \quad x, y \in \mathbb{Z}_4.$$

This means that if C is a linear code over $\mathbb{Z}_4$ of length n, size M and minimum Lee distance d, then $\phi_L(C)$ is a possibly nonlinear binary code with parameters $[2n, M, d]$, where d is the minimum Hamming distance of $\phi_L(C)$.

When extending the Lee distance from $\mathbb{Z}_4$ to the more general ring extensions, the homogeneous weight was mostly used. The homogeneous weight has a lot of advantages, which made them useful in constructing codes over rings. It is related to exponential sums (see [5] and [20] for example), making it easier to find bounds by using some number theoretic arguments such as the Weil bound. The homogeneous weight also gives rise to codes with high divisibility properties.

Another extension of the Lee weight is also possible and has been used by different researchers. For example the weight w_L on $\mathbb{Z}_{2^s}$, defined by

$$w_L(x) := \begin{cases} x & \text{if } x \leq 2^{s-1}, \\ 2^s - x & \text{if } x > 2^{s-1}, \end{cases}$$

was used partly in [4], [6] and [23]. A simple Gray map for this weight maps codes over $\mathbb{Z}_{2^s}$ to (mostly) nonlinear binary codes. This extension was generalized to $\mathbb{Z}_m$ as the Lee weight by letting $w_L(x) = \min\{x, m - x\}$ in some works, however no Gray map has been offered for such a weight.

In [22], the Lee weight on $\mathbb{Z}_{2^s}$ given above was generalized to the rings $\mathbb{Z}_{p^s}$ and the Galois rings $GR(p_s, m)$, together with a simple description of a Gray map projecting codes over $\mathbb{Z}_{p^s}$ to codes over the finite prime field $\mathbb{F}_p = \mathbb{Z}_p$. In this work, we study codes over $\mathbb{Z}_{p^s}$ together with this Lee weight from many angles such as Singleton bounds, independence, kernels and duality.

The rest of the paper is organized as follows: In section 2, we recall the extended Lee weight, the Gray map and some properties for codes over $\mathbb{Z}_{p^s}$ from [22]. In section 3, some bounds on codes over $\mathbb{Z}_{p^s}$ concerning both length and size of the codes are given and MLDS and MLDR codes are defined accordingly. In section 4, the notions of kernel and independence are investigated. In section 5, some results about self-duality and self-orthogonality are found.

2. The Extended Lee Weight and Its Gray Map

We recall that a new weight on $\mathbb{Z}_{p^s}$, a generalization of w_L, was defined in [22] as follows:

$$w_L(x) := \begin{cases} x & \text{if } x \leq p^{s-1}, \\ p^{s-1} & \text{if } p^{s-1} < x \leq p^s - p^{s-1}, \\ p^s - x & \text{if } p^s - p^{s-1} < x \leq p^s - 1, \end{cases}$$

where p is prime. Note that for $p = 2$ and $s = 2$ this reduces to the Lee weight for $\mathbb{Z}_4$ and for $p = 2$ and any s, this is the weight that was used briefly by Carlet in [4] and by Dougherty and Fernández-Córdoba in [6]. We can define a Gray map from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_p^{p^{s-1}}$ just as was done for the homogeneous weight as follows:

$$\begin{array}{lcl}
0 & \to & (000\cdots000),\\
1 & \to & (100\cdots000),\\
2 & \to & (110\cdots000),\\
 & \cdot & \\
 & \cdot & \\
p^{s-1} & \to & (111\cdots111),\\
p^{s-1}+1 & \to & (211\cdots111),\\
p^{s-1}+2 & \to & (221\cdots111),\\
 & \cdot & \\
 & \cdot & \\
p^{s-1}+p^{s-1}-1 & \to & (222\cdots221),\\
2p^{s-1} & \to & (222\cdots222),\\
2p^{s-1}+1 & \to & (322\cdots222),\\
 & \cdot & \\
 & \cdot & \\
2p^{s-1}+p^{s-1}-1 & \to & (333\cdots332),\\
3p^{s-1} & \to & (333\cdots333),\\
 & \cdot & \\
 & \cdot & \\
(p-1)p^{s-1} & \to & ((p-1)\cdots(p-1)),\\
(p-1)p^{s-1}+1 & \to & (0(p-1)\cdots(p-1)),\\
 & \cdot & \\
 & \cdot & \\
p^s-2 & \to & (000\cdots0(p-1)(p-1)),\\
p^s-1 & \to & (000\cdots00(p-1)).
\end{array}$$

We simply put 1's in the first x coordinates and 0's in the other coordinates for all $x \le p^{s-1}$. If $x > p^{s-1}$ then the Gray map takes x to $\overline{q}+\phi_L(r)$, where ϕ_L is the Gray map for w_L, $\overline{q} = (qqq\cdots qqq)$ and q and r are such that

$$x = qp^{s-1} + r,$$

which can be found by division algorithm. Here, $0 \le x \le p^s - 1$, $0 \le q \le p-1$, $0 \le r \le p^{s-1}-1$. Here by putting $p = 2$, we get the same Gray map given in [23] and [6], which is

$$\begin{array}{lcl}
0 & \to & (000\cdots000),\\
1 & \to & (100\cdots000),\\
2 & \to & (110\cdots000),\\
 & \cdot & \\
 & \cdot & \\
2^{s-1} & \to & (111\cdots111),\\
2^{s-1}+1 & \to & (011\cdots111),\\
2^{s-1}+2 & \to & (001\cdots111),\\
 & \cdot & \\
 & \cdot & \\
2^s-2 & \to & (000\cdots011),\\
2^s-1 & \to & (000\cdots001).
\end{array}$$

As an example, when $p = 3$, $s = 2$ we get the extended Lee weight on $\mathbb{Z}_9$ is defined as

$$w_L(x) := \begin{cases} x & \text{if } x \le 3,\\ 3 & \text{if } 3 < x \le 6,\\ 9-x & \text{if } 6 < x \le 8. \end{cases}$$

The Gray map takes $\mathbb{Z}_9$ to $\mathbb{Z}_3^3$ as follows:

$$\begin{array}{lll}
0 & \to & (000),\\
1 & \to & (100),\\
2 & \to & (110),\\
3 & \to & (111),\\
4 & \to & (211),\\
5 & \to & (221),\\
6 & \to & (222),\\
7 & \to & (022),\\
8 & \to & (002).
\end{array}$$

We define the Lee distance on $\mathbb{Z}_{p^s}$ as

$$d_L(x, y) := w_L(x - y), \quad x, y \in \mathbb{Z}_{p^s}.$$

Note that this is a metric on $\mathbb{Z}_{p^s}$ and by extending w_L and d_L linearly to $(\mathbb{Z}_{p^s})^n$ in an obvious way, we get a weight and a metric on $(\mathbb{Z}_{p^s})^n$.

Theorem 2.1. *The map $\phi_L : (\mathbb{Z}_{p^s}, d_L) \longrightarrow (\mathbb{F}_p^{p^{s-1}}, d_H)$ is a distance preserving (not necessarily linear) map, where d_L and d_H denote the Lee and the Hamming distances respectively.*

The proof of this theorem can be found in [22] with the following corollary:

Corollary 2.2. *If C is a linear code over $\mathbb{Z}_{p^s}$ of length n, size M and minimum Lee distance d, then $\phi_L(C)$ is a (possibly nonlinear) code over $\mathbb{F}_p$ of length np^{s-1}, size M and minimum Hamming distance d.*

The concepts of minimum Lee distance and minimum Lee weight are the same for linear codes over $\mathbb{Z}_{p^s}$.

A Gray map from $GR(p^s, m)$ to $\mathbb{F}_p^{p^{s-1}m}$ can also be defined by extending $\phi_L : (\mathbb{Z}_{p^s}, d_L) \longrightarrow (\mathbb{F}_p^{p^{s-1}}, d_H)$ (see [22], Section 3), which means that most of the work done in this paper is applicable to Galois rings.

3. Singleton Bounds for Codes Over $\mathbb{Z}_{p^s}$

A Singleton bound for codes over a finite quasi-Frobenius ring is already given in [19] as an MDS bound. Since this result is given for any weight function, it can be specified for the extended Lee weight.

Definition 3.1 (Complete weight). *[19] Let R be a finite commutative quasi-Frobenius ring, and let $V := R^n$ be a free module of rank n consisting of all n-tuples of elements of R. For every $x = (x_1, \cdots, x_n) \in V$ and $r \in R$, the complete weight of x is defined by*

$$n_r(x) := |\{i\,|x_i = r\}|.$$

Definition 3.2 (General weight function). *[19] Let $a_r,(0 \neq)r \in R$, be positive real numbers, and set $a_0 = 0$. Then*

$$w(x) := \sum_{r \in R} a_r n_r(x) \tag{1}$$

is called a general weight function.

Note that when $a_r = 1$, $r \in R - \{0\}$, $w(x)$ gives the Hamming weight of x.

The following theorem gives a Singleton bound for any finite quasi-Frobenius ring and any weight function.

Theorem 3.3. *[19] Let C be a code of length n over a finite commutative quasi-Frobenius ring R. Let $w(x)$ be a general weight function on C, as in (1), and with maximum a_r−value A. Suppose the minimum weight of the elements in C is d. Then*

$$\left\lfloor \frac{d-1}{A} \right\rfloor \leq n - \log_{|R|} |C|,$$

where $\lfloor b \rfloor$ is the integer part of b.

Since $\mathbb{Z}_{p^s}$ is a finite commutative Frobenius ring by letting $w(x) = w_L(x)$, we have p^{s-1} as the maximum a_r−value. Applying these information to Theorem 3.3 we get the following:

Theorem 3.4. *Let C be a code of length n over $\mathbb{Z}_{p^s}$ with minimum distance d. Then*

$$\left\lfloor \frac{d-1}{p^{s-1}} \right\rfloor \leq n - \log_{p^s} |C|.$$

Codes meeting this bound are called MLDS (Maximum Lee Distance Separable) codes. In [18], another bound was found over $\mathbb{Z}_l$ with a different generalization of the Lee weight. Now we will find a similar result for codes over $\mathbb{Z}_{p^s}$ with $w_L(x)$ by the same method used.

Definition 3.5 (Rank, Free Rank). *Let C be any finitely generated submodule of $\mathbb{Z}_{p^s}^n$, that is isomorphic to*

$$\mathbb{Z}_{p^s}/p^{a_1}\mathbb{Z}_{p^s} \oplus \mathbb{Z}_{p^s}/p^{a_2}\mathbb{Z}_{p^s} \oplus \cdots \oplus \mathbb{Z}_{p^s}/p^{a_{n-1}}\mathbb{Z}_{p^s},$$

where a_i are positive integers with $p^{a_1}|p^{a_2}| \cdots |p^{a_{n-1}}|p^s$. Then

$$rank(C) := |\{i \,|a_i \neq 0\}|$$

is called the rank of C and

$$free\, rank(C) := |\{i \,|a_i = s\}|$$

is called the free rank of C.

Any linear code over $\mathbb{Z}_{p^s}$ has a generator matrix, which is permutationally equivalent to a matrix of the form:

$$G = \begin{bmatrix} I_{\delta_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,s} \\ 0 & pI_{\delta_1} & pA_{1,2} & pA_{1,3} & \cdots & \cdots & pA_{1,s} \\ 0 & 0 & p^2I_{\delta_2} & p^2A_{2,3} & \cdots & \cdots & p^2A_{2,s} \\ \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & p^{s-2}I_{\delta_{s-2}} & p^{s-2}A_{s-2,s-1} & p^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & \cdots & 0 & p^{s-1}I_{\delta_{s-1}} & p^{s-1}A_{s-1,s} \end{bmatrix}. \tag{2}$$

This means that after a finite number of permutations of columns and rows of the generator matrix, we can get a matrix of the form (2). A generator matrix G, which is of the form (2), is called a generator matrix in standard form.

Then a code C over $\mathbb{Z}_{p^s}^n$ is of type $(p^s)^{\delta_0}(p^{s-1})^{\delta_1} \cdots (p)^{\delta_{s-1}}$, and

$$\begin{aligned} rank(C) &= \delta_0 + \delta_1 + \cdots + \delta_{s-1}, \\ free\, rank(C) &= \delta_0. \end{aligned}$$

Let $C^\perp$, namely the dual of C, be defined as

$$C^\perp := \left\{v \in \mathbb{Z}_{p^s}^n | \langle v, w\rangle = 0 \text{ for all } w \in C\right\},$$

where $\langle v, w\rangle = \sum v_i w_i \pmod{p^s}$. The code $C^\perp$ is isomorphic to

$$\mathbb{Z}_{p^s}/p^{s-a_1}\mathbb{Z}_{p^s} \oplus \mathbb{Z}_{p^s}/p^{s-a_2}\mathbb{Z}_{p^s} \oplus \cdots \oplus \mathbb{Z}_{p^s}/p^{s-a_{n-1}}\mathbb{Z}_{p^s}.$$

From [18], [15], [7], [8], [6], and the definitions above, the relationship between the rank of a code and its dual's free rank can be given as follows:

$$rank(C) + free\ rank(C^\perp) = n. \tag{3}$$

For a submodule $D \subseteq V := (\mathbb{Z}_{p^s})^n$ and a subset $M \subseteq N := \{1, 2, \ldots, n\}$, we define

$$\begin{aligned} &D(M) := \left\{x \in D \,\middle|\, \mathrm{supp}(x) \subseteq M\right\}, \\ &D^* := Hom_{\mathbb{Z}_{p^s}}(D, \mathbb{Z}_{p^s}), \end{aligned}$$

where $Hom(\cdot,\cdot)$ is the hom functor, and

$$\mathrm{supp}(x) := \{i \in N \,| x_i \neq 0\}.$$

From the fundamental theorem of finitely generated abelian groups, we have $D^* \cong D$. Shiromoto also gave the following basic exact sequence:

Lemma 3.6. *[18]Let C be a code of length n over $\mathbb{Z}_l$ and $M \subseteq N$. Then there is an exact sequence as $\mathbb{Z}_l$-modules*

$$0 \to C^\perp(M) \overset{inc}{\to} V(M) \overset{f}{\to} C^* \overset{res}{\to} C(N-M)^* \to 0$$

where the maps inc, res denote the inclusion map, the restriction map, respectively, and f is a $\mathbb{Z}_l$-homomorphism such that

$$\begin{aligned} f:\ & V \to D^* \\ & y \to (\hat{y} : x \to \langle x, y\rangle). \end{aligned}$$

We can adjust Lemma 3.6 to our case:

Lemma 3.7. *Let C be a code of length n over $\mathbb{Z}_{p^s}$ and $M \subseteq N$. Then there is an exact sequence as $\mathbb{Z}_{p^s}$-modules*

$$0 \to C^\perp(M) \overset{inc}{\to} V(M) \overset{f}{\to} C^* \overset{res}{\to} C(N-M)^* \to 0,$$

where the maps inc, res denote the inclusion map, the restriction map, respectively, and f is a $\mathbb{Z}_{p^s}$-homomorphism such that

$$\begin{aligned} f:\ & V \to D^* \\ & y \to (\hat{y} : x \to \langle x, y\rangle). \end{aligned}$$

Note that for any $x \in V$, if $\mathrm{supp}(x) \subseteq M \subseteq N$, then for any general weight function we have $wt(x) \leq a_r\,|M|$. In our case:

$$w_L(x) \leq p^{s-1}\,|M|.$$

So we have the following lemma for $w_L(x)$:

Lemma 3.8. *Let C be a code of length n over $\mathbb{Z}_{p^s}$, then $C(M)^* = 0$ for any subset $M \subseteq N$ such that $|M| < d/p^{s-1}$, where d is the minimum Lee weight of C.*

Proof. *For any* $\bar{c} \neq 0 \in C$

$$\left|supp(\bar{c})\right| p^{s-1} \geq w_L(\bar{c}) \geq d. \tag{4}$$

If $|M| < d/p^{s-1}$, *then*

$$d > |M| p^{s-1}, \tag{5}$$

which means

$$\left|supp(\bar{c})\right| p^{s-1} \geq d > |M| p^{s-1}$$

by (4) and (5). But this means $\left|supp(\bar{c})\right| > |M|$, *i.e.* $supp(\bar{c}) \not\subseteq M$. *So* $C \cap V(M) = \{0\}$ *and* $C(M)^* = Hom_{\mathbb{Z}_{p^s}}(C \cap V(M), \mathbb{Z}_{p^s}) = 0$. □

By Lemma 3.8, we have the following bound:

Theorem 3.9. *Let C be a code of length n over* $\mathbb{Z}_{p^s}$ *with the minimum Lee weight d. Then*

$$\left\lfloor \frac{d-1}{p^{s-1}} \right\rfloor \leq n - rank(C).$$

Proof. We will follow the steps of Shiromoto in [18]. In the exact sequence of Lemma 3.7, replace C with $C^{\perp}$. Then the exact sequence transforms into the following one:

$$0 \to C(M) \overset{inc}{\to} V(M) \overset{f}{\to} (C^{\perp})^* \overset{res}{\to} C^{\perp}(N-M)^* \to 0. \tag{6}$$

Apply $* = Hom_{\mathbb{Z}_{p^s}}(\cdot, \mathbb{Z}_{p^s})$ and take an arbitrary subset $M \subseteq N$ such that

$$|M| = \left\lfloor \frac{d-1}{p^{s-1}} \right\rfloor.$$

Since $C(M)^* = 0$ by Lemma 3.8 and $V(M)^* \cong V(M)$, the exact sequence (6) leads us to the following short exact sequence:

$$0 \to C^{\perp}(N-M) \to C^{\perp} \to V(M) \to 0. \tag{7}$$

$V(M) \cong (\mathbb{Z}_{p^s})^{|M|}$ is a projective module. Hence (7) is a split, that is,

$$C^{\perp} \cong C^{\perp}(N-M) \oplus V(M).$$

Therefore

$$free\ rank(C^{\perp}) \geq free\ rank(V(M)) = |M| = \left\lfloor \frac{d-1}{p^{s-1}} \right\rfloor.$$

From (3) we have

$$n - rank(C) \geq \left\lfloor \frac{d-1}{p^{s-1}} \right\rfloor.$$

□

Codes meeting the bound above are called MLDR (Maximum Lee Distance with respect to Rank) codes. The following example illustrates a code which is both MLDS and MLDR.

Example 3.10. *Let C be the linear code over* $\mathbb{Z}_p$, *whose generator matrix is* $G = [1]$. *So* $C = \{(0), (1), \cdots, (p-1)\}$, $\log_{|R|}|C| = \log_{p^1}|C| = 1$, $A = p-1$, $d = 1$, *and* $n = 1$. *Hence* $\left\lfloor \frac{d-1}{A} \right\rfloor = n - \log_{|R|}|C| = 0$ *and* $\left\lfloor \frac{d-1}{p^{1-1}} \right\rfloor = n - \log_{p^1}|C| = 0$.

4. Kernel and Independence of $\phi_L(C)$

For finite fields and vector spaces the notions of kernel and independence are strongly related (see [13]). In this section, we investigate the same notions for Gray images of linear codes over $\mathbb{Z}_{p^s}$. The kernel of a code C over $\mathbb{F}_p$, where p is a prime, denoted by $K(C)$, is defined as the set

$$K(C) := \{v \,|v \in C, v + C = C\}.$$

For further information we refer to [16]. Since $\phi_L(C)$ is a code over $\mathbb{F}_p$ (not necessarily linear), we can define

$$K(\phi_L(C)) := \left\{\phi_L(v) \,\middle|\, v \in C, \phi_L(v) + \phi_L(C) = \phi_L(C)\right\}.$$

In [6], authors gave some results about $K(\phi_L(C))$, ϕ_L-independence and modular independence over $\mathbb{Z}_{2^s}$. We have similar results for $\mathbb{Z}_{p^s}$.

First we define modular independence. We say that vectors $v_1, v_2, \ldots, v_t$ are modular independent over $\mathbb{Z}_{p^s}$ if $\sum\limits_{i=1}^{t} \alpha_i v_i = \mathbf{0}$ then $\alpha_i \in \langle p\rangle$ for all i. The Gray images of modularly independent vectors on $\mathbb{Z}_{p^s}$ might not be linearly independent on $\mathbb{Z}_p$. For counter example, we refer to [6]. A set of vectors in $\mathbb{Z}_{p^s}$ is said to be ϕ_L-independent, if their Gray images are linearly independent over $\mathbb{Z}_p$.

Lemma 4.1. *Let G be the generating matrix of a linear code of type $(p^s)^{\delta_0}(p^{s-1})^{\delta_1}\cdots(p)^{\delta_{s-1}}$ over $\mathbb{Z}_{p^s}$ in standard form. Let $v_{i,1}, v_{i,2}, \ldots, v_{i,\delta_i}$ be the vectors of order p^{s-i}. Then the vectors in the set $\left\{\alpha v_{i,j} | 1 \le \alpha \le p^{s-i-1}\right\}$ are ϕ_L-independent in $\mathbb{F}_p^{p^{s-1}n}$.*

Proof. Let G be the generator matrix of the code in standard form. The Gray images of $1, 2, \ldots, p^{s-1}$ form an upper triangular matrix and so the Gray image of the vectors in the first δ_0 coordinates are linearly independent. All initial nonzero coordinates of submatrices $p^i I_{\delta_i}$ form an uppertriangular matrix and their entries are all less than or equal to p^{s-1}. Therefore the other cases of the form $p^i I_{\delta_i}$ form submatrix of the above mentioned upper triangular matrix. Hence they are also linearly independent. □

Theorem 4.2. *Let $v_1, v_2, \ldots, v_k$ be modular independent vectors in $\mathbb{Z}_{p^s}^n$. Then there exist modular independent vectors $w_1, w_2, \ldots, w_k$ which are ϕ_L-independent in $\mathbb{F}_p^{p^{s-1}n}$ such that $\langle v_1, v_2, \ldots, v_k\rangle = \langle w_1, w_2, \ldots, w_k\rangle$.*

Proof. Any set of modular independent vectors over $\mathbb{Z}_{p^s}$ are permutationally equivalent to a set of vectors that form a generator matrix in standard form as shown in [15]. Therefore by Lemma 4.1 these vectors are ϕ_L-independent. □

The following proposition gives a restriction to the order of elements whose Gray images belong to $K(\phi_L(C))$.

Proposition 4.3. *Let C be a linear code over $\mathbb{Z}_{p^s}$. If $v \in C$ has order greater than p^2 then $K(\phi_L(C))$ does not contain $\phi_L(v)$.*

Proof. For the rest of the proof and the rest of the paper, let $\overline{a}_i\overline{b}_j\overline{c}_k$ be the codeword of length $i + j + k$, whose first i entries are a, the next j entries are b, and the remaining k entries are c.

Since $ord(v) > p^2$, v has a number i as its coordinate with $ord(i) > p^2$. We have the following three cases for $i \in \mathbb{Z}_{p^s}$ with $ord(i) > p^2$:

(i) If $0 < i < p^{s-1}$ then $ord(i) = p^k$, $k > 2$, since $ord(i) \left| \left|\mathbb{Z}_{p^s}\right| \right. = p^s$. That means $i = p^{s-k}u_i$, where $(u_i, p^s) = 1$, i.e., $(u_i, p) = 1$. Since $0 < i < p^{s-1}$

$$\phi_L(i) = \overline{1}_i\overline{0}_{p^{s-1}-i},$$

and since $s-k \leq s-2$, we have $pi = p^{s-k+1}u_i < p^s$. We know that $i \neq p^{s-1}u_j$ or $i \neq p^{s-2}u_j$ for any u_j such that $(u_j, p) = 1$. So by using division algorithm we can write

$$\begin{aligned} i &= qp^{s-2} + r', \quad 0 < r' < p^{s-2}, \\ pi &= qp^{s-1} + r, \quad 0 < r = pr' < p^{s-1}. \end{aligned}$$

Without loss of generality assume that $i > r$. Then,

$$\begin{aligned} \phi_L(i) + \phi_L(pi) &= \overline{1}_i \overline{0}_{p^{s-1}-i} + \overline{q}_{p^{s-1}} + \overline{1}_r \overline{0}_{p^{s-1}-r} \\ &= \overline{q+2}_r \overline{q+1}_{i-r} \overline{q}_{p^{s-1}-i} \notin \phi_L(C), \end{aligned}$$

since $r \neq 0$, $r-i \neq 0$ and $p^{s-1} - i \neq 0$. Now assume $i = r$. Then,

$$\begin{aligned} \phi_L(i) + \phi_L(pi) &= \overline{1}_i \overline{0}_{p^{s-1}-i} + \overline{q}_{p^{s-1}} + \overline{1}_i \overline{0}_{p^{s-1}-i} \\ &= \overline{q+2}_i \overline{q}_{p^{s-1}-i} \notin \phi_L(C), \end{aligned}$$

since $i \neq 0$ and $p^{s-1} - i \neq 0$.

(ii) If $p^{s-1} < i < p^s - p^{s-1}$ then $mp^{s-1} < i < (m+1)p^{s-1}$, where $m \in \{1, 2, 3, \cdots, p-2\}$. Since $ord(i) > p^2$, $i \neq p^{s-1}u_j$ or $i \neq p^{s-2}u_j$ for any $u_j \in \{1, 2, 3, \cdots, p-2, p-1\}$. Let

$$\begin{aligned} i &= mp^{s-1} + r, \quad 0 < r < p^{s-1}, \\ r &= qp^{s-2} + r', \quad 0 < r' < p^{s-2}. \end{aligned}$$

So

$$pi = (mp^{s-1} + r)p = pr = qp^{s-1} + pr'.$$

Without loss of generality assume that $r > pr'$. Then,

$$\begin{aligned} \phi_L(i) + \phi_L(pi) &= \overline{1}_r \overline{0}_{p^{s-1}-r} + \overline{m}_{p^{s-1}} + \overline{q}_{p^{s-1}} + \overline{1}_{pr'} \overline{0}_{p^{s-1}-pr'} \\ &= \overline{q+m+2}_{pr'} \overline{q+m+1}_{r-pr'} \overline{q+m}_{p^{s-1}-r} \notin \phi_L(C), \end{aligned}$$

since $0 < pr' < p^{s-1}$, $r - pr' \neq 0$ and $p^{s-1} - r \neq 0$.

(iii) If $p^s - p^{s-1} < i < p^s$ then $0 < -i < p^{s-1}$. So $\phi_L(-i) + \phi_L(-pi) \notin \phi_L(C)$ as we proved in the first case. We see that for each $v \in \mathbb{Z}_{p^s}^n$ we have either $\phi_L(v) + \phi_L(pv) \notin \phi_L(C)$ or $\phi_L(-v) + \phi_L(-pv) \notin \phi_L(C)$. Hence either $\phi_L(v) + \phi_L(C) \neq \phi_L(C)$ or $\phi_L(-v) + \phi_L(C) \neq \phi_L(C)$ when $ord(v) > p^2$.

□

So the Gray image of the code, which is generated by all vectors of C with order less than or equal to p^2 should include $K(\phi_L(C))$. Then we have the following corollary and lemmas, which generalize the results in [6]:

Corollary 4.4. *Let C be a linear code over $\mathbb{Z}_{p^s}$ with generator matrix of the form (2).Then $K(\phi_L(C))$ is contained in the Gray image of the code generated by the matrix:*

$$\begin{bmatrix} p^{s-2}I_{\delta_0} & p^{s-2}A_{0,1} & p^{s-2}A_{0,2} & p^{s-2}A_{0,3} & \cdots & \cdots & p^{s-2}A_{0,s} \\ 0 & p^{s-2}I_{\delta_1} & p^{s-2}A_{1,2} & p^{s-2}A_{1,3} & \cdots & \cdots & p^{s-2}A_{1,s} \\ 0 & 0 & p^{s-2}I_{\delta_2} & p^{s-2}A_{2,3} & \cdots & \cdots & p^{s-2}A_{2,s} \\ \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & p^{s-2}I_{\delta_{s-2}} & p^{s-2}A_{s-2,s-1} & p^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & \cdots & 0 & p^{s-1}I_{\delta_{s-1}} & p^{s-1}A_{s-1,s} \end{bmatrix}.$$

Lemma 4.5. *Let C be a linear code over $\mathbb{Z}_{p^s}$ and $v, w \in C$. Then we have*

$$\phi_L(p^{s-1}v + w) = \phi_L(p^{s-1}v) + \phi_L(w)$$

for each $v, w \in C$.

Proof. Let $v_i, w_i \in \mathbb{Z}_{p^s}$ be the i^{th} coordinates of v, w respectively. Then by division algorithm we can write

$$\begin{array}{lll} w_i = q_w p^{s-1} + r_w, & 0 \le q_w \le p-1, & 0 \le r_w < p^{s-1}, \\ v_i = q_v p + r_v, & 0 \le q_v < p^{s-1}, & 0 \le r_v < p. \end{array}$$

So $p^{s-1}v_i = p^{s-1}r_v$, where $0 \le p^{s-1}r_v < p^s$. Therefore

$$\begin{aligned} \phi_L(p^{s-1}v_i + w_i) &= \phi_L(p^{s-1}r_v + q_w p^{s-1} + r_w) = \phi_L(p^{s-1}(r_v + q_w) + r_w) \\ &= \overline{r_v + q_w}_{p^{s-1}} + \overline{1}_{r_w}\overline{0}_{p^{s-1}-r_w} = \overline{r_v}_{p^{s-1}} + \overline{q_w}_{p^{s-1}} + \overline{1}_{r_w}\overline{0}_{p^{s-1}-r_w} \\ &= \phi_L(p^{s-1}r_v) + \phi_L(q_w p^{s-1} + r_w) = \phi_L(p^{s-1}v_i) + \phi_L(w_i). \end{aligned}$$

Applying this method coordinate-wise, the result follows. □

Theorem 4.6. *Let C be a linear code over $\mathbb{Z}_{p^s}$ with the generator matrix of the form (2). Then the Gray image of the code C' generated by*

$$\begin{bmatrix} p^{s-1}I_{\delta_0} & p^{s-1}A_{0,1} & p^{s-1}A_{0,2} & p^{s-1}A_{0,3} & \cdots & \cdots & p^{s-1}A_{0,s} \\ 0 & p^{s-1}I_{\delta_1} & p^{s-1}A_{1,2} & p^{s-1}A_{1,3} & \cdots & \cdots & p^{s-1}A_{1,s} \\ 0 & 0 & p^{s-1}I_{\delta_2} & p^{s-1}A_{2,3} & \cdots & \cdots & p^{s-1}A_{2,s} \\ \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & p^{s-1}I_{\delta_{s-2}} & p^{s-1}A_{s-2,s-1} & p^{s-1}A_{s-2,s} \\ 0 & 0 & 0 & \cdots & 0 & p^{s-1}I_{\delta_{s-1}} & p^{s-1}A_{s-1,s} \end{bmatrix} \tag{8}$$

is a linear subcode of $K(\phi_L(C))$.

Proof. Let $v, w \in C$, then $p^{s-1}v \in C' \subseteq C$. Then $\phi_L(p^{s-1}v) \in \phi_L(C')$ and $\phi_L(w) \in \phi_L(C)$. By Lemma 4.5

$$\phi_L(p^{s-1}v + w) = \phi_L(p^{s-1}v) + \phi_L(w) \in \phi_L(C),$$

since $p^{s-1}v, w \in C$. This holds for every $w \in C$, which means $\phi_L(p^{s-1}v) + \phi_L(C) \subseteq \phi_L(C)$. Two different codewords will have different images. Therefore $\phi_L(p^{s-1}v) + \phi_L(C) = \phi_L(C)$, which tells us that $\phi_L(p^{s-1}v) \in K(\phi_L(C))$. □

Lemma 4.7. *Let C be a linear code over $\mathbb{Z}_{p^s}$, $\lambda \in \mathbb{Z}_{p^s}$ and $v \in C$ such that $\phi_L(v) \notin K(\phi_L(C))$. Then $\phi_L(\lambda v) \in K(\phi_L(C))$ if and only if $ord(\lambda v) = p$.*

Proof. ($\Longrightarrow$)Suppose that $ord(\lambda v) = p$, then $\phi_L(\lambda v) \in K(\phi_L(C))$ by Theorem 4.6.
($\Longleftarrow$)Now assume $\phi_L(v) \notin K(\phi_L(C))$ and $\phi_L(\lambda v) \in K(\phi_L(C))$. We have two cases.

(i) If $ord(v) > p^2$ and $v = (v_1, v_2, \cdots, v_n)$, then there exists v_i, $1 \le i \le n$, such that $ord(v_i) > p^2$. Let $ord(v_i) = p^k$ with $k > 2$. Then $v_i = p^{s-k}u_i$, where u_i is a unit. By division algorithm, we have

$$\begin{array}{lll} u_i = q_u p + r_u, & 0 \le q_u \le p^{s-1} - 1, & 0 < r_u < p, \\ v_i = q_v p^{s-1} + r_v, & 0 \le q_v \le p - 1, & 0 < r_v < p^{s-1}, \end{array}$$

where $r_u \neq 0$, since u_i is a unit and $r_v \neq 0$, since $ord(v_i) > p^2$. If $\phi_L(\lambda v_i) \in K(\phi_L(C))$, then by Proposition 4.3 $\lambda = p^{k-2}u_\lambda$ or $\lambda = p^{k-1}u_\lambda$, where u_λ is a unit. For $\lambda = p^{k-1}u_\lambda$ we have $ord(\lambda v_i) = p$, so $\phi_L(\lambda v_i) \in$

$K(\phi_L(C))$ by Theorem 4.6. If $\lambda = p^{k-2}u_\lambda$, then $ord(\lambda v_i) = p^2$ and $\lambda v_i = p^{s-2}u_\lambda u_i = q_u u_\lambda p^{s-1} + r_u u_\lambda p^{s-2}$, where $0 < r_u u_\lambda p^{s-2} < p^{s-1}$. Without loss of generality assume that $r_u u_\lambda p^{s-2} < r_v$, then we have

$$\phi_L(\lambda v_i) + \phi_L(v_i) = \overline{(q_u + q_v + 2)}_{r_u u_\lambda p^{s-2}}\overline{(q_u + q_v + 1)}_{r_v - r_u u_\lambda p^{s-2}}\overline{(q_u + q_v)}_{p^{s-1}-r_v} \notin \phi_L(C),$$

since $r_u u_\lambda p^{s-2} \neq 0$, $r_v - r_u u_\lambda p^{s-2} \neq 0$, $p^{s-1} - r_v \neq 0$. If $r_u u_\lambda p^{s-2} = r_v$, then

$$\phi_L(\lambda v_i) + \phi_L(v_i) = \overline{(q_u + q_v + 2)}_{r_v}\overline{(q_u + q_v)}_{p^{s-1}-r_v} \notin \phi_L(C),$$

since $p^{s-1} - r_v \neq 0$, $r_v \neq 0$.

(ii) If $ord(v) = p^2$ and $v = (v_1, v_2, \cdots, v_n)$, then there exists v_i, $1 \leq i \leq n$, such that $ord(v_i) = p^2$. Then $v_i = p^{s-2}u_i$, where u_i is a unit. By division algorithm, we have $v_i = q_v p^{s-1} + r_v$, $0 \leq q_v \leq p-1$, $0 < r_v < p^{s-1}$, since $ord(v_i) = p^2$. If $\phi_L(\lambda v_i) \in K(\phi_L(C))$, then by Proposition 4.3 $ord(\lambda v_i) = p^2$ or $ord(\lambda v_i) = p$. If $ord(\lambda v_i) = p$, we have $\phi_L(\lambda v_i) \in K(\phi_L(C))$ by Theorem 4.6. If $ord(\lambda v_i) = p^2$ then λ is a unit and $\lambda v_i = p^{s-1}q + r$, $0 < r < p^{s-1}$, $r \neq 0$, since $ord(\lambda v_i) = p^2$. Without loss of generality assume that $r_v > r$, then we have

$$\phi_L(\lambda v_i) + \phi_L(v_i) = \overline{(q + q_v + 2)}_{r}\overline{(q + q_v + 1)}_{r_v - r}\overline{(q_u + q_v)}_{p^{s-1}-r_v} \notin \phi_L(C),$$

since $r \neq 0$, $r_v - r \neq 0$, $p^{s-1} - r_v \neq 0$. If $r = r_v$, then

$$\phi_L(\lambda v_i) + \phi_L(v_i) = \overline{(q_u + q_v + 2)}_{r_v}\overline{(q_u + q_v)}_{p^{s-1}-r_v} \notin \phi_L(C),$$

since $p^{s-1} - r_v \neq 0$, $r_v \neq 0$. In both cases $\phi_L(\lambda v) + \phi_L(v) \notin \phi_L(C)$, whenever $ord(\lambda v) \neq p$.

□

Theorem 4.8. *Let C be a linear code over $\mathbb{Z}_{p^s}$ of type $(p^s)^{\delta_0}(p^{s-1})^{\delta_1} \cdots (p)^{\delta_{s-1}}$. If $m = \dim(K(\phi_L(C)))$, then*

$$m \in \left\{ \sum_{i=0}^{s-1} \delta_i, \sum_{i=0}^{s-1} \delta_i + 1, \sum_{i=0}^{s-1} \delta_i + 2, \cdots, \sum_{i=0}^{s-1} \delta_i + \delta_{s-2} - 2, \sum_{i=0}^{s-1} \delta_i + \delta_{s-2} \right\}.$$

Proof. By Theorem 4.6, the image of any codeword of order p is in $K(\phi_L(C))$. If there is a codeword v of order greater than p^2, then $\phi_L(v) \notin K(\phi_L(C))$. Moreover, if $\phi_L(v) \notin K(\phi_L(C))$, then $\phi_L(\lambda v) \in K(\phi_L(C))$ if and only if $ord(\lambda v) = p$ by Lemma 4.7. Otherwise $\phi_L(\lambda v) + \phi_L(v) \notin \phi_L(C)$. So for $\phi_L(v) \notin K(\phi_L(C))$ and $\phi_L(\lambda v) \in \phi_L(C'') \subseteq K(\phi_L(C))$ we have $ord(\lambda v) = p$. This means we have the Gray images of first $\sum_{i=0}^{s-3} \delta_i$ vectors of (8) as generators of $K(\phi_L(C))$. Furthermore, we can show that the contribution of the Gray images of first $\sum_{i=0}^{s-3} \delta_i$ vectors of (2) to $K(\phi_L(C))$ is restricted to that. To see this, let v be one these vectors in (2). Then $ord(v) > p^2$ and $\phi_L(v) \notin K(\phi_L(C))$ by Proposition 4.3. For any scalar product of v, say λv, then $\phi_L(\lambda v) \in K(\phi_L(C))$ if and only if $ord(\lambda v) = p$ by Lemma 4.7. If $ord(v) = p^k$, $k > 2$, $v = u_v p^k$, this happens only when $\lambda = p^{s-k-1}u_\lambda$, where u_λ and u_v are units. Therefore $\lambda v = p^{s-1}u$, where $u = u_v u_\lambda$ is a unit too. This shows that the only contribution of the Gray image of v to $K(\phi_L(C))$ is its scalar products with the $p^{s-1}u$ and their linear combinations. Also we know that the Gray image of the last δ_{s-1} rows of (8) are generators of $K(\phi_L(C))$ by Theorem 4.6. We don't know whether each of the Gray images of δ_{s-2} remaining vectors generate $K(\phi_L(C))$ certainly. But we know that if their Gray images are not included in generators of $K(\phi_L(C))$, the Gray image of their scalar products with pu, where u is a unit, are all included in $K(\phi_L(C))$. Hence we can have at least the Gray image of the code generated by (8), and at most the Gray image of the code generated by

$$\begin{bmatrix} p^{s-1}I_{\delta_0} & p^{s-1}A_{0,1} & p^{s-1}A_{0,2} & p^{s-1}A_{0,3} & \cdots & \cdots & p^{s-1}A_{0,s} \\ 0 & p^{s-1}I_{\delta_1} & p^{s-1}A_{1,2} & p^{s-1}A_{1,3} & \cdots & \cdots & p^{s-1}A_{1,s} \\ 0 & 0 & p^{s-1}I_{\delta_2} & p^{s-1}A_{2,3} & \cdots & \cdots & p^{s-1}A_{2,s} \\ \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & p^{s-2}I_{\delta_{s-2}} & p^{s-2}A_{s-2,s-1} & p^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & \cdots & 0 & p^{s-1}I_{\delta_{s-1}} & p^{s-1}A_{s-1,s} \end{bmatrix} \tag{9}$$

as $K(\phi_L(C))$. Thus we have the following bound for m:

$$p^{\sum_{i=0}^{s-1}\delta_i} \leq p^m \leq p^{\sum_{i=0, i\neq s-2}^{s-1}\delta_i} \cdot p^{2\delta_{s-2}},$$

which means

$$\sum_{i=0}^{s-1}\delta_i \leq m \leq \sum_{i=0}^{s-1}\delta_i + \delta_{s-2}.$$

Let $\widetilde{C}$ be the code generated by matrix (9). Since $K(\phi_L(C))$ is at most $\phi_L(\widetilde{C})$, $K(\phi_L(C)) \subseteq \phi_L(\widetilde{C})$. So,

$$K(\phi_L(C)) = \left\{c \in \widetilde{C} : \phi_L(c) + \phi_L(C) = \phi_L(C)\right\}.$$

Let $\{v_0, v_1, \cdots, v_k\}$ be the set of generators of $\phi_L(\widetilde{C})$, namely $\langle v_0, v_1, \cdots, v_k\rangle = \phi_L(\widetilde{C})$, which means $\dim(\phi_L(\widetilde{C})) = k+1$. Assume that $\dim(K(\phi_L(C))) = k$, and without loss of generality let $K(\phi_L(C)) = \langle v_1, \cdots, v_k\rangle$. If $v_0 \in \phi_L(\widetilde{C}) \subseteq \phi_L(C)$, then we have $v_0 + v_i \in \phi_L(C)$ for all $i = 1, \cdots, k$, since $v_i \in K(\phi_L(C))$. But $v_0 + v_i \in \phi_L(\widetilde{C})$ for all $i = 1, \cdots, k$, that means $v_0 \in K(\phi_L(\widetilde{C})) \subseteq K(K(\phi_L(C))) \subseteq K(\phi_L(C))$, which is a contradiction. Hence $m \neq \sum_{i=0}^{s-1}\delta_i + \delta_{s-2} - 1$. Therefore we have the following

$$m \in \left\{\sum_{i=0}^{s-1}\delta_i, \sum_{i=0}^{s-1}\delta_i + 1, \sum_{i=0}^{s-1}\delta_i + 2, \cdots, \sum_{i=0}^{s-1}\delta_i + \delta_{s-2} - 2, \sum_{i=0}^{s-1}\delta_i + \delta_{s-2}\right\}.$$

□

5. Linearity and Duality of $\phi_L(C)$

Self-dual codes are important since many of the best codes known are of this type. Numerous researchers have investigated their Gray images to find (not necessarily linear) codes with optimal or extremal parameters. Most of the best codes are nonlinear and they can be viewed as Gray images of linear codes. On the other hand, linearity makes things easier. Therefore it is also very important to know when the image $\phi_L(C)$ is nonlinear/linear. Also some researchers looked into when the images of self-dual codes are also self-dual. The aim of this section is to present some knowledge about these two topics for codes over $\mathbb{Z}_{p^s}$.

Theorem 5.1. *Let C be a linear code over $\mathbb{Z}_{p^s}$ with the generating matrix of the form given in (2). If $\delta_i > 0$ for any $0 \leq i \leq s-3$ then $\phi_L(C)$ is not linear.*

Proof. We have elements $v \in C$ such that $ord(v) > p^2$ by Proposition 4.3, so by Lemma 4.7 they are not in $K(\phi_L(C))$, since $ord(v) > p^2 > p$. Hence $\phi_L(C)$ is not a linear code over$\mathbb{F}_p$. □

Definition 5.2 (Free Code). *A code C over $\mathbb{Z}_{p^s}$ is said to be a free code if $rank(C) = free\ rank(C)$.*

Theorem 5.3. *Let C be a linear code over $\mathbb{Z}_{p^s}$. If $p > 2$ then the Gray image of a free code is not linear.*

Proof. If C is a free code, then it has a generating matrix of the form

$$G = \begin{bmatrix} I_{\delta_0} & A \end{bmatrix},$$

where A is an $\delta_0 \times (n - \delta_0)$ matrix over $\mathbb{Z}_{p^s}$. Let v_i be the i^{th} row of G. Since every row of G is a codeword, if $\phi_L(C)$ is linear then $-\phi_L(v_1)$ must be included in $\phi_L(C)$. But

$$-\phi_L(v_1) = (-\phi_L(1), -\phi_L(v_{1,2}), \cdots, -\phi_L(v_{1,n})) \notin \phi_L(C),$$

because $-\phi_L(1) \neq -\phi_L(x)$ for any $x \in \mathbb{Z}_{p^s}$. □

The image of a self-dual code C over $\mathbb{Z}_{p^s}$ under the Gray map only has the cardinality of a self-dual code if $p = 2$ and $s = 2$, since a self-dual code should include exactly half of the ambient space, which means $\frac{sn}{2} = \frac{p^{s-1}n}{2}$. This implies $s = p^{s-1}$ and hence $p = s = 2$. So for $p > 2$ we know that none of the self-dual codes has self-dual Gray image. However a code might have a self-dual Gray image if it is not self-dual.

Example 5.4. *Let C be the linear code over $\mathbb{Z}_{27}$ generated by*

$$G = \begin{bmatrix} 3 & 0 & 6 & 9 \\ 0 & 3 & 3 & 0 \end{bmatrix}.$$

Since $\langle(3,0,6,9),(0,3,3,0)\rangle = 18 \neq 0$ on $\mathbb{Z}_{27}$, C is not self-dual code over $\mathbb{Z}_{27}$. However

$$\begin{aligned} \left\langle \phi_L(3,0,6,9), \phi_L(0,3,3,0) \right\rangle &= 0, \\ \left\langle \phi_L(3,0,6,9), \phi_L(0,3,3,0) \right\rangle &= 0, \\ \left\langle \phi_L(0,3,3,0), \phi_L(0,3,3,0) \right\rangle &= 0, \end{aligned}$$

on $\mathbb{Z}_3$.

The following theorem gives specific type of linear codes over $\mathbb{Z}_{p^s}$, whose Gray images are self-orthogonal codes over $\mathbb{Z}_{p^s}$.

Theorem 5.5. *Any linear code C over $\mathbb{Z}_{p^s}$ of type $\left(p^{s-1}\right)^{\delta_1}\left(p^{s-2}\right)^{\delta_2}\cdots\left(p^2\right)^{\delta_{s-2}}(p)^{\delta_{s-1}}$ has a Gray image that is a self-orthogonal code.*

Proof. If C is of type $\left(p^{s-1}\right)^{\delta_1}\left(p^{s-2}\right)^{\delta_2}\cdots\left(p^2\right)^{\delta_{s-2}}(p)^{\delta_{s-1}}$, then it has a generating matrix of the form

$$G = \begin{bmatrix} pI_{\delta_1} & pA_{1,2} & pA_{1,3} & \cdots & \cdots & pA_{1,s} \\ 0 & p^2I_{\delta_2} & p^2A_{2,3} & \cdots & \cdots & p^2A_{2,s} \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & p^{s-2}I_{\delta_{s-2}} & p^{s-2}A_{s-2,s-1} & p^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & 0 & p^{s-1}I_{\delta_{s-1}} & p^{s-1}A_{s-1,s} \end{bmatrix}.$$

Let $v = (v_1,\ldots,v_n), w = (w_1,\ldots,w_n) \in C$ are rows of G with order p^{s-i_1} and p^{s-i_2}, where $i_1 \geq i_2 \geq 1$. So each v_k is in $\left\{0, p^{i_1}, 2p^{i_1}, \ldots, p^s - p^{i_1}\right\}$ and each w_k is in $\left\{0, p^{i_2}, 2p^{i_2}, \ldots, p^s - p^{i_2}\right\}$, where $1 \leq k \leq n$. For any element m in $\mathbb{Z}_{p^s}$ of order p^{s-e} we have

$$\phi_L(m) = \overline{(q+1)}_{p^e t}\overline{(q)}_{(p^{s-1-e}-t)p^e},$$

where $m = p^{s-1}q + r$, $0 \leq r = p^e t < p^{s-1}$, $0 \leq q \leq p-1$. We will consider $\left\langle \phi_L(v_k), \phi_L(w_k) \right\rangle$ instead of $\left\langle \phi_L(v), \phi_L(w) \right\rangle$, since $\phi_L(v) = (\phi_L(v_1),\ldots,\phi_L(v_n))$, $\phi_L(w) = (\phi_L(w_1),\ldots,\phi_L(w_n))$, and therefore $\left\langle \phi_L(v), \phi_L(w) \right\rangle = \sum\limits_{i=1}^{n} \left\langle \phi_L(v_i), \phi_L(w_i) \right\rangle$. In both Gray images the number of successively repeated coordinates are divisible by a power of p (at least by p). So in coordinatewise product $\phi_L(v_k)\cdot\phi_L(w_k) = (v_{k,1}w_{k,1},\ldots,v_{k,p^{s-1}}w_{k,p^{s-1}})$ the coordinates will be repeated at least p times successively. So $\phi_L(v_k)\cdot\phi_L(w_k) = (\overline{(a_1)}_p, \overline{(a_2)}_p, \ldots, \overline{(a_{p^{s-2}})}_p)$, where a_l is the l^{th} repeating coordinate. Hence

$$\left\langle \phi_L(v_k), \phi_L(w_k) \right\rangle = \sum_{i=1}^{p^{s-1}} \left(\phi_L(v_k)\cdot\phi_L(w_k)\right)_i = \sum_{j=1}^{p^{s-2}} pa_j = 0,$$

which means $\phi_L(C) \subseteq \left(\phi_L(C)\right)^{\perp}$. □

Acknowledgement: The authors would like to thank the anonymous referees for their valuable comments and suggestions.

References

[1] J. Borges, C. Fernández, J. Rifà, Every $\mathbb{Z}_{2k}$-code is a binary propelinear code, Electronic Notes in Discrete Mathematics 10 (2001) 100–102.

[2] J. Borges, C. Fernández, J. Rifà, Propelinear structure of $\mathbb{Z}_{2k}$-linear codes, Technical Report arxiv:0907.5287 (2009).

[3] J. Borges, K. T. Phelps, J. Rifà, The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non- $\mathbb{Z}_4$-linear codes, IEEE Trans. Inform. Theory 49(8) (2003) 2028–2034.

[4] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, IEEE Trans Inform Theory, 44 (1998) 1543–1547.

[5] I. Constantinescu, W. Heise , A metric for codes over residue class rings of integers, Problemy Peredachi Informatsii 33 (1997) 22–28.

[6] S. T. Dougherty, C. Fernández-Córdoba, Codes over $\mathbb{Z}_{2^k}$ gray map and self-dual codes, Adv. Math. Comm 5 (2011) 571–588.

[7] S. T. Dougherty, H. Liu, Independence of vectors in codes over rings, Design Codes and Cryptography 51 (2009) 55–68.

[8] S. T. Dougherty, K. Siromoto, MDR codes over $\mathbb{Z}_m$, IEEE Trans Inform Theory 46(1) (2000) 265–269.

[9] S. T. Dougherty, J-L. Kim, H. Kulosman, MDS codes over finite principal ideal rings, Designs Codes and Cryptography 50 (2009) 77–92.

[10] C. Fernández-Córdoba, J. Pujol, M. Villanueva, On rank and kernel of $\mathbb{Z}_4$-linear codes, Lecture Notes in Computer Science 5228 (2008) 46–55.

[11] C. Fernández-Córdoba, J. Pujol, M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel, Design Codes and Cryptography 56(1) (2009) 43–59.

[12] A. R. Hammons, V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans Inform Theory 40 (1994) 301–319.

[13] K. M. Hoffman, R. Kunze, Linear Algebra, (2nd Edition), Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1971.

[14] W. C. Huffman, Decompositions and extremal Type II codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 44 (1998) 800–809.

[15] Y. H. Park, Modular independence and generator matrices for codes over $\mathbb{Z}_m$, Design Codes and Cryptography 50(2) (2009) 147–162.

[16] K. T. Phelps, J. Rifà and M. Villanueva, Kernels and p-kernels of p^r-ary 1-perfect codes, Design Codes and Cryptography 37(2) (2005) 243–261.

[17] K. T. Phelps, J. Rifà, M. Villanueva, On the additive $\mathbb{Z}_4$-linear and non- $\mathbb{Z}_4$-linear Hadamard codes: Rank and kernel, IEEE Trans. Inform. Theory 55(1) (2005) 316–319.

[18] K. Shiromoto, A basic exact sequence for the Lee and Euclidean weights of linear codes over $\mathbb{Z}_l$, Linear Algebra and its Applications 295 (1999) 191–200.

[19] K. Shiromoto, Singleton bounds for codes over finite rings, Journal of Algebraic Combinatorics 12 (2000) 95–99.

[20] J. F. Voloch, J. L. Walker, Homogeneous weights and exponential sums, Finite Fields Appl 9 (2003) 310–321.

[21] B. Yıldız, A Combinatorial construction of the Gray map over Galois rings, Discrete Mathematics 309(10) (2009) 3408–3412.

[22] B. Yıldız, Z. Ödemiş Özger, Generalization of the Lee weight to $\mathbb{Z}_{p^k}$, TWMS J. App.&Eng. Math. 2(2) (2012) 145–153.

[23] B. Yıldız, Z. Ödemiş Özger, Linear codes over $\mathbb{Z}_{2^s}$ with the extended Lee weight, AIP Conf. Proc 1389 (2011) 621–624. DOI:10.1063/1.3636807.