ON CODES OVER $\mathbb{Z}_{p^s}$ WITH THE EXTENDED LEE WEIGHT

PhD Student Zeynep ÖDEMİŞ ÖZGER

Joint work with: Bahattin YILDIZ and Steven DOUGHERTY

July 2013

A brief history of the codes over rings

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.([4]) solved a long standing problem in non-linear 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.

A brief history of the codes over rings

For codes over rings, weights other than the Hamming weight were considered. For example, in [4], the authors used the Lee weight on $\mathbb{Z}_4$, which we will denote by w_L and was defined as

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

A brief history of the codes over rings

The Gray map

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

with

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

turns out to be a non-linear isometry from $(\mathbb{Z}_4^n, \text{Lee distance})$ to $(\mathbb{F}_2^{2n}, \text{Hamming distance})$. 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 non-linear binary code with parameters $[n, M, d]$.

Extending Lee distance to more general rings

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 [2] 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.

Extending Lee distance to more general rings

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 [3]. 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.

Summary and Outline

In this work, we generalize the Lee weight on $\mathbb{Z}_{2^s}$ given above 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 $\mathbb{F}_p = \mathbb{Z}_p$. 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:

1. In Section 2, we recall the extended Lee weight, the Gray map and some properties for codes over $\mathbb{Z}_{p^s}$ from [4].
2. 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.
3. In Section 4 the notions of kernel and independence are investigated.
4. In Section 5 some results about self-duality and self-orthogonality are found.

A New Extension to $\mathbb{Z}_{p^s}$

We recall that a new weight on $\mathbb{Z}_{p^s}$, a generalization of w_L, was defined in [4] as follows:

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

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].

The Gray map

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:

$$\begin{array}{lcl}
0 & \longrightarrow & (000\cdots000),\\
1 & \longrightarrow & (100\cdots000),\\
2 & \longrightarrow & (110\cdots000),\\
 & \vdots & \\
p^{s-1} & \longrightarrow & (111\cdots111),\\
p^{s-1}+1 & \longrightarrow & (211\cdots111),\\
p^{s-1}+2 & \longrightarrow & (221\cdots111),\\
 & \vdots & \\
p^{s-1}+p^{s-1}-1 & \longrightarrow & (222\cdots221),\\
2p^{s-1} & \longrightarrow & (222\cdots222),
\end{array}$$

The Gray map

$$
\begin{array}{lcl}
2p^{s-1}+1 & \rightarrow & (322\cdots 222), \\
 & \vdots & \\
2p^{s-1}+p^{s-1}-1 & \rightarrow & (333\cdots 332), \\
3p^{s-1} & \rightarrow & (333\cdots 333), \\
 & \vdots & \\
(p-1)p^{s-1} & \rightarrow & ((p-1)\cdots(p-1)), \\
(p-1)p^{s-1}+1 & \rightarrow & (0(p-1)\cdots(p-1)), \\
 & \vdots & \\
p^s-2 & \rightarrow & (000\cdots 0(p-1)(p-1)), \\
p^s-1 & \rightarrow & (000\cdots 00(p-1)).
\end{array}
$$

We simply put a 1 in the first x coordinates and a 0 in the other coordinates for all $x \leq p^{s-1}$. If $x > p^{s-1}$ then the Gray map takes x to $\bar{q} + \phi_L(r)$, where ϕ_L is the Gray map for w_L, $\bar{q} = (qqq\cdots qqq)$ and q and r are such that $x = qp^{s-1} + r$, which can be found by division algorithm. Here, $0 \leq x \leq p^s - 1$, $0 \leq q \leq p-1$, $0 \leq r \leq p^{s-1} - 1$.

The Gray map

Here by putting $p = 2$, we get the same Gray map given in [3] and [6], which is

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

The Gray map

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

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

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

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

The Lee distance

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

$$d_L(x,y) := w_L(x-y), :::::: x,y \in \mathbb{Z}_{p^s}. \tag{2.1}$$

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

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 [4] with the following corollary:

Corollary

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 non-linear) code over $\mathbb{F}_p$ of length np^{s-1}, size M and minimum Hamming distance d.

A Gray map from $GR(p^s,m)$ to $\mathbb{F}_p^{p^{s-1}m}$ can also be defined by extending this map (see [4], Section 3), which means that most of the work done in this paper is applicable to Galois rings.

A Singleton bound for codes over a finite quasi-Frobenius ring is already given in [1] as an MDS bound. Since this result is given for any weight function, it can be specified for the extended Lee weight.

Definition (Complete weight)

[1] 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

$$n_r(x) := |\{i \,|x_i = r\}| . \tag{3.1}$$

Definition (General weight function)

[1] Let $a_r, (0 \neq) r \in R$, be positive real numbers, and set $a_0 = 0$. Then

$$w(x) := \sum_{r \in R} a_r n_r(x) \tag{3.2}$$

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

[1] Let C be a code of length n over a finite commutative QF ring R. Let $w(x)$ be a general weight function on C, as in (3.2), and with maximum a_r-value A. Suppose the minimum weight of $w(x)$ on C is d. Then

$$\left\lfloor \frac{d-1}{A} \right\rfloor \leq n - \log_{|R|} |C| , \tag{3.3}$$

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.

MLDS codes

Applying these informations to Theorem we get the following:

Theorem

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

$$\left\lfloor \frac{d-1}{p^{s-1}} \right\rfloor \leq n - \log_{p^s} |C| . \tag{3.4}$$

Codes meeting this bound are called MLDS (Maximum Lee Distance Separable) codes. In [8], 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.

Rank, free-rank

Definition (Rank, Free-rank)

Let C be any finitely generated submodule of $\mathbb{Z}_{p^s}^n$, that is isomorphic to

$$\mathbb{Z}_{p^s}/p^{a_1}\mathbb{Z}_{p^s} \oplus \mathbb{Z}_{p^s}/p^{a_2}\mathbb{Z}_{p^s} \oplus \cdots \oplus \mathbb{Z}_{p^s}/p^{a_{n-1}}\mathbb{Z}_{p^s}, \tag{3.5}$$

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

$$rank(C) := |\{i\,|a_i \neq 0\}|, \tag{3.6}$$

is called the rank of C and

$$free\ rank(C) := |\{i\,|a_i = s\}| \tag{3.7}$$

is called the free rank of C.

Generating matrix

Any code over $\mathbb{Z}_{p^s}$ has a generator matrix of the form:

$$G = \begin{bmatrix} I_{\delta_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,s} \\ 0 & pI_{\delta_1} & pA_{1,2} & pA_{1,3} & \cdots & \cdots & pA_{1,s} \\ 0 & 0 & p^2 I_{\delta_2} & p^2 A_{2,3} & \cdots & \cdots & p^2 A_{2,s} \\ \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & p^{s-2} I_{\delta_{s-2}} & p^{s-2} A_{s-2,s-1} & p^{s-2} A_{s-2,s} \\ 0 & 0 & 0 & \cdots & 0 & p^{s-1} I_{\delta_{s-1}} & p^{s-1} A_{s-1,s} \end{bmatrix}. \quad (3.8)$$

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 [8], [6], [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:

$$rank(C) + free\ rank(C^\perp) = n \tag{3.9}$$

Support and duality functor

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

$$\begin{aligned} D(M) &:= \{x \in D \,|\, \mathrm{supp}(x) \subseteq M\}, \\ D^* &:= Hom_{\mathbb{Z}_{p^s}}(D, \mathbb{Z}_{p^s}), \end{aligned} \tag{3.10}$$

where

$$\mathrm{supp}(x) := \{i \in N \,|\, x_i \neq 0\}. \tag{3.11}$$

From the fundamental theorem of finitely generated abelian groups, we have $D^* \cong D$.

Shiromoto's work

Shiromoto also gave the following basic exact sequence:

Lemma

[8]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

$$0 \to C^{\perp}(m) \xrightarrow{inc} V(M) \xrightarrow{f} C^* \xrightarrow{res} C(N-M)^* \to 0, \tag{3.12a}$$

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

$$\begin{aligned} f: \quad & V \to D^* \\ & y \to (\hat{y} : x \to \langle x, y \rangle . \end{aligned} \tag{3.13}$$

Adjusting Shiromoto's work

We can adjust Lemma 8 to our case:

Lemma

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

$$0 \to C^{\perp}(m) \xrightarrow{inc} V(M) \xrightarrow{f} C^{*} \xrightarrow{res} C(N-M)^{*} \to 0, \tag{3.14a}$$

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

$$\begin{aligned} f: \quad & V \to D^{*} \\ & y \to (\hat{y} : x \to \langle x, y \rangle). \end{aligned} \tag{3.15}$$

Lemma

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

$$w_L(x) \leq p^{s-1} |M| . \tag{3.16}$$

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

Lemma

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.

MLDR codes

By Lemma 10, we have the following bound:

Theorem

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

$$\left\lfloor \frac{d-1}{p^{s-1}} \right\rfloor \leq n - rank(C). \tag{3.17}$$

Codes meeting the bound above are called MLDR (Maximum Lee distance with respect to Rank) codes.

Kernel

The kernel of a code C, denoted by $K(C)$, is defined as the set

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

Since $\phi_L(C)$ is a code (not necessarily linear), we can define

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

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, v_t are modular independent over $\mathbb{Z}_{p^s}$ if $\sum \alpha_i v_i = \mathbf{0}$ then $\alpha_i \in \langle p \rangle$ for all i.

Lemma

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 $v_{i,1}, v_{i,2}, \cdots, v_{i,\delta_i}$ be the vectors of order p^{s-i}. Then the vectors in the set $\{\alpha v_{i,j} | 1 \le \alpha \le p^{s-i-1}\}$ are ϕ_L-independent in $\mathbb{F}_p^{p^{s-1}n}$.

Theorem

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

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

Proposition

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 $\phi_L(v)$.
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 $K(\phi_L(C))$.

An upper bound for $K(\phi_L(C))$

Then we have the following corollary and lemmas, which generalize the results in [6]:

Corollary

Let C be a linear code over $\mathbb{Z}_{p^s}$ with generator matrix of the form (3.8). Then $K(\phi_L(C))$ is contained in the Gray image of the code generated by the matrix:

$$\begin{bmatrix} p^{s-2}I_{\delta_0} & p^{s-2}A_{0,1} & p^{s-2}A_{0,2} & p^{s-2}A_{0,3} & \cdots & \cdots & p^{s-2}A_{0,s} \\ 0 & p^{s-2}I_{\delta_1} & p^{s-2}A_{1,2} & p^{s-2}A_{1,3} & \cdots & \cdots & p^{s-2}A_{1,s} \\ 0 & 0 & p^{s-2}I_{\delta_2} & p^{s-2}A_{2,3} & \cdots & \cdots & p^{s-2}A_{2,s} \\ \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & p^{s-2}I_{\delta_{s-2}} & p^{s-2}A_{s-2,s-1} & p^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & \cdots & 0 & p^{s-1}I_{\delta_{s-1}} & p^{s-1}A_{s-1,s} \end{bmatrix}. \tag{4.1}$$

A lower bound for $K(\phi_L(C))$

Lemma

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 $v, w \in C$.

Theorem

Let C be a linear code over $\mathbb{Z}_{p^s}$ with the generator matrix of the form (3.8). Then the Gray image of the code C' generated by

$$\begin{bmatrix}
p^{s-1}I_{\delta_0} & p^{s-1}A_{0,1} & p^{s-1}A_{0,2} & p^{s-1}A_{0,3} & \cdots & \cdots & p^{s-1}A_{0,s} \\
0 & p^{s-1}I_{\delta_1} & p^{s-1}A_{1,2} & p^{s-1}A_{1,3} & \cdots & \cdots & p^{s-1}A_{1,s} \\
0 & 0 & p^{s-1}I_{\delta_2} & p^{s-1}A_{2,3} & \cdots & \cdots & p^{s-1}A_{2,s} \\
\cdots & \cdots & 0 & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & p^{s-1}I_{\delta_{s-2}} & p^{s-1}A_{s-2,s-1} & p^{s-1}A_{s-2,s} \\
0 & 0 & 0 & \cdots & 0 & p^{s-1}I_{\delta_{s-1}} & p^{s-1}A_{s-1,s}
\end{bmatrix} \tag{4.2}$$

Bound for $K(\phi_L(C))$

Lemma

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 $ord(\lambda v) = p$.

Theorem

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

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

The aim of this section is to present some knowledge about these two topics for codes over $\mathbb{Z}_{p^s}$.

Theorem

Let C be a linear code with the generating matrix of the form given in (3.8). If $\delta_i > 0$ for $0 \leq i \leq s-3$ then $\phi_L(C)$ is not linear.

Theorem

Let C be a linear code. If $p > 2$ then the image of a free code is not linear.

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 image. However a code might have a self-dual image if it is not self-dual.
First we need to seek for self-orthogonal images.

Theorem

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

Future work

1. We will try to prove that there is no MacWilliams Identity for these codes.
2. We will find a similar bound for dimension of $\phi_L(C)$'s rank which is defined as $\dim \langle \phi_L(C) \rangle$.
3. We will find out whether there is a relationship between the columns of the parity check matrix of a code and its minimum distance.
4. We will try to find a decoding algorithm and to do this we will examine cosets and coset leaders of $\phi_L(C)$.

References


J. Borges,C. Fernández and J. Rifà, Every $\mathbb{Z}_{2k}$-code is a binary propelinear code, *Electronic Notes in Discrete Mathematics*, 10, Elsevier Science, 2001.


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


J. Borges, K.T. Phelps and 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), pp. 2028-2034, 2003.


C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, *IEEE Trans Inform Theory,* vol. 44, pp. 1543-1547, 1998.


I. Constantinescu and W. Heise , A metric for codes over residue class rings of integers, *Problemy Peredachi Informatsii,* vol. 33, pp. 22-28, 1997.


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


S.T. Dougherty and H. Liu, Independence of vectors in codes over rings, *Design Codes and Cryptography*, pp 55-68, 2009.


S.T. Dougherty and K. Siromoto, MDR codes over $\mathbb{Z}_m$, *IEEE Trans Inform Theory,* vol 46(1), pp 265-269, 2000.

References


S.T. Dougherty, J-L. Kim and H. Kulosman, MDS codes over finite principal ideal rings, to appear in *Designs, Codes and Cryptography.*


C. Fernández-Córdoba,J. Pujol and M. Villanueva, On rank and kernel of $\mathbb{Z}_4$-linear codes, *Lecture Notes in Computer Science*, n. 5228, pp. 46-55, 2008.


C. Fernández-Córdoba, J. Pujol and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel, *Design Codes and Cryptography*, DOI: 10.1007/s10623-009-9340-9, 2009.


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


W.C. Huffman, Decompositions and extremal Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, 44, 800-809, 1998.


Y.H. Park, Modular independence and generator matrices for codes over $\mathbb{Z}_m$, *Design Codes and Cryptography*, vol 50(2), pp 147-162, 2009.


K.T. Phelps, J. Rifà and 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), pp. 316-319, 2005.


K. Shiromoto, A basic exact sequence for the Lee and Euclidean weights of linear

References


K. Shiromoto, Singleton bounds for codes over finite rings, *Journal of Algebraic Combinatorics*, vol 12, pp 95-99, 2000.


J.F. Voloch and J.L. Walker, Homogeneous weights and exponential sums, *Finite Fields Appl,* vol. 9, pp. 310-321, 2003.


B. Yıldız and Z. Ödemiş Özger, Linear codes over $\mathbb{Z}_{2^s}$ with the extended Lee weight, *AIP Conf. Proc,* vol. 1389, pp. 621-624, 2011. DOI:10.1063/1.3636807.


B. Yıldız and Z. Ödemiş Özger, Generalization of the Lee weight to $\mathbb{Z}_{p^k}$, *TWMS J. App.&Eng. Math.*, vol. 2 no:2, pp. 145-153, 2012.


B. Yıldız, A Combinatorial construction of the Gray map over Galois rings, *Discrete Mathematics*, 309(10), 3408-3412, 2009.