

On Linear Codes over \mathbb{Z}_{2^s}

Manish K. Gupta*, Mahesh C. Bhandari[†] and
Arbind K. Lal[‡]

October 20, 2002

Abstract

In an earlier paper the authors studied simplex codes of type α and β over \mathbb{Z}_4 and obtained some known binary linear and nonlinear codes as Gray images of these codes. In this correspondence, we study weight distributions of simplex codes of type α and β over \mathbb{Z}_{2^s} . The generalized Gray map is then used to construct binary codes. The linear codes meet the Griesmer bound and a few non-linear codes are obtained that meet the Plotkin / Johnson bound. We also give the weight hierarchies of the first order Reed-Muller codes over \mathbb{Z}_{2^s} . The above codes are also shown to satisfy the chain condition.

Keywords: Linear codes over rings, Generalized Gray map, Simplex code, Reed-Muller code, p -dimension, Generalized Hamming weights (GHWs), Lee weight, Gray image, Weight distributions.

1 Introduction

Codes over \mathbb{Z}_{p^s} have been studied in the early seventies by Blake [4, 5], Spiegel [28] and Priti Shankar [26] etc. But not much attention was paid to such codes in the early eighties [33]. The reason for this seems partly to come from the difficulties arising from the presence of zero divisors in \mathbb{Z}_{p^s} . At the end of eighties Nechaev [21] and later Hammons, Kumar, Calderbank, Sloane and Solé [12] have observed that certain non-linear binary codes with good parameters are

*M. K. Gupta is with the Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287 USA. E-mail:m.k.gupta@ieee.org. A part of this paper is contained in his Ph.D. Thesis from IIT Kanpur, INDIA.

[†]M.C. Bhandari and A.K. Lal are with the Department of Mathematics, Indian Institute of Technology, Kanpur, INDIA. E-mails: {mcb,arlal}@iitk.ac.in.

linear over \mathbb{Z}_4 . In particular, they have shown that the Kerdock and Preparata-like codes (slightly different from the original Preparata codes but sharing the same distance structure) are images of some linear codes over \mathbb{Z}_4 that are dual to each other [12]. To show this they have exploited the isometry between $(\mathbb{Z}_4^n, \text{Lee distance})$ and $(\mathbb{Z}_2^{2n}, \text{Hamming distance})$. This has motivated a great deal of research in codes over rings (see [6, 14, 15, 27, 32]). Recently in [3], the authors have investigated simplex codes of type α and β over \mathbb{Z}_4 and determined some fundamental properties. Some known binary linear codes (meeting the Griesmer bound) and nonlinear codes were obtained as Gray image of these codes. For applications, see [2, 10, 18, 20, 23, 29].

A natural question that comes to one's mind is the extension of these results to codes over \mathbb{Z}_{p^s} . A Major hurdle is the generalization of the ‘‘Gray map.’’ In [24], Ana *Sălăgean*-Mandache has shown that except for the well-known case $p = s = 2$, it is not possible to construct a weight function on \mathbb{Z}_{p^s} for which \mathbb{Z}_{p^s} is isometric to \mathbb{Z}_p^s with the Hamming metric. However there exists an isometry between $\mathbb{Z}_{2^s} \rightarrow \mathbb{Z}_2^{2^{s-1}}$ appeared in [7]. The generalization of these isometries up to finite chain rings was considered in [11, 14, 22]. More recently an isometry between codes over \mathbb{Z}_{2^s} and codes over \mathbb{Z}_4 has been introduced in [31].

In this correspondence, we study basic properties of simplex codes of type α and β and first order Reed-Muller codes over \mathbb{Z}_{2^s} . The binary linear codes obtained using the binary image meet the Griesmer bound and hence are optimal, and some binary nonlinear uniformly packed codes are obtained. It is observed that type β simplex codes meet the Griesmer bound for codes over rings [27]. Section 2 contains preliminaries and some useful results. Definitions and basic properties of simplex codes of type α and β are given in section 3. Section 4 contains definitions and properties of the first order Reed-Muller codes over \mathbb{Z}_{2^s} .

2 Preliminaries

Calderbank and Sloane [6] have shown that the generator matrix G of any linear code \mathcal{C} of length n over \mathbb{Z}_{p^s} is

$$G = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & \cdots & A_{0s-1} & A_{0s} \\ \mathbf{0} & pI_{k_1} & pA_{12} & \cdots & pA_{1s-1} & pA_{1s} \\ \mathbf{0} & \mathbf{0} & p^2I_{k_2} & \cdots & p^2A_{2s-1} & p^2A_{2s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & p^{s-1}I_{k_{s-1}} & p^{s-1}A_{s-1s} \end{bmatrix}, \quad (1)$$

where A_{ij} are matrices over \mathbb{Z}_{p^s} and the columns are grouped into blocks of sizes $k_0, k_1, \dots, k_{s-1}, k_s$, respectively. Let $k = \sum_{i=0}^{s-1} (s-i)k_i$. Then $|\mathcal{C}| = p^k$.

For $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$, $d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$ is called the *Hamming distance* between \mathbf{x} and \mathbf{y} and $w_H(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0})$, the *Hamming weight* of \mathbf{x} . The *minimum Hamming distance* of \mathcal{C} is denoted by d_H . The Lee weight [17] of $a \in \mathbb{Z}_q$ is given by $w_L(a) = \min\{a, q - a\}$. For $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{Z}_q^n$, $w_L(\mathbf{x}) = \sum_{i=1}^n w_L(x_i)$ and for $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$, the *Lee distance* between \mathbf{x} and \mathbf{y} , denoted, $d_L(\mathbf{x}, \mathbf{y}) = w_L(\mathbf{x} - \mathbf{y})$. The minimum Lee distance d_L of a code \mathcal{C} is defined analogously.

2.1 p -dimension of Linear Codes over \mathbb{Z}_{p^s}

Let \mathcal{C} be a linear code over \mathbb{Z}_{p^s} . Consider the radical series $\mathcal{C} \supset p\mathcal{C} \supset p^2\mathcal{C} \supset \dots \supset p^{s-1}\mathcal{C} \supset p^s\mathcal{C} = \{0\}$ of \mathcal{C} . In this series, each associated quotient $p^l\mathcal{C}/p^{l+1}\mathcal{C}$, $0 \leq l \leq s-1$, is a vector space over the field \mathbb{Z}_p with basis $v_{l1} + p^{l+1}\mathcal{C}, v_{l2} + p^{l+1}\mathcal{C}, \dots, v_{lt_l} + p^{l+1}\mathcal{C}$, say. Then the ordered collection $\mathcal{B} = \{v_{01}, \dots, v_{0t_0}, v_{11}, \dots, v_{1t_1}, \dots, v_{s-1,1}, \dots, v_{s-1,t_{s-1}}\} \subset \mathcal{C}$ satisfies:

1. Given $\mathbf{v} \in \mathcal{C}$, there exists unique $\lambda_i \in \mathbb{Z}_p$ such that $\mathbf{v} = \sum_{\mathbf{v}_i \in \mathcal{B}} \lambda_i \mathbf{v}_i$.
2. For any ℓ , $0 \leq \ell \leq s-1$ and any $j, 1 \leq j \leq t_\ell$, $p v_{\ell j} \in p^{\ell+1}\mathcal{C}$.
3. Any p -linear combination of vectors in \mathcal{B} is zero (i.e., $\sum_i \lambda_i \mathbf{v}_i = 0$ for $\lambda_i \in \mathbb{Z}_p$ and $\mathbf{v}_i \in \mathcal{B}$ if and only if each $\lambda_i = 0$).

Any ordered set $D \subset \mathcal{C}$ with the above three properties is called a p -basis for the code \mathcal{C} and the cardinality of the set D is called the p -dimension of \mathcal{C} , denoted $p\text{-dim}(\mathcal{C})$. Recently Vazirani, Saran and Sundar Rajan have used the concept of p -dimension extensively in [30]. Observe that $p\text{-dim}(\mathbb{Z}_{p^s}^n) = sn$. For a subset \mathcal{B} of \mathcal{C} to be a p -basis for \mathcal{C} it is necessary and sufficient that every vector in \mathcal{C} be a unique p -linear combination of vectors in \mathcal{B} . In this correspondence, $\langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle$ will denote the p -linear combination of the vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$. Let

$$\mathcal{D} = \left[\begin{array}{cccccc}
 I_{k_0} & A_{01} & A_{02} & \cdots & A_{0s-1} & A_{0s} \\
 pI_{k_0} & pA_{01} & pA_{02} & \cdots & pA_{0s-1} & pA_{0s} \\
 \mathbf{0} & pI_{k_1} & pA_{12} & \cdots & pA_{1s-1} & pA_{1s} \\
 \vdots & \vdots & \vdots & & \vdots & \vdots \\
 \vdots & \vdots & \vdots & & \vdots & \vdots \\
 p^{s-1}I_{k_0} & p^{s-1}A_{01} & p^{s-1}A_{02} & \cdots & p^{s-1}A_{0s-1} & p^{s-1}A_{0s} \\
 \mathbf{0} & p^{s-1}I_{k_1} & p^{s-1}A_{12} & \cdots & p^{s-1}A_{1s-1} & p^{s-1}A_{1s} \\
 \mathbf{0} & \mathbf{0} & p^{s-1}I_{k_2} & \cdots & p^{s-1}A_{2s-1} & p^{s-1}A_{2s} \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & p^{s-1}I_{k_{s-1}} & p^{s-1}A_{s-1s}
 \end{array} \right]. \quad (2)$$

Then the rows of \mathcal{D} form a p -basis for the code \mathcal{C} having G given in (1) as the generator matrix. Thus, $p\text{-dim}(\mathcal{C}) = k = \sum_{i=0}^{s-1} (s-i)k_i$. The matrix \mathcal{B} given below is needed in the proof of Lemma 1 and is row-equivalent to the matrix \mathcal{D} (using block permutations applied to its rows):

$$\mathcal{B} = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & \cdots & A_{0s-1} & A_{0s} \\ pI_{k_0} & pA_{01} & pA_{02} & \cdots & pA_{0s-1} & pA_{0s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ p^{s-1}I_{k_0} & p^{s-1}A_{01} & p^{s-1}A_{02} & \cdots & p^{s-1}A_{0s-1} & p^{s-1}A_{0s} \\ \hline \mathbf{0} & pI_{k_1} & pA_{12} & \cdots & pA_{1s-1} & pA_{1s} \\ \mathbf{0} & p^2I_{k_1} & p^2A_{12} & \cdots & p^2A_{1s-1} & p^2A_{1s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & p^{s-1}I_{k_1} & p^{s-1}A_{12} & \cdots & p^{s-1}A_{1s-1} & p^{s-1}A_{1s} \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & p^{s-1}I_{k_{s-1}} & p^{s-1}A_{s-1s} \end{bmatrix}. \quad (3)$$

2.2 Generalized Gray Map

Let \mathbb{F}_q be a field with q elements and let \mathbf{u} and $\mathbf{1}$ be the vectors of length q such that \mathbf{u} lists all the elements of \mathbb{F}_q and $\mathbf{1}$ is the vector of all 1's. For a fixed positive integer s , $0 \leq i \leq s-1$, define

$$c_i := (\mathbf{1} + \delta_{i,0}(\mathbf{u} - \mathbf{1})) \otimes \cdots \otimes (\mathbf{1} + \delta_{i,s-2}(\mathbf{u} - \mathbf{1}))$$

where $\delta_{i,j}$ is the Kronecker delta symbol and \otimes represents the tensor product (expanded from right to left). Observe that the entries of c_i 's are elements of \mathbb{F}_q . Let $C = \{c_0, c_1, \dots, c_{s-1}\}$. It has been observed (see [11]) that C spans a first-order Reed-Muller code $RM(1, s-1)$ over \mathbb{F}_q . Thus all the codewords of the code spanned by C , except c_{s-1} and its multiples are permutationally equivalent and have Hamming weight $(q-1)q^{s-2}$. Using C , Greferath and Schmidt [11] have extended the well-known Gray map over \mathbb{Z}_4 to a finite chain ring R of length s . For a prime p , let \mathbb{F}_p be the residue field of R , $\nu : R \rightarrow \mathbb{F}_p$ the natural surjection, and let T be a set of representative of \mathbb{F}_p in R . Then for any $r \in R$, there exist unique $r_i \in T$, $0 \leq i \leq s-1$ such that $r = r_0 + r_1p + \cdots + r_{s-1}p^{s-1}$. With the above notations, the *generalized Gray map* is the bijection

$$\gamma : R \rightarrow C, \quad r \mapsto \nu(r_0)c_0 + \nu(r_1)c_1 + \cdots + \nu(r_{s-1})c_{s-1}.$$

In particular, for $R = \mathbb{Z}_{2^s}$ the extended Gray map coincides with that of Carlet's Generalized Gray map (see [7]). In this case, the residue field consists of $\mathbb{F}_2 = \{0, 1\}$ and hence for $0 \leq i \leq s-1$, the entries of c_i 's are either 0 or 1, and $\gamma(1) = c_0, \gamma(2) = c_1, \dots, \gamma(2^{s-1}) = c_{s-1}$. Thus, for $u \in \mathbb{Z}_{2^s}$, $u \neq 0$, one has

$$wt(\gamma(u)) = \begin{cases} 2^{s-2}, & u \neq 2^{s-1} \\ 2^{s-1}, & u = 2^{s-1}. \end{cases} \quad (4)$$

This weight is (up to a constant factor) the same as the homogeneous weight introduced by Constantinescu, Heise and Honold [9] (see also [16]). Thus this weight will be called *homogeneous weight* of u and we denote it by $w_{HW}(u)$. From now on we will restrict γ to the case $R = \mathbb{Z}_{2^s}$. Also, the Gray isometry from $\mathbb{Z}_{2^s}^n$ to $\mathbb{Z}_2^{2^{s-1}n}$ is the coordinate-wise extension of γ from \mathbb{Z}_{2^s} to $\mathbb{Z}_2^{2^{s-1}}$ and with an abuse of notation we call it γ .

Definition 1 *A binary code is called \mathbb{Z}_{2^s} -linear if it is permutation equivalent to $\gamma(\mathcal{C})$ for some linear code \mathcal{C} over \mathbb{Z}_{2^s} .*

A necessary and sufficient condition for \mathbb{Z}_8 -linearity is given in [7]. It is also shown that any \mathbb{Z}_{2^s} -linear code is distance invariant and $d_H(\gamma(u), \gamma(v)) = w_{HW}(u - v)$ [7]. The minimum homogeneous weight, d_{HW} , of \mathcal{C} can be defined in the usual sense. Note that for $s = 2$, $d_{HW} = d_L$.

To state the next lemma (to be used in Section 3.1), we need the following notation. For a fixed integer s define $G_{s-j} := (c_j, c_{j+1}, \dots, c_{s-1})^t$ for $0 \leq j \leq s-1$. Note that in this notation, G_s is a generator matrix of the binary first-order Reed-Muller code $RM(1, s-1)$.

Lemma 1 *For $p = 2$, the images of the rows of the matrix \mathcal{B} given by (3) under the generalized Gray map γ are linearly independent over \mathbb{Z}_2 .*

PROOF. Applying the generalized Gray map γ to the rows of \mathcal{B} yields

$$\gamma(\mathcal{B}) = \begin{bmatrix} G_s \otimes I_{k_0} & * & \cdots & * & * \\ & G_{s-1} \otimes I_{k_1} & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ & & \cdots & G_1 \otimes I_{k_{s-1}} & * \end{bmatrix}.$$

Since the G_i 's for $1 \leq i \leq s$ are linearly independent, the result follows. \blacksquare

Remark 1 *Lemma 1 implies 'the image set of a 2-basis of \mathcal{C} under the generalized Gray map gives rise to a linearly independent set over \mathbb{Z}_2 '. The converse of this need not be true in general. For example, If $s = 2$, then $\{(1011), (0111)\}$ is \mathbb{Z}_2 -independent but $\{(3\ 2), (1\ 2)\}$ is not.*

A linear code \mathcal{C} over \mathbb{Z}_{2^s} of length n , 2-dimension k , minimum Hamming distance d_H , minimum Lee distance d_L , and minimum homogeneous distance d_{HW} is called an $[n, k, d_H, d_L, d_{HW}]$ code or simply an $[n, k]$ code. Note that, for an $[n, k]$ linear code \mathcal{C} over \mathbb{Z}_{p^s} , the dual code \mathcal{C}^\perp is an $[n, sn - k]$ linear code. \mathcal{C} is called \mathbb{Z}_2 -linear if $\gamma(\mathcal{C})$ is a binary linear code. Thus, if \mathcal{C} is an $[n, k, d_H, d_L, d_{HW}]$ \mathbb{Z}_2 -linear code then $\gamma(\mathcal{C})$ has parameters $[2^{s-1}n, k, d_{HW}(\mathcal{C})]$.

2.3 GHWs of Linear Codes over \mathbb{Z}_{p^s}

Let \mathcal{C} be an $[n, k]$ linear code over \mathbb{Z}_{p^s} . The definitions of Generalized Hamming weights (GHWs), weight hierarchies and chain condition given in [13] for linear codes over $GF(q)$ can be extended in a similar fashion for linear codes over \mathbb{Z}_{p^s} . The only difference is that we replace the word ‘dimension’ by ‘ p -dimension’ everywhere. Thus for $1 \leq r \leq k$, the r^{th} generalized Hamming weight of \mathcal{C} is defined as $d_r(\mathcal{C}) = \min\{w_S(\mathcal{D}_r) \mid \mathcal{D}_r \text{ is an } [n, r] \text{ subcode of } \mathcal{C}\}$, where $w_S(\mathcal{D}_r)$ is the support size of a subcode \mathcal{D}_r of \mathcal{C} with $p\text{-dim}(\mathcal{D}_r) = r$.

The following theorem summarizes the basic properties of GHW’s.

Theorem 1 [1] *Let \mathcal{C} be an $[n, k]$ linear code over \mathbb{Z}_{p^s} and \mathcal{C}^\perp be the dual code defined with respect to the standard inner product in \mathbb{Z}_{p^s} . Then*

1. (Monotonicity): $1 \leq d_1(\mathcal{C}) \leq d_2(\mathcal{C}) \leq \dots \leq d_k(\mathcal{C}) \leq n$ and if, $d_r(\mathcal{C}) = d_{r+1}(\mathcal{C}) = \dots = d_{r+s-1}(\mathcal{C})$, then $d_{r+s-1}(\mathcal{C}) < d_{r+s}(\mathcal{C})$.
2. (Duality): The weight hierarchies of \mathcal{C} and its dual code \mathcal{C}^\perp are related by $\{d_r(\mathcal{C}) \mid 1 \leq r \leq k\} = \underbrace{\{1, \dots, 1\}}_s, \dots, \underbrace{\{n, \dots, n\}}_s \setminus \{n+1 - d_r(\mathcal{C}^\perp) \mid 1 \leq r \leq sn - k\}$.

The next lemma connects the support size of a code with its Lee and homogeneous weights.

Lemma 2 *If \mathcal{D} is an $[n, r]$ linear code over \mathbb{Z}_{2^s} then*

1. $\sum_{\mathbf{c} \in \mathcal{D}} w_L(\mathbf{c}) = 2^{r+s-2} w_S(\mathcal{D})$ and
2. $\sum_{\mathbf{c} \in \mathcal{D}} w_{HW}(\mathbf{c}) = 2^{r+s-2} w_S(\mathcal{D})$.

PROOF. Consider the $(2^r \times n)$ matrix consisting of all codewords in \mathcal{D} . For $0 \leq m \leq s$, let n_{m-1} be the number of columns that contain the entries $0, 1 \cdot 2^{s-m}, 2 \cdot 2^{s-m}, 3 \cdot 2^{s-m}, \dots, (2^m - 1) \cdot 2^{s-m}$ equally often. Then $\sum_{m=1}^s n_{m-1} = w_S(\mathcal{D})$ and since there are 2^r rows, one has

$$\begin{aligned} \sum_{\mathbf{c} \in \mathcal{D}} w_L(\mathbf{c}) &= \sum_{m=1}^s \left(n_{m-1} \frac{2^r}{2^m} \left(\sum_{t=0}^{(2^m-1)} w_L(t \cdot 2^{s-m}) \right) \right) \\ &= \sum_{m=1}^s (n_{m-1} 2^{r-m} (2^{s+m-2})) = 2^{r+s-2} \cdot w_S(\mathcal{D}) \end{aligned} \quad (5)$$

as $\sum_{t=0}^{(2^m-1)} w_L(t \cdot 2^{s-m}) = 2^{s-m} \sum_{t=1}^{2^m-1} \min\{t, 2^m - t\} = 2^{s+m-2}$. This completes part 1. For part 2, replace Lee weight by homogeneous weight in equation (5) and use (4) to get $\sum_{t=0}^{2^m-1} w_{HW}(t \cdot 2^{s-m}) = 2^{s-1} + \sum_{t \neq 2^{m-1}} w_{HW}(t \cdot 2^{s-m}) = 2^{s-1} + (2^m - 2)2^{s-2} = 2^{s+m-2}$. ■

Remark 2 For $s = 2$, Lemma 2 was first proved by K. Yang et al in [34] and later it has been done in higher generality by Constantinescu et al in [9].

Corollary 1 (Plotkin-Type Bound) Let \mathcal{C} be an $[n, k, d_L, d_{HW}]$ code over \mathbb{Z}_{2^s} . Then $d_L \leq \frac{2^{k+s-2}n}{(2^k-1)}$ and $d_{HW} \leq \frac{2^{k+s-2}n}{(2^k-1)}$.

PROOF. Every nonzero codeword has Lee weight at least d_L . Thus the total sum of Lee weights of codewords is at least $(2^k - 1)d_L$ and an upper bound for the total sum of Lee weights of codewords is $2^{k+s-2}n$. Therefore $(2^k - 1)d_L \leq 2^{k+s-2}n$. A similar argument holds for the case of homogeneous weights. ■

The proof of the following corollary follows immediately from Lemma 2.

Corollary 2 If $1 \leq r \leq k$, then the r^{th} GHW of \mathcal{C} satisfy $d_r(\mathcal{C}) \geq \max \left\{ \left\lceil \frac{(2^r-1)d_L}{2^{r+s-2}} \right\rceil, \left\lceil \frac{(2^r-1)d_{HW}}{2^{r+s-2}} \right\rceil \right\}$.

Remark 3 Using Lemma 2, for $1 \leq r \leq k$, the r^{th} GHW can also be defined as $d_r(\mathcal{C}) = \frac{1}{2^{r+s-2}} \min \left\{ \sum_{\mathbf{d} \in D_r} w_L(\mathbf{d}) \mid D_r \text{ is an } [n, r] \text{ subcode of } \mathcal{C} \right\}$.

Similar definition holds for w_{HW} . If $r = 1$, we get Corollary 3 from Lemma 2.

Corollary 3 Let \mathcal{C} be a linear code over \mathbb{Z}_{2^s} , then $d_H \geq \max \left\{ \left\lceil \frac{d_L}{2^{s-1}} \right\rceil, \left\lceil \frac{d_{HW}}{2^{s-1}} \right\rceil \right\}$.

Definition 2 A linear code \mathcal{C} over \mathbb{Z}_{2^s} is said to be of type α (β) if

$$d_H = \left\lceil \frac{d_{HW}}{2^{s-1}} \right\rceil \left(d_H > \left\lceil \frac{d_{HW}}{2^{s-1}} \right\rceil \right).$$

3 \mathbb{Z}_{2^s} -Simplex Codes of Type α and β

Let G_k^α be a $k \times 2^{sk}$ matrix over \mathbb{Z}_{2^s} with $G_1^\alpha = [0 \ 1 \ 2 \ 3 \ \cdots \ (2^s - 1)]$, and for $k \geq 2$, $G_k^\alpha = \left[\begin{array}{c} (0 \ 1 \ 2 \ 3 \ \cdots \ (2^s - 1)) \otimes \mathbf{1} \\ \mathbf{1} \otimes G_{k-1}^\alpha \end{array} \right]$, where $\mathbf{1}$ (the all 1 vector) in the first row is of length $2^{s(k-1)}$ and that in the second row is of length 2^s .

Clearly, the code S_k^α generated by G_k^α over \mathbb{Z}_{2^s} has length 2^{sk} and 2-dimension sk . The following remarks are straight forward.

Remark 4 If A_{k-1} denotes the $(2^{s(k-1)} \times 2^{s(k-1)})$ array consisting of all codewords in S_{k-1}^α and if J is the matrix of all 1's then the $(2^{sk} \times 2^{sk})$ array of codewords of S_k^α is given by

$$\begin{bmatrix} A_{k-1} & A_{k-1} & A_{k-1} & \cdots & A_{k-1} \\ A_{k-1} & J + A_{k-1} & 2J + A_{k-1} & \cdots & (2^s - 1)J + A_{k-1} \\ A_{k-1} & 2J + A_{k-1} & 2^2J + A_{k-1} & \cdots & (2^{s+1} - 2)J + A_{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & (2^s - 1)J + A_{k-1} & (2^{s+1} - 2)J + A_{k-1} & \cdots & (2^s - 1)^2J + A_{k-1} \end{bmatrix}.$$

Remark 5 If R_1, R_2, \dots, R_k denote the rows of the matrix G_k^α then $w_H(R_i) = 2^{sk} - 2^{s(k-1)}$, $w_H(2^{s-1}R_i) = 2^{sk-1}$, $w_L(R_i) = 2^{s(k+1)-2}$, and $w_{HW}(R_i) = 2^{s(k+1)-2}$.

For each m , $0 \leq m \leq s$, let $S_m = \{0, 1 \cdot 2^{s-m}, 2 \cdot 2^{s-m}, \dots, (2^m - 1) \cdot 2^{s-m}\}$. Note that $S_{s-1} = Z$, the set of all zero divisors of \mathbb{Z}_{2^s} and $S_s = \mathbb{Z}_{2^s}$. A codeword $\mathbf{c} = (c_1, \dots, c_n) \in S_k^\alpha$ is said to be of *type* m if all of its components belong to the set S_m . It may be observed that each element of \mathbb{Z}_{2^s} occurs equally often in every row of G_k^α . Writing 2^s in place of 2^{s+j} for $j > 0$ (as $2^s \equiv 2^{s+j} \pmod{2^s}$), we have the following lemma.

Lemma 3 Let $\mathbf{c} \in S_k^\alpha$ be a type m codeword. Then all the components of \mathbf{c} will occur equally often 2^{sk-m} times.

PROOF. Any $\mathbf{x} \in S_{k-1}^\alpha$ gives rise to the following 2^s codewords of S_k^α
 $\mathbf{y}_1 = (\mathbf{x} \mid \mathbf{x} \mid \mathbf{x} \mid \cdots \mid \mathbf{x})$, $\mathbf{y}_2 = (\mathbf{x} \mid \mathbf{1} + \mathbf{x} \mid \mathbf{2} + \mathbf{x} \mid \cdots \mid (\mathbf{2}^s - \mathbf{1}) + \mathbf{x})$,
 $\mathbf{y}_3 = (\mathbf{x} \mid \mathbf{2} + \mathbf{x} \mid \mathbf{2}^2 + \mathbf{x} \mid \cdots \mid (\mathbf{2}^s - \mathbf{2}) + \mathbf{x})$, \dots , and
 $\mathbf{y}_{2^s} = (\mathbf{x} \mid (\mathbf{2}^s - \mathbf{1}) + \mathbf{x} \mid (\mathbf{2}^s - \mathbf{2}) + \mathbf{x} \mid \cdots \mid \mathbf{1} + \mathbf{x})$, where $\mathbf{i} = (i \ i \ \cdots \ i)$. Hence the proof follows easily by induction on k and the Remark 4. \blacksquare

To determine weight distribution of S_k^α one needs to determine the number of codewords of type m in S_k^α for $1 \leq m \leq s$. Let C_m be the matrix defined by

$$C_m = [2^{s-m}R_1^t, \dots, 2^{s-1}R_1^t, \dots, 2^{s-m}R_k^t, \dots, 2^{s-1}R_k^t]^t,$$

where R_i is the i^{th} row of the matrix G_k^α and the superscript t denotes the transpose. The subcodes $\mathcal{D}^{(m)}$ of \mathcal{C} generated by the 2-linear combinations of the rows of C_m will have 2^{mk} codewords. Note that out of these codewords we get a codeword of type m duplicated $2^{(m-1)k}$ times. Thus, for all m , $1 \leq m \leq s$, a codeword of type m will occur $2^{mk} - 2^{(m-1)k}$ times in S_k^α . This proves the following lemma.

Lemma 4 Let $0 < m \leq s$. Then the number of codewords of type m in S_k^α is $2^{(m-1)k}(2^k - 1)$.

Theorem 2 The Hamming, Lee and homogeneous weight distributions of S_k^α are:

$$1. A_H(0) = 1, \quad A_H(2^{sk-m}(2^m - 1)) = 2^{(m-1)k}(2^k - 1) \text{ for } 1 \leq m \leq s,$$

2. $A_L(0) = 1, A_L(2^{s(k+1)-2}) = 2^{sk} - 1$ and

3. $A_{HW}(0) = 1, A_{HW}(2^{s(k+1)-2}) = 2^{sk} - 1.$

PROOF. Let $\mathbf{c} \in S_k^\alpha$ be a codeword of type $m (\neq 0)$. Then by Lemma 3, $w_H(\mathbf{c}) = 2^{sk} - 2^{sk-m}$ and thus by Lemma 4, $A_H(2^{sk-m}(2^m - 1)) = 2^{(m-1)k}(2^k - 1)$. For $m = 0$, $A_H(0) = 1$. Also, by Lemma 3 $w_L(\mathbf{c}) = 2^{sk-m} \left(\sum_{t=0}^{(2^m-1)} w_L(t \cdot 2^{s-m}) \right) = 2^{s(k+1)-2}$ which is independent of m . Thus all type $m(\neq 0)$ codewords will have same Lee weight. Similar argument holds for homogeneous weight. \blacksquare

Remark 6 1. S_k^α is an equidistant code with respect to Lee and homogeneous distances. The study of unicity as a equidistant code can be done as it was done for \mathbb{Z}_4 linear codes by Carlet in [8].

2. S_k^α is of type α .

3. For $s = 1, S_k^\alpha$ reduces to an extended binary simplex code \hat{S}_k .

4. The Lee weight distribution of the code S_k^α was first determined by Satyanarayana [25].

5. The minimum weights of S_k^α are $d_H = 2^{sk-1}$ and $d_L = d_{HW} = 2^{s(k+1)-2}$.

Let G_k^β be the $k \times n(k)$ matrix with $G_2^\beta = \left[\begin{array}{c|c} \mathbf{1} & (0 \ 2 \ 4 \ 6 \cdots (2^s - 2)) \\ \hline G_1^\alpha & \mathbf{1} \end{array} \right],$

and for $k > 2,$ $G_k^\beta = \left[\begin{array}{c|c} \mathbf{1} & (0 \ 2 \ 4 \ 6 \cdots (2^s - 2)) \otimes \mathbf{1} \\ \hline G_{k-1}^\alpha & \mathbf{1} \otimes G_{k-1}^\beta \end{array} \right],$ where G_{k-1}^α is the

generator matrix of S_{k-1}^α and $n(k)$ is the length of the linear code S_k^β generated by G_k^β over \mathbb{Z}_{2^s} . Here all the five $\mathbf{1}$'s are of appropriate sizes. The definition of the matrix G_2^β gives $n(2) = 3 \cdot 2^{s-1}$ and the structure of the matrix G_k^β with an inductive argument implies $n(k) = 2^{(s-1)(k-1)}(2^k - 1)$. The two rows of G_2^β generate a free module and the same is true of the k rows of G_k^β (using an induction argument). Thus the 2-dimension of S_k^β is sk .

We now show by induction on k , that no two columns of G_k^β are multiples of each other. It is clearly true for $k = 2$. Let the result be true for any two columns of G_{k-1}^β . Let \mathbf{c}_1 and \mathbf{c}_2 be any two columns of G_k^β . Observe that G_k^β can be split into $(2^{s-1} + 1)$ blocks as $B_0, B_1, B_2, \dots, B_{2^{s-1}}$ with the corresponding first row of G_k^β as $(1 \cdots 1 \mid 0 \cdots 0 \mid 2 \cdots 2 \mid \cdots \mid (2^s - 2) \cdots (2^s - 2))$. When $\mathbf{c}_1, \mathbf{c}_2 \in B_i$ ($1 \leq i \leq 2^{s-1}$) they are not multiples by induction hypothesis. If $\mathbf{c}_1, \mathbf{c}_2 \in B_0$ then they are not multiples as each column of G_{k-1}^α is distinct and the top row of B_0 is the all 1 vector. Now let $\mathbf{c}_1 \in B_0$ and $\mathbf{c}_2 \in B_i$ ($1 \leq i \leq 2^{s-1}$).

Then for $\lambda \in \mathbb{Z}_{2^s}$, $\lambda \mathbf{c}_2 = \begin{pmatrix} z \\ \star \end{pmatrix}$ for some zero divisor z . Thus $\lambda \mathbf{c}_2 \neq \mathbf{c}_1$. Finally let $\mathbf{c}_1 \in B_i$ and $\mathbf{c}_2 \in B_j$ ($1 \leq i \neq j \leq 2^{s-1}$). Then c_1 and c_2 are not multiples as their first entries can be multiples of each other, but then there is at least one 1 in the remaining entries. Thus S_k^β is a $[2^{(s-1)(k-1)}(2^k - 1), sk]$ code.

Remark 7 If A_{k-1} denotes the $(2^{s(k-1)} \times 2^{s(k-1)})$ array consisting of all codewords in S_{k-1}^α , B_{k-1} denotes the $2^{s(k-1)} \times 2^{(s-1)(k-2)}(2^{k-1} - 1)$ array of codewords in S_{k-1}^β and if J is the matrix of all 1's then the $2^{sk} \times 2^{(s-1)(k-1)}(2^k - 1)$ array of all codewords of S_k^β is given by

$$\begin{bmatrix} A_{k-1} & B_{k-1} & B_{k-1} & B_{k-1} & \cdots & B_{k-1} \\ J + A_{k-1} & B_{k-1} & 2J + B_{k-1} & 2^2 J + B_{k-1} & \cdots & (2^s - 2)J + B_{k-1} \\ 2J + A_{k-1} & B_{k-1} & 2^2 J + B_{k-1} & 2^3 J + B_{k-1} & \cdots & (2^s - 2^2)J + B_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (2^s - 1)J + A_{k-1} & B_{k-1} & (2^s - 2)J + B_{k-1} & (2^s - 2^2)J + B_{k-1} & \cdots & 2J + B_{k-1} \end{bmatrix}.$$

Let U, Z be the set of units and zero divisors of \mathbb{Z}_{2^s} , respectively. Then the following propositions help in determining weight distributions of S_k^β .

Proposition 1 For $1 \leq j \leq k$, let R_j be the j^{th} row of G_k^β . Then

1. $\sum_{i \in U} \omega_i = 2^{s(k-1)}$ and each zero divisor in \mathbb{Z}_{2^s} occurs $2^{(s-1)(k-2)}(2^{k-1} - 1)$ times in R_j .
2. $w_H(R_j) = 2^{(s-1)(k-1)-s} [(2^k - 1)(2^s - 1) + 1]$, $w_{HW}(R_j) = 2^{sk-k-1}(2^k - 1)$ for all j , $1 \leq j \leq k$.
3. $w_L(R_1) = 2^{s(k-1)} + 2^{sk-2} - 2^{sk-k-1}$.

PROOF. The proof follows directly from above using the definition of R_j . ■

The next proposition gives the structure of codewords of S_k^β .

Proposition 2 Let $\mathbf{c} \in S_k^\beta$. If one of the coordinates of \mathbf{c} is a unit then $\sum_{i \in U} \omega_i = 2^{s(k-1)}$ and each zero divisor in \mathbb{Z}_{2^s} occurs $2^{(s-1)(k-2)}(2^{k-1} - 1)$ times in \mathbf{c} .

PROOF. By Remark 7, there exist $\mathbf{y}_1 \in S_{k-1}^\alpha$ and $\mathbf{y}_2 \in S_{k-1}^\beta$ such that \mathbf{c} can have any of the following 2^s forms

$$\begin{aligned} \mathbf{c} &= \left(\mathbf{y}_1 \mid \mathbf{y}_2 \mid \mathbf{y}_2 \mid \cdots \mid \mathbf{y}_2 \right), \quad \mathbf{c} = \left(\mathbf{1} + \mathbf{y}_1 \mid \mathbf{y}_2 \mid \mathbf{2} + \mathbf{y}_2 \mid \cdots \mid (\mathbf{2}^s - \mathbf{2}) + \mathbf{y}_2 \right), \\ \mathbf{c} &= \left(\mathbf{2} + \mathbf{y}_1 \mid \mathbf{y}_2 \mid \mathbf{2}^2 + \mathbf{y}_2 \mid \cdots \mid (\mathbf{2}^s - \mathbf{2}^2) + \mathbf{y}_2 \right), \dots, \text{ or} \\ \mathbf{c} &= \left((\mathbf{2}^s - \mathbf{1}) + \mathbf{y}_1 \mid \mathbf{y}_2 \mid (\mathbf{2}^s - \mathbf{2}) + \mathbf{y}_2 \mid \cdots \mid \mathbf{2} + \mathbf{y}_2 \right), \text{ where } \mathbf{i} = (i \ i \dots \ i). \end{aligned}$$

The proof now follows by induction. ■

Let \mathcal{C} be a linear code over \mathbb{Z}_{2^s} and $D = \{\mathbf{c} \in \mathcal{C} \mid c_i = 0 \text{ or } 2^{s-1} \text{ for all } i\}$. Then $\mathcal{C}^{(2)} = \left\{ \frac{1}{2^{s-1}} \mathbf{c} \mid \mathbf{c} \in D \right\}$ is called the torsion code of \mathcal{C} and the binary code $\mathcal{C}^{(1)} = \mathcal{C} \pmod{2}$ is called the reduction code of \mathcal{C} . If \mathcal{C} is a free module then $\mathcal{C}^{(2)} = \mathcal{C}^{(1)}$. Hence the reduction and torsion codes of $S_k^\alpha \left(S_k^\beta \right)$ are equal. The next proposition determines these binary codes.

Proposition 3 *The torsion code of $S_k^\alpha \left(S_k^\beta \right)$ is equivalent to $2^{(s-1)k}$ copies of the extended binary simplex code ($2^{(s-1)(k-1)}$ copies of the binary simplex code).*

PROOF. The proof follows by induction on k and is similar to the proof given for codes over \mathbb{Z}_4 (see [3]). \blacksquare

Theorem 3 *The Hamming and homogeneous weight distributions of S_k^β are*

1. $A_H(0) = 1, A_H(2^{(s-1)(k-1)}[2^{k-m}\{2^m - 1\} + \{2^{1-m} - 1\}]) = 2^{(m-1)k}(2^k - 1), 1 \leq m \leq s$ and
2. $A_{HW}(0) = 1, A_{HW}(2^{sk-1}) = 2^k - 1, A_{HW}(2^{sk-k-1}(2^k - 1)) = 2^k(2^{(s-1)k} - 1).$

PROOF. Using Theorem 2, Remark 7 and induction on k , the possible non-zero Hamming (homogeneous) weights of S_k^β are $\{2^{(s-1)(k-1)}(2^{k-m}(2^m - 1) + (2^{1-m} - 1)) \mid 1 \leq m \leq s\} \cup \{2^{sk-1}, 2^{sk-k-1}(2^k - 1)\}$. By Lemma 4, a Hamming weight of type m occurs $2^{(m-1)k}(2^k - 1)$ times. Moreover homogeneous weight 2^{sk-1} occurs $2^k - 1$ times. Thus the other weight occurs $2^{sk} - 2^k$ times. \blacksquare

The next corollary follows directly from Theorem 3.

Corollary 4 1. S_k^β is of type β .

2. For $s = 1$, S_k^β reduces to the binary simplex code S_k .

3. $d_H(S_k^\beta) = 2^{s(k-1)}$ and $d_{HW}(S_k^\beta) = 2^{sk-k-1}(2^k - 1)$.

Recently a Griesmer bound for codes over finite quasi-Frobenius rings has been obtained by Shiromoto and Strome in [27]. In particular, they prove:

Theorem 4 [27] *For a free linear code \mathcal{C} of length n , dimension k and minimum Hamming distance d_H over \mathbb{Z}_{p^s} the following inequality holds:*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_H}{p^i} \right\rceil.$$

Applying the above inequality to S_k^β for $p = 2$ yields:

Proposition 4 *The simplex codes of type β meet the Griesmer bound for codes over \mathbb{Z}_{p^s} .*

3.1 Gray Image Families

In this section we study the Gray images of the above simplex codes in two ways. The first method consists of applying the generalized Gray map defined in section 2.2 to the linear $[n, k, d_H, d_{HW}]$ code \mathcal{C} over \mathbb{Z}_{2^s} . This code, denoted $\gamma(\mathcal{C})$, is (possibly) non-linear, is of length $2^{s-1}n$, has minimum Hamming distance d_{HW} (since for any \mathbb{Z}_{2^s} linear code, $d_H(\gamma(u), \gamma(v)) = w_{HW}(u - v) = d_{HW}(u, v)$ [7]), and also has 2^k codewords. The second method consists of applying the generalized Gray map γ to the matrix of the 2-basis of \mathcal{C} . This matrix has full row-rank (see Lemma 1) and hence can be taken as the generator matrix of a binary linear code. The code obtained by the second method also has length $2^{s-1}n$ and dimension k . It will be denoted by \mathcal{C}_γ .

For example, let \mathcal{B} be the matrix given in (3) for $p = 2$. The rows of \mathcal{B} form a 2-basis for \mathcal{C} . Then the code \mathcal{C}_γ is a $\left[2^{s-1}n, k, \geq \left\lfloor \frac{d_{HW}}{2^{s-1}} \right\rfloor\right]$ binary linear code. Note that $\gamma(\mathcal{C})$ and \mathcal{C}_γ have the same number of codewords but they are not equal in general. In this section, we study $\gamma(\mathcal{C})$ and \mathcal{C}_γ codes for the simplex codes of type α and β and also determine their weight hierarchies.

Let \bar{S}_k^α be the punctured code of S_k^α obtained by deleting the zero coordinate. Then the following remark is immediate.

Remark 8 (i) $\gamma(\bar{S}_k^\alpha)$ is a binary code of length $2^{s-1}(2^{sk} - 1)$ and minimum Hamming distance $2^{s(k+1)-2}$. It meets the Plotkin bound (cf. [19]) and $n \leq 2d_H$.
(ii) $\gamma(S_k^\beta)$ is a binary code of length $2^{k(s-1)}(2^k - 1)$ and minimum Hamming distance $2^{sk-k-1}(2^k - 1)$. It is an example of a code having $n = 2d_H$ (cf. [19]).

The next two results determine the binary linear codes generated by the generalized Gray map of the 2-basis \bar{S}_k^α and S_k^β .

Theorem 5 Let $\mathcal{C} = \bar{S}_k^\alpha$. Then \mathcal{C}_γ is a $[2^{s-1}(2^{sk} - 1), sk, 2^{s(k+1)-2}]$ binary linear code consisting of 2^{s-1} copies of the binary simplex code S_{sk} with Hamming weight distribution the same as the homogeneous weight distribution of \bar{S}_k^α .

PROOF. By Lemma 1, \mathcal{C}_γ is a binary linear code of length $2^{s-1}(2^{sk} - 1)$ and dimension sk . Let \mathcal{G}_k^α be a generator matrix of S_k^α in 2-basis form. Then

$$\mathcal{G}_k^\alpha = \begin{bmatrix} (0 \ 1 \ 2 \ 3 \ \dots \ (2^s - 1)) \otimes \mathbf{1} \\ 2(0 \ 1 \ 2 \ 3 \ \dots \ (2^s - 1)) \otimes \mathbf{1} \\ \vdots \\ 2^{s-1}(0 \ 1 \ 2 \ 3 \ \dots \ (2^s - 1)) \otimes \mathbf{1} \\ \mathbf{1} \otimes G_{k-1}^\alpha \\ \mathbf{1} \otimes 2G_{k-1}^\alpha \\ \vdots \\ \mathbf{1} \otimes 2^{s-1}G_{k-1}^\alpha \end{bmatrix} \quad \& \quad \gamma(\mathcal{G}_k^\alpha) = \begin{bmatrix} \gamma((0 \ 1 \ 2 \ 3 \ \dots \ (2^s - 1)) \otimes \mathbf{1}) \\ \gamma(2(0 \ 1 \ 2 \ 3 \ \dots \ (2^s - 1)) \otimes \mathbf{1}) \\ \gamma(2^2(0 \ 1 \ 2 \ 3 \ \dots \ (2^s - 1)) \otimes \mathbf{1}) \\ \vdots \\ \gamma(2^{s-1}(0 \ 1 \ 2 \ 3 \ \dots \ (2^s - 1)) \otimes \mathbf{1}) \\ \mathbf{1} \otimes \gamma(G_{k-1}^\alpha) \end{bmatrix}.$$

The proof is by induction on k . For $k = 2$, the result follows trivially. Assume

the result holds for $k - 1$, i.e., $\gamma(\mathcal{G}_{k-1}^\alpha)$ yields a binary code in which every non-zero codeword is of weight 2^{sk-2} . Then by the induction hypothesis the possible non-zero weight from the lower portion of the matrix $\gamma(\mathcal{G}_k^\alpha)$ will be $2^s \cdot 2^{sk-2} = 2^{s(k+1)-2}$. From the structure of the first s rows of $\gamma(\mathcal{G}_k^\alpha)$ it is easy to verify that any linear combination of these rows with other rows coming from the lower portion has weight 2^{sk+s-2} . Puncturing the first 2^{s-1} columns corresponding to the first column of \mathcal{G}_k^α and rearranging the rest of the columns yields the code having 2^{s-1} copies of S_{sk} . ■

Theorem 6 *Let $\mathcal{C} = S_k^\beta$. Then \mathcal{C}_γ is the binary MacDonal code $M_{sk, (s-1)k}$, with parameters $[2^{sk} - 2^{(s-1)k}, sk, 2^{sk-1} - 2^{(s-1)k-1}]$ and Hamming weight distribution same as the homogeneous weight distribution of S_k^β .*

PROOF. By induction on k . Let \mathcal{G}_k^β be a generator matrix of S_k^β in 2-basis form then

$$\gamma(\mathcal{G}_k^\beta) = \left[\begin{array}{c|c} \begin{array}{c} \gamma(\mathbf{1}) \\ \gamma(\mathbf{21}) \\ \vdots \\ \gamma(2^{s-1}\mathbf{1}) \end{array} & \begin{array}{c} \gamma((0\ 2\ 4\ 6 \dots (2^s - 2))) \otimes \mathbf{1} \\ \gamma(2(0\ 2\ 4\ 6 \dots (2^s - 2))) \otimes \mathbf{1} \\ \vdots \\ \gamma(2^{s-1}(0\ 2\ 4\ 6 \dots (2^s - 2))) \otimes \mathbf{1} \end{array} \\ \hline \gamma(\mathcal{G}_{k-1}^\alpha) & \mathbf{1} \otimes \gamma(\mathcal{G}_{k-1}^\beta) \end{array} \right],$$

where \mathcal{G}_{k-1}^α is the generator matrix of S_{k-1}^α in 2-basis form. It is easy to verify that the result holds for $k = 2$. Assume that result holds for S_{k-1}^β . Then $\gamma(\mathcal{G}_{k-1}^\beta)$ yields a binary code with possible non-zero weights either 2^{sk-s-1} or $2^{sk-s-k}(2^{k-1} - 1)$. By Theorem 5, $\gamma(\mathcal{G}_{k-1}^\alpha)$ is a binary code in which every non-zero codeword is of weight 2^{sk-2} . Thus possible non-zero weights from lower portion of the above matrix will be either $2^{s-1}(2^{sk-s-1}) + 2^{sk-2}$ or $2^{s-1}(2^{sk-s-1} - 2^{sk-s-k}) + 2^{sk-2}$. Now the proof follows (easily from the structure of first s rows of the above matrix) by showing that the resulting weight of any linear combination of first s rows in the lower portion of the matrix does not change. ■

Note that the codes \mathcal{C}_γ of \bar{S}_k^α and S_k^β are binary linear codes meeting the Griesmer bound hence are optimal. For another representation of MacDonal codes see [15]. Finally, the weight hierarchy of S_k^α and S_k^β are given by the following two theorems.

Theorem 7 *S_k^α satisfies the chain condition and its weight hierarchy is given by $d_r(S_k^\alpha) = \sum_{i=1}^r 2^{sk-i} = 2^{sk} - 2^{sk-r}$, $1 \leq r \leq sk$.*

PROOF. By Remark 6, any r -dimensional subcode of S_k^α is of constant homogeneous weight. Hence by definition (see Remark 3)

$$d_r(S_k^\alpha) = \frac{1}{2^{r+s-2}} \sum_{\mathbf{c}(\neq 0) \in \mathcal{D}_r} w_{HW(\mathbf{c})} = \frac{2^{sk+s-2}}{2^{r+s-2}} \sum_{\mathbf{c}(\neq 0) \in \mathcal{D}_r} 1 = 2^{sk-r}(2^r - 1). \text{ Let}$$

$$\begin{aligned} D_1 &= \langle 2^{s-1}R_1 \rangle, & D_2 &= \langle 2^{s-1}R_1, 2^{s-1}R_2 \rangle, \dots, \\ D_k &= \langle 2^{s-1}R_1, \dots, 2^{s-1}R_k \rangle, \\ D_{k+1} &= \langle 2^{s-2}R_1, 2^{s-1}R_1, 2^{s-1}R_2, \dots, 2^{s-1}R_k \rangle, \dots, \text{ and} \\ D_{sk} &= \langle R_1, 2R_1, \dots, 2^{s-1}R_1, \dots, R_k, 2R_k, \dots, 2^{s-1}R_k \rangle. \end{aligned}$$

Then $D_1 \subseteq D_2 \subseteq \dots \subseteq D_{sk}$ and for $1 \leq r \leq sk$, $w_S(D_r) = d_r(S_k^\alpha)$. ■

Theorem 8 For $1 \leq i \leq k$, $(i-1)s < r \leq is$ and $n(k) = 2^{(s-1)(k-1)}(2^k - 1)$, $d_r(S_k^\beta) = n(k) - 2^{(s-1)(k-1)}(2^{k-r} - 2^{i-r})$. Moreover S_k^β satisfies the chain condition.

PROOF. The proof follows by induction on k . Clearly the result holds for $k = 2$. Assume that the result holds for S_{k-1}^β . Hence, for $1 \leq i \leq k-1$, there exists an r -dimensional subcode of S_{k-1}^β with minimum support size $n(k-1) - 2^{(s-1)(k-2)}(2^{k-1-r} - 2^{i-r})$. By Remark 7,

$$d_r(S_k^\beta) = 2^{s-1}d_r(S_{k-1}^\beta) + d_r(S_{k-1}^\alpha). \quad (6)$$

But all r -dimensional subcodes of S_{k-1}^α have constant support size $(2^{sk-s} - 2^{sk-s-r})$. Thus simplifying (6) yields the result. The case $i = k$ is trivial. Let

$$\begin{aligned} D_1 &= \langle 2^{s-1}R_1 \rangle, & D_2 &= \langle 2^{s-2}R_1, 2^{s-1}R_1 \rangle, \dots, & D_s &= \langle R_1, 2R_1, 2^2R_2, \dots, 2^{s-1}R_1 \rangle, \\ D_{s+1} &= \langle R_1, 2R_1, 2^2R_2, \dots, 2^{s-1}R_1, 2^{s-1}R_2 \rangle, \dots, \\ D_{2s} &= \langle R_1, 2R_1, 2^2R_2, \dots, 2^{s-1}R_1, R_2, 2R_2, \dots, 2^{s-1}R_2 \rangle, \dots, \text{ and} \\ D_{sk} &= \langle R_1, 2R_1, 2^2R_2, \dots, 2^{s-1}R_1, R_2, 2R_2, \dots, 2^{s-1}R_2, \dots, R_k, 2R_k, 2^2R_k, \dots, 2^{s-1}R_k \rangle. \end{aligned}$$

Now $D_1 \subseteq D_2 \subseteq \dots \subseteq D_{sk}$ is the required chain of subcodes. ■

The dual code of S_k^α is a code of length 2^{sk} and 2-dimension $s(2^{sk} - k)$, whereas the dual code of S_k^β is a code of length $2^{(s-1)(k-1)}(2^k - 1)$ and 2-dimension $s(2^{(s-1)(k-1)}(2^k - 1) - k)$. The weight hierarchies of duals can be obtained from Theorem 1, 7 and 8. The code $\gamma((S_k^\beta)^\perp)$ is a uniformly packed code as it meets the Johnson bound [19]. There exist other type α and type β codes over \mathbb{Z}_{2^s} . For example, the first order Reed-Muller code $\mathcal{R}^{1, m-s+1}$ defined in the next section is of type α and the uplifted extended Hamming code \mathcal{H}_{2^s} of length 8 in [6] is of type β .

4 First Order Reed-Muller Code over \mathbb{Z}_{2^s}

In [12], Hammons et al have constructed a linear code over \mathbb{Z}_4 (called a quaternary first order Reed-Muller code) whose Gray image is the binary first order

Reed-Muller code. In this section we construct a linear code over \mathbb{Z}_{2^s} whose image under the generalized Gray map γ is the binary first order Reed-Muller code. Some basic properties of these are also obtained.

Let $1 \leq i \leq m - s + 1$. Let \mathbf{v}_i be a vector of length 2^{m-s+1} consisting of successive blocks of 0's and 1's each of size $2^{(m-s+1)-i}$ and let $\mathbf{1} = (111 \dots 11) \in \mathbb{Z}_2^{2^{m-s+1}}$. Let G be a $(m - s + 2) \times 2^{m-s+1}$ matrix given by (consisting of the rows as $\mathbf{1}$ and $2^{s-1}\mathbf{v}_i$ ($1 \leq i \leq m - s + 1$))

$$G = \begin{bmatrix} 0 & 0 & \dots & 0 & 0 & 2^{s-1} & 2^{s-1} & \dots & 2^{s-1} & 2^{s-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 2^{s-1} & \dots & 0 & 2^{s-1} & 0 & 2^{s-1} & \dots & 0 & 2^{s-1} \\ 1 & 1 & \dots & 1 & 1 & 1 & 1 & \dots & 1 & 1 \end{bmatrix} \quad (7)$$

The code generated by G is called the *first order Reed-Muller code over \mathbb{Z}_{2^s}* , denoted $\mathcal{R}^{1,m-s+1}$. It is a $[2^{m-s+1}, m + 1, 2^{m-s}, 2^{m-s+1}, 2^{m-1}]$ type α linear code over \mathbb{Z}_{2^s} . Its generator matrix in 2-basis is given by

$$\mathcal{G} = \begin{bmatrix} 0 & 0 & \dots & 0 & 0 & 2^{s-1} & 2^{s-1} & \dots & 2^{s-1} & 2^{s-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 2^{s-1} & \dots & 0 & 2^{s-1} & 0 & 2^{s-1} & \dots & 0 & 2^{s-1} \\ 1 & 1 & \dots & 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 2 & 2 & \dots & 2 & 2 & 2 & 2 & \dots & 2 & 2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2^{s-1} & 2^{s-1} & \dots & 2^{s-1} & 2^{s-1} & 2^{s-1} & 2^{s-1} & \dots & 2^{s-1} & 2^{s-1} \end{bmatrix} \quad (8)$$

Remark 9 For $s = 2$, $\mathcal{R}^{1,m-s+1}$ reduces to the quaternary first order Reed-Muller code $ZRM(1, m)$ defined in Hammons et al [12]. In [10], Davis and Jedwab have also introduced two more generalizations of Reed-Muller codes, viz $ZRM_{2^s}(r, m)$ and $RM_{2^s}(r, m)$.

We now find weight distributions of the code $\mathcal{R}^{1,m-s+1}$.

Proposition 5 *The Hamming and homogeneous weight distributions of $\mathcal{R}^{1,m-s+1}$ are:*

1. $A_H(0) = 1, A_H(2^{m-s}) = 2^{m-s+2} - 2$ and $A_H(2^{m-s+1}) = 2^{m+1} - 2^{m-s+2} + 1,$
2. $A_{HW}(0) = 1, A_{HW}(2^m) = 1$ and $A_{HW}(2^{m-1}) = 2^{m+1} - 2.$

PROOF. Note that first s rows of the matrix \mathcal{G} given in (8) have Hamming weight 2^{m-s+1} and remaining $m - s + 1$ rows are of Hamming weight 2^{m-s} . It is easy to see that any non-trivial 2-linear combination of the last $m - s + 1$ rows also has Hamming weight 2^{m-s} . Hence $A_H(2^{m-s}) = 2^{m-s+2} - 2$. Since $-2^{s-1} = 2^{s-1}$

in \mathbb{Z}_{2^s} , every other non-trivial 2-linear combination has weight 2^{m-s+1} . Thus $A_H(2^{m-s+1}) = 2^{m+1} - 2^{m-s+2} + 1$. Similar arguments hold for homogeneous weight. \blacksquare

Theorem 9 *The weight hierarchy of $\mathcal{R}^{1,m-s+1}$ is given by*

$$d_t(\mathcal{R}^{1,m-s+1}) = \begin{cases} \sum_{i=0}^{t-1} 2^{m-s-i}, & 1 \leq t \leq m-s+1 \\ 2^{m-s+1}, & m-s+1 < t \leq m+1. \end{cases}$$

Moreover, $\mathcal{R}^{1,m-s+1}$ satisfies the chain condition.

PROOF. By Corollary 2,

$$d_t(\mathcal{R}^{1,m-s+1}) \geq \left\lceil \frac{(2^t - 1)2^{m-1}}{2^{t+s-2}} \right\rceil = \begin{cases} \sum_{i=0}^{t-1} 2^{m-s-i}, & 1 \leq t \leq m-s+1 \\ 2^{m-s+1}, & m-s+1 < t \leq m+1. \end{cases} \quad (9)$$

Let $1 \leq t \leq m-s+1$ and let D be a t -dimensional subcode of $\mathcal{R}^{1,m-s+1}$ generated by any t rows chosen from the last $m-s+1$ rows of (8). Then the chosen t rows share $2^{m-s+1-t}$ common zero bit positions. Hence the support size of D is $\sum_{i=0}^{t-1} 2^{m-s-i}$. If $t > m-s+1$ then trivially equality holds in (9). Suppose

$$\begin{aligned} D_1 &= \langle 2^{s-1}\mathbf{v}_{m-s+1} \rangle, & D_2 &= \langle 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} \rangle, \dots, \\ D_{m-s+1} &= \langle 2^{s-1}\mathbf{v}_1, \dots, 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} \rangle, \\ D_{m-s+2} &= \langle \mathbf{2}^{s-1}, 2^{s-1}\mathbf{v}_1, \dots, 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} \rangle, \dots, \text{ and} \\ D_{m-1} &= \langle \mathbf{1}, \mathbf{2}, \mathbf{2}^2, \dots, \mathbf{2}^{s-1}, 2^{s-1}\mathbf{v}_1, \dots, 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} \rangle. \end{aligned}$$

Then $D_1 \subseteq D_2 \subseteq \dots \subseteq D_{m+1}$ and $w_s(D_r) = d_r(\mathcal{R}^{1,m-s+1})$, $1 \leq r \leq m+1$. \blacksquare

The map γ is non-linear over \mathbb{Z}_{2^s} as $\gamma(2+3) \neq \gamma(2) + \gamma(3)$. However we have the following lemma.

Lemma 5 *Let $T = \{2^i : 0 \leq i \leq s-1\} \cup \{0\}$. Then $\gamma(a+b) = \gamma(a) + \gamma(b)$, for all $a, b \in T$.*

PROOF. The proof follows by the definition of the map γ . \blacksquare

Theorem 10 *$\mathcal{R}^{1,m-s+1}$ is \mathbb{Z}_2 -linear.*

PROOF. Let $\mathbf{c} \in \mathcal{R}^{1,m-s+1}$. Then \mathbf{c} can be written as a 2-linear combination of the rows of the matrix \mathcal{G} given in (8). Since γ maps \mathcal{G} to a generator matrix of a binary first order Reed-Muller code (with some permutation of the rows (see (8) and Lemma 5)). Thus $\gamma(\mathbf{c})$ belongs to the binary linear first order Reed-Muller code. Hence $\mathcal{R}^{1,m-s+1}$ is \mathbb{Z}_2 -linear. \blacksquare

The results presented in this correspondence can be generalized to codes over \mathbb{Z}_{p^s} and will be reported elsewhere.

Acknowledgements

The authors thank D. G. Glynn, T. A. Gulliver and Patrick Solé for their helpful remarks.

References

- [1] A. E. Ashikhmin, “On generalized hamming weights for galois ring linear codes,” *Designs, Codes and Cryptography*, vol. 14, 1998, pp. 107–126.
- [2] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.
- [3] M. C. Bhandari, M. K. Gupta, and A. K. Lal, “On \mathbb{Z}_4 simplex codes and their gray images,” AAECC-13, *Lecture Notes in Computer Science*, vol. 1719, 1999, pp. 170–180.
- [4] I. F. Blake, “Codes over certain rings,” *Inform. Control*, vol. 20, 1972, pp. 396–404.
- [5] I. F. Blake, “Codes over integer residue rings,” *Inform. Control*, vol. 29, 1975, pp. 295–300.
- [6] A. R. Calderbank and N. J. A. Sloane, “Modular and p -adic cyclic codes,” *Designs, Codes and Cryptography*, vol. 6, 1995, pp. 21–35.
- [7] C. Carlet, “ \mathbb{Z}_{2^k} -linear codes,” *IEEE Trans. Inform. Theory*, vol. 44, no. 4, 1998, pp. 1543–1547.
- [8] C. Carlet, “One weight \mathbb{Z}_4 -linear codes ” Int. Conf. on Coding, Crypto and related Areas, Mexico *Springer Lecture Notes in Computer Science*, 1999, pp. 57–72.
- [9] I. Constantinescu, W. Heise, and T. Honold “ Monomial extensions of isometries between codes over \mathbb{Z}_m ” Proc. Workshop ACCT’96, Sozopol, Bulgaria, 1996, pp. 98–104.
- [10] J. A. Davis and J. Jedwab, “Peak to mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes,” *IEEE Trans. Inform. Theory*, vol. 45, no. 7, 1999, pp. 2397–2417.
- [11] M. Greferath, and S. E. Schmidt, “Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code,” *IEEE Trans. Inform. Theory*, vol. 45, no. 7, 1999, pp. 2522–2524.

- [12] A. Roger Hammons, P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé, “The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes,” *IEEE Trans. Inform. Theory*, vol. 40, no. 2, 1994, pp. 301–319.
- [13] T. Helleseth, T. Klove, V. I. Levenshtein, and ϕ . Ytrehus, “Bounds on the minimum support weights,” *IEEE Trans. Inform. Theory*, vol. 41, no. 2, 1995, pp. 432–439.
- [14] T. Honold, and I. Landjev, “Linearly representable codes over chain rings,” *Abh. Math. Sem. Univ. Hamburg*, vol. 69, 1999, pp. 187–203.
- [15] T. Honold, and I. Landjev, “Linear codes over finite chain rings,” *Electronic Journal of Combinatorics*, vol. 7, no. 1, 2000, Research Paper 11.
- [16] I. Konstantinesku, and V. Khauize, “A metric for codes over residue class rings of integers,” *Problemy Peredachi Informatsii*, vol. 33, no. 3, 1997, pp. 22–28.
- [17] C. Y. Lee, “Some properties of non-binary error-correcting codes,” *IEEE Trans. Inform. Theory*, vol. 4, 1958, pp. 77–82.
- [18] F. J. MacWilliams, “Error correcting codes for multi-level transmission,” *Bell System Technical Journal*, 1961, pp. 281–308.
- [19] F. J. MacWilliams and N. J. A. Sloane, *Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.
- [20] J. L. Massey and T. M. Mittelholzer, “Convolutional codes over rings,” in *Proc. Joint Swedish-USSR Int. Workshop in Inform. Theory*, Gotland, Sweden, 1989, pp. 14–18.
- [21] A. A. Nechaev, “Kerdock code in a cyclic form,” *Discrete Math. Appl.*, vol. 1, 1991, pp. 365–384.
- [22] A. A. Nechaev and A. S. Kuzmin, “Linearly presentable codes,” *Proc. IEEE Int. Sympos. Inf. Theory Appl.*, 1996, pp. 31–34.
- [23] E. E. Nemirovskiy, “Codes on residue class rings with multi-frequency phase telegraphy,” *Radiotekhnika I elektronika*, vol. 9, 1984, pp. 1745–1753.
- [24] Ana Sălăgean-Mandache, “On the isometries between \mathbb{Z}_{p^k} and \mathbb{Z}_p^k ,” *IEEE Trans. Inform. Theory*, vol. 45, no. 6, 1999, pp. 2146–2148.
- [25] C. Satyanarayana, “Lee metric codes over integer residue rings,” *IEEE Trans. Inform. Theory*, vol. 25, no. 2, 1979, pp. 250–254.

- [26] Priti Shankar, “On BCH codes over arbitrary integer rings,” *IEEE Trans. Inform. Theory*, vol. 25, no. 4, 1979, pp. 480–483.
- [27] K. Shiromoto and L. Storme “ A griesmer bound for codes over finite quasi-frobenius rings” Proc. Workshop WCC 2001, Int. workshop in coding and Cryptography, January 8–12, 2001, Paris, France, to appear in *Discr. Applied Math.*
- [28] Eugene Spiegel, “Codes over \mathbb{Z}_m ,” *Inform. Control*, vol. 35, 1977, pp. 48–51.
- [29] B. SundarRajan, *Transform Domain Study of Cyclic and Abelian Codes over Residue Class Integer Rings*, Ph.D. thesis, Deptt. of Elec. Engg., IIT Kanpur, Kanpur, India, 1989.
- [30] V. V. Vazirani, H. Saran, and B. SundarRajan, “An efficient algorithm for constructing minimal trellises for codes over finite abelian groups,” *IEEE Trans. Inform. Theory*, vol. 42, no. 6, 1996, pp. 1839–1854.
- [31] G. Vega and H. Tapia-Recillas, “On \mathbb{Z}_{2^s} -linear and quaternary codes,” *IEEE Trans. Inform. Theory*, (submitted), 2001.
- [32] Z.X. Wan, *Quaternary Codes*, World Scientific, Singapore, 1997.
- [33] Siri K. Wasan, “On codes over \mathbb{Z}_m ,” *IEEE Trans. Inform. Theory*, vol. 28, no. 1, 1982, pp. 117–120.
- [34] K. Yang, T. Helleseth, P. V. Kumar, and A. G. Shangbhag, “On the weight hierarchy of Kerdock codes over \mathbb{Z}_4 ,” *IEEE Trans. Inform. Theory*, vol. 42, no. 5, 1996, pp. 1587–1593.

Keywords: Linear codes over rings, Generalized Gray map, Simplex code, Reed-Muller code, p -dimension, Generalized Hamming weights (GHWs), Lee weight, Gray image, Weight distributions.

Contact Author

Manish K. Gupta
Room GWC 354, Department of Computer Science and Engineering,
College of Engineering and Applied Sciences,
Arizona State University, Tempe
Arizona, USA 85287-5406

Telephone: +480-965-2776

Fax: +480-965-2751

E-mail: manish.gupta@asu.edu, m.k.gupta@ieee.org