On Quaternary MacDonald Codes

Charles J. Colbourn and Manish K. Gupta *
Department of Computer Science and Engineering, Arizona State University,
Tempe 85287-5406, U.S.A.
Email:{charles.colbourn,manish.gupta}@asu.edu

December 11, 2002

Abstract

This paper studies two families of codes over $\mathbb{Z}_4$, MacDonald codes of type α and type β. The torsion code, weight distribution, and Gray image properties are studied. Some interesting optimal binary codes are also obtained. Two nonlinear families of binary codes are obtained via the Gray map.

Keywords: Codes over rings, Gray image, simplex codes, torsion code, weight distribution, MacDonald codes, projective multiset.

1 Introduction

There has been much interest and research in codes over finite rings in recent years. In particular codes over $\mathbb{Z}_4$ have been widely studied [1, 5, 10, 12]. Recently two families of self orthogonal $\mathbb{Z}_4$ codes, type α and β simplex codes, have been studied [1]. Using these codes we construct MacDonald codes over $\mathbb{Z}_4$.

Binary MacDonald codes were introduced in [8] and q-ary version ($q \geq 3$) of these over finite fields were employed in [9] to solve a classical combinatorial problem. These codes and the generalized MacDonald codes have a natural geometrical representation as a projective multiset [3]. In [11] Tamari has shown that these codes are unique. Recently Honold and Landjev [6] have also shown that certain MacDonald codes are linearly representable over

*This work was partly supported by ARO grant DAAD19-01-1-0406

non-trivial chain rings using a selected class of multisets in projective Hjelmslev geometries. Another representation of these was found by Bhandari, Gupta and Lal in [1]. In this paper we consider Macdonald codes over $\mathbb{Z}_4$ and investigate some of their properties.

A *linear code* $\mathcal{C}$, of length n, over $\mathbb{Z}_4$ is an additive subgroup of $\mathbb{Z}_4^n$. An element of $\mathcal{C}$ is a *codeword of* $\mathcal{C}$ and a *generator matrix* of $\mathcal{C}$ is a matrix whose rows generate $\mathcal{C}$. The *Hamming weight* $w_H(x)$ of a vector x in $\mathbb{Z}_4^n$ is the number of non-zero components. The *Lee weight* $w_L(x)$ of a vector $x = (x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^n \min\{|x_i|, |4-x_i|\}$. The *Euclidean weight* $w_E(x)$ of a vector x is $\sum_{i=1}^n \min\{x_i^2, (4-x_i)^2\}$. The Euclidean weight is useful in connection with lattice constructions. The *Chinese Euclidean weight* $w_{CE}(x)$ of a vector $x \in \mathbb{Z}_m^n$ is $\sum_{i=1}^n \left\{2 - 2\cos\left(\frac{2\pi x_i}{m}\right)\right\}$. The Hamming, Lee and Euclidean distances $d_H(x,y)$, $d_L(x,y)$ and $d_E(x,y)$ between two vectors x and y are $w_H(x-y)$, $w_L(x-y)$ and $w_E(x-y)$, respectively. The minimum Hamming, Lee and Euclidean weights, d_H, d_L and d_E, of $\mathcal{C}$ are the smallest Hamming, Lee and Euclidean weights among all non-zero codewords of $\mathcal{C}$, respectively. The *Gray map* $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ is the coordinate-wise extension of the function from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ defined by $0 \to (0,0), 1 \to (0,1), 2 \to (1,1), 3 \to (1,0)$. The image $\phi(\mathcal{C})$ of a linear code $\mathcal{C}$ over $\mathbb{Z}_4$ of length n under the Gray map is a binary code of length $2n$.

The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as $\{x \in \mathbb{Z}_4^n \mid x \cdot y = 0 \text{ for all } y \in \mathcal{C}\}$ where $x \cdot y$ is the standard inner product of x and y. $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and $\mathcal{C}$ is *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

Two codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are *permutation-equivalent*.

In this paper we obtain two families of MacDonald codes over $\mathbb{Z}_4$ from $\mathbb{Z}_4$-simplex codes of type α and β, S_k^α and S_k^β. Some fundamental properties of these codes are studied. Section 2 contains some preliminaries and notation. Definitions of MacDonald codes are given in section 3. Section 4 describes their main properties. Section 5 gives conclusions.

2 Preliminaries and Notations

Any linear code $\mathcal{C}$ over $\mathbb{Z}_4$ is permutation-equivalent to a code with generator matrix G (the rows of G generate $\mathcal{C}$) of the form

$$G = \begin{bmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 0 & 2I_{k_1} & 2C \end{bmatrix} \tag{1}$$

where A, B_1, B_2 and C are matrices with entries 0 or 1 and I_k is the identity matrix of order k. One can associate two binary linear codes with $\mathcal{C}$. The *residue code* is

$$\mathcal{C}^{(1)} = \{\mathbf{c} \pmod 2 \mid \mathbf{c} \in \mathcal{C}\}$$

and the *torsion code* is

$$\mathcal{C}^{(2)} = \{\mathbf{c} \in \mathbb{Z}_2^n \mid 2\mathbf{c} \in \mathcal{C}\}.$$

If $k_1 = 0$ then $\mathcal{C}^{(1)} = \mathcal{C}^{(2)}$. For details and further references see [10],[12].

A vector $\mathbf{v}$ is a 2-*linear combination* of the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ if $\mathbf{v} = l_1\mathbf{v}_1 + \ldots + l_k\mathbf{v}_k$ with $l_i \in \mathbb{Z}_2$ for $1 \leq i \leq k$. A subset $S = \{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_k\}$ of $\mathcal{C}$ is a 2-*basis* for $\mathcal{C}$ if for each $i = 1, 2, ..., k-1$, $2\mathbf{v}_i$ is a $2-$linear combination of $\mathbf{v}_{i+1}, ..., \mathbf{v}_k$, $2\mathbf{v}_k = 0$, $\mathcal{C}$ is the 2-linear span of S and S is 2-linearly independent [1]. The number of elements in a 2-basis for $\mathcal{C}$ is the 2-*dimension* of $\mathcal{C}$.

It is easy to verify that the rows of the matrix

$$\mathcal{B} = \begin{bmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 2I_{k_0} & 2A & 2B_1 \\ 0 & 2I_{k_1} & 2C \end{bmatrix} \tag{2}$$

form a 2-basis for the code $\mathcal{C}$ generated by G given in (1).

A linear code $\mathcal{C}$ over $\mathbb{Z}_4$ (over $\mathbb{Z}_2$) of length n, 2-dimension k, minimum distance d_H, d_L and d_E is called an $[n, k, d_H, d_L, d_E]$ ($[n, k, d_H]$) or simply an $[n, k]$ code.

Let $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$ and let $\omega_j(\mathbf{c}) = |\{k \mid c_k = j\}|$. Then the correlation of $\mathbf{c} \in \mathcal{C}$ is defined as $\theta(\mathbf{c}) = (\omega_0(\mathbf{c}) - \omega_2(\mathbf{c})) + i(\omega_1(\mathbf{c}) - \omega_3(\mathbf{c}))$; where i $= \sqrt{-1}$ [10]. The symmetrized weight enumerator (swe) of $\mathcal{C}$ over $\mathbb{Z}_4$ is given by $swe(x, y, z) = \sum_{\mathbf{c}\in\mathcal{C}} x^{\omega_0(\mathbf{c})} y^{\omega_1(\mathbf{c})+\omega_3(\mathbf{c})} z^{\omega_2(\mathbf{c})}$[10].

3 Quaternary MacDonald Codes of Type α and β

Quaternary simplex codes of type α and β have been recently studied in [1]. A type α simplex code S_k^α is a linear code over $\mathbb{Z}_4$ with parameters $\left[2^{2k}, 2k, 2^{2k-1}, 2^{2k}, 3 \cdot 2^{2k-1}\right]$ and an inductive generator matrix given by

$$G_k^\alpha = \left[\begin{array}{c|c|c|c} 0\,0\cdots0 & 1\,1\cdots1 & 2\,2\cdots2 & 3\,3\cdots3 \\ \hline G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha \end{array}\right] \tag{3}$$

with G_1^α =[0 1 2 3]. A type β simplex code S_k^β is a punctured version of S_k^α with parameters $\left[2^{k-1}(2^k-1), 2k, 2^{2(k-1)}, 2^{k-1}(2^k-1), 2^k(3 \cdot 2^{k-2}-1)\right]$ and an inductive generator matrix given by

$$G_2^\beta = \left[\begin{array}{cccc|c|c} 1 & 1 & 1 & 1 & 0 & 2 \\ 0 & 1 & 2 & 3 & 1 & 1 \end{array}\right], \tag{4}$$

and for $k > 2$

$$G_k^\beta = \left[\begin{array}{c|c|c} 1\,1\cdots1 & 0\,0\cdots0 & 2\,2\cdots2 \\ \hline G_{k-1}^\alpha & G_{k-1}^\beta & G_{k-1}^\beta \end{array}\right], \tag{5}$$

where G^{α}_{k-1} is the generator matrix of S^{α}_{k-1}. For details the reader is referred to [1].

Now we define the MacDonald codes via the generator matrices of simplex codes. For $1 \leq u \leq k-1$, let $G^{\alpha}_{k,u}\left(G^{\beta}_{k,u}\right)$ be the matrix obtained from $G^{\alpha}_{k}\left(G^{\beta}_{k}\right)$ by deleting columns corresponding to the columns of $G^{\alpha}_{u}\left(G^{\beta}_{u}\right)$. i.e,

$$G^{\alpha}_{k,u} = \left[\begin{array}{c|c} G^{\alpha}_{k} & \backslash \frac{\mathbf{0}}{G^{\alpha}_{u}} \end{array}\right], \tag{6}$$

and

$$G^{\beta}_{k,u} = \left[\begin{array}{c|c} G^{\beta}_{k} & \backslash \frac{\mathbf{0}}{G^{\beta}_{u}} \end{array}\right], \tag{7}$$

where $[A \backslash B]$ denotes the matrix obtained from the matrix A by deleting the columns of the matrix B and $\mathbf{0}$ in (6) (resp.(7)) is a $(k-u) \times 2^{2u}$ (resp. $(k-u) \times 2^{u-1}(2^u-1)$) zero matrix.

The code $\mathcal{M}^{\alpha}_{k,u}\left(\mathcal{M}^{\beta}_{k,u}\right)$ generated by the matrix $G^{\alpha}_{k,u}\left(G^{\beta}_{k,u}\right)$ is the punctured code of $S^{\alpha}_{k}\left(S^{\beta}_{k}\right)$ and is a *MacDonald code*. The q-ary MacDonald code $\mathcal{M}_{k,u}(q)$ over the finite field $\mathbb{F}_q$ is a unique $\left[\frac{q^k-q^u}{q-1}, k, q^{k-1}-q^{u-1}\right]$ code in which every nonzero codeword has weight either q^{k-1} or $q^{k-1}-q^{u-1}$ [3].

4 Properties

In this section we summarize the main properties of $\mathbb{Z}_4$ MacDonald codes. $\mathcal{M}^{\alpha}_{k,u}$ is a code of length $n = 2^{2k} - 2^{2u}$ and 2-dimension $2k$ and $\mathcal{M}^{\beta}_{k,u}$ is a $\mathbb{Z}_4$ code of length $n = n(k,u) = 2^{2k-1} - 2^{2u-1} - 2^{k-1} + 2^{u-1} = (2^{k-1} - 2^{u-1})(2^k + 2^u - 1)$ and 2-dimension $2k$.

Lemma 1 *The torsion code of $\mathcal{M}^{\alpha}_{k,u}$ is a binary linear*

$$\left[2^{2k} - 2^{2u}, k, 2^{2k-1} - 2^{2u-1}\right]$$

two weight code with weight distribution $A_H(0) = 1$, $A_H(2^{2k-1} - 2^{2u-1}) = 2^{k-u}(2^u - 1)$ and $A_H(2^{2k-1}) = (2^{k-u} - 1)$.

Proof. The generator matrix of the torsion code can be obtained by replacing 2 by 1 in $2G^{\alpha}_{k,u}$. The result now follows easily (see [1]).

□

Remark 1 *The above torsion code has some zero columns.*

Lemma 2 *The torsion code of $\mathcal{M}^{\beta}_{k,u}$ is a binary*

$$\left[2^{k-1}\left(2^k - 1\right) - 2^{u-1}\left(2^u - 1\right), k, 2^{2k-2} - 2^{2u-2}\right]$$

two weight code with weight distribution $A_H(0) = 1$, $A_H(2^{2k-2} - 2^{2u-2}) = 2^{k-u}(2^u - 1)$ and $A_H(2^{2k-2}) = (2^{k-u} - 1)$.

Proof. Similar to the proof of Lemma 1.

□

Remark 2 *The torsion code of $\mathcal{M}_{k,u}^{\beta}$ includes optimal codes and codes meeting the Griesmer bound; for example, some values are given below.*

$\mathcal{M}_{k,u}^{\beta}$	$[n,k,d]$	Type of the code
$\mathcal{M}_{2,1}^{\beta}$	$[5,2,3]$	Optimal and Griesmer
$\mathcal{M}_{3,1}^{\beta}$	$[27,3,15]$	Optimal and Griesmer
$\mathcal{M}_{3,2}^{\beta}$	$[22,3,12]$	Optimal
$\mathcal{M}_{4,1}^{\beta}$	$[119,4,63]$	Optimal and Griesmer
$\mathcal{M}_{4,2}^{\beta}$	$[114,4,60]$	Optimal
$\mathcal{M}_{4,3}^{\beta}$	$[92,4,48]$	Optimal

Remark 3 *Each of the first $k-u$ rows of (6) has total number of units 2^{2k-1} and total number of non-zero divisors 2^{2k-2}. Further each of the last u rows has total number of units $2^{2k-1}-2^{2u-1}$ and total number of non-zero divisors $2^{2k-2}-2^{2u-2}$.*

We have a general result about the structure of the code.

Lemma 3 *Let $\mathbf{c} \in \mathcal{M}_{k,u}^{\alpha}, \mathbf{c} \neq 0$. If all the components of $\mathbf{c}$ are zero divisors then there are two type of codewords*

- *I:* $\omega_0(\mathbf{c}) = \omega_2(\mathbf{c}) = 2^{2k-1} - 2^{2u-1}$
- *II:* $\omega_0(\mathbf{c}) = 2^{2k-1} - 2^{2u}$ *and* $\omega_2(\mathbf{c}) = 2^{2k-1}$.

If at least one component of $\mathbf{c}$ is a unit then there are three type of codewords

- *III:* $\omega_1(\mathbf{c}) + \omega_3(\mathbf{c}) = 2^{2k-1} - 2^{2u-1}$ *and* $\omega_0(\mathbf{c}) = \omega_2(\mathbf{c}) = 2^{2k-2} - 2^{2u-2}$.
- *IV:* $\omega_1(\mathbf{c}) + \omega_3(\mathbf{c}) = 2^{2k-1}$ *and* $\omega_0(\mathbf{c}) = 2^{2k-2} - 2^{2u}, \omega_2(\mathbf{c}) = 2^{2k-2}$.
- *V:* $\omega_1(\mathbf{c}) + \omega_3(\mathbf{c}) = 2^{2k-1}$ *and* $\omega_0(\mathbf{c}) = \omega_2(\mathbf{c}) = 2^{2k-2} - 2^{2u-1}$.

Proof. The matrix (6) can also be written as

$$G_{k,u}^{\alpha} = \left[\begin{array}{c|c} G_{k,k-1}^{\alpha} & G_{k-1,u}^{\alpha} \end{array} \right].$$

Now the proof is by induction on k and is similar to the proof for S_k^{α} (see [1]).

□

The next theorem gives the Hamming and Lee weight distributions.

Theorem 1 *The Hamming and Lee weight distributions of* $\mathcal{M}_{k,u}^{\alpha}$ *are*

- $$\begin{array}{rcl} A_H(0) & = & 1 \\ A_H(2^{2k-1}-2^{2u-1}) & = & 2^{k-u}(2^u-1) \\ A_H(2^{2k-1}) & = & (2^{k-u}-1) \\ A_H(3\cdot 2^{2k-2}) & = & 2^{k-u}(2^{k-u}-1) \\ A_H(3(2^{2k-2}-2^{2u-2})) & = & 2^{2k-u}(2^u-1) \\ A_H(3\cdot 2^{2k-2}-2^{2u-1}) & = & 2^{k-u}(2^u-1)(2^{k-u}-1). \end{array}$$

- $A_L(0)=1, A_L(2^{2k}-2^{2u})=2^{2k-2u}(2^{2u}-1), A_L(2^{2k})=2^{2(k-u)}-1.$

Proof. By Lemma 3, each non-zero codeword of $\mathcal{M}_{k,u}^{\alpha}$ has Hamming weight either $2^{2k-1}-2^{2u-1}, 2^{2k-1}, 3\cdot 2^{2k-2}, 3(2^{2k-2}-2^{2u-2})$ or $3\cdot 2^{2k-2}-2^{2u-1}$ and Lee weight either $2^{2k}-2^{2u}$ or 2^{2k}. The counting of the weights followed by the weight distribution of the torsion code of $\mathcal{M}_{k,u}^{\alpha}$ (see Lemma 1) and the argument is similar to that used in [1, 2].

□

Theorem 2 *The image of* $\mathcal{M}_{k,u}^{\alpha}$ *under the Gray map is a non-linear*

$$\left(2^{2k+1}-2^{2u+1}, 2^{2k}, 2^{2k}-2^{2u}\right)$$

binary two weight code with possible weights $2^{2k}-2^{2u}$ *and* 2^{2k}.

Proof. Let u and v be the first and the second row of the generator matrix of $\mathcal{M}_{k,u}^{\alpha}$. If $\bar{u}$ and $\bar{v}$ denotes the reduction modulo 2. Then $2\bar{u}\star\bar{v}\notin\mathcal{M}_{k,u}^{\alpha}$, where $\star$ denotes the componentwise multiplication. The result follows from Proposition 3.16 (cf. page 46) of [12].

□

Theorem 3 *The image of* $\mathcal{M}_{k,u}^{\beta}$ *under the Gray map is a binary non-linear*

$$\left(2^{2k}-2^{2u}-2^k+2^u, 2^{2k}\right)$$

code.

Proof. Similar to the proof of Theorem 2. It can also be proved by induction on k.

□

5 Conclusions

In this paper we have introduced $\mathbb{Z}_4$ MacDonald codes and investigated some of their properties. These codes give rises to some optimal two weight binary codes and codes meeting the Griesmer bound. The geometrical properties of these codes related to multisets in projective Hjelmslev geometry over $\mathbb{Z}_4$ needs further investigation. It also appears interesting to prove the uniqueness of these codes. Other properties of these codes such as different weight hierarchies, 2-base images, and so on, will be reported elsewhere. One can also extend these ideas to a more general rings like $\mathbb{Z}_{p^s}$.

References

[1] M. C. Bhandari, M. K. Gupta and A. K. Lal. *On $\mathbb{Z}_4$ simplex codes and their gray images* Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-13, Lecture Notes in Computer Science **1719** (1999), 170–180.

[2] M. K. Gupta, *On Some Linear Codes over $\mathbb{Z}_{2^s}$*, PhD Thesis, Department of Mathematics, IIT Kanpur, India, (July 2000). 1–98.

[3] S. Dodunekov and J. Simonis. *Codes and projective multisets.* The Electronic Journal of Combinatorics **5** (1998) R37.

[4] S. T. Dougherty, M. Harada and P. Solé, *Shadow codes over $\mathbb{Z}_4$.* Finite Fields and Their Appl., **7** (2001) 507–529.

[5] A. R. Hammons, P. 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, **40** (1994), 301–319.

[6] T. Honold and I. Landjev. *Linear codes over finite chain rings.* The Electronic Journal of Combinatorics, **7** (2000) R11.

[7] I. N. Landjev. *The geometric approach to linear codes.* 2002, preprint.

[8] J. E. MacDonald. *Design methods for maximum minimum-distance error-correcting codes.* IBM Journal of Res. and Devlop. **4** (1960), 43–57.

[9] A. M. Patel. *Maximal q-ary linear codes with large minimum distance.* IEEE Trans. Inform. Theory, **21** (1975), 106–110.

[10] E. M. Rains and N. J. A. Sloane. *Self-Dual Codes* in V. Pless and W. C. Huffman (Eds.) **The Handbook of Coding Theory**. North-Holland, New York, 1998.

[11] F. Tamari. *On linear codes which attain the Solomon-Stiffler bound.* Disc. Math. **49** (1984) 179–191.

[12] Z. Wan. **Quaternary Codes**. World Scientific, Singapore, 1997.