Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 136–141*

Formally self-dual codes and Gray maps

Steven T. Dougherty prof.steven.dougherty@gmail.com
University of Scranton

Abstract. In this paper we investigate binary formally self-dual codes as images of codes over rings using various Gray maps.

1 Introduction

Formally self-dual binary codes are widely studied objects. Their importance comes from the fact that their weight enumerators are held invariant by the MacWilliams relations. Usually, however only even formally self-dual codes are studied. In this paper, we shall study formally self-dual binary codes, including odd codes, especially those that are the images of formally self-dual codes over rings via a Gray map. We begin with the necessary definitions.

A code of length n over a ring R is a subset of R^n. To R^n we attach the standard inner-product, namely $[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \overline{\mathbf{w}_i}$ where $\overline{\mathbf{w}_i}$ is an involution of the ring acting on $\mathbf{w}_i$. The involution can be the identity as well. We denote by $C^{\perp} = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \ \forall \mathbf{w} \in C\}$. If the ring is Frobenius we know that $|C||C^{\perp}| = |R|^n$. If $C = C^{\perp}$ then we say that the code is self-dual. Let C be a code over R and let wt be a weight defined over R. Then we define the weight enumerator with respect to that weight as $W_C(y) = \sum_{\mathbf{c} \in C} y^{wt(\mathbf{c})}$. If a code C satisfies $W_C(y) = W_{C^{\perp}}(y)$ then C is said to be formally self-dual with respect to that weight enumerator. In this paper, we shall be concerned with binary codes that are formally self-dual with respect to the Hamming weight enumerator and codes over rings that are formally self-dual with respect to the Lee weight enumerator.

We shall describe three Gray maps corresponding to these different rings. The first is the well known Gray map from $\mathbb{Z}_4 \to \mathbb{F}_2^2$ defined by $\phi_{\mathbb{Z}_4}(0) = (00), \phi_{\mathbb{Z}_4}(1) = (01), \phi_{\mathbb{Z}_4}(2) = (11), \phi_{\mathbb{Z}_4}(3) = (10)$, see [7] for a complete description. The second Gray map is associated with the ring

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle.$$

For $k = 1$, the Gray map is defined as $\phi_{R_1}(a + bu_1) = (b, a + b)$. Then the Gray map for R_k is defined recursively as: $\phi_{R_k}(a + bu_k) = (\phi_{R_{k-1}}(b), \phi_{R_{k-1}}(a) + \phi_{R_{k-1}}(b))$ where $a, b \in R_{k-1}$. For a complete description of codes over this family of rings see [5], [6]. The third Gray map is associated with the ring

$$A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle.$$

For $k = 1$, the Gray map is defined as $\phi_{A_1}(a + bv_1) = (a, a + b)$. Then the Gray map for A_k is defined recursively as: $\phi_{A_k}(a + bu_k) = (\phi_{A_{k-1}}(a), \phi_{A_{k-1}}(a) + \phi_{A_{k-1}}(b))$ where $a, b \in A_{k-1}$. For a complete description of codes over this family of rings see [3]. The maps ϕ_{R_k} and ϕ_{A_k} are linear but the map $\phi_{\mathbb{Z}_4}$ is not. Over a ring R a code is said to be linear if it is a submodule of R^n.

The simplest way to define the Lee weight in all of these cases is to say that the Lee weight of an element in these spaces is the Hamming weight of its binary image. It follows immediately that each of the Gray maps defined above are linear isometries from the Lee weight of that ring to the binary Hamming weight. Throughout this work, when we say formally self-dual code over $\mathbb{Z}_4$, A_k or R_k it is with respect to the Lee weights and for binary codes it is with respect to the Hamming weight. Combining the results in [1], [2], [3], [4], [6] we have the following.

Theorem 1. *If C is a formally self-dual code over $\mathbb{Z}_4, R_k$ or A_k then the image under the corresponding Gray map is a binary formally self-dual code.*

Over A_k, two inner-products are defined, namely the usual Euclidean inner-product and the Hermitian inner-product. The involution for the Hermitian inner product is defined by $\overline{v_i} = 1 + v_i$. It is shown that the image under the Gray map of a Euclidean self-dual code is a self-dual code and the image under the Gray map of a Hermitian self-dual code is a formally self-dual code. Likewise, for R_k the Gray map is linear so the image under this Gray map of a self-dual code is a self-dual code. For $\mathbb{Z}_4$, the Gray maps are not linear, so the images under the Gray map of a self-dual code need not be self-dual. In [4], the images of self-dual codes over $\mathbb{Z}_4$ for codes of length less than or equal to 9 are classified in terms of being self-dual or not.

A code C with the property $W_C(y) = W_{C^\perp}(y)$ is said to be formally self-dual with respect to that weight enumerator. A binary formally self-dual code with only even weights is said to be an even formally self-dual code and an odd formally self-dual code otherwise. A great deal of work has been done on even formally self-dual codes but much less has been done on odd formally self-dual codes. We shall extend this definition and say that a formally self-dual code in the spaces defined above is a code whose Lee weight enumerator is equal to the Lee weight enumerator of its orthogonal. Further, we say that it is an even formally self-dual code if all of the Lee weights are even and odd otherwise.

2 Binary formally self-dual codes

The following lemma is elementary.

Lemma 1. *Let C be a binary formally self-dual code and let $\mathbf{1}$ be the all one vector. Define the subcode $C_0 = \{\mathbf{v} \mid \mathbf{v} \in C, [\mathbf{v}, \mathbf{1}] = 0\}$. If C is even then $C = C_0$. If C is odd then C_0 has codimension 1 in C and consists of the even vectors of C.*

Proof. Any odd vector has inner-product 1 with $\mathbf{1}$ and any even code has inner-product 0 with $\mathbf{1}$. The result follows. □

We shall now give an alternate, much shorter, constructive and elementary proof of Theorem 3.1, Corollary 3.2, Theorem 3.5, Corollary 3.6, Theorem 3.7 and Corollary 3.8 in [8].

Theorem 2. *Let C be an odd formally self-dual binary code of even length n. Let C_0 be the subcode of even vectors. The code*

$$\overline{C} = \langle \{(0,0,\mathbf{c}) \mid \mathbf{c} \in C_0\} \cup \{(1,0,\mathbf{c}) \mid \mathbf{c} \in C - C_0\}, (1,1,\mathbf{1}) \rangle \tag{1}$$

is an even formally self-dual code of length $n+2$ with weight enumerator

$$W_{\overline{C}} = x^2 W_{C_{0,0}}(x,y) + xy W_{C_{1,0}}(x,y) + y^2 W_{C_{0,0}}(y,x) + xy W_{C_{1,0}}(y,x).$$

The code

$$\overline{C} = \langle \{(0,0,\mathbf{c}) \mid \mathbf{c} \in C_0\} \cup \{(1,1,\mathbf{c}) \mid \mathbf{c} \in C - C_0\}, (1,0,\mathbf{1}) \rangle \tag{2}$$

is an odd formally self-dual code of length $n+2$ with weight enumerator:

$$W_{\overline{C}} = x^2 W_{C_{0,0}}(x,y) + y^2 W_{C_{1,0}}(x,y) + xy W_{C_{0,0}}(y,x) + xy W_{C_{1,0}}(y,x).$$

Moreover, any code with these weight enumerators is a formally self-dual code.

Proof. Let C be an odd formally self-dual code. Then by the Lemma 1, there exists a vector $\mathbf{t}$ such that $C = \langle C_0, \mathbf{t} \rangle$, where C_0 is the subcode of even vectors. Then define $C_{\alpha,\beta} = C_0 + \alpha\mathbf{t} + \beta\mathbf{1}$. Let $C^{\perp} = D$ and let D_0 be the subcode of D of even vectors. Then there exists a vector $\mathbf{t}'$ such that $D = \langle D_0, \mathbf{t}' \rangle$. Then define $D_{\alpha,\beta} = D_0 + \alpha\mathbf{t}' + \beta\mathbf{1}$. We shall form two codes $\overline{C}$ and $\overline{D}$ that are orthogonals of each other and have the same weight enumerator. We let $\overline{C} = \bigcup(v_{\alpha,\beta}, C_{\alpha,\beta})$ and $\overline{D} = \bigcup(w_{\alpha,\beta}, D_{\alpha,\beta})$, where $(v_{\alpha,\beta}, C_{\alpha,\beta})$ is the set of all vectors in $C_{\alpha,\beta}$ with the vector $v_{\alpha,\beta}$ adjoined to the vector and $(w_{\alpha,\beta}, D_{\alpha,\beta})$ is defined likewise. For $\overline{C}$ and $\overline{D}$ to be orthogonal we need $[v_{\alpha,\beta}, w_{\alpha',\beta'}] = [C_{\alpha,\beta}, D_{\alpha,\beta}]$, where $[C_{\alpha,\beta}, D_{\alpha,\beta}]$ is the inner-product of any vector in $C_{\alpha,\beta}$ with any vector in $D_{\alpha,\beta}$. Notice $[C_{\alpha,\beta}, D_{\alpha,\beta}] = [c_0 + \alpha\mathbf{t} + \beta\mathbf{1}, d_0 + \alpha\mathbf{t}' + \beta\mathbf{1}] = \alpha\beta' + \alpha'\beta$, with $c_0 \in C_0$ and $d_0 \in D_0$. To insure linearity we need $v_{\alpha,\beta} = \alpha v_{1,0} + \beta v_{0,1}$ and $w_{\alpha,\beta} = \alpha w_{1,0} + \beta w_{0,1}$. Then using $v_{1,0} = (1,0), v_{0,1} = (1,1)$ and $w_{1,0} = (0,1), v_{0,1} = (1,1)$ gives the code in Equation 1. It is elementary that $W_{C_{\alpha,\beta}} = W_{D_{\alpha,\beta}}$. Moreover the weight enumerator of $\overline{C}$ and $\overline{D}$ is $W_{\overline{C}} = x^2 W_{C_{0,0}}(x,y) + xy W_{C_{1,0}}(x,y) + y^2 W_{C_{0,0}}(y,x) + xy W_{C_{1,0}}(y,x)$. Therefore we have that the code $\overline{C}$ and $\overline{D}$ are formally self-dual, it is even since each vector has an even vector adjoined to it and every odd vector has an odd vector adjoined to it. Since this weight enumerator is invariant under

the action of the MacWilliams relations, any code with this weight enumerator is a formally self-dual code.

The remaining proofs are identical, all that is required is to say what $v_{\alpha,\beta}$ and $w_{\alpha,\beta}$ are. For the code in Equation 2, we have $v_{1,0} = (1,1)$, $v_{0,1} = (1,0)$ and $w_{1,0} = (1,1)$, $w_{0,1} = (0,1)$. □

3 Gray images of formally self-dual codes

In this section, we shall investigate formally self-dual codes over rings with a Gray map to the binary space.

Theorem 3. *There exist odd formally self-dual codes of all lengths over A_k for all k.*

Proof. It is shown in [3] that $\langle v_i \rangle$ is a Hermitian self-dual code of length 1 for all i and for all k. Moreover, the Lee weight of v_i is 1 and hence odd. This gives that there are odd formally self-dual codes for all lengths. □

Lemma 2. *The direct product of formally self-dual codes over a ring R is a formally self-dual code.*

Proof. Let C and D be formally self-dual codes with respect to weight enumerator $W_C(y)$. It follows that $W_C(y) = W_{C^\perp}(y)$ and $W_D(y) = W_{D^\perp}(y)$. Then $W_{C\times D}(y) = W_C(y)W_D(y) = W_{C^\perp}(y)W_{D^\perp}(y) = W_{C^\perp \times D^\perp}(y)$. Noticing that $(C \times D)^\perp = C^\perp \times D^\perp$, we have that $C \times D$ is a formally self-dual code. □

Theorem 4. *Linear odd formally self-dual codes exist over $\mathbb{Z}_4$ and R_k for all lengths greater than 1.*

Proof. We show the result for $\mathbb{Z}_4$ first. It is easy to see that there are no linear odd formally self-dual codes of length 1 since the only linear codes or length 1 are the ideals of $\mathbb{Z}_4$. For length 2 the code generated by $(1,0)$ is an odd formally self-dual code. This follows since it is equivalent to its orthogonal. Using direct products we get that there are odd formally self-dual codes for all even lengths. For length 3 the code generated by $(1,0)$ and the self-dual code generated by (2) is an odd formally self-dual code of length 3 by Lemma 2. The proof for codes over R_k is similar, noting that we replace the self-dual code $\langle 2 \rangle$ of length one with the self-dual code $\langle u_i \rangle$ in R_k, see [5]. □

We let $\mathbf{2}$ be the all 2 vector in $\mathbb{Z}_4^n$, $\mathbf{u_1 u_2 \dots u_k}$ be the all $u_1 u_2 \dots u_k$ vector in R_k^n and $\mathbf{1}$ be the all one-vector (over any ring). Note that the Gray image of these vectors is the binary all-one vector.

Theorem 5. *Let C be a formally self-dual code. The code C is even over $\mathbb{Z}_4$ if and only if $\mathbf{2} \in C$. The code C is even over R_k if and only if $\mathbf{u_1 u_2 \dots u_k} \in C$. The code C is even over A_k if and only if $\mathbf{1} \in C$.*

Proof. We note that if a vector over $\mathbb{Z}_4$ has odd Lee weight then it has an odd number of ± 1 in its coordinates. Then its inner-product with $\mathbf{2}$ is 2. If it has an even Lee weight then it has an even number of ± 1 in its coordinates. Then it is orthogonal to $\mathbf{2}$. Hence if the code is even then all of the vectors are orthogonal to $\mathbf{2}$. This implies that $\mathbf{2} \in C^{\perp}$. However, since the code is formally self-dual then $\mathbf{2} \in C$ since this is the only vector that has Lee weight $2n$. The proof for R_k and A_k are the same noticing that the Gray image of $\mathbf{u_1 u_2 \dots u_k}$ and $\mathbf{1}$ are the binary all-one vector. □

Lemma 3. *Let C be an odd formally self-dual code over $\mathbb{Z}_4$ or R_k then the subcode of even vectors has index 2 in C.*

Proof. Let C be an odd formally self-dual code over $\mathbb{Z}_4$ or R_k. Then let $C_0 = \{\mathbf{c} \mid [\mathbf{c}, \mathbf{2}] = 0\}$ for codes over $\mathbb{Z}_4$ and $C_0 = \{\mathbf{c} \mid [\mathbf{c}, \mathbf{u_1 u_2 \dots u_k}] = 0\}$ for codes over R_k. Then it is clear that these codes are subcodes. Now if a vector over $\mathbb{Z}_4$ has odd weight then its inner product with $\mathbf{2}$ is 2. Notice that if $\mathbf{c}$ has inner-product weight 2 with $\mathbf{2}$ then $[3\mathbf{c}, \mathbf{2}] = 3[\mathbf{c}, \mathbf{2}] = 2$. Hence there is one coset of C_0 consisting of all odd-vectors. For R_k we have the same result, noticing that the inner-product of $\mathbf{u_1 u_2 \dots u_k}$ with any odd vector is $u_1 u_2 \dots u_k$. Any other element α we have $[\alpha\mathbf{c}, \mathbf{u_1 u_2 \dots u_k}] = \alpha u_1 u_2 \dots u_k$. This product is either 0 or $u_1 u_2 \dots u_k$. Hence, there are two cosets. □

Consider the code generated by $(1, 0)$ over A_1. The subcode of even vectors is $\{(0, 0), (1, 0)\}$, but this subcode is not linear, since, for example, $v_1(1, 0) = (v_1, 0)$ is not in the code. Hence over A_k the subcode of even vectors is not necessarily linear.

Notice then that we cannot mimic the construction in Theorem 2. Since, for example, over $\mathbb{Z}_4$ we would have that $v_{\alpha,\beta}$ would be length 1. Then $[C_{\alpha,\beta}, D_{\alpha',\beta'}] = 2(\alpha\beta' + \alpha'\beta)$ so $v_{\alpha,\beta}$ and $w_{\alpha,\beta}$ would have to be 0 or 2, but then $[v_{1,0}, w_{0,1}]$ would need to be 2, giving a contradiction. The same situation occurs over R_k.

For the next theorem we need to extend the definition of the Lee weight enumerator. That is for a code C define $W_C(x, y) = \sum_{\mathbf{c} \in C} x^{2^k n - wt(\mathbf{c})} y^{wt(\mathbf{c})}$. Notice, this is precisely the Hamming weight enumerator of the binary image of the code under the Gray map. If C is a code then D is a neighbor of C if they share a subcode C_0 and there exists vectors $\mathbf{c}$ and $\mathbf{d}$ with $C = \langle C_0, \mathbf{c} \rangle$ and $D = \langle D_0, \mathbf{d} \rangle$.

Theorem 6. *Let C be an odd formally self-dual code over A_k or $\mathbb{Z}_4$ of length n. Then C is a neighbor of an even formally self-dual code.*

Proof. Let C be an odd formally self-dual code over $\mathbb{Z}_4$ and let C_0 be the subcode of even vectors. Let $D = C^{\perp}$ and let D_0 be the subcode of D of even vectors. Then we notice that $W_{C_0}(x, y) = W_{D_0}(x, y)$. Let $\overline{C} = \langle C_0, \mathbf{2} \rangle$ and $\overline{D} = \langle D_0, \mathbf{2} \rangle$. Then $W_{\overline{C}}(x, y) = W_C(x, y) + W_C(y, x) = W_{\overline{D}}(x, y)$. If $\mathbf{c} \in \overline{C}$ and

$\mathbf{d} \in \overline{D}$ then $[\mathbf{c}, \mathbf{d}] = [\mathbf{c}_0 + \alpha\mathbf{2}, \mathbf{d}_0 + \alpha\mathbf{2}] = 0$. Since $|\overline{C}| = |\overline{D}|$ then $\overline{C}^{\perp} = \overline{D}$. Then $\overline{C}$ is an even formally self-dual code. The same proof applies for R_k replacing $\mathbf{2}$ with $\mathbf{u_1 u_2 \dots u_k}$. □

The major importance of these codes is that formally self-dual codes over R_k produce binary formally self-dual codes that have k distinct automorphisms and that formally self-dual codes over $\mathbb{Z}_4$ produce non-linear formally self-dual codes which may have higher minimum distance than any linear formally self-dual codes. Codes over A_k are important in that a formally self-dual code over A_k can be constructed using any 2^{k-1} binary codes, see [3] for details.

Acknowledgement The author is thankful to Stefka Bouyuklieva, Yasemin Cengellenmis, Cristina Fernandez-Cordoba and Yoonjin Lee for helpful comments.

References

[1] M. Bilal, J. Borges, S. T. Dougherty, C. Fernández-Córdoba, Maximum Distance Separable Codes over Z_4 and $Z_2 \times \mathbb{Z}4$, *Des. Codes Cryptogr.*, **61**, No. 1, 31–40, 2011.

[2] J. Borges, C. Fernandez-Cordoba, S. T. Dougherty, Self-Dual Codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$, in submission.

[3] Y. Cengellenmis and A. Dertli, Cyclic and Skew Cyclic Codes over an Infinite Family of Rings with a Gray Map, in submission.

[4] C. Fernandez-Cordoba, S. T. Dougherty, Codes over $\mathbb{Z}_{2^k}$, Gray maps and Self-Dual Codes, *Advances in Mathematics of Communication*, **5**, No. 4, 571–588, 2011.

[5] S.T. Dougherty, B. Yildiz and S. Karadeniz, Self-Dual Codes over R_k and Binary Self-Dual Codes, in submission.

[6] S.T. Dougherty, B. Yildiz and S. Karadeniz, Codes over R_k, Gray Maps and their Binary Images, *Finite Fields Appl.*, **17**, No. 3, 205–219, 2011.

[7] 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, *I*EEE Trans. Inform. Theory, **40**, 301–319, 1994.

[8] S. Han, H. Lee, Y. Lee, Binary Formally Self-Dual Odd Codes, *Des. Codes Cryptogr.*, **61**, 141–150, 2011.