Bull. Korean Math. Soc. **55** (2018), No. 2, pp. 341–357
https://doi.org/10.4134/BKMS.b160842
pISSN: 1015-8634 / eISSN: 2234-3016

ADDITIVE SELF-DUAL CODES OVER FIELDS OF EVEN ORDER

Steven T. Dougherty, Jon-Lark Kim, and Nari Lee

Abstract. We examine various dualities over the fields of even orders, giving new dualities for additive codes. We relate the MacWilliams relations and the duals of $\mathbb{F}_{2^{2s}}$ codes for these various dualities. We study self-dual codes with respect to these dualities and prove that any subgroup of order 2^s of the additive group is a self-dual code with respect to some duality.

1. Introduction

In classical coding theory, the primary alphabet for codes has been finite fields. In particular, it is the finite fields of even order that have received the most attention because of their application in electronic communication. Codes over these alphabets have generally been defined as vector spaces over these fields. Recently in coding theory, the number of useful alphabets has increased dramatically, especially to finite Frobenius rings. This generalization occurred because the MacWilliams Theorems extended to this family of rings but no further. In this paper, we shall generalize the classical setting in a slightly different way. Namely, we shall be largely concerned with additive codes. That is, we are concerned with codes which are subgroups of $\mathbb{F}_q^n$ in terms of the additive structure of the space rather than being vector spaces over the field. We then define a duality based on the structure of the additive code. This allows for a wider range of dualities and for more self-dual codes. Additive self-dual codes have numerous applications in mathematics. Recently, they have found application in secret sharing schemes; see [4] for example.

We introduce definitions and notations that we use throughout this paper in Section 2 and describe new dualities for the additive groups in a generalized setting in Section 3. We also relate the MacWilliams relations and the duals of

Received October 19, 2016; Revised November 12, 2017; Accepted November 22, 2017.
2010 *Mathematics Subject Classification.* Primary 11T71, 94B05.
Key words and phrases. additive codes, Hermitian inner-product, trace inner-product, self-dual codes.
J.-L. Kim was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1B03933259).

codes for the dualities in Section 4. The dualities obtained by the four inner-products for fields of even orders are described in Section 5. We also apply building-up constructions which were used only for linear self-dual codes to additive self-dual codes to construct self-dual codes in Section 6.

2. Definitions and notations

The *trace function* $Tr : \mathbb{F}_{2^r} \to \mathbb{F}_2$ is defined to be

$$Tr(a) = a + a^2 + a^4 + \cdots + a^{2^{r-1}}. \tag{1}$$

It is well known that $Tr(\alpha a + \beta b) = \alpha Tr(a) + \beta Tr(b)$, where α and β are in $\mathbb{F}_2$.

If r is even, we let $r = 2k$ and define an involution on the finite field as $\overline{a} = a^{2^k}$. Then $\overline{\overline{a}} = (a^{2^k})^{2^k} = a^{2^r} = a$.

We say that a code is *additive* if it is a subgroup of the additive group of $\mathbb{F}_{2^r}$. If the code is a vector space, then we say that the code is *linear*. It is immediate that a code can be additive without being linear; for example the subgroup $\{0, 1\}$ is an additive code over $\mathbb{F}_{2^r}$, $r > 1$, of length 1 and is not linear.

We have four standard inner-products found in the existing literature for fields of characteristic 2, defined as follows. The first is the standard Euclidean inner-product:

$$[\mathbf{v}, \mathbf{w}]_E = \sum v_i w_i. \tag{2}$$

Also, $[\alpha\mathbf{v}, \mathbf{w}]_E = [\mathbf{v}, \alpha\mathbf{w}]_E$ implying $[\alpha\mathbf{v}, \mathbf{w}]_E = 0$ if and only if $[\mathbf{v}, \alpha\mathbf{w}]_E = 0$ for any $\alpha \in \mathbb{F}_{2^r}$.

The second is the Hermitian inner-product:

$$[\mathbf{v}, \mathbf{w}]_H = \sum v_i \overline{w_i}. \tag{3}$$

Also, $[\alpha\mathbf{v}, \mathbf{w}]_H = [\mathbf{v}, \bar{\alpha}\mathbf{w}]_H$ implying $[\alpha\mathbf{v}, \mathbf{w}]_H = 0$ if and only if $[\mathbf{v}, \bar{\alpha}\mathbf{w}]_H = 0$ for any $\alpha \in \mathbb{F}_{2^r}$.

The third is the trace inner-product:

$$[\mathbf{v}, \mathbf{w}]_T = Tr(\sum v_i w_i). \tag{4}$$

Also, $[\alpha\mathbf{v}, \mathbf{w}]_T = [\mathbf{v}, \alpha\mathbf{w}]_T$ implying $[\alpha\mathbf{v}, \mathbf{w}]_T = 0$ if and only if $[\mathbf{v}, \alpha\mathbf{w}]_T = 0$ for any $\alpha \in \mathbb{F}_{2^r}$.

The fourth is the trace Hermitian inner-product:

$$[\mathbf{v}, \mathbf{w}]_{TH} = Tr(\sum v_i \overline{w_i}). \tag{5}$$

Also, $[\alpha\mathbf{v}, \mathbf{w}]_{TH} = [\mathbf{v}, \bar{\alpha}\mathbf{w}]_{TH}$ implying $[\alpha\mathbf{v}, \mathbf{w}]_{TH} = 0$ if and only if $[\mathbf{v}, \bar{\alpha}\mathbf{w}]_{TH} = 0$ for any $\alpha \in \mathbb{F}_{2^r}$.

We can define an orthogonal based on each of these inner-products. Let C be a code over $\mathbb{F}_{2^r}$ (not necessarily additive). Then

$$C^E = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}]_E = 0, \ \forall \ \mathbf{w} \in C\}, \tag{6}$$

$$C^H = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}]_H = 0, \ \forall \ \mathbf{w} \in C\}, \tag{7}$$

$$C^T = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}]_T = 0, \ \forall \ \mathbf{w} \in C\}, \tag{8}$$

$$C^{TH} = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}]_{TH} = 0, \ \forall \ \mathbf{w} \in C\}. \tag{9}$$

Of course, the Hermitian inner-product and trace Hermitian inner-product and their corresponding orthogonals are only defined when r is even. We can apply these inner-products to linear codes but we can also extend this application to additive codes. We note that each of these orthogonals are additive whether or not C is.

Lemma 2.1. *Assume C is a linear code. Then $C^E = C^T$ and if r is even, then $C^H = C^{TH}$.*

Proof. It is relatively easy to show that each of the inner-products is non-degenerate by looking at vectors which are zero on all but one coordinate and using the fact that the trace map is not identically zero. Since the inner-products are non-degenerate, if C is a linear code over $\mathbb{F}_{2^r}$ of length n, then the orthogonal code C^X where $X \in \{E, H, T, TH\}$ satisfies $|C| \cdot |C^X| = 2^{rn}$ [10]. It is also immediate that $C^E \subseteq C^T$ and $C^H \subseteq C^{TH}$ since $Tr(0) = 0$. Thus using the above equality, we have that $|C^E| = |C^T| = |C^H| = |C^{TH}|$, implying that $C^E = C^T$ and if r is even, then $C^H = C^{TH}$. □

Example 2.2. Of course, when the code is not linear, the previous result is false. Consider the trivial example of the additive code $C = \{0, 1\}$ of length 1 over $\mathbb{F}_4$. Then $C^E = C^H = \langle C \rangle^E = \{0\}$ but $C^T = C^{TH} = \{0, 1\}$.

In this section, we have defined dual codes under four inner-products. We say that we have a *duality from inner-products* to describe the scenario that yields these dual codes. In the next section, we will define dual codes that arise from group characters. In Sections 4 and 5, we will explore the connection between these two types of duality.

3. Codes over groups

We now study dualities of codes over additive abelian groups G derived from the dual group $\widehat{G}$ of G. The results of this section apply for example, to the case that G is the additive group of $\mathbb{F}_{2^r}$.

Recall that a character of G is a homomorphism from G to the multiplicative group of the complex numbers.

There is a bijective correspondence between the elements of G and those of $\widehat{G} = \{\pi \mid \pi \text{ a character of } G\}$. For each $\alpha \in G$ denote the corresponding character by χ_α.

Definition. A *code C over G of length n* is a subset of G^n and C is said to be *additive* if it is an additive subset of G^n.

We could say that the code is linear over the group but we prefer to use the term linear when the alphabet is a ring and reserve additive for when we only consider the algebraic properties of the additive group.

Given this setup, we say that a *duality from group characters* is given by a bijection $M : \alpha \to \chi_\alpha$ between G and $\widehat{G}$ and an associated orthogonality defined as follows.

Definition. For a code C over G of length n, define the *dual code under the duality* $M : \alpha \to \chi_\alpha$ by $C^M = \{(g_1, g_2, \ldots, g_n) \in G^n \,|\, \Pi_{i=1}^n \chi_{g_i}(c_i) = 1 \text{ for all } (c_1, c_2, \ldots, c_n) \in C\}$.

Because there are many different bijections between G and $\widehat{G}$, there are many different dualities associated with a given group. The duality M will be identified with a matrix we also call M, as we shall see later in this section. We will see in Sections 4 and 5 under what circumstances the dual codes defined from inner-products in Section 2 can be viewed as special cases of the dual codes defined by dualities over abelian groups examined in this section.

Notice that in Example 2.2, we are not applying the orthogonality given by the duality but rather the duality given by Equation (6), Equation (7), Equation (8) and Equation (9). Hence, strictly applying the duality orthogonality rather than the duality given in the equations will give a different orthogonal for these codes.

We associate an element of $\widehat{G^n}$ with an element of G^n with the natural correspondence, and since $(\widehat{G})^n = \widehat{G^n}$, the code C^M is associated with the set $\{\chi \in \widehat{G^n} \,|\, \chi(c) = 1 \text{ for all } c \in C\}$.

To produce the MacWilliams relations for these codes we will need the following well known lemmas. We will also need the following definitions. For a function $f : G \to A$, where A is a complex algebra, the Fourier Transform $\widehat{f}$ of f is a function $\widehat{f} : \widehat{G} \to A$ defined by:

$$\widehat{f}(\pi) = \sum_{x \in G} \pi(x) f(x). \tag{10}$$

Let $(\widehat{G} : H) = \{\pi \in \widehat{G} \,|\, \pi|_H = 1\}$, where H is a subgroup of G.

Lemma 3.1 (Poisson summation formula [10])**.** *Let G be a finite abelian group and H a subgroup of G. For every $a \in G$,*

$$\sum_{x \in H} f(a + x) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G} : H)} \pi(-a) \widehat{f}(\pi). \tag{11}$$

Lemma 3.2 ([10])**.** *Suppose $f_i : G \to A$ are functions, $i = 1, 2, \ldots, n$ and A a complex algebra. Let $f : G^n \to A$ be given by*

$$f(y_1, \ldots, y_n) = \prod_{i=1}^n f_i(y_i).$$

Then $\widehat{f} = \prod \widehat{f}_i$; *i.e., if* $\pi = (\pi_1, \ldots, \pi_n)$ *in* $\widehat{G^n} = \prod_{i=1}^n \widehat{G}$, *then* $\widehat{f}(\pi) = \prod_{i=1}^n \widehat{f}_i(\pi_i)$.

For the remainder of this section, let G have order s and let its elements be denoted by α_j for $j = 0, 1, \ldots, s-1$, with $\alpha_0 = 0$. To each $\alpha \in G$ associate a set of s independent indeterminates x_α. We will sometimes denote x_{α_j} by x_j. Let A be the complex algebra $\mathbb{C}[x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{s-1}}] = \mathbb{C}[x_0, x_1, \ldots, x_{s-1}]$. Let $f : G^n \to A$ be given by

$$f(y_1, y_2, \ldots, y_n) = \Pi_{i=1}^n x_{\alpha_{y_i}}.$$

As in Lemma 3.2, if $y = (y_1, y_2, \ldots, y_n) \in G^n$, $f(y) = \Pi_{i=1}^n f_i(y_i)$ where $f_i : G \to A$ with $f_i(y_i) = x_{\alpha_{y_i}}$. Let C be a code over G of length n. The *complete weight enumerator of* C is defined to be

$$W_C(x_0, x_1, \ldots, x_{s-1}) = \sum_{c \in C} f(c).$$

The composition of $c = (c_1, \ldots, c_n) \in G^n$, denoted by *comp*$(c)$, is $(z_0, z_1, \ldots, z_{q-1})$ where $z_i = z_i(c)$ is the number of components c_i equal to α_i. Clearly

$$\sum_{i=0}^{q-1} z_i = n.$$

For Theorem 3.3, we need to define the MacWilliams relations first. For a matrix M let

$$M \cdot (x_0, x_1, \ldots, x_{s-1}) = (M(x_0, x_1, \ldots, x_{s-1})^t)^t.$$

Theorem 3.3. *Let* C *be an additive code over* G, $|G| = s$, *with complete weight enumerator* $W_C(x_0, x_1, \ldots, x_{s-1})$. *Then the complete weight enumerator of the orthogonal is given by*:

$$W_{C^M}(x_0, x_1, \ldots, x_{s-1}) = \frac{1}{|C|} W_C(M \cdot (x_0, x_1, \ldots, x_{s-1})).$$

Proof. The proof follows in a manner similar to the standard proof as given on page 144 of [9]. Let C be a code and let c be a codeword of C. Let c_i be the i-th coordinate of a codeword c.

Define the function $f_i(c_i) = x_{c_i}$ and $f(c) = \prod_{i=1}^n f_i(c_i)$. In other words, it is giving the monomial corresponding to this vector in the complete weight enumerator.

Then we have

$$\widehat{f}(\chi_c) = \sum_{v \in G^n} \chi_c(v) x_0^{z_0(c)} x_1^{z_1(c)} \cdots x_{s-1}^{z_{s-1}(c)} \tag{12}$$

$$= \prod_{r=0}^{s-1} \left(\sum_{i=0}^{s-1} \chi_{\alpha_r}(\alpha_i) x_i \right)^{z_r(c)}. \tag{13}$$

Then apply Lemma 3.1 and Equation (11), using C as the subgroup H and G^n as the group in that lemma with a equal to the identity, and we have:

$$\sum_{x\in C} f(x) = \frac{1}{|(\widehat{G^n} : C)|} \sum_{\pi\in(\widehat{G^n}:C)} \widehat{f}(\pi).$$

Then using Lemma 3.2 we have that $\widehat{f}(\pi) = \sum_{x\in C} \pi(x)f(x)$ gives that the action of the matrix M on the weight enumerator gives us the MacWilliams relations, where M is defined as follows:

$$M_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\alpha_j). \qquad \square$$

The next definition applies only if the group G has an involution. Next fix an additive involution of the group G (if it exists). That is, the involution is a map $\alpha \to \bar{\alpha}$ from G to G with $\overline{\alpha+\beta} = \overline{\alpha} + \overline{\beta}$ and $\bar{\bar{\alpha}} = \alpha$. Then define the following Hermitian type orthogonality.

Definition. For a code C over G of length n, define

$$C^{MH} = \{(g_1, g_2, \ldots, g_n) \,|\, \prod_{i=1}^{i=n} \chi_{g_i}(\overline{c_i}) = 1 \text{ for all } (c_1, \ldots, c_n) \in C\}.$$

With the same proof as above we have that the action of the matrix MH on the weight enumerator gives us the MacWilliams relations, where MH is defined as follows:

$$(MH)_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\overline{\alpha_j}). \tag{14}$$

This gives the following theorem.

Theorem 3.4. *Let C be an additive code of length n over G , with $|G| = s$ and complete weight enumerator $W_C(x_0, x_1, \ldots, x_{s-1})$. Then the complete weight enumerator of the orthogonal C^{MH} is given by*:

$$W_{C^{MH}}(x_0, x_1, \ldots, x_{s-1}) = \frac{1}{|C|} W_C(MH \cdot (x_0, x_1, \ldots, x_{s-1})). \tag{15}$$

We define the ordinary *weight enumerator* of C to be the following homogeneous polynomial:

$$\mathcal{W}_C(x) = \sum_{i=0}^{n} A_i(C) x^i y^{n-i},$$

where $A_i(C)$ denotes the number of vectors of weight i in C.

Corollary 3.5. *Let C be an additive code over a group G with $|G| = s$. Fix a duality M and a Hermitian duality MH. Then*

$$\mathcal{W}_{C^M}(x, y) = \frac{1}{|C|} \mathcal{W}_C(x + (s-1)y, x - y) \tag{16}$$

and

$$\mathcal{W}_{C^{MH}}(x, y) = \frac{1}{|C|} \mathcal{W}_C(x + (s-1)y, x - y). \tag{17}$$

Corollary 3.6. *Let C be an additive code of length n over an additive group G of order s. Fix a duality M and a Hermitian duality MH. Then*

$$|C||C^M| = |G|^n \tag{18}$$

and

$$|C||C^{MH}| = |G|^n. \tag{19}$$

Proof. In Corollary 3.5, let $x = y = 1$ and we have $|C^M| = \frac{1}{|C|}s^n$ which gives $|C^M||C| = |G|^n$. The proof is identical for C^{MH}. □

Corollary 3.7. *Let C be an additive code of length n over an additive group G of order s. Fix a duality M. Then*

$$C = (C^M)^M. \tag{20}$$

Proof. We know that $C \subseteq (C^M)^M$. Therefore by applying Corollary 3.6, we have that $C = (C^M)^M$. □

If K is a subgroup of G, then K is a non-trivial code of length 1. By the above corollary, we have $|K||K^M| = |G|$.

Example 3.8. Note here that Example 2.2 does not contradict this corollary as that example uses the orthogonality given by the inner-products and not by the orthogonality given by the group's character table. The two orthogonals are only necessarily equal when the code is linear, not if the code is merely additive.

It is also possible to obtain Corollary 3.6 and the previous statement by realizing that C^M is isomorphic to $\widehat{G^n/C}$. Hence the cardinality of C^M is the number of cosets of C in G^n.

4. MacWilliams relations

In this section, we shall apply the results on complete weight enumerators given in Section 3 to the four inner-products of Section 2 yielding the traditional MacWilliams relations. MacWilliams relations for codes over fields were first given in MacWilliams' landmark works (see [7] and [8]).

In [2], the MacWilliams relations for C^{TH} and C^T are given. We shall state them in a slightly different manner. Notice that our definition of χ is different but the proof is the same. The MacWilliams relations for the other two weight enumerators are well known, see [9] for example.

Let M_E, M_H, M_T and M_{TH} be 2^r by 2^r matrices with elements from the complex numbers defined as follows. Let $\mathbb{F}_{2^r} = \mathbb{F}_2[x]/\langle p_r(x)\rangle$ where $p_r(x)$ is an irreducible polynomial over $\mathbb{F}_2$ of degree r. Let $\chi : \mathbb{F}_{2^r} \to \mathbb{C}$, $\chi(b_0 + b_1x + b_2x^2 + \cdots + b_{r-1}x^{r-1}) = (-1)^{\sum b_i}$. Then

$$(M_E)_{a,b} = \chi(ab), \tag{21}$$

$$(M_H)_{a,b} = \chi(a\bar{b}), \tag{22}$$

$$(M_T)_{a,b} = \chi_{\mathbb{F}_2}(Tr(ab)), \tag{23}$$

$$(M_{TH})_{a,b} = \chi_{\mathbb{F}_2}(Tr(a\bar{b})), \tag{24}$$

where $\chi_{\mathbb{F}_2}(0) = 1$ and $\chi_{\mathbb{F}_2}(1) = -1$.

Then we can state the MacWilliams relations as follows. For a matrix M let

$$M \cdot (x_0, x_1, \ldots, x_{2^r-1}) = (M(x_0, x_1, \ldots, x_{2^r-1})^t)^t$$

so that the result is a row vector with 2^r elements. Also cwe_C is defined to be W_C for $G = \mathbb{F}_{2^r}$ as a group under addition.

Theorem 4.1. *If C is a linear code over $\mathbb{F}_{2^r}$, then*

$$cwe_{C^T}(x_0, x_1, \ldots, x_{2^r-1}) = \frac{1}{|C|} cwe_C(M_T \cdot (x_0, x_1, \ldots, x_{2^r-1})), \tag{25}$$

$$cwe_{C^{TH}}(x_0, x_1, \ldots, x_{2^r-1}) = \frac{1}{|C|} cwe_C(M_{TH} \cdot (x_0, x_1, \ldots, x_{2^r-1})), \tag{26}$$

$$cwe_{C^H}(x_0, x_1, \ldots, x_{2^r-1}) = \frac{1}{|C|} cwe_C(M_H \cdot (x_0, x_1, \ldots, x_{2^r-1})), \tag{27}$$

and

$$cwe_{C^E}(x_0, x_1, \ldots, x_{2^r-1}) = \frac{1}{|C|} cwe_C(M_E \cdot (x_0, x_1, \ldots, x_{2^r-1})). \tag{28}$$

Proof. Follows immediately from Theorem 3.3 and Theorem 3.4. □

Example 4.2. For $\mathbb{F}_2$ there is only one duality, namely $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. We explicitly give the matrixes for $\mathbb{F}_4$, using the ordering $0, 1, \omega, 1+\omega$ for the indices of the matrix:

$$M_E = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}, M_H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}, \tag{29}$$

$$M_T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}, M_{TH} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{30}$$

It is well known that a finite field is a Frobenius ring. Hence the MacWilliams relations given in [10] for the Euclidean orthogonal hold in this case. Specifically, it is shown that the matrix M_E, as we have defined it, gives the MacWilliams relations as long as the function χ is a generating character of $\widehat{R}$ where R is a ring and $\widehat{R}$ is the character module of R as a module over itself. In [1], Corollary 3.6 states the following, which is given as Lemma 4.1 in [10]. We state it in terms of commutative rings.

Lemma 4.3. *A character of a finite commutative ring R is a generating character of $\widehat{R}$ if and only if* $\ker(\chi)$ *contains no nonzero ideals.*

This means that the MacWilliams relations for the complete weight enumerator are given by a matrix M if $M_{a,b} = \tau(ab)$ where τ is a generating character for the ring R.

The standard MacWilliams relations for finite fields uses the character χ as defined above. Consider the function $\sigma : \mathbb{F}_{2^r} \to \mathbb{C}^*$, where $\mathbb{C}^*$ is the non-zero complex numbers, defined by $\sigma(a) = \chi(Tr(a))$. Then $\sigma(a+b) = \chi_{\mathbb{F}_2}(Tr(a+b)) = \chi_{\mathbb{F}_2}(Tr(a)+Tr(b)) = \chi_{\mathbb{F}_2}(Tr(a))\ \chi_{\mathbb{F}_2}(Tr(b)) = \sigma(a)\sigma(b)$. Hence, it is a character and moreover its kernel contains no non-trivial ideals. This implies that the MacWilliams relations using M_T are also MacWilliams relations for the Euclidean weight enumerator (provided the code is linear). The same can be said for M_{TH} and the Hermitian inner-product.

5. Self-dual and formally self-dual codes

Throughout this section our codes are additive codes over $\mathbb{F}_{2^r}$ and the orthogonals are always the orthogonal given by the duality of the underlying group not the inner-product used on fields. Let C^M be the orthogonal of a code C with a given duality M. Then C is a *self-dual* code with respect to this duality if and only if $C = C^M$ and *self-orthogonal* if $C \subseteq C^M$. An element is self-orthogonal if its inner-product with itself with respect to a duality is 1. The code C is *formally self-dual* if C has the same weight distribution and as its dual C^M. Note that the usual inner-product has the field as the image but in our case the inner-product has its image in $\mathbb{C}$; hence we want the inner-product to be 1 and not 0 to be self-orthogonal.

Theorem 5.1. *If r is odd, then there are no additive self-dual codes of length one under any duality.*

Proof. Let C^M be the orthogonal under some duality. Then we have that $|C||C| = |C||C^M| = |\mathbb{F}_{2^r}|$, by Corollary 3.6. This gives that $|C|^2 = 2^r$ and so 2^r must be a square. If r is odd, then 2^r is not a square and we have the result. □

The proof of the following lemma is standard.

Lemma 5.2. *Let C and D be additive self-dual (formally self-dual) codes of length n and m respectively. Then $C \times D$ is an additive self-dual (formally self-dual) code of length $n+m$.*

Theorem 5.3. *The code $C = \{(\alpha, \alpha) \mid \alpha \in \mathbb{F}_{2^r}\}$ is an additive self-dual code of length 2 with respect to all dualities.*

Proof. For any (α, α) and (β, β) in C we have

$$\chi_\alpha(\beta)\chi_\alpha(\beta) = \chi_\alpha(\beta)^2 = 1$$

since $\chi_\alpha(\beta) = \pm 1$ as $\mathbb{F}_{2^r}$ under addition is an elementary abelian 2-group. Hence the code is self-orthogonal with respect to any duality. As $|C| = |\mathbb{F}_{2^s}|$, we have the result. □

This leads to the following corollary.

Corollary 5.4. *Given any duality on the field $\mathbb{F}_{2^r}$, there are self-dual codes of all even lengths.*

Proof. The result follows immediately from Theorem 5.3 and Lemma 5.2. □

5.1. The principal dualities for the field extended to the group

We shall now describe the dualities given by the four usual inner-products for fields of even order as extended to a duality for the additive group of the finite field. We shall denote by C^E, C^H, C^T, and C^{TH} the duals of the additive code C given in Section 2, and denote by M_E, M_H, M_T, and M_{TH} the matrices given in Equations (21) through (24) in Section 4; if the field under consideration is $\mathbb{F}_4$, these matrices are given in Example 4.2.

Example 5.5. Consider the duality for the additive group of $\mathbb{F}_4$ given by the matrix M_E in Equation (29). Using this as the duality for the additive group of $\mathbb{F}_4$ we have that $\chi_\omega(\omega) = 1$. This gives that $\{0, \omega\}$ is a self-dual code of length 1. Notice, of course, that this code is not a self-dual code over the field with the Euclidean inner-product but it is a self-dual code over the additive group with the prescribed duality. This expands the number of ways we can extend the notion of duality for additive codes. Namely, we are not restricted to the trace and the trace Hermitian but rather we can get self-dual codes for a variety of inner-products.

Example 5.6. Consider the Hermitian duality given by the matrix M_H in Equation (29). With this duality, there are no self-dual codes of length 1. Given the duality for M_T given in Equation (30), the code $\{0, 1\}$ is a self-dual code of length 1. Consider the Trace Hermitian duality given in Equation (30); then $\{0, 1\}$, $\{0, \omega\}$ and $\{0, \omega^2\}$ are all self-dual codes of length 1.

Example 5.7. Notice that M_E and M_T provide the same MacWilliams relations for linear codes over $\mathbb{F}_4$. They do not provide the same MacWilliams relations for additive codes. Consider the code of length 1, $C = \{0, \omega\}$. Since C is not linear, we cannot use the MacWilliams relations in Theorem 4.1 but Theorem 3.3. Using M_E the MacWilliams relations give the weight enumerator of the orthogonal as $x_0 + x_\omega$. Using M_T the MacWilliams relations give the weight enumerator as $x_0 + x_{\omega^2}$. This is only possible since the code C in question is not a linear code over $\mathbb{F}_4$ but rather only an additive code over the group.

Example 5.8. Consider the duality given by M_E, as given in Equation (21), for $\mathbb{F}_{16} = \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle$. The codes $\{0, x+1, x^2, x^2+x+1\}$ and $\{0, x^2x^3 +$

$x^2 + x^3\}$ are self-dual codes of length 1 with respect to the duality given by the matrix M_E. The codes $\{0, 1, x, x + 1\}$ and $\{0, 1, x^2, x^2 + 1\}$ are self-dual with respect to M_T.

Theorem 5.9. *Let M_E be a duality on the additive group of $\mathbb{F}_{2^r}$ be given by Equation* (21)*, and let C^{M_E} be the orthogonal based on this duality. If C is linear, then $C^E = C^{M_E}$.*

Proof. Let $\mathbf{w} \in C^E$. Then for all $\mathbf{v} \in C$ we have $\sum v_i w_i = 0$. This gives $\prod \chi_{v_i}(w_i) = \prod \chi(v_i w_i) = \chi(\sum v_i w_i) = \chi(0) = 1$. Then $C^E \subseteq C^M$. Furthermore, $|C||C^E| = |C||C^M| = |\mathbb{F}_{2^r}^n|$ when they are linear [10], which gives that the two sets have the same cardinality and hence are equal. □

The following theorem has the same proof; simply replace w_i with $\overline{w_i}$.

Theorem 5.10. *Let M_H be the duality on the additive group of $\mathbb{F}_{2^r}$ be given by Equation* (22)*, and let C^{M_H} be the orthogonal based on this duality. If C is linear, then $C^H = C^{M_H}$.*

Theorem 5.11. *For the duality M_E, there are 2^{r-1} self-orthogonal elements in $\mathbb{F}_{2^r}$.*

Proof. For any non-trivial character of $\mathbb{F}_{2^r}$, half the elements map to 1 and half to -1 as the character is a surjective homomorphism onto $\{-1, 1\}$. Thus half the elements, i.e., 2^{r-1} elements are self-orthogonal. □

In $\mathbb{F}_4$, both 0 and $1 + \omega$ have corresponding vectors with even weight and $0^2 = 0$ and $\omega^2 = 1 + \omega$. Therefore, 0 and ω are self-orthogonal elements of $\mathbb{F}_4$ with respect to M_E.

Theorem 5.12. *For the duality M_T, there are 2^{r-1} self-orthogonal elements in $\mathbb{F}_{2^r}$.*

Proof. The proof is similar to that of Theorem 5.11. □

Theorem 5.13. *There exists additive self-dual codes of all lengths over $\mathbb{F}_4$ for the duality given by M_E, M_T and M_{TH}.*

Proof. Follows directly from Lemma 5.2 and the codes in Examples 5.5 and 5.6. □

5.2. The duality M_r

Let $\mathbb{F}_{2^r}$ be the finite field of order 2^r. We have that $\mathbb{F}_{2^r} = \mathbb{F}_2[x]/\langle p_r(x)\rangle$ where $p_r(x)$ is an irreducible polynomial over $\mathbb{F}_2$ of degree r. Then every element can be written as $a_0 + a_1 x + \cdots + a_{r-1}x^{r-1}$ with $a_i \in \mathbb{F}_2$ for $0 \leq i \leq r-1$. Define $\chi_r(a_0 + a_1 x + \cdots + a_{r-1}x^{r-1}) = (-1)^{a_{r-1}}$.

Lemma 5.14. *The map χ_r is a generating character for $\widehat{\mathbb{F}_{2^r}}$.*

Proof. First

$$\begin{aligned}&\chi_r(a_0 + a_1x + \cdots + a_{r-1}x^{r-1} + b_0 + b_1x + \cdots + b_{r-1}x^{r-1})\\ &= (-1)^{a_{r-1}+b_{r-1}} = (-1)^{a_{r-1}}(-1)^{b_{r-1}}\\ &= \chi_r(a_0 + a_1x + \cdots + a_{r-1}x^{r-1})\chi_r(b_0 + b_1x + \cdots + b_{r-1}x^{r-1}).\end{aligned}$$

Therefore it is a character. As a field has no nontrivial ideals, by Lemma 4.3 χ_r is either a generating character or the trivial character. Because $\chi_r(x^{r-1}) = -1$, χ_r is nontrivial and hence is a generating character. □

Define $(M_r)_{a,b} = \chi_r(ab)$ where a, b are elements of $\mathbb{F}_{2^r}$. This defines a duality on $\mathbb{F}_{2^r}$. Notice that this character gives M_T for $\mathbb{F}_4$. Since it is a generating character, this can also be used to give the MacWilliams relations for the Euclidean dual.

Theorem 5.15. *Let C be the code of length 1 over $\mathbb{F}_{2^{2s}}$, $C = \{(a_0 + a_1x + \cdots + a_{2s-1}x^{2s-1}) \mid a_i = 0$ if $i \geq s\}$. Then C is a self-dual code of length 1 with respect to the duality M_{2s}.*

Proof. First we note that $|C| = 2^s$ and $2^s2^s = 2^{2s}$; so it has the proper cardinality. We note that the sum of two polynomials with degree at most $s-1$ is again a polynomial of degree at most $s-1$ and so it is an additive code.

Note that the product of two polynomials of degree at most $s-1$ is a polynomial of degree at most $2s-2$. Hence $(M_{2s})_{a,b} = \chi_{2s}(ab) = 1$ for all $a, b, \in C$. Hence the code is self-orthogonal and therefore self-dual. □

Corollary 5.16. *There exist self-dual codes of all lengths for the duality M_{2s}.*

Proof. Simply apply Lemma 5.2. □

Theorem 5.17. *Let G be the additive group of $\mathbb{F}_2^{2s}$. Let H be any subgroup of order 2^s. Then H is a self-dual code with respect to some duality.*

Proof. Consider the duality given by M_{2s} and let C be the self-dual code in Theorem 5.15 of length 1 with respect to the duality M_{2s}. The code C has additive generators $c_1, c_2, \ldots, c_s$ and let $d_1, d_2, \ldots, d_s$ be the generators that extends this basis to $\mathbb{F}_{2^{2s}}$. Let $c'_1, c'_2, \ldots, c'_s$ be the additive generators of H and let $d'_1, d'_2, \ldots, d'_s$ be the generators that extends this basis to $\mathbb{F}_{2^{2s}}$. Define a group isomorphism Ψ where $\Psi(c_i) = c'_i$ and $\Psi(d_i) = d'_i$. Then Ψ is a group automorphism of the additive group of $\mathbb{F}_{2^{2s}}$. Let $\chi = \chi_{M_{2s}} \circ \Psi$. Then χ is a duality of the additive group of $\mathbb{F}_{2^{2s}}$. Then H is a self-dual code of length 1 with respect to the duality of χ. □

5.3. The duality M_v

We shall now exhibit another duality for all fields $\mathbb{F}_{2^{2s}}$ which has additive self-dual codes for length 1. For each element α in $\mathbb{F}_{2^{2s}}$, let $\mathbf{v}_\alpha$ be the vector

in $\mathbb{F}_2^{2s}$ associated to the element formed by the coefficients of the polynomial of α. Let $[\mathbf{v}_\alpha, \mathbf{v}_\beta]$ be the ordinary inner-product of $\mathbf{v}_\alpha$ and $\mathbf{v}_\beta$. Define

$$\chi_\alpha(\beta) = (-1)^{[\mathbf{v}_\alpha, \mathbf{v}_\beta]}. \tag{31}$$

We have the following for $\alpha, \alpha' \in \mathbb{F}_{2^s}$:

$$\begin{aligned}\chi_\alpha(\beta)\ \chi_{\alpha'}(\beta) &= (-1)^{[\mathbf{v}_\alpha, \mathbf{v}_\beta]}(-1)^{[\mathbf{v}_{\alpha'}, \mathbf{v}_\beta]} \\ &= (-1)^{[\mathbf{v}_{\alpha+\alpha'}, \mathbf{v}_\beta]} \\ &= \chi_{\alpha+\alpha'}(\beta).\end{aligned}$$

Hence this is a character of $\mathbb{F}_{2^s}$.

Let $(M_v)_{\alpha,\beta} = \chi_\alpha(\beta)$. Let C be a self-dual code in $\mathbb{F}_2^{2s}$. Then $C' = \{\alpha \mid \mathbf{v}_\alpha \in C\}$ be a self-dual code of length 1 with respect to M_v. This gives the following theorem.

Theorem 5.18. *There exists self-dual codes of length* 1 *for* M_v *for all* $\mathbb{F}_{2^{2s}}$.

For $\mathbb{F}_4$, the duality is given by

$$M_{TH} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{32}$$

Here a self-dual code of length 2 over $\mathbb{F}_2$ is $\{(00), (11)\}$ which corresponds to the self-dual code of length 1 given by $C' = \{0, 1 + \omega\}$.

5.4. Formally self-dual codes

A code is said to be *formally self-dual* with respect to a weight enumerator if the code and its orthogonal have the same weight enumerator.

Given the results in Lemma 2.1, we have the following.

Theorem 5.19. *A linear code is trace formally self-dual with respect to the complete weight enumerator if and only if it is Euclidean formally self-dual with respect to the complete weight enumerator. A linear code is trace Hermitian formally self-dual with respect to the complete weight enumerator if and only if it is Hermitian formally self-dual with respect to the complete weight enumerator.*

Example 5.20. The code $\{(0,0), (0,1), (1,0), (1,1)\}$ over $\mathbb{F}_4$, which has complete weight enumerator $x_0^2 + 2x_0x_1 + x_1^2$, is additive. It is also trace and Hermitian trace formally self-dual with respect to the complete weight enumerator. It is neither Hermitian nor Euclidean formally self-dual since it is not a linear code. Note that the dual of the code is $\{(0,0)\}$ under either the Euclidean or Hermitian inner-products. It is easy to check that the code is actually self-dual under either trace or Hermitian trace inner-products.

The code $\langle(1, \omega)\rangle$ over $\mathbb{F}_4$ is formally self-dual with respect to all four inner-products with complete weight enumerator $x_0^2 + x_1x_\omega + x_\omega x_{\omega^2} + x_1x_{\omega^2}$. It is not self-dual with respect to any of the inner-products; so it is possible to have

non self-dual codes which are formally self-dual with respect to the complete weight enumerator for all four inner-products.

6. Building-up construction

Building-up constructions for linear self-dual codes over various finite fields were studied in [3], [5], and [6]. In this section, we give building-up constructions for trace and trace Hermitian self-dual additive codes over $\mathbb{F}_{2^r}$ discussed in Section 2 so that trace and trace Hermitian self-orthogonal codes can be obtained.

We note that $|\{y \in \mathbb{F}_{2^r} : Tr(y) = 1\}| = 2^{r-1}$. Similarly, $|\{y \in \mathbb{F}_{2^r} : Tr(\bar{y}) = 1\}| = 2^{r-1}$.

Theorem 6.1. *Let C_T be an $(n, 2^{\frac{rn}{2}}, d_T)$ trace self-dual additive code with a generator matrix G_T over $\mathbb{F}_{2^r}$, where $\frac{rn}{2}$ is an integer. Suppose that a_0 is a nonzero element of $\mathbb{F}_{2^r}$ and that $\mathbf{x} \in \mathbb{F}_{2^r}^n$ is a vector such that $[\mathbf{x}, \mathbf{x}]_T = Tr(a_0)$. Let $a_i \in \mathbb{F}_{2^r}$ such that $Tr(a_0 a_i) = [\mathbf{x}, \mathbf{g_i}]_T$, where $\mathbf{g_i}$ denotes the i-th row of G_T and $1 \le i \le \frac{rn}{2}$. Then the following matrix G_{T_O} generates an $(n+2, 2^{\frac{rn}{2}+1}, d_{T_O})$ trace self-orthogonal additive code C_{T_O} with $d_{T_O} \le d_T + 2$. If $r = 1$, then C_{T_O} is an $(n+2, 2^{\frac{n+2}{2}}, d_{T_O})$ trace self-dual additive code.*

$$G_{T_O} = \left(\begin{array}{c|cc} & a_{\frac{rn}{2}} & a_{\frac{rn}{2}} \\ G_T & \vdots & \vdots \\ & a_2 & a_2 \\ & a_1 & a_1 \\ \hline \mathbf{x} & a_0 & 0 \end{array}\right). \tag{33}$$

Proof. It is easy to see that C_{T_O} has cardinality $2^{\frac{rn}{2}+1}$. It is also clear that the bottom row of G_{T_O} is orthogonal to itself since $[\mathbf{x}, \mathbf{x}]_T = Tr(a_0)$. Note that the first $\frac{rn}{2}$ rows of G_{T_O} are orthogonal to each other. That is,

$$[(\mathbf{g_i}|a_i a_i), (\mathbf{g_j}|a_j a_j)]_T = 0 + [(a_i a_i), (a_j a_j)]_T = 0.$$

Now it remains to show that the bottom row of G_{T_O} is orthogonal to any other rows of G_{T_O}. Since $Tr(a_0 a_i) = [\mathbf{x}, \mathbf{g_i}]_T$,

$$[(\mathbf{x}|a_0 0), (\mathbf{g_i}|a_i a_i)]_T = [\mathbf{x}, \mathbf{g_i}]_T + [(a_0 0), (a_i a_i)]_T = Tr(a_0 a_i) + Tr(a_0 a_i) = 0$$

in $\mathbb{F}_2$ for $1 \le i \le \frac{rn}{2}$. This completes the proof. □

Example 6.2. Let α be a root of a primitive polynomial $x^3 + x + 1$ in $\mathbb{F}_2[x]$. The following is a generator matrix G_T for a $(2, 2^3, 1)$ trace self-dual additive code over $\mathbb{F}_{2^3}$.

$$G_T = \begin{pmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha^4 \\ 1 & 1 \end{pmatrix}. \tag{34}$$

Let $a_0 = \alpha^5 \in \mathbb{F}_{2^3}$. We adjoin the row $\mathbf{x} = (\alpha^2\alpha^3)$ which satisfies $[\mathbf{x}, \mathbf{x}]_T = 1 = Tr(\alpha^5)$. Then

$$G_{T_O} = \left(\begin{array}{cc|cc} \alpha & \alpha^2 & \alpha^3 & \alpha^3 \\ \alpha^2 & \alpha^4 & \alpha^5 & \alpha^5 \\ 1 & 1 & \alpha^2 & \alpha^2 \\ \hline \alpha^2 & \alpha^3 & \alpha^5 & 0 \end{array}\right). \tag{35}$$

Since the rows of G_T satisfy that $Tr(a_0 a_i) = [\mathbf{x}, \mathbf{g_i}]_T$ for $i = 1, 2, 3$, G_{T_O} generates a $(4, 2^4, 2)$ trace self-orthogonal additive code.

Theorem 6.3. *Let C_T be an $(n, 2^{\frac{rn}{2}}, d_T)$ trace self-dual additive code with a generator matrix G_T over $\mathbb{F}_{2^r}$, where $\frac{rn}{2}$ is an integer. Suppose that a is a nonzero element of $\mathbb{F}_{2^r}$ and $\mathbf{x} \in \mathbb{F}_{2^r}^n$ a vector such that $[\mathbf{x}, \mathbf{x}]_T = Tr(a)$. Let $b \in \mathbb{F}_{2^r}$ such that $Tr(ab) = 1$ and $Tr(b) = 0$. Suppose that a zero is placed when $[\mathbf{x}, \mathbf{g_i}]_T = 0$ and b is placed when $[\mathbf{x}, \mathbf{g_i}]_T = 1$, where $\mathbf{g_i}$ denotes the i-th row of G_T and $1 \le i \le \frac{rn}{2}$. Then the following matrix G_{T_E} generates an $(n+1, 2^{\frac{rn}{2}+1}, d_{T_E})$ trace self-orthogonal additive code C_{T_E} with $d_{T_E} \le d_T + 1$. If $r = 2$, then C_{T_E} is an $(n+1, 2^{n+1}, d_{T_E})$ trace self-dual additive code.*

$$G_{T_E} = \left(\begin{array}{c|c} & 0 \\ G_T & or \\ & b \\ \hline \mathbf{x} & a \end{array}\right). \tag{36}$$

Proof. It is easy to see that C_{T_E} has cardinality $2^{\frac{rn}{2}+1}$. It is also clear that the bottom row of G_{T_E} is orthogonal to itself since $[\mathbf{x}, \mathbf{x}]_T = Tr(a)$. Note that the first $\frac{rn}{2}$ rows of G_{T_E} are orthogonal to each other as $Tr(b^2) = Tr(b) = 0$.

Now it remains to show that the bottom row of G_{T_E} is orthogonal to any other rows of G_{T_E}.

If $[\mathbf{x}, \mathbf{g_i}]_T = 0$, then

$$[(\mathbf{x}|a), (\mathbf{g_i}|0)]_T = [\mathbf{x}, \mathbf{g_i}]_T + Tr(a \cdot 0) = 0.$$

If $[\mathbf{x}, \mathbf{g_i}]_T = 1$, then

$$[(\mathbf{x}|a), (\mathbf{g_i}|b)]_T = [\mathbf{x}, \mathbf{g_i}]_T + Tr(a \cdot b) = 0$$

in $\mathbb{F}_2$ for $1 \le i \le \frac{rn}{2}$. This completes the proof. □

Example 6.4. Let α be a root of a primitive polynomial $x^4 + x + 1$ in $\mathbb{F}_2[x]$. The following is a generator matrix G_T for a $(1, 2^2, 1)$ trace self-dual additive code over $\mathbb{F}_{2^4}$.

$$G_T = \begin{pmatrix} 1 \\ \alpha \end{pmatrix}. \tag{37}$$

Let $a = \alpha^6 \in \mathbb{F}_{2^4}$. We adjoin the row $\mathbf{x} = (\alpha^3)$ which satisfies $[\mathbf{x}, \mathbf{x}]_T = 1 = Tr(\alpha^6)$. Then

$$G_{T_E} = \left(\begin{array}{c|c} 1 & \alpha^5 \\ \alpha & 0 \\ \hline \alpha^3 & \alpha^6 \end{array}\right). \tag{38}$$

Note that $b = \alpha^5$ satisfies that $Tr(ab) = Tr(\alpha^{11}) = 1$ and $Tr(b) = Tr(\alpha^5) = 0$. Thus we obtain a $(2, 2^3, 1)$ trace self-orthogonal additive code over $\mathbb{F}_{2^4}$ which is generated by G_{T_E}.

Theorem 6.5. *Let C_{TH} be an $(n, 2^{\frac{rn}{2}}, d_{TH})$ trace Hermitian self-dual additive code with a generator matrix G_{TH} over $\mathbb{F}_{2^r}$ for an even r. Suppose that a is a nonzero element of $\in \mathbb{F}_{2^r}$ and $\mathbf{x} \in \mathbb{F}_{2^r}^n$ a vector such that $[\mathbf{x}, \mathbf{x}]_{TH} = Tr(\bar{a})$. Here $\bar{a}$ denotes the conjugate of a. Let $b \in \mathbb{F}_{2^r}$ such that $Tr(a\bar{b}) = 1$ and $Tr(\bar{b}) = 0$. Then the following matrix G_{TH_E} generates an $(n+1, 2^{\frac{rn}{2}+1}, d_{TH_E})$ trace Hermitian self-orthogonal additive code C_{TH_E} with $d_{TH_E} \leq d_{TH} + 1$ if b is adjoined when $[\mathbf{x}, \mathbf{g_i}]_{TH} = 1$ and 0 when $[\mathbf{x}, \mathbf{g_i}]_{TH} = 0$ for $1 \leq i \leq \frac{rn}{2}$. Here $\mathbf{g_i}$ denotes the i-th row of G_{TH}. If $r = 2$, then C_{TH_E} is an $(n+1, 2^{n+1}, d_{TH_E})$ trace Hermitian self-dual additive code.*

$$G_{TH_E} = \left(\begin{array}{c|c} & 0 \\ G_{TH} & or \\ & b \\ \hline \mathbf{x} & a \end{array}\right). \tag{39}$$

Proof. The proof is similar to that of Theorem 6.3. □

Example 6.6. Let α be a root of a primitive polynomial $x^6 + x^4 + x^3 + x + 1$ in $\mathbb{F}_2[x]$. The following is a generator matrix for a $(1, 2^3, 1)$ trace Hermitian self-dual additive code over $\mathbb{F}_{2^6}$.

$$G_{TH} = \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}. \tag{40}$$

Let $a = \alpha^{25} \in \mathbb{F}_{2^6}$. If we adjoin the row $\mathbf{x} = (\alpha^{29})$ which satisfies $[\mathbf{x}, \mathbf{x}]_{TH} = 1 = Tr(\alpha^{25})$, then

$$G_{TH_E} = \left(\begin{array}{c|c} 1 & \alpha^{15} \\ \alpha & \alpha^{15} \\ \alpha^2 & 0 \\ \hline \alpha^{29} & \alpha^{25} \end{array}\right). \tag{41}$$

Note that $b = \alpha^{15}$ satisfies that $Tr(a\bar{b}) = Tr(\alpha^{19}) = 1$ and $Tr(\bar{b}) = Tr(\alpha^{57}) = 0$. Now we obtain a $(2, 2^4, 1)$ trace Hermitian self-orthogonal additive code over $\mathbb{F}_{2^6}$ which is generated by G_{TH_E}.

References

[1] H. L. Claasen and R. W. Goldbach, *A field-like property of finite rings*, Indag. Math. (N.S.) **3** (1992), no. 1, 11–26.

[2] W. C. Huffman, *On the theory of $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes*, Adv. Math. Commun. **7** (2013), no. 3, 349–378.

[3] J.-L. Kim, *New extremal self-dual codes of lengths 36, 38, and 58*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 386–393.

[4] J.-L. Kim and N. Lee, *Secret sharing schemes based on additive codes over $GF(4)$*, AAECC (2016). doi:10.1007/s00200-016-0296-5.

[5] J.-L. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A **105** (2004), no. 1, 79–95.

[6] ———, *An efficient construction of self-dual codes*, Bull. Korean Math. Soc. **52** (2015), no. 3, 915–923.

[7] F. J. MacWilliams, *Combinatorial Problems of Elementary Group Theory*, Ph.D. thesis, Harvard University, 1961.

[8] ———, *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. **42** (1963), 79–94.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. I*, North-Holland Publishing Co., Amsterdam, 1977.

[10] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18518, USA
Email address: marinmersennedeparis@gmail.com

Jon-Lark Kim
Department of Mathematics
Sogang University
Seoul 04107, Korea
Email address: ctryggoggo1@gmail.com

Nari Lee
Department of Mathematics
Sogang University
Seoul 04107, Korea
Email address: narilee3@gmail.com