

Additive G -Codes over $\mathbb{F}_q$ and their Dualities

S.T. Dougherty^a, C. Fernández-Córdoba^b

^a*Department of Mathematics, University of Scranton*

^b*Department of Information and Communications Engineering, Universitat Autònoma de Barcelona*

Abstract

We define additive G -codes over finite fields. We prove that if C is an additive G -code over $\mathbb{F}_q$ with duality M then its dual with respect to this duality C^M is an additive G -code. We prove that if M and M' are two dualities, then C^M and $C^{M'}$ are equivalent codes. Finally, we study the existence of self-dual codes for a variety of dualities and relate them to formally self-dual and linear self-dual codes.

Keywords: additive codes, G -codes, self-dual codes

2000 MSC: 94B25, 94B60

1. Introduction

In this paper, we shall consider additive G -codes over finite fields. In [9], linear G -codes over finite Frobenius rings were studied by examining ideals in the corresponding group ring RG . The rank, kernel and self-duality were studied for the particular case of codes in $\mathbb{Z}_4G$ in [6]. In [8], [9] and [12], group ring constructions were used to construct self-dual codes over rings and fields. Special attention was given to self-dual codes over the infinite family of rings R_k , with an eye to their image as binary self-dual codes. In [7], group rings with infinite rings were used to study finite codes that were ideals in group rings by examining the projection of ideals in the infinite group ring to finite codes.

Here, we expand on these ideas by examining codes which are additive rather than linear and whose alphabet is a finite field. Additive codes have applications in quantum coding and in cryptography and have received a great deal of attention lately.

Additive codes were first defined by Delsarte in 1973 in terms of association schemes [3], [4], where the set of points X in the association scheme is endowed with the structure of an abelian group. In general, an additive code, in a translation association scheme, is defined as a subgroup of the underlying abelian group. In classical theory coding, the primary alphabet for codes has been finite fields. On one hand, additive codes over finite fields have become more important recently due to their application to the construction of quantum error-correcting codes given in [2]. On the other hand, in the last years, the used alphabet has been extended to finite Frobenius rings, and also the product

of finite Frobenius Rings. In this sense, additive codes over rings have become more relevant [1],[15]. Additive codes also allow for a variety of dualities to be used (see [10], [11] for example). We shall examine these various dualities, focusing on codes which are equal to their dual under specific dualities.

The family of cyclic codes is one of the most widely studied family of codes, firstly over finite fields and later over Frobenius rings. Cyclic codes of length n over R can be seen as ideals in the group ring RC_n , where C_n is the cyclic group of order n . As a generalization of cyclic codes the so called additive G-codes are ideals in an arbitrary group ring RG [14], [7], [9].

We begin with the necessary definitions and notations. We denote the finite field of order $q = p^e$, p a prime, by $\mathbb{F}_q$.

A code over a finite field $\mathbb{F}_q$ of length n is a subset of $\mathbb{F}_q^n$. If the code is a subspace then we say that it is a linear code. If it is an additive subgroup of $\mathbb{F}_q^n$, then we say that it is an additive code. Any additive code over a field of prime order is necessarily a linear code. However, additive codes need not be linear. For example, the field $\mathbb{F}_p$ is a non-trivial additive code of length 1 in $\mathbb{F}_{p^e}$, $e > 1$, but there are no non-trivial linear codes of length 1 over a field.

For any two vectors $\mathbf{v} = (v; 1, \dots, v_n)$, $\mathbf{w} = (w_1, \dots, w_n) \in \mathbb{F}_q^n$, define the Hamming distance to be $d_H(\mathbf{v}, \mathbf{w}) = |\{i \mid v_i \neq w_i\}|$. The Hamming weight of a vector is the number of non-zero coordinates of the vector and corresponds to $d_H(\mathbf{v}, \mathbf{0})$, where $\mathbf{0}$ denotes the all-zero vector. The minimum Hamming weight of a code is the smallest weight of all non-zero vectors and the minimum Hamming distance is the minimum of $\{d_H(\mathbf{v}, \mathbf{w}) \mid \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}$. For any code C the Hamming weight enumerator is defined as

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n - wt_H(\mathbf{c})} y^{wt_H(\mathbf{c})}.$$

Since the finite field $\mathbb{F}_q$, $q = p^e$, is a vector space over $\mathbb{F}_p$ of dimension e , each element of $\mathbb{F}_q$ can be written as

$$a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{e-1}\zeta^{e-1}, \quad (1)$$

for some ζ . We let K_i be the i dimensional subspace of this vector space formed by letting $a_j = 0$, for $j > i - 1$ in the representation given in Equation 1. Namely,

$$K_i = \{a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{e-1}\zeta^{e-1} \mid a_j = 0 \text{ if } j > i - 1\}. \quad (2)$$

Lemma 1.1. *Let $q = p^e$, p a prime, and let $K_i \subset \mathbb{F}_q$ as defined in Equation 2. Then K_i is an additive subgroup of $(\mathbb{F}_q, +)$.*

Proof. Any two elements in K_i are of the form $a = a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{i-1}\zeta^{i-1}$ and $b = b_0 + b_1\zeta + b_2\zeta^2 + \dots + b_{i-1}\zeta^{i-1}$. Then $a + b = (a_0 + b_0) + (a_1 + b_1)\zeta + (a_2 + b_2)\zeta^2 + \dots + (a_{i-1} + b_{i-1})\zeta^{i-1}$ which is in K_i . $\square$

We note that this does not imply that the corresponding finite field of the same size is a subfield, (in general it is not), but rather that this space is an additive subgroup of the finite field.

Let N be a matrix with elements from the finite field $\mathbb{F}_q$. We denote by $\langle N \rangle_{p^i}$ the span of N with coefficients from K_i . Namely, if $\mathbf{v} \in \langle N \rangle_{p^i}$, then $\mathbf{v} = \sum \alpha_k N_k$, where N_k is the k -th row of N and $\alpha_k \in K_i$. Denote also by $\langle N \rangle = \langle N \rangle_{p^e}$.

Let $G = \{g_1, g_2, \dots, g_n\}$ be a finite group of order n . The group algebra $\mathbb{F}_q G$ consists of elements of the form:

$$\sum_{i=1}^n \alpha_i g_i,$$

$\alpha_i \in \mathbb{F}_q, g_i \in G$.

Addition in the group algebra is done by coordinate addition, namely

$$\sum_{i=1}^n \alpha_i g_i + \sum_{i=1}^n \beta_i g_i = \sum_{i=1}^n (\alpha_i + \beta_i) g_i.$$

The product of two elements in a group algebra is given by

$$\left(\sum_{i=1}^n \alpha_i g_i \right) \left(\sum_{j=1}^n \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j g_i g_j.$$

We associate each element in the group algebra with an element in $\mathbb{F}_q^n$. Namely, let $\Theta : \mathbb{F}_q G \rightarrow \mathbb{F}_q^n$ be the canonical map that sends $a_{g_1} g_1 + a_{g_2} g_2 + \dots + a_{g_n} g_n$ to $(a_{g_1}, a_{g_2}, \dots, a_{g_n})$. Note that an additive code in $\mathbb{F}_q^n$ corresponds via the map Θ to an additive subgroup of $\mathbb{F}_q G$. It is easy to see that a linear code in $\mathbb{F}_q^n$ corresponds to an ideal in $\mathbb{F}_q G$. We are mainly concerned with additive G -codes, which we define now.

Definition 1.2. *An additive G -code is a subgroup of $\mathbb{F}_q G$ that is invariant under the action of multiplication by elements of G .*

Note that unlike in the linear case, we are not asserting that the code corresponds to an ideal in the group algebra but simply that it is additive and held invariant by the action of the group. We note that given a vector in an additive G -code, multiplication by an element of the group G is necessarily in the code but multiplication by an element of the field may not be in the code. As such, additive G -codes need not be ideals in $\mathbb{F}_q G$. In essence, these codes are a richer class of codes that are in $\mathbb{F}_q^n$.

Let C be an additive G -code. It follows immediately that if $\text{Aut}(C)$ is the group of automorphisms of the code C , where an automorphism is a permutation of the columns of C fixing C , then G is a subgroup of $\text{Aut}(C)$.

We expand the definition of equivalent codes beyond the definition of automorphisms to the following.

Definition 1.3. *Two additive codes C and C' in $\mathbb{F}_q^n$ are equivalent if $|C| = |C'|$ and there exists a permutation of coordinates π , and n permutations ψ_i on the set of elements of $\mathbb{F}_q$ satisfying $\psi_i(0) = 0$ for $i \in \{1, \dots, n\}$ such that $(\psi_1(c_{\pi(1)}), \dots, \psi_n(c_{\pi(n)})) \in C'$ for all $(c_1, \dots, c_n) \in C$.*

Example 1.4. Consider the following codes in $\mathbb{F}_4^3$, where $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$:

$$\begin{aligned} C_1 &= \{(0, 0, 0), (0, 1, 1)\}, \\ C_2 &= \{(0, 0, 0), (\omega, \omega, 0)\}, \\ C_3 &= \{(0, 0, 0), (1, 0, \omega^2)\}. \end{aligned}$$

These three codes are equivalent additive codes. The code C_2 is obtained from C_1 by permuting the first and third coordinates, $\pi = (1, 3)$ and applying the permutation of elements given by $\psi_1 = \psi_2 = (1, \omega)$ and $\psi_3 = Id$. The code C_3 is obtained from C_2 by permuting the second and the third coordinate, $\pi = (2, 3)$, and applying $\psi_1 = (1, \omega)$, $\psi_2 = Id$ and $\psi_3 = (\omega, \omega^2)$.

Notice that we are not only allowing for multiplication of a coordinate by a constant because these codes are not necessarily linear codes but rather additive codes.

We note that each of the three equivalent codes given in Example 1.4 have the same Hamming weight enumerator, namely $W_C(x, y) = x^3 + xy^2$. This fact is true for equivalent codes as it is shown in the following lemma.

Lemma 1.5. Let C and C' be additive codes in $\mathbb{F}_q^n$ that are equivalent, then:

- The minimum Hamming distance of C and C' are the same.
- The minimum Hamming weight of C and C' are the same.
- $W_C(x, y) = W_{C'}(x, y)$.

Proof. It is immediate that permuting the coordinates does not change the Hamming weight of a vector. Then the statement follows from the fact that $\psi_i(0) = 0$ for all $i \in \{1, \dots, n\}$, which gives that applying ψ_i on a coordinate does not change the Hamming weight of any vector. $\square$

We now discuss the definitions for codes over a group. The group that is used as an alphabet is not the same as the group G , so we shall denote the alphabet by H . This group will be used to define the duality which gives rise to the orthogonal of codes. In general, throughout this paper, H will refer to the additive group of the finite field of order q .

A character of the finite group H is a homomorphism from H to the multiplicative group of the Complex numbers, $\mathbb{C}^*$. Sometimes, characters are described as having images in $\mathbb{Q}/\mathbb{Z}$, however we shall use the complex version as was done in [10] and [11]. The set of all characters of the group H , denoted by $\hat{H}$ is defined by

$$\hat{H} = \{\chi : \chi \text{ is a character of } H\},$$

and it is a group. This group is isomorphic to H , but not in a canonical manner. The isomorphism that we chose between H and $\hat{H}$ gives a character table M . Let $\{h_i\}$ denote the elements of the group and we let $\phi : H \rightarrow \hat{H}$ be the isomorphism. We establish the following notation. Let the character χ_{h_i} be the

image of h_i under the isomorphism ϕ , namely $\chi_{h_i} = \phi(h_i)$. Index the rows by $\phi(h_i)$ and the columns by the elements of the group where the element of the table M corresponding to (χ_{h_i}, h_j) is $\chi_{h_i}(h_j)$.

Example 1.6. Consider the additive group of $\mathbb{F}_5$. Let ξ be a primitive complex fifth root of unity. Then the duality that corresponds to the Euclidean inner-product for linear codes is given by $\chi_a(b) = \xi^{ab}$. This gives the following character table:

$$M_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \xi & \xi^2 & \xi^3 & \xi^4 \\ 1 & \xi^2 & \xi^4 & \xi & \xi^3 \\ 1 & \xi^3 & \xi & \xi^4 & \xi^2 \\ 1 & \xi^4 & \xi^3 & \xi^2 & \xi \end{pmatrix}.$$

Alternatively, we can take $\chi_a(b) = \xi^{-ab}$ which gives the following character table:

$$M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \xi^4 & \xi^3 & \xi^2 & \xi \\ 1 & \xi^3 & \xi & \xi^4 & \xi^2 \\ 1 & \xi^2 & \xi^4 & \xi & \xi^3 \\ 1 & \xi & \xi^2 & \xi^3 & \xi^4 \end{pmatrix}.$$

We note that there are four primitive complex roots of unity. The matrix M_2 can be thought of as taking a different primitive root. We can form two other dualities in a similar manner. Each character table gives a duality for $\mathbb{F}_5$. Since any additive code over $\mathbb{F}_5$ is also linear, each of these dualities coincides with the standard Euclidean duality.

We fix an isomorphism ϕ between H and $\widehat{H}$ and we consider the characters χ_{h_i} , $h_i \in H$, and the table M related to ϕ as described above. We shall refer to this isomorphism as a duality of H^n , where n is the length of the code, with respect to M or, simply, as the duality M of H .

Definition 1.7. Fix a duality M of H , that is, an isomorphism of H and $\widehat{H}$. Let C be a code over H . Then, the orthogonal of C with respect to this duality is defined as $C^M = \{(h_1, h_2, \dots, h_n) \mid \prod_{i=1}^n \chi_{h_i}(c_i) = 1 \text{ for all } (c_1, \dots, c_n) \in C\}$.

This duality of codes is specific to the fixed duality for the group H . We can get a different dual by changing the duality of the group.

Given that $(\widehat{H})^n = \widehat{H^n}$, each element of $\widehat{H^n}$ is associated with an element of H^n in a canonical way. The code C^M is associated with the set $\{\chi \in \widehat{H^n} \mid \chi(c) = 1 \text{ for all } c \in C\}$. The orthogonal code is necessarily additive.

We mainly consider only symmetric dualities, namely we want $\chi_a(b) = \chi_b(a)$. This gives that the character table M satisfies $M = M^T$.

If a code satisfies $C \subseteq C^M$ then the code is said to be self-orthogonal with respect to M . If the code satisfies $C = C^M$, then we say that the code is self-dual with respect to M . If $W_C(x, y) = W_{C^M}(x, y)$ then the code is said to be formally self-dual with respect to M .

Let C be a linear code over $\mathbb{F}_q$ with a fixed duality M . We have from [5] and [11] the following results.

Lemma 1.8. *Let C be a G -code over $\mathbb{F}_q$ and let M be a duality of C . Then,*

- $(C^M)^M = C$ for symmetric dualities;
- $|C||C^M| = q^n$;
- $cwe_{C^M}(X) = \frac{1}{|C|}cwe_C(M \cdot X)$, $X = (x_0, x_1, \dots, x_{q^e-1})$.

We define some dualities over finite fields. Let $\mathbb{F}_q$ be a finite field, $q = p^e$, p a prime. Let ξ be a primitive complex p -th root of unity, $\xi = e^{\frac{2\pi i}{p}}$. Every element in $\mathbb{F}_q$ can be written as $a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{e-1}\zeta^{e-1}$. Then associate to each element $a \in \mathbb{F}_q$ its vector $\mathbf{a}$ in K_e .

First, we define the standard Euclidean duality, M_E , as

$$(M_E)_{a,b} = \xi^{[\mathbf{a}, \mathbf{b}]},$$

where $[\mathbf{a}, \mathbf{b}] = \sum a_i b_i$, which is the standard inner-product in $\mathbb{F}_q^n$. This duality corresponds to the standard Euclidean duality for linear codes. By that we mean if C is a linear code then $C^{M_E} = C^\perp$.

The trace function $Tr : \mathbb{F}_{p^e} \rightarrow \mathbb{F}_p$ is defined to be $Tr(a) = a + a^p + a^{p^2} + \dots + a^{p^{e-1}}$. It is well known that $Tr(\alpha a + \beta b) = \alpha Tr(a) + \beta Tr(b)$, where α and β are in $\mathbb{F}_p$. We can define the duality M_T by

$$(M_T)_{a,b} = \xi^{Tr(ab)}.$$

If e is an even integer and $p = 2$, then let $e = 2k$ and define an involution on the finite field as $\bar{a} = a^{2^k}$. This gives $\bar{\bar{a}} = (a^{2^k})^{2^k} = a^{2^e} = a$. We can define the duality M_{TH} by

$$(M_{TH})_{a,b} = \xi^{Tr(a\bar{b})}.$$

Finally, let $\chi(a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{e-1}\zeta^{e-1}) = \xi^{a_{e-1}}$ for $\xi = e^{\frac{2\pi i}{p}}$. Define

$$(M_r)_{a,b} = \chi(a \cdot b).$$

Example 1.9. *The following are some symmetric dualities obtained for $\mathbb{F}_4$ using the ordering $0, 1, \omega, \omega^2$ for the indices in the matrix (see [10]).*

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

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

Example 1.10. Consider $\mathbb{F}_9 = \mathbb{F}_3[x]/\langle x^2 + 1 \rangle$. Consider the elements of $\mathbb{F}_9$ in the following order $\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$, and $\xi = e^{\frac{2\pi i}{3}}$. Then the duality M_r in $\mathbb{F}_9$ is given by the following character table:

$$M_r = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \xi & \xi^2 & 1 & \xi & \xi^2 & 1 & \xi & \xi^2 \\ 1 & \xi^2 & \xi & 1 & \xi^2 & \xi & 1 & \xi^2 & \xi \\ 1 & 1 & 1 & \xi^2 & \xi^2 & \xi^2 & \xi & \xi & \xi \\ 1 & \xi & \xi^2 & \xi^2 & 1 & \xi & \xi & \xi^2 & 1 \\ 1 & \xi^2 & \xi & \xi^2 & \xi & 1 & \xi & 1 & \xi^2 \\ 1 & 1 & 1 & \xi & \xi & \xi & \xi^2 & \xi^2 & \xi^2 \\ 1 & \xi & \xi^2 & \xi & \xi^2 & 1 & \xi^2 & 1 & \xi \\ 1 & \xi^2 & \xi & \xi & 1 & \xi^2 & \xi^2 & \xi & 1 \end{pmatrix}.$$

We note that the MacWilliams relations for the Hamming weight enumerator are the same for all dualities (see [10] for details). Namely,

$$W_{C^M}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y)$$

for all dualities M . This follows from the fact that collapsing the first row and any other row gives the matrix

$$\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}.$$

2. Orthogonals

In this section, we consider the properties of the orthogonal code C^M for a given duality M .

Theorem 2.1. Let C be an additive code in $\mathbb{F}_q^n$. Let M and M' be two dualities of C . Then C^M and $C^{M'}$ are equivalent codes.

Proof. Let C be an additive code in $\mathbb{F}_q^n$ and let M and M' be two of its dualities. Consider the characters χ_h and χ'_h related to M and M' , respectively, and take the ordering $h_0 = 0, h_1, \dots, h_{q^n-1}$ for the indices in the matrices. Since the character group is isomorphic to the group, any two representations of the character group are isomorphic, see [5] for details. Then there is a group isomorphism $\phi : \hat{G}_M \rightarrow \hat{G}_{M'}$ given by $\phi(\chi_i) = \chi'_{\psi(i)}$, with ψ a permutation in the set of elements $\{h_0 = 0, h_1, \dots, h_{q^n-1}\}$ satisfying $\psi(0) = 0$.

By definition, we have that $(y_1, \dots, y_n) \in C^M$ if and only if $\prod_{i=1}^n \chi_{y_i}(c_i) = 1$ for all $\mathbf{c} = (c_1, \dots, c_n) \in C$, that is, $\prod_{i=1}^n \chi'_{\psi(y_i)}(c_i) = 1$ for all $\mathbf{c} = (c_1, \dots, c_n) \in C^M$ that is equivalent to $(\psi(y_1), \dots, \psi(y_n)) \in C^{M'}$. Therefore, the codes C^M and $C^{M'}$ are equivalent. $\square$

Example 2.2. Consider the additive code over $\mathbb{F}_4$ $C = \{(0,0), (1,1)\}$, and the matrices M_E , M_T and M_{TH} for $\mathbb{F}_4$ given in Example 1.9. Then, we obtain the following additive codes:

$$C^E = \{(0,0), (1,1), (\omega, \omega), (\omega^2, \omega^2), (1, \omega^2), (0, \omega), (\omega, 0), (\omega^2, 1)\},$$

$$C^T = C^{TH} = \{(0,0), (1,1), (\omega, \omega), (\omega^2, \omega^2), (\omega, \omega^2), (\omega^2, \omega), (1,0), (0,1)\}.$$

Each one of the 3 codes can be obtained from another one just applying a permutation ψ of the elements of $\mathbb{F}_q$ satisfying $\psi(0) = 0$.

	C^E	C^T	C^{TH}
C^E	Id	$(1, \omega, \omega^2)$	$(1, \omega^2)$
C^T		Id	(ω^2, ω)
C^{TH}			Id

The Hamming weight enumerator for all of these codes is $x^2 + 2xy + 5y^2$. Applying the MacWilliams relations to this weight enumerator we get $x^2 + y^2$ which is the weight enumerator of C .

Corollary 2.3. Let C be an additive code in $\mathbb{F}_q^n$. Let M and M' be two dualities of C . Then $d_H(C^M) = d_H(C^{M'})$ and $W_{C^M}(x, y) = W_{C^{M'}}(x, y)$.

Proof. Follows directly from Theorem 2.1 and Lemma 1.5. $\square$

Classically, one of the most important results about cyclic codes is that the dual of a cyclic code is a cyclic code under the standard Euclidean duality. We now generalize this result, showing that the dual under any orthogonality of a code held invariant by the action of a finite group G is an additive code held invariant by the action of the group G .

Theorem 2.4. Let C be an additive G -code in $\mathbb{F}_q^n$, and let M be a symmetric duality on the additive group of $\mathbb{F}_q$. Then C^M is an additive G -code in $\mathbb{F}_q^n$.

Proof. We know that C^M is an additive code, so all that remains is to show that C^M is held invariant by the action of the group G . Let $\mathbf{w} = (w_1, w_2, \dots, w_n) \in C^M$, and $g_j \in G$. We want to show that $\mathbf{z} = \mathbf{w}g_j \in C^M$. By definition, we have that

$$\prod_{i=1}^{i=n} \chi_{w_i}(c_i) = 1, \quad \forall \mathbf{c} = (c_1, \dots, c_n) \in C.$$

Let $\mathbf{d} \in C$ and let $\mathbf{c} = \mathbf{d}g_j$. We have $\mathbf{c} \in C$ since C is a G -code. Then, we have

$$\prod_{i=1}^{i=n} \chi_{z_i}(d_i) = \prod \chi_{w_i}(c_i) = 1,$$

which gives that $\mathbf{z} \in C^M$ and so C^M is held invariant by the action of the group G , giving that C^M is a G -code. $\square$

It is interesting to note then that if C is an additive G code and M and M' are two dualities on the additive group of $\mathbb{F}_q$, then C^M and $C^{M'}$ are equivalent codes and both are G -codes.

3. Construction of G -Codes and Quasi- G -Codes

Let $G = \{g_1, g_2, \dots, g_n\}$ be a group of order n . Let $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_n}g_n \in \mathbb{F}_q G$. Define the matrix $\sigma(v) \in M_n(\mathbb{F}_q)$, first given in [13], to be

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \quad (3)$$

We note that this matrix consists simply of all elements that are formed by the action of an element of G on the element v . We shall use this matrix to generate codes. This matrix is not necessarily a minimal generating set in any sense. For example, if $\alpha_{g_i} = 1$ for all g_i then the matrix has n repeated rows. But a code generated by this matrix is ensured to be invariant under the action of G .

In general, the G -code obtained from the action of G over an element v is defined as

$$C(v) = \langle \sigma(v) \rangle.$$

We note that this code is a linear code over $\mathbb{F}_q$ and in the notation of this paper $C(v) = \langle \sigma(v) \rangle_{p^e}$. We are concerned with the span of this matrix using K_i as coefficients as well to generate additive codes. We shall show in Theorem 3.2, that the K_i span of this matrix is an additive G -code.

Lemma 3.1. *Let N be any matrix with rows that are elements from $\mathbb{F}_q^n$, $q = p^e$, p prime. Then the $\langle N \rangle_{p^i}$ is a subgroup of $\mathbb{F}_q^n$.*

Proof. Let $\mathbf{v}_i$ be the rows of N . Let $\mathbf{w} = \sum \alpha_j \mathbf{v}_j$ and $\mathbf{u} = \sum \beta_j \mathbf{v}_j$, where $\alpha_j, \beta_j \in K_i$. Then $\mathbf{w} + \mathbf{u} = \sum (\alpha_j + \beta_j) \mathbf{v}_j$ and $\alpha_j + \beta_j \in K_i$. Therefore, the K_i span of N is a subgroup of $\mathbb{F}_q^n$. $\square$

We note that in this theorem all that is required is that the set of coefficients is an additive subgroup of $\mathbb{F}_q$. Namely, other additive subgroups can easily be used to construct codes as well.

Let $v \in \mathbb{F}_q G$ and denote $A_i(v) = \langle \sigma(v) \rangle_{p^i}$, the K_i span of $\sigma(v)$.

Theorem 3.2. *Let G be a finite group of order n , $v \in \mathbb{F}_q G$ and M be a duality of $\mathbb{F}_q$. Then $A_i(v)$ is an additive G -code of length n and we have the following chains of additive codes:*

$$A_1(v) \subseteq A_2(v) \subseteq \dots \subseteq A_e(v). \quad (4)$$

$$A_e(v)^M \subseteq A_{e-1}(v)^M \subseteq \dots \subseteq A_1(v)^M. \quad (5)$$

Proof. By Lemma 3.1, we know that $A_i(v)$ is an additive code. Next, we show that it is a G -code. If $\mathbf{w}_j$ is a row of the matrix $\sigma(v)$ and $\mathbf{z} = \sum \alpha_j \mathbf{w}_j$, $\alpha_j \in \mathbb{F}_{p^i}$ then acting by an element g in G on $\mathbf{z}$ to get $\mathbf{z}'$, we have $\mathbf{z}' = \sum \alpha_j \mathbf{w}'_j$, where $\mathbf{w}'_j$ is formed from $\mathbf{w}_j$ by the action of g . We notice that $\mathbf{w}'_j$ is another row

of $\sigma(v)$ and so this vector is in $A_i(v)$ giving that $A_i(v)$ is invariant under the action of G and so $A_i(v)$ is a G -code.

The first chain follows from that fact that if $\mathbf{z} = \sum \alpha_j \mathbf{w}_j$, $\alpha_j \in K_i$, then since $K_i \subset K_{i+1}$ we have that $\mathbf{z} \in A_{i+1}(v)$. The second chain follows from the first, noticing that taking the orthogonal reverses the inclusion. $\square$

The following definition was first given in [9]. The version we give is a direct generalization of this earlier definition as applied to additive codes. It is a generalization of the notion of quasi-cyclic codes.

Definition 3.3. *Let G be a finite group of order n and A be an alphabet. Let D be a code in A^{sn} where the coordinates can be partitioned into n sets of size s where each set is assigned an element of G . If the code D is held invariant by the action of multiplying the coordinate set marker by every element of G then the code D is called a quasi-group code of index s .*

Example 3.4. *Let G be the dihedral group D_4 (which is also the Klein-4 group). Then, using Equation 3, we generate a dihedral additive code by taking the $\mathbb{F}_2$ span of*

$$\begin{pmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega \\ \omega & 0 & 1 & 0 \\ 0 & \omega & 0 & 1 \end{pmatrix}.$$

This is an additive code with 16 elements. Taking the natural projection to binary elements, we have a binary code generated by

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

It is easy to see that this code is a quasi-dihedral code of index 2 with dimension 4.

Let $\Pi : K_i \rightarrow \mathbb{F}_p^i$ be the canonical projection. That is, if $a_0 + a_1\xi + \cdots + a_{i-1}\xi^{i-1} \in K_i$, for $\xi = e^{\frac{2\pi i}{p}}$, then

$$\Pi(a_0 + a_1\xi + \cdots + a_{i-1}\xi^{i-1}) = (a_0, a_1, \dots, a_{i-1}).$$

Theorem 3.5. *If C is an additive G -code over $\mathbb{F}_{p^e}$ of length n then $\Pi(C)$ is a linear quasi- G -code of length ne .*

Proof. The action of the group moves the set of e coordinates corresponding to the projection of an element in $\mathbb{F}_{p^e}$. Moreover it is easy to check that Π is a homomorphism of groups. Then the result follows from the definition of quasi- G -cyclic. $\square$

Corollary 3.6. *Let G be a finite group, $v \in \mathbb{F}_q G$ and M be a duality of $\mathbb{F}_q$. Then $\Pi(A_i(v))$ is a linear quasi- G -code over $\mathbb{F}_p$ and we have the following chains of linear codes:*

$$\Pi(A_1(v)) \subseteq \Pi(A_2(v)) \subseteq \cdots \subseteq \Pi(A_e(v)). \quad (6)$$

$$\Pi(A_e(v)^M) \subseteq \Pi(A_{e-1}(v)^M) \subseteq \cdots \subseteq \Pi(A_1(v)^M). \quad (7)$$

Proof. The result follows from Theorem 3.2 and Theorem 3.5. $\square$

Note that we do not know if the projection of the orthogonal with respect to M is related to the standard orthogonal of $\Pi(A_i(v))$ as a code over $\mathbb{F}_p$.

Example 3.7. *Let $G = \{1, \alpha, \beta, \gamma\}$ be the Klein-4 group. Let $v = 1 + 1\alpha + \omega\beta + \omega\gamma \in \mathbb{F}_4 G$ and*

$$\sigma(v) = \begin{pmatrix} 1 & 1 & \omega & \omega \\ 1 & 1 & \omega & \omega \\ \omega & \omega & 1 & 1 \\ \omega & \omega & 1 & 1 \end{pmatrix}.$$

Then $A_1(v)$ is the additive G -code $\{(0, 0, 0, 0), (1, 1, \omega, \omega), (\omega, \omega, 1, 1), (\omega^2, \omega^2, \omega^2, \omega^2)\}$ and $A_2(v)$ is the code with cardinality 16 generated by

$$\begin{pmatrix} 1 & 1 & \omega & \omega \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The canonical projection over $\mathbb{F}_4$ is given by $\Pi(0) = (0, 0), \Pi(1) = (1, 0), \Pi(\omega) = (0, 1)$ and $\Pi(\omega^2) = (1, 1)$. The linear quasi-Klein-code $\Pi(A_1)$ is

$$\{(0, 0, 0, 0, 0, 0, 0, 0), (1, 0, 1, 0, 0, 1, 0, 1), (0, 1, 0, 1, 1, 0, 1, 0), (1, 1, 1, 1, 1, 1, 1, 1)\}.$$

The linear quasi-Klein-code $\Pi(A_2)$ is generated by

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Under the duality M_E we have $A_2(v) = A_2(v)^{M_E}$. The code $A_1(v)$ has $|A_1(v)^{M_E}| = 64$ and consists of precisely half the vectors in E_8 , the even code.

4. Self-Dual Codes

Self-dual codes are a widely studied family of codes. The vast majority of this study has been about linear self-dual codes over both fields and rings. We shall study codes that may not be linear, but are still self-dual with respect to some duality. A code C is a self-dual code with respect to the duality M if $C = C^M$. This implies that $|C| = q^{\frac{n}{2}}$ where n is the length of the code and $\mathbb{F}_q$ is the alphabet since $|C||C^M| = |\mathbb{F}_q^n|$. Additive self-dual codes over fields of even order were studied in [10], here we shall extend some of these ideas and expand on them for any q .

Theorem 4.1. *Let $q = p^e$. If e is odd then there is no self-dual code of length 1 corresponding to any duality.*

Proof. If C were a self-dual code of length 1, then $|C|^2 = q$, which gives that $|C| = p^{\frac{e}{2}}$ which is a contradiction if e is odd. $\square$

The following lemma has the standard proof, see [5] for example.

Lemma 4.2. *If C is a self-dual code over $\mathbb{F}_q$ of length n with respect to duality M and D is a self-dual code of length m with respect to M then $C \times D$ is a self-dual code of length $n + m$ with respect to M .*

This lemma leads naturally to the following theorem.

Theorem 4.3. *If C is a self-dual code of length 1 with respect to duality M . Then the n fold product of C is a self-dual code of length n that is a G -code for any group G of order n .*

Proof. The fact that the code is self-dual follows from Lemma 4.2. Given any permutation of the coordinates the code C remains the same. Therefore, the action of any group fixes C and so the code is a G -code for any group G of order n . $\square$

Self-dual codes naturally give rise to formally self-dual codes in the next theorem.

Theorem 4.4. *If C is a self-dual code over a group H with respect to the duality M , then C is a formally self-dual code with respect to M' for all dualities M' of H .*

Proof. Since $C = C^M$ and C^M and $C^{M'}$ are equivalent by Theorem 2.1, we have that $W_C(x, y) = W_{C^{M'}}(x, y)$ and the code is formally self-dual with respect to M' by Lemma 1.5. $\square$

This theorem guarantees that if we have a self-dual code, then we can produce numerous formally self-dual codes by changing the duality.

4.1. Self-dual codes with respect to M_E , M_T and M_r

In [10], the existence of self-dual codes over $\mathbb{F}_2$ is proven for any self-duality.

Theorem 4.5. [10] *There exists a linear self-dual code with respect to a duality M of all even lengths.*

We want to generalize the previous theorem to $\mathbb{F}_q$ considering different dualities.

Theorem 4.6. *There exists a linear self-dual code in terms of the usual inner-product of length se over $\mathbb{F}_p$ if and only if there exists an additive self-dual code with respect to M_E of length s over $\mathbb{F}_q$, $q = p^e$.*

Proof. We know that $\mathbb{F}_q = \mathbb{F}_p(\zeta)$, where $q = p^e$. For any element $a \in \mathbb{F}_q$, let $\mathbf{a}$ be its corresponding vector. Namely, if $a = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{e-1}\zeta^{e-1}$ then $\mathbf{a} = (a_0, a_1, \dots, a_{e-1})$. Let C be an additive self-dual code of length s over $\mathbb{F}_q$. Then if $(c_1, c_2, \dots, c_s), (d_1, d_2, \dots, d_s) \in C$, we have $\prod \chi_{c_i}(d_i) = 1$ which implies $[(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_s), (\mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_s)] = 0$ in $\mathbb{F}_p$. Let D be the set of length se vectors formed from the elements of C , namely, $D = \{(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_s) \mid (c_1, c_2, \dots, c_s) \in C\}$. Then any two vectors $(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_s), (\mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_s) \in D$ are orthogonal, so that $D \subseteq D^\perp$. We note that the sum of any two vectors in D must again be in D since C is additive and addition of the vectors corresponds to standard addition in $\mathbb{F}_q$. Since C is self-dual, $|C| = q^{\frac{s}{2}}$. Moreover, $|C| = |D|$ and this gives that $|D| = p^{\frac{es}{2}}$. Hence, D is a self-orthogonal code with $|D||D^\perp| = p^{\frac{es}{2}}$ which gives that $D = D^\perp$.

If D is a linear self-dual code over $\mathbb{F}_p$ of length se , then let C be the code over $\mathbb{F}_q$ formed from D , namely $C = \{(c_1, c_2, \dots, c_s) \mid (\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_s) \in D\}$. Then, since D is self-orthogonal, for any two $(c_1, c_2, \dots, c_s), (d_1, d_2, \dots, d_s) \in C$, we have $\prod \chi_{c_i}(d_i) = \xi^0 = 1$. Hence, the code is self-orthogonal. Then by the identical cardinality argument given in the first half of the proof we have $C = C^{M_E}$. $\square$

Corollary 4.7. *Let $q = p^e$, p a prime.*

- *If $p = 2$ then additive self dual codes over $\mathbb{F}_q$ exist with respect to M_E for all even lengths if e is odd and for all lengths if e is even.*
- *If $p \equiv 1 \pmod{4}$ then additive self-dual codes over $\mathbb{F}_q$ exist with respect to M_E for all lengths over $\mathbb{F}_q$ if e is even and for all even lengths if e is odd.*
- *If $p \equiv 3 \pmod{4}$ then additive self-dual codes over $\mathbb{F}_q$ exist with respect to M_E for all even lengths if e is even and for all lengths congruent to 0 $\pmod{4}$ if e is odd.*

Proof. Follows from Theorem 4.6, Theorem 4.5 and that fact that if $p \equiv 1 \pmod{4}$ then self-dual codes exist for all even lengths and if $p \equiv 3 \pmod{4}$ then self-dual codes exist for all lengths congruent to 0 $\pmod{4}$. $\square$

Even more can be said about these self-dual codes. If $p \equiv 1 \pmod{4}$ and e is even, then there exists an additive self-dual code of length 1 over $\mathbb{F}_q$, $q = p^e$. We know that this code is not linear since there cannot be a linear code of length 1 that is neither the entire field nor just the zero element. Then using Lemma 4.2, we have that there exist additive self-dual codes of all lengths over $\mathbb{F}_q$ that are not linear.

Example 4.8. *Consider the binary self-dual $[8, 4, 4]$ Hamming code with the standard duality. Consider the duality with respect to M_E over $\mathbb{F}_{2^e}$, $e > 1$. As an additive self-dual code over $\mathbb{F}_4$ as in Theorem 4.6, we get a $(4, 16, 3)$ additive*

self-dual code. It is generated by

$$\begin{pmatrix} 1 & 0 & \omega & \omega^2 \\ 0 & 1 & \omega^2 & \omega \\ \omega & 0 & \omega^2 & 1 \\ 0 & \omega & 1 & \omega^2 \end{pmatrix}.$$

As a code over $\mathbb{F}_{16}$, we get a $(2, 16, 2)$ additive self-dual code. As a code over $\mathbb{F}_{256}$ it is a $(1, 16, 1)$ additive self-dual code.

Example 4.9. There is no self-dual code of length 2 over $\mathbb{F}_3$ with the standard duality. As such, by Theorem 4.6, there is no self-dual code with respect to M_E of length 1 over $\mathbb{F}_9$. However, the code $\{0, x + 2, 2x + 1\}$ is a self-dual code with respect to M_T of length 1 over $\mathbb{F}_9$. This gives that C and C^{M_E} are formally self-dual codes. The corresponding $\mathbb{F}_3$ code is $\{(0, 0), (1, 2), (2, 1)\}$. Its dual is $\{(0, 0), (1, 1), (2, 2)\}$. These codes are formally self-dual as well.

Proposition 4.10. Let C be an additive code over $\mathbb{F}_q$. If C is a self-dual code with respect to M_E , then C is self-dual with respect to M_T .

Proof. Let C be an additive code of length s over $\mathbb{F}_q$ and consider the character χ related to M_T , that is, $\chi_a(b) = \xi^{Tr(ab)}$ for $a, b \in \mathbb{F}_q$. For $(c_1, c_2, \dots, c_s), (d_1, d_2, \dots, d_s) \in C$ we have $[(c_1, c_2, \dots, c_s), (d_1, d_2, \dots, d_s)] = \prod_{i=1}^s \chi_{c_i}(d_i) = \prod_{i=1}^s \xi^{Tr(c_i d_i)} = \xi^{\sum_{i=1}^s Tr(c_i d_i)} = \xi^{Tr(\sum_{i=1}^s c_i d_i)}$ because of the linearity of the trace function.

If C is self-dual with respect to M_E then, for $(c_1, c_2, \dots, c_s), (d_1, d_2, \dots, d_s) \in C$ we have $\sum_{i=1}^s c_i d_i = 0$ and, therefore $\xi^{Tr(\sum_{i=1}^s c_i d_i)} = 1$ that implies that C is self-orthogonal with respect to M_T . Self-duality follows from the fact that the cardinality condition in both cases is the same, namely that $|C|^2 = q^s$. $\square$

We note however, that this theorem is not biconditional as shown in the next example.

Example 4.11. Consider the field of order 9, $\mathbb{F}_9 = \mathbb{F}_3[x]/\langle x^2 + 1 \rangle$ as in Example 1.10. Here we have $Tr(0) = Tr(x) = Tr(x^2) = 0$. Now $(1 + x)^2 = 2x$ and $(2 + 2x)^2 = 2x$ which gives for any of these elements a , $\xi^{Tr(a^2)} = \xi^0 = 1$. Namely, these three elements are self-orthogonal. Hence, the code $\{0, 1 + x, 2 + 2x\}$ is an additive self-dual code of length 1 with respect to M_T . Moreover, $(2 + x)^2 = (1 + 2x)^2 = x$ and so by the same reasoning the code $\{0, 2 + x, 1 + 2x\}$ is an additive self-dual code of length 1 with respect to M_T . These two codes do not correspond to a Euclidean self-dual code given in Proposition 4.10 since there is no self-dual code of length 1 over $\mathbb{F}_9$ with respect to M_E .

Theorem 4.12. Let p be a prime. The additive code $\mathbb{F}_p^n$ is a self-dual code of length n with respect to M_T in $\mathbb{F}_{p^2}^n$. Moreover, it is a G -code for all groups G of order n .

Proof. Since the code is the entire space $\mathbb{F}_p^n$, it is held invariant by the action of any group of order n .

Given any two vectors $\mathbf{v}, \mathbf{w} \in \mathbb{F}_p$, we have that $\sum \text{Tr}(v_i w_i) = 0$ since the trace of any element in the ground field is 0. Therefore, this code is self-orthogonal with respect to M_T . Then $|\mathbb{F}_p^n| = p^n$ and $p^n p^n = p^{2n} = (p^2)^n$ which is the size of the ambient space. Therefore, the code is self-dual. $\square$

Example 4.13. Let p be any prime. The code $C = \mathbb{F}_p$ is a self-dual code with respect to M_T of length 1. Then $C = \mathbb{F}_p$ has weight enumerator $W_C(x, y) = x + (p-1)y$. Applying the MacWilliams relations, we have:

$$\frac{1}{p} W_C(x + (p^2 - 1)y, x - y) = x + (p-1)y.$$

In particular, Theorem 4.12 gives that the code $C = \mathbb{F}_p^n$ is a cyclic self-dual code with respect to M_T . In general, cyclic self-dual codes are found examining algebraic properties of the factors of $x^n - 1$. However, this does not apply to the present situation since the cyclic codes here do not correspond to ideals in the polynomial ring.

Theorem 4.14. Let $q = p^e$, p a prime, with $e = 2s$ for some integer s . Let C be the code of length 1 consisting of all elements of $\mathbb{F}_q$ with $a_i = 0$ for $i > s-1$. Then C is a self-dual code with respect to M_r .

Proof. The code C is additive since the sum of any two elements in C which are polynomials in ζ of degree at most $s-1$, is a polynomial in ζ of degree at most $s-1$. The cardinality of the code C is p^s , since there are p choices each for $a_0, a_1, \dots, a_{s-1}$. This gives $|C|^2 = (p^s)^2 = |\mathbb{F}_q|$. Take the product of any two elements in C . Since both elements are at most of degree $s-1$ in ζ , their product is of degree at most $2s-2$ and hence their product has $a_{2s-1} = 0$. Then, if $a, b \in C$, we have $\chi_a(b) = 1$. Therefore, the code C is self-orthogonal and $|C|^2 = q$ and so the code is self-dual. $\square$

Example 4.15. By Theorem 4.14, the code $C = \mathbb{F}_p$ is a self-dual code with respect to M_r in $\mathbb{F}_{p^2}$. Theorem 4.12 gives that $C = C^{M_T}$ in this case. This means that in this particular case $C^{M_r} = C^{M_T}$.

Corollary 4.16. There exist self-dual codes with respect to M_r for all lengths n that are G -codes for all groups G of order n .

Proof. The self-dual codes with respect to duality M_r exist for length $n = 1$ by Theorem 4.14. Then self-dual codes with respect to M_r exist for any length n by Lemma 4.2 and they are G -codes by Theorem 4.3. $\square$

For any linear code C over the field $\mathbb{F}_q$, let $C^\perp$ denote the standard dual, namely $C^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in C\}$. We note that the code $C^\perp$ is a linear code, even when C is not.

Theorem 4.17. Let M be either M_E , M_T or M_r . Then for any linear code C we have

$$\text{cwe}_{C^\perp}(X) = \frac{1}{|C|} \text{cwe}_C(M \cdot X).$$

Specifically, M works for the MacWilliams relations for linear codes over the field.

Proof. We know that $\mathbb{F}_q$ is a Frobenius ring. Then we know that a generating character on the character module is any character that is non-trivial on the minimal ideal of the ring. Since the ring is a field, this is a trivial statement. Therefore, these dualities are given by a generating character and so either suffice for the MacWilliams relations for linear codes. (See [5] for background details.) $\square$

This theorem indicates that the MacWilliams relations for linear codes are not unique and that these three different dualities give the MacWilliams relations for linear codes. This means that two different matrices M will always give the complete weight enumerator of $C^\perp$ from the complete weight enumerator of C . This does not, however, mean that they give the same MacWilliams relations for additive codes. This is easily seen in the next example.

Example 4.18. Let $C = \{0, 1\}$ be an additive code over $\mathbb{F}_4$. Considering the dualities M_E and M_T , we obtain the following dual codes $C^{M_E} = \{0, \omega\}$ and $C^{M_T} = \{0, 1\}$. Note that these two codes have different complete weight enumerators, $cwe_{C^{M_E}}(x_0, x_1, x_2, x_3) = x_0 + x_2$ and $cwe_{C^{M_T}}(x_0, x_1, x_2, x_3) = x_0 + x_1$, but they give $cwe_C = x_0 + x_1$ when applying the MacWilliams relations to each one of the two matrices M_E and M_T . Of course, both of these dualities give the same MacWilliams relations for the Hamming weight enumerator which coincide in both cases, $W_{C^E}(x, y) = W_{C^M}(x, y) = x + y$.

In Corollary 4.7, we have shown that there exist numerous additive self-dual codes that are not linear. This result is very important for the following reason. The MacWilliams relations for linear codes over $\mathbb{F}_q$ are given by $cwe_{C^\perp}(X) = \frac{1}{|C|} cwe(M_E \cdot X)$ which is the same as the MacWilliams relations for additive codes using M_E as the duality. If I is the set of polynomials in q variables that are held invariant by the action of $\frac{1}{\sqrt{q}} M_E$, then the possible weight enumerators for both sets of self-dual codes (additive and linear) are the same. Usually, we ask that the codes also have even length for linear codes.

Let I' be the set of polynomials held invariant by $\frac{1}{\sqrt{q}} M_E$ and the action of the matrix guaranteeing that the length must be even. Then there exist elements in I' that are weight enumerators of additive self-dual codes with respect to M_E but not linear self-dual codes with respect to the usual inner-product. For example, consider the self-dual code C of length 1 over $\mathbb{F}_q$, $q = p^e$, e even. The code $C \times C$ has length 2 but has vectors with Hamming weight 1. No vector with Hamming weight 1 can be self-orthogonal over $\mathbb{F}_q$ in the usual inner-product so this cannot be the weight enumerator of a self-dual code with respect to the usual inner-product.

4.2. Self-duality in chains of additive G -codes

Let G be a finite group of order n , $v \in \mathbb{F}_q G$ and M be a duality of $\mathbb{F}_q$. Recall the chains of additive G -codes of length n $A_1(v) \subseteq A_2(v) \subseteq \cdots \subseteq A_e(v)$ and

$A_e(v)^M \subseteq A_{e-1}(v)^M \subseteq \cdots \subseteq A_1(v)^M$ given in Equations (6) and (7). We begin the study of these chains with a lemma.

Lemma 4.19. *Let $v \in \mathbb{F}_q G$. Then we have $|A_i(v)| < |A_{i+1}(v)|$ for $1 \leq i \leq e-1$.*

Proof. The code $A_i(v)$ has a minimal generating set of vectors, say $\{\mathbf{v}_i \mid 1 \leq i \leq t\}$. Then, given a codeword $\mathbf{w} \in A_i(v)$, there is a unique way of writing $\mathbf{w} = \sum_{i=1}^t \alpha_i \mathbf{v}_i$, for some $t \geq 1$. Then, there are precisely p^i multiples of $\mathbf{w}$. Namely, $\beta \mathbf{w} = \beta \sum_{i=1}^t \alpha_i \mathbf{v}_i$. However, there are p^{i+1} multiples of $\mathbf{w}$ in $A_{i+1}(v)$. Therefore, the two codes are not equal. Given the containment of $A_i(v)$ in $A_{i+1}(v)$, we have that $A_i(v) \subset A_{i+1}(v)$ which gives the result. $\square$

In general, we want to look in this chain to find additive self-dual codes.

Theorem 4.20. *Consider $A_1(v) \subseteq A_2(v) \subseteq \cdots \subseteq A_e(v)$ the chain of additive G -codes of length n defined in Equation (6). There is at most one j , $1 \leq j \leq e-1$ such that $A_j(v)$ is self-dual with respect to M , for any duality M .*

Proof. By Lemma 4.19, $|A_i(v)| < |A_{i+1}(v)|$ for $1 \leq i \leq e-1$. Therefore, at most only one code in the chain can satisfy $|A_j(v)|^2 = q^s$. $\square$

Corollary 4.21. *Consider $A_e(v)^M \subseteq A_{e-1}(v)^M \subseteq \cdots \subseteq A_1(v)^M$ the chain of additive G -codes of length n defined in Equation (7). There is at most one j , $1 \leq j \leq e-1$ such that $A_j(v)^M$ is self-dual with respect to M , for any duality M .*

Corollary 4.22. *Consider $A_1(v) \subseteq A_2(v) \subseteq \cdots \subseteq A_e(v)$ the chain of additive G -codes of length n defined in Equation (6). Let j , $1 \leq i \leq e-1$, be the possible index for $A_j(v)$ being self-dual code with respect to M . If $A_j(v)$ is not formally self-dual with respect to M , then $A_j(v)$ is not self-dual with respect to any duality M' .*

Proof. From Theorem 4.20, consider the index j , $1 \leq j \leq e-1$, such that $A_j(v)$ may be self-dual with respect to M . Assume $A_j(v) = A_j^M(v)$. Then, if $A_j(v)$ is not formally self-dual with respect to any other M' , we get a contradiction by Theorem 4.4. $\square$

Therefore, for the possible index j in the chain $A_1(v) \subseteq A_2(v) \subseteq \cdots \subseteq A_e(v)$ with the proper cardinality, if it is not formally self-dual to $A_j(v)$, for a fixed M , then there is no self-dual code in the chain with respect to any duality.

Example 4.23. *We illustrate these results with the following three examples. Let $K_4 = \{1, \alpha, \beta, \gamma\}$ be the Klein-4 group. Let v be an element in $\mathbb{F}_4 K_4$. Then we have $A_1(v) \subset A_2(v)$ and $A_2(v)^M \subset A_1(v)^M$ for any duality M .*

- If $v = 1 + 0\alpha + 1\beta + 0\gamma$ then

$$\sigma(v) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Deleting identical rows we have the matrix:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Then the code $A_1(v)$ has 4 elements and cannot be self-dual. The code $A_2(v)$ has cardinality 16 and is self-orthogonal with-respect to M_E and M_T . Therefore, it is self-dual with respect to both dualities.

- If $v = 1 + 0\alpha + 0\beta + 0\gamma$ then

$$\sigma(v) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $A_1(v)$ has 16 elements and is self-orthogonal with respect to M_T and is therefore a self-dual code with respect to M_T . The code $A_2(v)$ is $\mathbb{F}_4^4$, i.e. the entire space. The code $A_1(v)$ is not self-orthogonal with respect to duality M_E and, therefore, in the chain $A_1(v) \subset A_2(v)$ there is no self-dual code with respect to M_E .

- If $v = \omega^2 + 0\alpha + 0\beta + 0\gamma$ then

$$\sigma(v) = \begin{pmatrix} \omega^2 & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & \omega^2 \end{pmatrix}.$$

Then $A_1(v)$ has 16 elements and is self-orthogonal with respect to M_E and is therefore a self-dual code with respect to M_E . The code $A_2(v)$ is $\mathbb{F}_4^4$, i.e. the entire space. The code $A_1(v)$ is not self-orthogonal with respect to duality M_T and, therefore, in the chain $A_1(v) \subset A_2(v)$ there is no self-dual code with respect to M_T .

4.3. Constructions

We shall show how self-orthogonal and self-dual codes can be constructed in this setting. In [8], it was shown that if R is a finite commutative Frobenius ring and G is a group of order n , with v an element in RG , satisfying $v = v^T$, $v^2 = 0$ and $|C_v| = |R|^{\frac{n}{2}}$ then C_v is a self-dual code.

In our setting, the situation is different. Consider the matrix given in Equation 3. It is quite possible that the matrix $\sigma(v)$ generates a self-orthogonal code over the additive group K_i , but this does not guarantee that the code over K_{i+1} is also going to be self-orthogonal. As a trivial example, consider the code of length 1 over $\mathbb{F}_4$ generated by (1). Using the duality M_T , this code is a self-dual code over the additive group $K_1 = \mathbb{F}_2$. However, over $\mathbb{F}_4$, this code is the entire ambient space which is obviously not self-orthogonal. This simple example, however, leads to an important computational technique.

In the search for self-dual codes using the matrix $\sigma(v)$. It happens quite often that the dimension of $\langle \sigma(v) \rangle$ is greater than $\frac{n}{2}$ which prohibits the matrix from generating a self-dual code that is invariant under the action of G . However, it is possible that $\langle \sigma(v) \rangle_{p^i}$ may be a self-dual code for a given duality M as we describe in the next theorem.

Theorem 4.24. *Let $v \in \mathbb{F}_{p^e}G$ for some finite group G . Assume that $\dim \langle \sigma(v) \rangle = d > \frac{n}{2}$. If $s = \frac{en}{2d}$ is an integer and $\langle \sigma(v) \rangle_{p^s}$ is self-orthogonal with respect to duality M , then the code C generated by the d linearly independent vectors of $\sigma(v)$ over the additive group K_s is a self-dual code with respect to M that is held invariant by the action of the group G .*

Proof. If the d vectors are linearly independent over $\mathbb{F}_{p^e}$ then they are independent over the additive group K_s . The size of the code they generate over K_s is $(p^s)^d = (p^{\frac{en}{2d}})^d = p^{\frac{en}{2}}$. Then since the code is self-orthogonal with respect to M , the code is self-dual. $\square$

5. Conclusion

Previous work about G -codes considered only linear codes over the finite field $\mathbb{F}_q$ (see [8], [9] for example.) Additive self-dual codes are defined over the field $\mathbb{F}_2$ as in [10]. In this paper, we have expanded both notions to consider additive self-dual G -codes over any finite field. We have discussed several dualities attached to these codes and we have examined the properties of these duals. We have found examples of additive self-dual codes of length 1 and have used this to show that additive self-dual codes exist for all lengths in certain cases.

Acknowledgements

This work has been partially supported by the Spanish MINECO under Grant PID2019-104664GB-I00 (AEI/FEDER, UE). The first author is grateful to the Universitat Autònoma de Barcelona where he stayed while this paper was written.

References

- [1] J. Bierbrauer, The theory of cyclic codes and a generalization to additive codes, *Designs, Codes and Cryptography*, vol. 25, pp. 189-206, 2002.
- [2] A.R. Calderbank, E.M. Rains, P.M. Shor, N.J.A. Sloane, Quantum error correction via codes over $\text{GF}(4)$, *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369-1387, 1998.
- [3] P. Delsarte, "An algebraic approach to the association schemes of coding theory", *Philips Research Rep. Suppl.*, vol. 10, vi+97, 1973.

- [4] P. Delsarte, V. Levenshtein, “Association Schemes and Coding Theory”, *IEEE Trans. Inform. Theory*, vol. 44(6), pp. 2477-2504, 1998.
- [5] S.T. Dougherty, Algebraic Coding Theory over Finite Commutative Rings, Springer Briefs in Mathematics. Springer, 2017.
- [6] S.T. Dougherty, C. Fernandez-Cordoba, R. Ten and B. Yildiz, Quaternary Group Rings: Ranks, Kernels and Self-Dual Codes, *Advances in Mathematics of Communications*, vol. 14(2), pp. 319-332, 2020.
- [7] S.T. Dougherty, J. Gildea, A. Korban, G -codes over Formal Power Series Rings and Finite Chain Rings, in submission.
- [8] S.T. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylyshchak, B. Yildiz, Bordered constructions of self-dual codes from group rings and new extremal binary self-dual codes., *Finite Fields Appl.*, vol. 57, pp. 108-127, 2019.
- [9] S.T. Dougherty, J. Gildea, R. Taylor and A. Tylyshchak, Group Rings, G -Codes and Constructions Of Self-Dual and Formally Self-Dual Codes, *Designs, Codes and Cryptography*, vol. 86(9), pp. 2115-2138, 2018.
- [10] S. T. Dougherty, J.-L. Kim, and N. Lee, Additive self-dual codes over fields of even order, *Bulletin of the Korean Mathematical Society*, vol. 55(2), pp. 341-357, 2018.
- [11] S.T. Dougherty, S. Meyers, Orthogonality from Group Characters, in submission.
- [12] J. Gildea, A. Kaya, R. Taylor, B. Yildiz, Constructions for self-dual codes induced from group rings. *Finite Fields Appl.*, vol. 51, pp. 71-92, 2018.
- [13] T. Hurley, Group Rings and Rings of Matrices, *Int. Jour. Pure and Appl. Math.*, vol. 31(3), pp. 319-335, 2006.
- [14] F.J. MacWilliams, Binary codes which are ideals in the group algebra of an Abelian group *Bell System Tech. J.*, vol. 49, pp. 987-1011, 1970.
- [15] S. Mahmoudi, K. Samei, Additive codes over Galois rings. *Finite Fields Appl.*, vol. 56, pp. 332-350, 2019.