Noname manuscript No.
(will be inserted by the editor)

Additive semisimple multivariable codes over $\mathbb{F}_4$

E. Martínez-Moro · A. Piñera-Nicolás · I.F. Rúa

the date of receipt and acceptance should be inserted later

Abstract The structure of additive multivariable codes over $\mathbb{F}_4$ (the Galois field with 4 elements) is presented. The semisimple case (i.e., when the defining polynomials of the code have no repeated roots) is specifically addressed. These codes extend in a natural way the abelian codes, of which additive cyclic codes of odd length are a particular case. Duality of these codes is also studied.

Keywords Additive multivariable codes, abelian codes, quantum codes, duality

Mathematics Subject Classification (2000) 11T61, 94B99, 81P70, 13M10

1 Introduction

Quantum codes are designed to detect and correct the errors produced in quantum computations [14,15]. These codes can be constructed with the help of specific classical codes, called *additive*, over $\mathbb{F}_4$ (the Galois field with 4 elements) [2]. An additive code of length n is a subgroup of $\mathbb{F}_4^n$ under addition. The particular case of additive cyclic codes has been considered in [5]. An additive code $\mathcal{C}$ is called *cyclic* if, whenever $c = (c_1, \ldots, c_n) \in C$, then its cyclic shift $(c_2, \ldots, c_n, c_1)$ is also a codeword in $\mathcal{C}$. These codes are related to properties of the ring $\mathbb{F}_4[X]/\langle X^n - 1\rangle$. In the case n odd, the semisimple structure of this ring can be used to obtain a complete description of the codes [7]. The case n even has been also considered [8].

Many authors have stated that many classical codes are ideals in certain algebras over a finite field, see for example [1,3,12]. In particular, *multivariable* codes have been considered, i.e., codes that can be viewed as ideals of the quotient ring $\mathbb{F}_4[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$ (where $t_i(X_i) \in \mathbb{F}_4[X_i]$ are fixed polynomials). Abelian codes, i.e., multivariable codes where $t_i(X_i) = X_i^{n_i} - 1$, for all $1 \leq i \leq r$, are particular cases, and they extend classical cyclic codes. These types of codes

E. Martínez-Moro · A. Piñera-Nicolás
Institute of Mathematics (IMUVa) and Applied Mathematics Department, Universidad de Valladolid. E-mail: edgar@maf.uva.es, anicolas@maf.uva.es

I.F. Rúa
Departamento de Matemáticas, Universidad de Oviedo. E-mail: rua@uniovi.es

have been also constructed if the underlying ring is not a field, but a finite chain ring [9,10].

In this paper we describe additive multivariable codes over the finite field $\mathbb{F}_4$, when the polynomials $t_i(X_i) \in \mathbb{F}_2[X_i]$ have no repeated-roots. The semisimple structure of the rings $\mathcal{A}_4 = \mathbb{F}_4[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$ and $\mathcal{A}_2 = \mathbb{F}_2[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$ is fundamental in this description.

The paper is organized as follows. In Section 2 we review the basic terminology and the results concerning the decomposition of the rings $\mathcal{A}_4$ and $\mathcal{A}_2$, and their relation. Section 3 is devoted to the description of the structure of the additive codes. In Section 4 we study the duals of abelian semisimple codes. Finally in Section 5 we characterize those non-trivial abelian semisimple codes that are self-dual.

2 Preliminaries

In this section we will obtain the structure of the ambient space of additive semisimple multivariable codes over the finite field $\mathbb{F}_4$. That is, we will describe explicitly the structure of the ring $\mathcal{A}_4 = \mathbb{F}_4[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$, where $t_i(X_i) \in \mathbb{F}_2[X_i]$ for all $i = 1, \ldots, r$. In order to obtain this description we will decompose this ring as a direct sum of ideals. See [13] for proofs and details about this decomposition.

2.1 Decomposition of $\mathbb{F}_q[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$

Let $q = p^e$ (p prime), and let $I = \langle t_1(X_1), \ldots, t_r(X_r)\rangle \lhd \mathbb{F}_q[X_1, \ldots, X_r]$ be the ideal generated by monic polynomials $t_i(X_i) \in \mathbb{F}_p[X_i]$, of degree n_i, $i = 1, \ldots, r$ (in this paper we are concerned with the case $q = 2^2$). Let H_i be the set of roots of $t_i(X_i)$ in an suitable extension field of $\mathbb{F}_q$ for each $i = 1, \ldots, r$. We require that $t_i(X_i)$ has no multiple roots for all $i = 1, \ldots, r$. We are interested in the decomposition of the algebra $\mathcal{A}_q = \mathbb{F}_q[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$.

Definition 1 Let $\mu = (\mu_1, \ldots, \mu_r) \in H_1 \times \ldots \times H_r$, then we define the $q-$class of μ as

$$C_q(\mu) = \left\{ (\mu_1^{q^s}, \ldots, \mu_r^{q^s}) \mid s \in \mathbb{N} \right\}.$$

Proposition 1 *Let $\mu = (\mu_1, \ldots, \mu_r) \in H_1 \times \ldots \times H_r$ and let q_i be the degree of the minimal polynomial of μ_i over $\mathbb{F}_q$ for each $i = 1, \ldots, r$. Then we have that*

1. *$|C_q(\mu)| = \mathrm{l.c.m.}(q_1, q_2, \ldots, q_r) = [\mathbb{F}_q(\mu_1, \ldots, \mu_r) : \mathbb{F}_q]$.*
2. *The set $\mathcal{C}_q$ of $q-$classes $C_q(\mu)$ is a partition of $H_1 \times \ldots \times H_r$.*
3. *For each ideal $\mathcal{I} \lhd \mathbb{F}_q[X_1, \ldots, X_r]/I$ the affine variety $V(\mathcal{I})$ of common zeros of the elements in $\mathcal{I}$ is a union of classes.*

Definition 2 Let K be an algebraic extension of $\mathbb{F}_q$ and let $\alpha \in K$. Let us denote by $\mathrm{Irr}(\alpha, \mathbb{F}_q)$ the minimal polynomial of α over the field $\mathbb{F}_q$. If $\mu = (\mu_1, \ldots, \mu_r) \in H_1 \times \ldots \times H_r$, then consider the following polynomials:

1. $p_{\mu,i}(X_i) = \mathrm{Irr}(\mu_i, \mathbb{F}_q)$, and $d_{\mu,i} = \deg p_{\mu,i}$ for all $i = 1, \ldots, r$.
2. $w_{\mu,i}(\mu_1, \ldots, \mu_{i-1}, X_i) = \mathrm{Irr}(\mu_i, \mathbb{F}_q(\mu_1, \ldots, \mu_{i-1}))$ for all $i = 2, \ldots, r$.

3. $\pi_{\mu,i}(\mu_1, \ldots, \mu_{i-1}, X_i) = p_{\mu,i}(X_i)/w_{\mu,i}(\mu_1, \ldots, \mu_{i-1}, X_i)$ for all $i = 2, \ldots, r$.

Remark 1 All the polynomials in the definition above can be seen as polynomials in $\mathbb{F}_q[X_1, \ldots, X_r]$ (substituting μ_i by X_i) and the following ring isomorphism holds

$$\mathbb{F}_q[X_1, \ldots, X_r]/\langle p_{\mu,1}, w_{\mu,2}, \ldots, w_{\mu,r}\rangle \cong \mathbb{F}_q(\mu_1, \ldots, \mu_r).$$

Moreover, if $\mu' \in C_q(\mu)$, then $p_{\mu,i} = p_{\mu',i}$ $i = 1, \ldots, r$ and $w_{\mu,i} = w_{\mu',i}, \pi_{\mu,i} = \pi_{\mu',i}$ $i = 2, \ldots, r$. Thus, if $C = C_q(\mu)$ is the $q-$class of μ, we will write $p_{C,i} = p_{\mu,i}, d_{C,i} = d_{\mu,i}, w_{C,i} = w_{\mu,i}, \pi_{C,i} = \pi_{\mu,i}$. Analogously, the ideal $\langle p_{C,1}, w_{C,2}, \ldots, w_{C,r}\rangle$ will be denoted by I_C.

Definition 3 Let $\mu = (\mu_1, \ldots, \mu_r) \in H_1 \times \ldots \times H_r$. If $C = C_q(\mu)$ is the $q-$class of μ, we define the following polynomial in $\mathbb{F}_q[X_1, \ldots, X_r]$

$$h_C(X_1, \ldots, X_r) = \prod_{i=1}^{r} \frac{t_i(X_i)}{p_{C,i}(X_i)} \prod_{i=2}^{r} \pi_{C,i}(X_i, \ldots, X_r).$$

Proposition 2 *Let $\mu = (\mu_1, \ldots, \mu_r) \in H_1 \times \ldots \times H_r$. If $C = C_q(\mu)$ is the $q-$class of μ, then*

1. *The annihilator of $\langle h_C + I\rangle$ (in $\mathcal{A}_q$) is $I_C + I$,*
2. *The set of zeros of h_C is $H_1 \times \ldots \times H_r \setminus C$,*
3. *The set of zeros of I_C is C.*

Theorem 1 (Decomposition of the ambient space $\mathcal{A}_q$)

$$\mathcal{A}_q = \mathbb{F}_q[X_1, \ldots, X_r]/I \cong \bigoplus_{C \in \mathcal{C}_q} \langle h_C + I\rangle$$

where $\langle h_C + I\rangle \cong \mathbb{F}_q[X_1, \ldots, X_r]/I_C$ is a finite field isomorphic to $\mathbb{F}_q(\mu_1, \ldots, \mu_r) \cong \mathbb{F}_{q^{|C|}}$, and so the algebra $\mathcal{A}_q$ is semisimple. Hence, there exists a unique set of primitive orthogonal idempotents $\{e_C + I\}_{C\in\mathcal{C}_q} \subseteq \mathcal{A}_q$ such that $1 + I = \sum_{C\in\mathcal{C}_q} e_C + I$ and $\mathcal{A}_q(e_C+I) \cong \langle h_C + I\rangle$. Namely, the idempotent e_C+I is exactly the element $g_C h_C+I$, with $g_C h_C + I_C = 1 + I_C$, and its set of zeros is $H_1 \times \ldots \times H_r \setminus C$

Remark 2 Notice that if $q = 4$, $r = 1$ and $t_1(X) = X^n - 1$ with n odd, we obtain the ambient space of additive cyclic codes over $\mathbb{F}_4$ described in [7]. In this case, if α is a primitive nth-root of unity and $\mu = \alpha^i$, then the exponents of the elements in the $q-$class $C = C_4(\mu)$ are the elements of the 4-cyclotomic coset containing i. Also, each direct summand $h_C + I \cong \mathbb{F}_{4^{\lambda_C}}$, where λ_C is the size of the $q-$class C, that is, the degree of the irreducible polynomial p_C.

Classical multivariable codes over $\mathbb{F}_4$ are defined as the ideals of the algebra $\mathcal{A}_4$. However, since additive codes are no longer closed under multiplication by arbitrary elements of $\mathbb{F}_4$, they do not correspond to ideals of this ring. This type of codes are related instead to submodules of $\mathcal{A}_4$, when viewed as a module over one of its subrings.

Lemma 1 *If $f \in \mathbb{F}_q[X_1, \ldots, X_r]$, then there exists a unique polynomial $NF(f) \in \mathbb{F}_q[X_1, \ldots, X_r]$ such that $f + I = NF(f) + I$, and $\deg_{X_i}(NF(f)) < n_i$. It is called the* normal form of f w.r.t. I. *Moreover, two polynomials $f, g \in \mathbb{F}_q[X_1, \ldots, X_r]$ satisfy $f + I = g + I$ if and only if $NF(f) = NF(g)$. In particular, all classes $f + I$, where $0 \neq f$ and $\deg_{X_i}(NF(f)) < n_i$, for all $1 \leq i \leq r$, are not zero.*

Proof Consider the lexicographic monomial order with $X_1 > X_2 > \cdots > X_r$. Then, $\{t_1(X_1), \ldots, t_r(X_r)\}$ is a Groebner basis of I (actually its reduced Groebner basis w.r.t. such an order), and so the result follows from [4, Chapter 2, Section 9, Theorem 3 and Proposition 4].

Definition 4 Let S be the set of elements $f+I \in \mathcal{A}_q$ such that $NF(f) \in \mathbb{F}_p[X_1, \ldots, X_r]$.

¿From now on, let us denote by J the ideal in $\mathbb{F}_p[X_1, \ldots, X_r]$ generated by $t_i(X_i)$, $i = 1, \ldots, r$, and by $\mathcal{A}_p$ the algebra $\mathbb{F}_p[X_1, \ldots, X_r]/J$ (notice that $t_i(X_i) \in \mathbb{F}_p[X_i]$, for all $i = 1, \ldots, r$).

Proposition 3 *There exists a ring monomorphism $\varphi : \mathcal{A}_p \to \mathcal{A}_q$ such that $\varphi(f+J) = f + I$, for all $f \in \mathbb{F}_p[X_1, \ldots, X_r]$. The set S is the image of this map, and so it is a subring of $\mathcal{A}_q$ isomorphic to $\mathcal{A}_p$.*

Proof Consider the ring homomorphisms $\pi_q \circ i : \mathbb{F}_p[X_1, \ldots, X_r] \to \mathcal{A}_q$, given by $(\pi_q \circ i)(f) = f + I$, and $\pi_p : \mathbb{F}_p[X_1, \ldots, X_r] \to \mathcal{A}_p$, given by $\pi_p(f) = f + J$. Since $\ker \pi_p \subseteq \ker \pi_q \circ i$, there exists a ring homomorphism $\varphi : \mathcal{A}_p \to \mathcal{A}_q$ such that $\varphi(f + J) = f + I$, for all $f \in \mathbb{F}_p[X_1, \ldots, X_r]$.

For all $f \notin J$, we have that $f + J = NF(f) + J$, where $0 \neq NF(f) \in \mathbb{F}_p[X_1, \ldots, X_r] \subseteq \mathbb{F}_q[X_1, \ldots, X_r]$, and $\deg_{X_i}(NF(f)) < n_i$. So, $\varphi(f+J) = \varphi(NF(f)+J) = NF(f) + I \neq I$, and the map is injective. Since $\mathrm{Im}(\varphi) \subseteq S$, a simple counting argument let us conclude the equality $\mathrm{Im}(\varphi) = S$, and so $\mathcal{A}_p \cong S$.

Definition 5 An *additive (semisimple) multivariable code over* $\mathbb{F}_q$ is a submodule of the module ${}_S\mathcal{A}_q$.

Remark 3 These codes are called *semisimple* because the roots of the polynomials $t_i(X_i)$ are required to be simple. If $q = 4$, $r = 1$, $t_1(X) = X^n - 1$, with n odd, additive multivariable codes over $\mathbb{F}_4$ are exactly the additive cyclic codes over $\mathbb{F}_4$ described in [7].

Remark 4 It is just a straight forward fact that a semisimple code on $\mathcal{A}_2$ can be seen as a shortened code of an abelian code choosing adequate polynomials $X_i^{n_i} - 1$ such that $t_i(X_i)|X_i^{n_i} - 1$ (thus we must shorten the codes in the positions not in t_i). This follows directly from the fact that the ideals of $\mathbb{F}[X]/\langle t(X)\rangle$ (t having simple roots) are shortened cyclic codes (see for example [11, Section 8.10]).

Example 1 We shall illustrate the contents of the paper with the help of the following running example. Let us consider $t_1(X_1) = X_1^7 + 1, t_2(X_2) = X_2^3 + 1$ polynomials in $\mathbb{F}_q[X_1, X_2]$. The normal form of an element $f + I$, which has the shape $\sum_{j=0}^{6} \sum_{i=0}^{2} f_{ij} X_1^j X_2^i$, will be written as the matrix

$$F = (f_{ij}) = \begin{bmatrix} f_{00} & f_{01} & \cdots & f_{06} \\ f_{10} & f_{11} & \cdots & f_{16} \\ f_{20} & f_{21} & \cdots & f_{26} \end{bmatrix}$$

.

We shall describe the decompositions of the algebras $\mathcal{A}_q$ for $q = 2$ and 4.

– If $q = 2$, then the set of 2−classes is the following one:

$$\begin{aligned}\mathcal{C}_2 = \{\ &\{(1,1)\}\ ,\ \{(\mu,1),(\mu^2,1),(\mu^4,1)\}\ ,\ \{(\mu^6,1),(\mu^5,1),(\mu^3,1)\}\ ,\\ &\{(1,\omega),(1,\omega^2)\}\ ,\{(\mu,\omega),(\mu^2,\omega),(\mu^4,\omega),(\mu,\omega^2),(\mu^2,\omega^2),(\mu^4,\omega^2)\}\ ,\\ &\{(\mu^6,\omega),(\mu^5,\omega),(\mu^3,\omega),(\mu^6,\omega^2),(\mu^5,\omega^2),(\mu^3,\omega^2)\}\}\end{aligned}$$

where $\mu \in \mathbb{F}_{2^3}, \omega \in \mathbb{F}_{2^2}$ such that $\mu^3 + \mu + 1 = \omega^2 + \omega + 1 = 0$. The algebra $\mathcal{A}_2$ is decomposed as the direct sum of six ideals, which are generated by the following idempotents:

$$\mathcal{K}_{\{(1,1)\}} = \left\langle \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix} \right\rangle , \quad \mathcal{K}_{C_2((\mu,1))} = \left\langle \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \end{bmatrix} \right\rangle ,$$

$$\mathcal{K}_{C_2((\mu^6,1))} = \left\langle \begin{bmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 1\,0\,0\,1\,0\,1\,1 \\ 1\,0\,0\,1\,0\,1\,1 \end{bmatrix} \right\rangle , \mathcal{K}_{C_2((1,\omega))} = \left\langle \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix} \right\rangle ,$$

$$\mathcal{K}_{C_2((\mu,\omega))} = \left\langle \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \end{bmatrix} \right\rangle , \ \mathcal{K}_{C_2((\mu^6,\omega))} = \left\langle \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,0\,1\,0\,1\,1 \\ 1\,0\,0\,1\,0\,1\,1 \end{bmatrix} \right\rangle .$$

– If $q = 4$, then the set of 4−classes is the following one:

$$\begin{aligned}\mathcal{C}_4 = \{\ &\{(1,1)\}\ ,\ \{(\mu,1),(\mu^2,1),(\mu^4,1)\}\ ,\ \{(\mu^6,1),(\mu^5,1),(\mu^3,1)\}\ ,\\ &\{(1,\omega)\}\ ,\ \{(1,\omega^2)\}\ ,\ \{(\mu,\omega),(\mu^2,\omega),(\mu^4,\omega)\}\ ,\\ &\{(\mu,\omega^2),(\mu^2,\omega^2),(\mu^4,\omega^2)\}\ ,\{(\mu^6,\omega),(\mu^5,\omega),(\mu^3,\omega)\}\ ,\\ &\{(\mu^6,\omega^2),(\mu^5,\omega^2),(\mu^3,\omega^2)\}\}\end{aligned}$$

Observe that each 2−class of even size splits into two 4−classes. The decomposition of $\mathcal{A}_4$ is given by the following direct sum of 9 ideals generated by the idempotents

$$\mathcal{I}_{\{(1,1)\}} = \left\langle \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix} \right\rangle , \quad \mathcal{I}_{C_4((\mu,1))} = \left\langle \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \end{bmatrix} \right\rangle ,$$

$$\mathcal{I}_{C_4((\mu^6,1))} = \left\langle \begin{bmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 1\,0\,0\,1\,0\,1\,1 \\ 1\,0\,0\,1\,0\,1\,1 \end{bmatrix} \right\rangle , \quad \mathcal{I}_{\{(1,\omega)\}} = \left\langle \begin{bmatrix} 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega} \\ \omega\ \omega\ \omega\ \omega\ \omega\ \omega\ \omega \end{bmatrix} \right\rangle ,$$

$$\mathcal{I}_{C_4((1,\omega^2))} = \left\langle \begin{bmatrix} 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ \omega\ \omega\ \omega\ \omega\ \omega\ \omega\ \omega \\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ \overline{\omega} \end{bmatrix} \right\rangle , \ \mathcal{I}_{C_4((\mu,\omega))} = \left\langle \begin{bmatrix} 1\ 1\ 1\ 0\ 1\ 0\ 0 \\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ 0\ \overline{\omega}\ 0\ 0 \\ \omega\ \omega\ \omega\ 0\ \omega\ 0\ 0 \end{bmatrix} \right\rangle$$

$$\mathcal{I}_{C_4((\mu,\omega^2))} = \left\langle \begin{bmatrix} 1\ 1\ 1\ 0\ 1\ 0\ 0 \\ \omega\ \omega\ \omega\ 0\ \omega\ 0\ 0 \\ \overline{\omega}\ \overline{\omega}\ \overline{\omega}\ 0\ \overline{\omega}\ 0\ 0 \end{bmatrix} \right\rangle , \ \mathcal{I}_{C_4((\mu^6,\omega))} = \left\langle \begin{bmatrix} 1\ 0\ 0\ 1\ 0\ 1\ 1 \\ \overline{\omega}\ 0\ 0\ \overline{\omega}\ 0\ \overline{\omega}\ \overline{\omega} \\ \omega\ 0\ 0\ \omega\ 0\ \omega\ \omega \end{bmatrix} \right\rangle ,$$

$$\mathcal{I}_{C_4((\mu^6,\omega^2))} = \left\langle \begin{bmatrix} 1\ 0\ 0\ 1\ 0\ 1\ 1 \\ \omega\ 0\ 0\ \omega\ 0\ \omega\ \omega \\ \overline{\omega}\ 0\ 0\ \overline{\omega}\ 0\ \overline{\omega}\ \overline{\omega} \end{bmatrix} \right\rangle .$$

(where $\overline{\omega} = \omega^2$). Notice that $\mathcal{A}_2$ is identified with the subalgebra S of $\mathcal{A}_4$ of elements whose normal form has coefficients 0 or 1.

2.2 Relation between the decompositions of $\mathcal{A}_4$ and $\mathcal{A}_2$

From now on, let us fix $q = 4$. In the following, we will describe the relation between the structures of the algebras $\mathcal{A}_4$ and $\mathcal{A}_2$. This will lead us, in the following section, to the description of the additive multivariable codes over $\mathbb{F}_4$. Since these decompositions are based on classes of roots, we first establish the relation between the $2-$classes $C_2(\mu)$ and the $4-$classes $C_4(\mu)$

Lemma 2 *Let μ_i be a root of the polynomial $t_i(X_i)$, $1 \leq i \leq r$. Let $q_i = \deg(\mathrm{Irr}(\mu_i, \mathbb{F}_4))$ and $k_i = \deg(\mathrm{Irr}(\mu_i, \mathbb{F}_2))$. If $\mu = (\mu_1, \ldots, \mu_r)$, then:*

1. *If k_i is odd for all $1 \leq i \leq r$, then $C_2(\mu) = C_4(\mu)$, and it has size $\mathrm{l.c.m.}(k_1, \ldots, k_r)$.*
2. *If there exists $i \in \{1, \ldots, r\}$ such that k_i is even, then $C_2(\mu) = C_4(\mu) \cup C_4(\mu^2)$, where $\mu^2 = (\mu_1^2, \ldots, \mu_r^2)$. The union is disjoint and both classes have equal size $\mathrm{l.c.m}(q_1, \ldots, q_r)$.*

The subset of $2-$classes in the first case will be denoted $\mathcal{C}_2^o$, where as the $2-$classes in the second case will be denoted $\mathcal{C}_2^e$.

Proof If k_i is odd for all $1 \leq i \leq r$, then the minimal polynomials $\{\mathrm{Irr}(\mu_i, \mathbb{F}_2)\}_{i=1}^r$ are also irreducible in $\mathbb{F}_4[X_i]$, and $q_i = k_i$. So, the result straightforwardly follows from Proposition 1.
In the second case assume w.l.o.g. that k_i is even, for all $1 \leq i \leq k$, and odd for all $k+1 \leq i \leq r$ (with $k \geq 1$). Then, for all $1 \leq i \leq k$, the minimal polynomial $\mathrm{Irr}(\mu_i, \mathbb{F}_2)$ is the product of two irreducible polynomials of degree q_i in $\mathbb{F}_4[X_i]$. The roots of these polynomials constitute the $4-$classes $C_4(\mu_i)$ and $C_4(\mu_i^2)$ respectively. Clearly, these are disjoint classes of equal size q_i and $C_2(\mu_i) = C_4(\mu_i) \cup C_4(\mu_i^2)$. Therefore, μ^2 does not belong to $C_4(\mu)$ and so $C_4(\mu^2)$ is disjoint with it. According to Proposition 1,

$$\begin{aligned}|C_2(\mu)| &= \mathrm{l.c.m}(k_1, \ldots, k_r) = \mathrm{l.c.m}(2q_1, \ldots, 2q_k, q_{k+1}, \ldots, q_r) = \\ &= 2\,\mathrm{l.c.m}(q_1, \ldots, q_k, q_{k+1}, \ldots, q_r) = 2|C_4(\mu)|\end{aligned}$$

and also

$$|C_2(\mu)| = |C_2(\mu^2)| = 2|C_4(\mu^2)|$$

hence we obtain the result.

Now, we can decompose the rings $\mathcal{A}_4$ and $\mathcal{A}_2$ into minimal ideals using Theorem 1. The decomposition for $\mathcal{A}_4$ is the following one:

$$\mathcal{A}_4 \cong \bigoplus_{C \in \mathcal{C}_4} \mathcal{I}_C$$

where, for all $C = C_4(\mu) \in \mathcal{C}_4$, we denote the ideal $\mathcal{I}_C = \langle e_C + I \rangle$, which is isomorphic to the finite field $\mathbb{F}_4(\mu)$ of size $4^{|C|}$, and $e_C + I$ is idempotent.
On the other hand, the decomposition of the ring $\mathcal{A}_2$ into minimal ideals is

$$\mathcal{A}_2 \cong \bigoplus_{C \in \mathcal{C}_2} \mathcal{K}_C = \left(\bigoplus_{C \in \mathcal{C}_2^o} \mathcal{K}_C \right) \oplus \left(\bigoplus_{C \in \mathcal{C}_2^e} \mathcal{K}_C \right)$$

where, for all $C = C_2(\mu) \in \mathcal{C}_2^o \cup \mathcal{C}_2^e$, $\mathcal{K}_C = \langle l_C + J \rangle$ is isomorphic to the field $\mathbb{F}_2(\mu)$, and so its size is $2^{|C|}$, and the element $l_C + J$ is idempotent.

Next, let us consider the ring automorphism $\tau : \mathbb{F}_4[X_1,\ldots,X_r] \to \mathbb{F}_4[X_1,\ldots,X_r]$, where

$$\tau\left(\sum_{i_1,\ldots,i_r} a_{i_1\ldots,i_r} X_1^{i_1}\cdots X_r^{i_r}\right) = \sum_{i_1,\ldots,i_r} a^2_{i_1\ldots,i_r} X_1^{i_1}\cdots X_r^{i_r}$$

Since $t_i(X_i) \in \mathbb{F}_2[X_i]$, for all $1 \le i \le r$, we have that $\tau(t_i(X_i)) = t_i(X_i)$, and so $\ker(\pi_4 \circ \tau) \subseteq \ker \pi_4$ (where $\pi_4 : \mathbb{F}_4[X_1,\ldots,X_r] \to \mathcal{A}_4$ is the canonical epimorphism). Hence, there exists a ring homomorphism $\tilde{\tau} : \mathcal{A}_4 \to \mathcal{A}_4$ such that $\tilde{\tau}(f+I) = \tau(f)+I$, for all $f+I \in \mathcal{A}_4$. This map is injective, since for all $f \notin I$, we have that $f+I = NF(f)+I$, where $0 \ne NF(f) \in \mathbb{F}_4[X_1,\ldots,X_r]$, and $\deg_{X_i}(NF(f)) < n_i$, and so $\tilde{\tau}(f+I) = \tau(NF(f))+I \ne I$. Clearly, this fact implies that $\tilde{\tau}$ is also bijective and so it is a ring automorphism. Its fixed subring is S.

Proposition 4 *Let $\mathcal{A}_4 \cong \bigoplus_{C\in\mathcal{C}_4} \mathcal{I}_C$ and $\mathcal{A}_2 \cong \bigoplus_{C\in\mathcal{C}_2^o} \mathcal{K}_C \oplus \bigoplus_{C\in\mathcal{C}_2^e} \mathcal{K}_C$ be the decompositions of $\mathcal{A}_4$ and $\mathcal{A}_2$ into minimal ideals, and let S be the subring of $\mathcal{A}_4$, isomorphic to $\mathcal{A}_2$, fixed by $\tilde{\tau}$. If φ is the embedding of $\mathcal{A}_2$ in $\mathcal{A}_4$ (see Proposition 3), then the following hold.*

1. *If $C \in \mathcal{C}_2^o$, then:*
   (a) $C \in \mathcal{C}_4$, $\tilde{\tau}(\mathcal{I}_C) = \mathcal{I}_C$, and $\tilde{\tau}|_{\mathcal{I}_C}$ is a field automorphism of order 2.
   (b) $\varphi(\mathcal{K}_C) = \mathcal{I}_C \cap S$, so it is the subfield of $\mathcal{I}_C$ isomorphic to $\mathbb{F}_{2^{|C|}}$.
   (c) $\mathcal{I}_C$ is $2-$dimensional $\mathcal{K}_C$-vector space.
2. *If $C \in \mathcal{C}_2^e$, then:*
   (a) $C = C_1 \cup C_2$, where $C_1, C_2 \in \mathcal{C}_4$, $\tilde{\tau}(\mathcal{I}_{C_1}) = \mathcal{I}_{C_2}$, $\tilde{\tau}(\mathcal{I}_{C_2}) = \mathcal{I}_{C_1}$, and $\tilde{\tau}|_{\mathcal{I}_{C_1}\to\mathcal{I}_{C_2}}$ is a field isomorphism.
   (b) $\varphi(\mathcal{K}_C) = (\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}) \cap S = \{(f+\tau(f))+I \mid f \in \mathcal{I}_{C_1}\}$ is isomorphic to the field $\mathcal{I}_{C_1} \cong \mathbb{F}_{4^{|C_1|}} = \mathbb{F}_{2^{|C|}}$.
   (c) $\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$ is $2-$dimensional $\mathcal{K}_C$-vector space.

Proof Notice that, if μ is a root of $f(X_1,\ldots,X_r)$, then μ^2 is a root of the polynomial $\tau(f(X_1,\ldots,X_r))$, and $\tau^2(f(X_1,\ldots,X_r)) = f(X_1,\ldots,X_r)$. So, $\tilde{\tau}$ induces a permutation of order 2 of the idempotents $\{e_C+I\}_{C\in\mathcal{C}_4}$, so that $\tilde{\tau}(e_C+I) = e_C+I$ if $C \in \mathcal{C}_2^o$, and $\tilde{\tau}(e_{C_1}+I) = e_{C_2}+I$, $\tilde{\tau}(e_{C_2}+I) = e_{C_1}+I$, if $C_1 \cup C_2 = C \in \mathcal{C}_2^e$, where $C_1, C_2 \in \mathcal{C}_4$. This permutation is translated into the field isomorphisms of the statements 1.(a) and 2.(a).

For the statement 1.(b), it suffices to notice that $C = C_4(\mu) = C_2(\mu)$, so that $\varphi(l_C+J) = e_C+I$, and $\varphi(\mathcal{K}_C) \subseteq \mathcal{I}_C \cap S$. A counting argument let us conclude the desired equality.

Let us now show the statement 2.(b). The zeros of the idempotent $\varphi(l_C+J)$ are exactly $H_1\times\ldots\times H_r \setminus C$. The zeros of $e_{C_i}+I$ $(i=1,2)$ are $H_1\times\ldots\times H_r\setminus C_i$, and so the idempotent $e_{C_1}+e_{C_2}+I \in \mathcal{I}_{C_1}\oplus\mathcal{I}_{C_2}$ has zeros $H_1\times\ldots\times H_r \setminus (C_1\cup C_2) = H_1\times\ldots\times H_r\setminus C$. Hence $\varphi(l_C+J) \subseteq (\mathcal{I}_{C_1}\oplus\mathcal{I}_{C_2})\cap S$, and the equality follows from another counting argument.

Finally, the statements (c) follow from the fact that φ is an embedding of the finite field $\mathcal{K}_C$ (of size $2^{|C|}$) into the ring $\mathcal{I}_C$ (if $C \in \mathcal{C}_2^o$), or $\mathcal{I}_{C_1}\oplus\mathcal{I}_{C_2}$ (if $C\in\mathcal{C}_2^e$), and so they can be regarded as $\mathcal{K}_C-$vector spaces. Since both have size $4^{|C|}$, we conclude that their dimension is 2.

Remark 5 For $C \in \mathcal{C}_2^o$, the idempotent $e_C + I$ is the identity of $\varphi(\mathcal{K}_C)$, and so $e_C + I \in \varphi(\mathcal{K}_C) = \langle X_1^{i_1} \dots X_r^{i_r} e_C + I \mid 0 \le i_l \le \deg(t_l(X_l)) \rangle_{\mathbb{F}_2}$. On the other hand, for $C_1 \cup C_2 = C \in \mathcal{C}_2^e$ the idempotent $e_{C_1} + e_{C_2} + I$ is the identity of $\varphi(\mathcal{K}_C)$, and so $\varphi(\mathcal{K}_C) = \langle X_1^{i_1} \dots X_r^{i_r}(e_{C_1} + e_{C_2}) + I \mid 0 \le i_l \le \deg(t_l(X_l)) \rangle_{\mathbb{F}_2}$.

Example 2 (Example 1 cont'd) Here is the list of odd and even 2−classes:

$$\begin{aligned}
\mathcal{C}_2^o &= \{\{(1,1)\}\ ,\ \{(\mu,1),(\mu^2,1),(\mu^4,1)\}\ ,\ \{(\mu^6,1),(\mu^5,1),(\mu^3,1)\}\}\} \\
\mathcal{C}_2^e &= \{(1,\omega),(1,\omega^2)\}\ ,\ \{(\mu,\omega),(\mu^2,\omega),(\mu^4,\omega),(\mu,\omega^2),(\mu^2,\omega^2),(\mu^4,\omega^2)\}\ , \\
&\quad \{(\mu^6,\omega),(\mu^5,\omega),(\mu^3,\omega),(\mu^6,\omega^2),(\mu^5,\omega^2),(\mu^3,\omega^2)\}\}
\end{aligned}$$

The ideal

$$\mathcal{I}_{\{(1,1)\}} = \left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}, \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix}, \begin{bmatrix} \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \\ \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \\ \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \end{bmatrix}, \begin{bmatrix} \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \\ \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \\ \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \end{bmatrix} \right\}$$

(where $\overline{w} = w^2$) is isomorphic to $\mathbb{F}_4$, and it is a 2−dimensional vector space over the finite field $\mathbb{F}_2 \cong \mathcal{K}_{\{(1,1)\}} = \left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}\ ,\ \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix} \right\}$ Moreover, the elements in $\mathcal{I}_{\{(1,1)\}}$ with coefficients equal to 0 or 1 (i.e, in S) are exactly those of $\mathcal{K}_{\{(1,1)\}}$.

The ideal $\mathcal{I}_{C_4((\mu,1))}$ is isomorphic to $\mathbb{F}_{4^3}$, and it is a 2−dimensional vector space over the finite field

$$\begin{aligned}
\mathbb{F}_{2^3} \cong \mathcal{K}_{C_2((1,1))} = &\left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}, \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \end{bmatrix}, \begin{bmatrix} 0\,1\,1\,1\,0\,1\,0 \\ 0\,1\,1\,1\,0\,1\,0 \\ 0\,1\,1\,1\,0\,1\,0 \end{bmatrix}, \begin{bmatrix} 0\,0\,1\,1\,1\,0\,1 \\ 0\,0\,1\,1\,1\,0\,1 \\ 0\,0\,1\,1\,1\,0\,1 \end{bmatrix}, \right. \\
&\left. \begin{bmatrix} 1\,0\,0\,1\,1\,1\,0 \\ 1\,0\,0\,1\,1\,1\,0 \\ 1\,0\,0\,1\,1\,1\,0 \end{bmatrix}, \begin{bmatrix} 0\,1\,0\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,1\,1 \end{bmatrix}, \begin{bmatrix} 1\,0\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,0\,1\,1 \end{bmatrix}, \begin{bmatrix} 1\,1\,0\,1\,0\,0\,1 \\ 1\,1\,0\,1\,0\,0\,1 \\ 1\,1\,0\,1\,0\,0\,1 \end{bmatrix} \right\}
\end{aligned}$$

The ideals related to the 2 and 4−classes of $(\mu^6, 1)$ behave similarly.

On the other hand, all the even classes follow the pattern of the 2−class $\{(1,\omega),(1,\omega^2)\}$. Namely, the ideal

$$\mathcal{K}_{C_2((1,\omega))} = \left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}, \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix}, \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix}, \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix} \right\}$$

is isomorphic to $\mathbb{F}_4$, and the direct sum of the ideals

$$\mathcal{I}_{\{(1,\omega)\}} = \left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}, \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \\ \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \end{bmatrix}, \begin{bmatrix} \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \\ 1\,1\,1\,1\,1\,1\,1 \\ \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \end{bmatrix}, \begin{bmatrix} \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \\ \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix} \right\}$$

$$\mathcal{I}_{\{(1,\omega^2)\}} = \left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}, \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \\ \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \end{bmatrix}, \begin{bmatrix} \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \\ \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix}, \begin{bmatrix} \overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega}\,\overline{\omega} \\ 1\,1\,1\,1\,1\,1\,1 \\ \omega\,\omega\,\omega\,\omega\,\omega\,\omega\,\omega \end{bmatrix} \right\}$$

is a vector space over it.

3 Additive multivariable codes

Next we take advantage of the decomposition of the rings $\mathcal{A}_4, \mathcal{A}_2$, and their relation in order to obtain a complete description of an additive semisimple multivariable code $\mathcal{D} \subseteq \mathcal{A}_4$. From now on we assume that $\mathcal{A}_4 \cong \bigoplus_{C\in\mathcal{C}_4} \mathcal{I}_C$ and $\mathcal{A}_2 \cong \bigoplus_{C\in\mathcal{C}_2^o} \mathcal{K}_C \oplus \bigoplus_{C\in\mathcal{C}_2^e} \mathcal{K}_C$ are the decompositions of $\mathcal{A}_4$ and $\mathcal{A}_2$ into minimal ideals, that φ is the embedding of $\mathcal{A}_2$ in $\mathcal{A}_4$, and that $S = \varphi(\mathcal{A}_2)$ is the subring of $\mathcal{A}_4$ fixed by the ring automorphism $\tilde{\tau}$. The main result in this section is the following.

Theorem 2 *Let $\mathcal{D} \subseteq \mathcal{A}_4$ be an additive semisimple code, i.e., a $S-$submodule of $\mathcal{A}_4$.*

1. *If $C \in C_2^o$, then the set $\mathcal{D}_C = \mathcal{D} \cap \mathcal{I}_C$ is a $\mathcal{K}_C-$vector subspace of $\mathcal{I}_C$ of dimension $0 \le s_C \le 2$.*
2. *If $C \in C_2^e$, with $C = C_1 \cup C_2$, and $C_1, C_2 \in \mathcal{C}_4$, then the set $\mathcal{D}_C = \mathcal{D} \cap (\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2})$ is a $\mathcal{K}_C-$vector subspace of dimension $0 \le s_C \le 2$.*
3. *$\mathcal{D} = \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C$, $|\mathcal{D}| = \prod_{C\in\mathcal{C}_2} 2^{s_C}$, and the decomposition is unique.*

Proof 1. $\mathcal{D}_C$ is an additive subgroup of the ideal $\mathcal{I}_C$, since $\mathcal{D}$ is a code. Moreover, because it is an additive code, it is invariant under multiplication by elements in S so, in particular, by elements in $\mathcal{I}_C \cap S = \varphi(\mathcal{K}_C)$. Henceforth, since φ is injective, $\mathcal{D}_C$ can be viewed as a vector space over the finite field $\mathcal{K}_C$, i.e., as a vector subspace of $\mathcal{I}_C$. Because $\dim_{\mathcal{K}_C} \mathcal{I}_C = 2$, we conclude the condition on the dimension of $\mathcal{D}_C$.
2. The argument above applies also in this case replacing $\mathcal{I}_C$ by $\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$.
3. For all $C \in \mathcal{C}_2$ we have that $\mathcal{D}_C \subseteq \mathcal{D}$, and so $\bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C \subseteq \mathcal{D}$. Conversely, if $m + I \in \mathcal{D}$, then

$$m + I = (1 + I)(m + I) = \left(\bigoplus_{C\in\mathcal{C}_4} (e_C + I) \right) (m + I) =$$

$$= \left(\bigoplus_{C\in\mathcal{C}_2^o} (e_C + I) \oplus \bigoplus_{\substack{C_1, C_2 \in \mathcal{C}_4 \\ C_1 \cup C_2 \in \mathcal{C}_2^e}} (e_{C_1} + e_{C_2} + I) \right) (m + I)$$

$$= \bigoplus_{C\in\mathcal{C}_2^o} (e_C m + I) \oplus \bigoplus_{\substack{C_1, C_2 \in \mathcal{C}_4 \\ C_1 \cup C_2 \in \mathcal{C}_2^e}} ((e_{C_1} + e_{C_2})m + I) \in \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C$$

since $e_C m + I \in \mathcal{D}_C$ (for all $C \in \mathcal{C}_2^o$), and $(e_{C_1} + e_{C_2})m + I \in \mathcal{D}_C$ (for all $C_1 \cup C_2 = C \in \mathcal{C}_2^e$). Clearly, $|D| = \prod_{C\in\mathcal{C}_2} 2^{s_C}$.
Finally, let us show that this decomposition is unique. Let $\mathcal{D} = \bigoplus_{C\in\mathcal{C}_2} \mathcal{E}_C$ where $\mathcal{E}_C \subseteq \mathcal{I}_C$, if $C \in \mathcal{C}_2^o$, and $\mathcal{E}_C \subseteq \mathcal{I}_{C_1} \oplus I_{C_2}$, if $C_1 \cup C_2 = C \in \mathcal{C}_2^e$. Then, $\mathcal{E}_C \subseteq \mathcal{I}_C \cap \mathcal{D} = \mathcal{D}_C$, in the first case, and $\mathcal{E}_C \subseteq (\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}) \cap \mathcal{D} = \mathcal{D}_C$, in the second one. A counting argument on the sizes of these sets proves the result.

Corollary 1 *The number of different additive semisimple codes in $\mathcal{A}_4$ is*

$$\prod_{C\in\mathcal{C}_2} (2^{|C|} + 3)$$

Of these, only $\prod_{C\in\mathcal{C}_2} (2^{|C|} + 2)$ codes can be generated by a single codeword.

Proof The number of subspaces in a 2−dimensional vector space over a finite field $\mathbb{F}_q$ is $1+\frac{q^2-1}{q-1}+1=q+3$. Hence, the result follows directly from the decomposition of the previous theorem.

A code $\mathcal{D}_C$ can be generated by a single codeword if and only if it is a cyclic $S-$submodule of $\mathcal{A}_4$. So, all the submodules $\mathcal{D}_C$ have to be also cyclic $S-$submodules, and the dimension of the vector subspace $\mathcal{D}_C$ over $\mathcal{K}_C$ has to be either 0 or 1. The number of possible codes obtained from these subspaces is exactly $\prod_{C\in\mathcal{C}_2}(1+(2^{|C|}+1))$.

3.1 Hamming distance

Next, we study the minimum distance of our codes. Let us first introduce the standard definitions.

Definition 6 If $f \in \mathbb{F}_q[X_1,\ldots,X_r]$, and $NF(f)=\sum_{i=1}^{r} f_{\alpha_1\ldots\alpha_r} X_1^{\alpha_1}\cdot\cdots\cdot X_r^{\alpha_r}$ is its normal form w.r.t. I, then we define the *Hamming weight of* $f+I$ *(denoted by* $\mathrm{wt}(f+I)$*), as the cardinality of* $\mathrm{supp}(NF(f))=\{(\alpha_1,\ldots,\alpha_r)\mid f_{\alpha_1\ldots\alpha_r}\neq 0\}$*, the support of* $NF(f)$*.*

The minimum distance of an additive (semisimple) multivariable code $\mathcal{D}\subseteq\mathcal{A}_4$ *is defined as the minimum Hamming weight of the nonzero elements in* $\mathcal{D}$*, and it is denoted by* $d(\mathcal{D})$*.*

The study of the codes with the best Hamming distance for given parameters is one of the central problems in Coding Theory. A good source of bounds and examples of the best known codes (block linear, and quantum error correcting codes) can be found in *Code Tables* [6]. There exist several bounds on distances for *classical multivariable semisimple codes over fields (BCH, Hartmann-Tzeng, Roos, ...) [13]. These bounds can be stated in the additive case due to the following fact:*

Proposition 5 *Let* $\mathcal{D}\subseteq\mathcal{A}_4$ *be an additive abelian code, and let* $T=\cup_{i=1}^{l}C_i$ *be a union of* C_4-*classes* $C_i=C_4(\mu_i)$ *such that:* $C_i\in T$ *if and only if*

– $C_i\in C_2^o$ *and* $\mathcal{D}_C\neq 0$

or

– $C_i\subseteq C'\in C_2^e$ *and* $\mathcal{D}_{C'}\neq 0$

Then $d(\mathcal{D})\geq d(\mathcal{D}^*)$*, where* $\mathcal{D}^*$ *is the classical multivariable code in* $\mathcal{A}_4$ *with set of defining roots equal to* T *[13].*

Proof It is enough to notice that, since T *is the set of defining roots of* $\mathcal{D}^*$*, then* $\mathcal{D}_{C_i}=\mathcal{I}_{C_i}$*, for all* $i=1,\ldots,l$*. Therefore* $\mathcal{D}\subseteq D^*$ *and the conclusion follows.*

Remark 6 1. In view of this result, if we used the classical approach for multivariable codes, the computation of the minimum distance of a multivariable additive abelian code in r variables would be reduced to computations of minimum distances of classical multivariable semisimple codes over a finite field in less number of variables ([13][Proposition 8, Chapter 6])
2. There might exist additive codes with a greater Hamming distance that the one stated by the former bound, as the following example shows. Generally, these codes are not multivariable codes in the classical sense.

Example 3 (Example 1 cont'd) We apply Theorem 2 to construct an additive code by choosing suitable chunks (i.e., subcodes) in the components of the decomposition of $\mathcal{A}_4$, in the following way:

– *In the component $\mathcal{I}_{\{(1,1)\}}$, we choose*

$$\mathcal{D}_{\{(1,1)\}} = \left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}, \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix} \right\},$$

which is a $1-$dimensional vector space over $\mathcal{K}_{\{(1,1)\}}$.

– *In the ideals $\mathcal{I}_{C_4((\mu,1))}$ and $\mathcal{I}_{C_4((\mu^6,1))}$, we choose $1-$dimensional vector spaces over $\mathcal{K}_{C_2((\mu,1))}$ and $\mathcal{K}_{C_2((\mu,1))}$, respectively. According to the proof of Corollary 1, we have $9 \left(= \frac{8^2-1}{8-1}\right)$ choices for each of them. Let us take*

$$\mathcal{D}_{C_2((\mu,1))} =_S \begin{bmatrix} 0 & 1 & \omega & \omega & \overline{\omega} & 1 & \overline{\omega} \\ 0 & 1 & \omega & \omega & \overline{\omega} & 1 & \overline{\omega} \\ 0 & 1 & \omega & \omega & \overline{\omega} & 1 & \overline{\omega} \end{bmatrix} \text{ and } \mathcal{D}_{C_2((\mu^6,1))} =_S \begin{bmatrix} 0 & \overline{\omega} & 1 & \overline{\omega} & \omega & \omega & 1 \\ 0 & \overline{\omega} & 1 & \overline{\omega} & \omega & \omega & 1 \\ 0 & \overline{\omega} & 1 & \overline{\omega} & \omega & \omega & 1 \end{bmatrix},$$

respectively.

Let us have a more detailed look at the subcode $D_{C_2((\mu,1))}$. Since it is only contained in the component $\mathcal{I}_{C_4((\mu,1))}$, which is generated by the polynomial $(1+X_1+X_1^2+X_1^4)(1+X_2+X_2^2)$, Proposition 5 ensures a minimum distance of 12, according to the BCH bound. But Sage computations [16] show that the actual distance is $d(\mathcal{D}_{C_2((\mu,1))}) = 18$.

– *We simply choose $\mathcal{D}_{C_2((1,\omega))} = \left\{ \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix} \right\}$.*

– *Finally, in the sums $\mathcal{I}_{C_4((\mu,\omega))} \oplus \mathcal{I}_{C_4((\mu,\omega^2))}$ and $\mathcal{I}_{C_4((\mu^6,\omega))} \oplus \mathcal{I}_{C_4((\mu^6,\omega^2))}$, we also consider $1-$dimensional vector spaces over $\mathcal{K}_{C_2((\mu,\omega))}$ and $\mathcal{K}_{C_2((\mu^6,\omega))}$, respectively. Corollary 1 shows that a total amount of 65 possibilities are allowed for each component. Let us choose*

$$\mathcal{D}_{C_2((\mu,\omega))} =_S \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & \omega & \overline{\omega} & \omega & 0 & \overline{\omega} & 1 \\ 0 & \overline{\omega} & \overline{\omega} & \overline{\omega} & 0 & \overline{\omega} & 0 \end{bmatrix} \text{ and } \mathcal{D}_{C_2((\mu^6,\omega))} =_S \begin{bmatrix} 1 & 1 & \omega & 0 & \overline{\omega} & \omega & \overline{\omega} \\ \omega & 1 & \overline{\omega} & \overline{\omega} & \omega & 0 & 1 \\ \overline{\omega} & 0 & 1 & \overline{\omega} & 1 & \omega & \omega \end{bmatrix},$$

respectively.

The additive code

$$\mathcal{D} = \mathcal{D}_{\{(1,1)\}} \oplus \mathcal{D}_{C_2((\mu,1))} \oplus \mathcal{D}_{C_2((\mu^6,1))} \oplus \mathcal{D}_{C_2((1,\omega))} \oplus \mathcal{D}_{C_2((\mu^6,\omega))} \oplus D_{C_2((\mu^6,\omega))}$$

of length 21 has $2^{19} = 2^{1+3+3+0+6+6}$ codewords. Sage computations show that this code has distance $d(\mathcal{D}) = 7$.

4 Duality for abelian codes

In this section we describe the dual code of an additive abelian code $\mathcal{D}$. Following Lemma 1, the elements of $\mathcal{A}_4$ can be uniquely represented as $f + I$, where $f = NF(f) = \sum_\alpha f_\alpha X^\alpha$, $\alpha = (\alpha_1, \ldots, \alpha_r)$, and $X^\alpha = X_1^{\alpha_1} \ldots X_r^{\alpha_r}$ (notice that $0 \le \alpha_i < n_i$, for all $1 \le i \le r$). Let us introduce the function $\bar{\cdot} : \mathcal{A}_4 \to \mathcal{A}_4$ that maps an element $f + I$ to $\overline{f+I} = \sum_\alpha f_\alpha X^{n-\alpha} + I$, where $n = (n_1, \ldots, n_r)$. It is a ring automorphism or order

2. With this notation, the symmetric function used to define orthogonality is the trace inner product $\langle\cdot,\cdot\rangle : \mathcal{A}_4 \times \mathcal{A}_4 \to \mathbb{F}_2$ *given by*

$$\langle f+I, g+I\rangle = \sum_\alpha Tr(f_\alpha g_\alpha^2) = \sum_\alpha (f_\alpha g_\alpha^2 + f_\alpha^2 g_\alpha)$$

where $Tr : \mathbb{F}_4 \to \mathbb{F}_2$ *is the trace function. So, given an additive abelian code* $\mathcal{D}$*, its dual code is defined as* $\mathcal{D}^\perp = \{f+I \in \mathcal{A}_4 \mid \langle f+I, g+I\rangle = 0$ *for all* $g+I \in \mathcal{D}\}$*. A code* $\mathcal{D}$ *is self-orthogonal if* $\mathcal{D} \subseteq \mathcal{D}^\perp$ *and self-dual if* $\mathcal{D} = \mathcal{D}^\perp$*. In the next section we will characterize this kind of codes.*

For the study of duality it is useful to introduce the map $(\cdot,\cdot) : \mathcal{A}_4 \times \mathcal{A}_4 \to S$ *given by*

$$(f+I, g+I) = (f+I)\,\overline{\tilde{\tau}(g+I)} + \tilde{\tau}(f+I)\,\overline{g+I}, \tag{1}$$

Notice that $(\cdot,\cdot)$ *is well-defined, since* $\tilde{\tau}(f+I)\,\overline{g+I} = \tilde{\tau}((f+I)\,\overline{\tilde{\tau}(g+I)})$*, and so* $(f+I, g+I)$ *is contained in the subring of* $\mathcal{A}_4$ *fixed by* $\tilde{\tau}$*, i.e., in* S*. Moreover,* $I = 0+I = (f+I, g+I)$ *if and only if* $(f+I)\overline{\tilde{\tau}(g+I)} = \tilde{\tau}(f+I)\,\overline{g+I}$ *if and only if* $(f+I)\overline{\tilde{\tau}(g+I)}$ *is in* S*.*

Notice that (1) resembles an Hermitian form, in the sense that it is $S-$*linear in the first argument and* $(g+I, f+I) = \overline{(f+I, g+I)}$*, for all* $f+I, g+I \in \mathcal{A}_4$*. This map is related to the trace inner product by the following way:*

Lemma 3 $(f+I, g+I) = (\sum_\alpha \langle f+I, X^\alpha g+I\rangle X^\alpha) + I$*, for all* $f+I, g+I \in \mathcal{A}_4$*.*

Proof

$$(f+I, g+I) = (f+I)\overline{\tilde{\tau}(g+I)} + \tilde{\tau}(f+I)\overline{g+I}$$

$$\left(\sum_\beta f_\beta X^\beta + I\right)\left(\sum_\gamma g_\gamma^2 X^{n-\gamma} + I\right) + \left(\sum_\beta f_\beta^2 X^\beta + I\right)\left(\sum_\gamma g_\gamma X^{n-\gamma} + I\right)$$

$$= \sum_\beta \sum_\gamma (f_\beta g_\gamma^2 + f_\beta^2 g_\gamma) X^{\beta+n-\gamma} + I = \sum_\alpha \left(\sum_\gamma (f_{\alpha+\gamma} g_\gamma^2 + f_{\alpha+\gamma}^2 g_\gamma)\right) X^\alpha + I$$

$$= \sum_\alpha \left(\sum_\delta (f_\delta g_{\delta-\alpha}^2 + f_\delta^2 g_{\delta-\alpha})\right) X^\alpha + I = \left(\sum_\alpha \langle f+I, X^\alpha g+I\rangle X^\alpha\right) + I$$

(we have applied the changes of index $\{\beta+n-\gamma = \alpha, \delta = \alpha+\gamma\}$*, and we have taken the subscripts modulo* n*)*

So, $(f+I, g+I) = I$ *if and only if* $\langle r+I, g+I\rangle = 0$ *for all* $r+I$ *in* ${}_S(f+I)$*, the* $S-$*submodule of* $\mathcal{A}_4$ *generated by* $f+I$*, i.e., if and only if* $g+I$ *is an element in the dual code of* ${}_S(f+I)$*, the code spanned by* $f+I$*.*

Notice that the composition of the ring automorphisms $\tilde{\tau}$ *and* $\bar{\cdot}$ *induces a permutation on the set* $\mathcal{C}_4$*, because if* $\mu = (\mu_1, \ldots, \mu_r)$ *is a root of* $f+I$*, then* $\mu' = (\mu_1^{-2}, \ldots, \mu_r^{-2})$ *is a root of* $\overline{\tilde{\tau}(f+I)}$*. If* $C = C_4(\mu)$ *is the 4-class of the root* μ*, then let us denote by* $C' = C_4(\mu')$ *the* $4-$*class of* μ'*. Observe that, if we choose* $C_1, C_2 \in \mathcal{C}_4$ *such that* $C_1 \cup C_2 \in \mathcal{C}_2^e$*, then* $C_1' \cup C_2' \in \mathcal{C}_2^e$ *too. So, if* $C = C_1 \cup C_2 \in \mathcal{C}_2$*, we also write* $C' = C_1' \cup C_2'$*, and the permutation can be extended to* $2-$*classes. It is clear that* $C_2((1^{-2}, \ldots, 1^{-2})) = C_2((1, \ldots, 1))$*, and so* $C_2((1, \ldots, 1))$ *is a fixed point of this permutation. On the other hand, no other* $2-$*class in* $\mathcal{C}_2^o$ *is fixed. Namely,* *if $C_2((1,\dots,1)) \neq C_2(\mu) = C_2(\mu') \in \mathcal{C}_2^o$ then, since $C_2(\mu^{-1}) = C_2(\mu')$, we have $\mu^{-1} \in C_2(\mu)$. For all $\delta \neq (1,\dots,1)$, we have $\delta \neq \delta^{-1}$, and so $C_2(\mu)$ can be partitioned in pairs (δ,δ^{-1}). Hence $C_2(\mu)$ must have even size, which is not possible.*

Given $C \in \mathcal{C}_2^o$, and an element $f + I \in \mathcal{I}_C$ (or $C \in \mathcal{C}_2^e$, and an element $f + I \in \mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$), we define

$$\mathcal{O}(f+I) = \left\{ g + I \in \mathcal{I}_{C'} (\textit{alt. } g + I \in \mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'}) \mid (f+I)\overline{\tilde{\tau}(g+I)} \in S \right\} \qquad (2)$$

We have the following result that completely describes the dual code $\mathcal{D}^\perp$ of a given abelian code $\mathcal{D}$.

Theorem 3 *Let $\mathcal{D}$ be an abelian additive code. If $\mathcal{D} = \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C$ is the unique decomposition of Theorem 2, and $\mathcal{D}^\perp = \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C^\perp$ is the unique decomposition of its dual code, then:*

1. *if $\mathcal{D}_C = 0$, then $\mathcal{D}_{C'}^\perp = \mathcal{I}_{C'}$ (if $C \in \mathcal{C}_2^o$), or $\mathcal{D}_{C'}^\perp = \mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'}$ (if $C = C_1 \cup C_2 \in \mathcal{C}_2^e$);*
2. *$\mathcal{D}_{C'}^\perp = 0$ if $\mathcal{D}_C = \mathcal{I}_C$ (when $C \in \mathcal{C}_2^o$), or if $\mathcal{D}_C = \mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$ (when $C = C_1 \cup C_2 \in \mathcal{C}_2^e$);*
3. *if $\mathcal{D}_C =_S (f+I)$ with $I \neq f+I$, then $\mathcal{D}_{C'}^\perp = \mathcal{O}(f+I)$. In such a case:*
   - *(a) If $C \in \mathcal{C}_2^o$, then $\mathcal{O}(f+I) =_S (\overline{\tilde{\tau}(g+I)})$, where $g + I \in \mathcal{I}_C$ is the multiplicative inverse of $f + I$ in the field $\mathcal{I}_C$.*
   - *(b) If $C = C_1 \cup C_2 \in \mathcal{C}_2^e$, with $C_1, C_2 \in \mathcal{C}_4$, then let us write $f + I = f_1 + f_2 + I$, where $f_i + I \in \mathcal{I}_{C_i}$ $(i = 1, 2)$. If $f_i + I \neq I$ $(i = 1, 2)$, then $\mathcal{O}(f+I) =_S (\overline{\tilde{\tau}(g_1 + g_2 + I)})$, where $g_i + I \in \mathcal{I}_{C_i}$ is the multiplicative inverse of $f_i + I$ in the field $\mathcal{I}_{C_i}$ $(i = 1, 2)$. Otherwise, if $f_i + I \neq I$ (and $f_{3-i} + I = I$), then $\mathcal{O}(f+I) =_S (e_{C_{3-i}'} + I)$, if $C \neq C'$ or $\overline{\mathcal{I}_{C_1}} \neq \mathcal{I}_{C_1}$, or $\mathcal{O}(f+I) = {}_S(e_{C_i'} + I)$, if $C = C'$ and $\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_1}$.*

Summarizing, the possibilities given in Table 1 hold.

	$\mathcal{D}_C$	$\mathcal{D}_{C'}^\perp$
$C \in \mathcal{C}_2^o$	$\{0\}$	$\mathcal{I}_{C'}$
	${}_S(f+I)$	${}_S(\overline{\tilde{\tau}(g+I)})$
	$\mathcal{I}_C$	$\{0\}$
$C \in \mathcal{C}_2^e$	$\{0\}$	$\mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'}$
	${}_S(f_i+I)$	${}_S(e_{C_{3-i}'} + I)$, if $C \neq C'$ or if $\overline{\mathcal{I}_{C_1}} \neq \mathcal{I}_{C_1}$
		${}_S(e_{C_i'} + I)$, if $C = C'$ and $\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_1}$
	${}_S(f_1 + f_2 + I)$	${}_S(\overline{\tilde{\tau}(g_1 + g_2 + I)})$
	$\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$	$\{0\}$

Table 1 Relation between the summands of orthogonal codes

Proof Observe that if $f + I \in \mathcal{I}_C$ (alt. $f + I \in \mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$) and $h + I \notin \mathcal{I}_{C'}$ (alt. $h + I \notin \mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'}$), then $\overline{\tilde{\tau}(h+I)} \in \mathcal{I}_{C^*} \neq \mathcal{I}_C$ (alt. $\overline{\tilde{\tau}(h+I)} \in \mathcal{I}_{C_1*} \oplus \mathcal{I}_{C_2*} \neq \mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$), and *so* $(f+I)\overline{\tilde{\tau}(h+I)} \in \mathcal{I}_C \cap \mathcal{I}_{C^*} = I$ *(alt.* $(f+I)\overline{\tilde{\tau}(h+I)} \in (\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}) \cap (\mathcal{I}_{C_1^*} \oplus \mathcal{I}_{C_2^*}) = I$*), i.e.,* $(f+I, h+I) = I$*. Therefore*

$$(\mathcal{D}_C)^{\perp} = \Big((\mathcal{D}_C)^{\perp} \cap \mathcal{I}_{C'}\Big) \oplus \bigoplus_{C' \neq D \in \mathcal{C}_2^o} \mathcal{I}_D \oplus \bigoplus_{D \in \mathcal{C}_2^e} (\mathcal{I}_{D_1} \oplus \mathcal{I}_{D_2})$$

(alt. $(\mathcal{D}_C)^{\perp} = \Big((\mathcal{D}_C)^{\perp} \cap (\mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'})\Big) \oplus \bigoplus_{D \in \mathcal{C}_2^o} \mathcal{I}_D \oplus \bigoplus_{C' \neq D \in \mathcal{C}_2^e} (\mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'})$*), and so*

$$\bigoplus_{C' \in \mathcal{C}_2} \mathcal{D}_{C'}^{\perp} = \bigoplus_{C \in \mathcal{C}_2} \mathcal{D}_C^{\perp} = \mathcal{D}^{\perp} = \left(\bigoplus_{C \in \mathcal{C}_2} \mathcal{D}_C\right)^{\perp}$$
$$= \bigoplus_{C \in \mathcal{C}_2^o} \Big((\mathcal{D}_C)^{\perp} \cap \mathcal{I}_{C'}\Big) \oplus \bigoplus_{C \in \mathcal{C}_2^e} \Big((\mathcal{D}_C)^{\perp} \cap (\mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'})\Big)$$

so that $\mathcal{D}_{C'}^{\perp} = (\mathcal{D}_C)^{\perp} \cap \mathcal{I}_{C'}$ *(alt.* $\mathcal{D}_{C'}^{\perp} = (\mathcal{D}_C)^{\perp} \cap (\mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'})$*). The first two items of the proposition now easily follow, since* $(\cdot,\cdot)$ *is nondegenerate when restricted to* $\mathcal{I}_C \times \mathcal{I}_{C'}$ *(alt.* $\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2} \times \mathcal{I}_{C_1'} \oplus \mathcal{I}_{C_2'}$*), where as the first part of the third item is a consequence of equation (2).*

In the case (a) *it is straightforward to check that*

$$(f+I, \overline{\tilde{\tau}(g+I)}) = (f+I)(g+I) + \tilde{\tau}((f+I)(g+I)) = (e_C+I) + \tilde{\tau}((e_C+I)) = I$$

so that ${}_S(\overline{\tilde{\tau}(g+I)}) \subseteq \mathcal{O}(f+I)$*. The fact that* $(\cdot,\cdot)$ *is nondegnerate implies the claimed equality, because both sets are* $1-$*dimensional* $\mathcal{K}_C$*-vector subspaces.*

In the case (b)*, if* $f_i + I \neq I$ $(i = 1,2)$*, then*

$$(f+I)\overline{\tilde{\tau}(\overline{\tilde{\tau}(g_1+g_2+I)})} = (f_1+f_2+I)(g_1+g_2+I) = e_{C_1} + e_{C_2} + I \in S$$

and so $(f+I, \overline{\tilde{\tau}(g_1+g_2+I)}) = I$*, i.e.,* ${}_S(\overline{\tilde{\tau}(g_1+g_2+I)}) \subseteq \mathcal{O}(f+I)$*. Again, the fact that* $(\cdot,\cdot)$ *is nondegenerate implies the claimed equality. Finally, if* $f_i + I \neq I$ *(and* $f_{3-i} + I = I$*), then*

$$(f+I)(\overline{\tilde{\tau}(e_{C_{3-i}'}+I)}) = (f_i+I)(e_{C_{3-i}}+I) = I \in S$$

and so ${}_S(e_{C_{3-i}'}+I) \subseteq \mathcal{O}(f+I)$*, if* $C \neq C'$ *or* $\overline{\mathcal{I}_{C_1}} \neq \mathcal{I}_{C_1}$*. The other content follows from the same argument as above. The case when* $C = C'$ *and* $\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_1}$ *is similar.*

Remark 7 Notice that, in the case 3b of the previous lemma, if $f_1 + I \neq I$, we can take $g_1 + I \in \mathcal{I}_{C_1}$ the multiplicative inverse of $f_1 + I$ in the field $\mathcal{I}_{C_1}$, and multiply $(f_1+f_2+I)(g_1+\tau(g_1)+I) = e_{C_1} + h_2 + I$, and so ${}_S(f_1+f_2+I) =_S (e_{C_1}+h_2+I)$. The same argument applies if $f_2 + I \neq I$.

Example 4 (Example 1 cont'd) Let us construct the orthogonal code of the $\mathcal{D}$ *presented in the example above. We first list the correspondence between* $2-$*classes:* $\{(1,1)\}$ *and* $C_2((1,\omega))$ *are fixed points in the permutation* $C \leftrightarrow C'$*. On the other hand,* $C_2((\mu,1)) \leftrightarrow C_2((\mu^6,1))$ *and* $C_2((\mu,\omega)) \leftrightarrow C_2((\mu^6,\omega))$ *Now, let us describe for each component* $\mathcal{D}_C$*, the corresponding component* $\mathcal{D}_{C'}^{\perp}$*, according to Table 1.*

– *Since* $\mathcal{D}_{\{(1,1)\}} =_S \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix}$ *and* $(1+X_1+X_1^2+X_1^3+X_1^4+X_1^5+X_1^6)(1+X_2+X_2^2)+I$ *is the identity of* $\mathcal{I}_{\{(1,1)\}}$*, which happens to be invariant under* $\overline{\tilde{\tau}}$*, we get that* $\mathcal{D}_{\{(1,1)\}}^{\perp} = \mathcal{D}_{\{(1,1)\}}$*.*

– *We have that* $\mathcal{D}_{C_2((\mu,1))} =_S \begin{bmatrix} 0 & 1 & \omega & \omega & \overline{\omega} & 1 & \overline{\omega} \\ 0 & 1 & \omega & \omega & \overline{\omega} & 1 & \overline{\omega} \\ 0 & 1 & \omega & \omega & \overline{\omega} & 1 & \overline{\omega} \end{bmatrix}$, *and that the inverse of the element* $(X_1+\omega X_1^2+\omega X_1^3+\omega^2 X_1^4+X_1^5+\omega^2 X_1^6)(1+X_2+X_2^2)+I$ *in the field* $\mathcal{I}_{C_2((\mu,1))}$ *is equal to* $(X_1+\omega^2 X_1+\omega^2 X_1^2+\omega^2 X_1^3+\omega X_1^4+X_1^5+\omega X_1^6)(1+X_2+X_2^2)+I$. *Therefore,* $\mathcal{D}^{\perp}_{C_2((\mu,1))'}$ *is generated by* $(\omega^2 X_1+X_1^2+\omega^2 X_1^3+\omega X_1^4+\omega X_1^5+X_1^6)(1+X_2+X_2^2)$, *and so* $\mathcal{D}^{\perp}_{C_2((\mu,1))'} = \mathcal{D}_{C_2((\mu^6,1))}$. *As a consequence*

$$\mathcal{D}^{\perp}_{C_2((\mu^6,1))'} = \mathcal{D}_{C_2((\mu,1))}.$$

– *From the trivial component* $\mathcal{D}_{C_2((1,\omega))} = \left\{ \begin{bmatrix} 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{bmatrix} \right\}$ *we get that*

$$\mathcal{D}^{\perp}_{C_2((1,\omega))'} = \mathcal{I}_{C_4((1,\omega)} \oplus \mathcal{I}_{C_4((1,\omega^2)}.$$

– *Finally, we consider* $\mathcal{D}_{C_2((\mu^6,\omega))} =_S \begin{bmatrix} 1 & 1 & \omega & 0 & \overline{\omega} & \omega & \overline{\omega} \\ \omega & 1 & \overline{\omega} & \overline{\omega} & \omega & 0 & 1 \\ \overline{\omega} & 0 & 1 & \overline{\omega} & 1 & \omega & \omega \end{bmatrix}$. *The element* $1 + X_1 + \omega X_1^2 + \omega^2 X_1^4 + \omega X_1^5 + \omega^2 X_1^6 + (\omega + X_1 + \omega^2 X_1^2 + \omega^2 X_1^3 + \omega X_1^4 + X_1^6)X_2 + (\omega^2 + X_1^2 + \omega^2 X_1^3 + X_1^4 + \omega X_1^5 + \omega X_1^6)X_2^2 + I$ *decomposes as* $f_1 + f_2 + I$, *where* $f_1 + I = (X_1 + X_1^3 + X_1^4 + X_1^5)(\omega^2 + \omega X_2 + X_2^2) \in \mathcal{I}_{C_4((\mu^6,\omega))}$, *and* $f_2 + I = (1 + \omega X_1 + \omega X_1^2 + \omega^2 X_1^3 + X_1^5 + \omega^2 X_1^6)(1 + \omega X_2 + \omega^2 X_2^2) \in \mathcal{I}_{C_4((\mu^6,\omega))}$. *The image of the sum of the inverses of* $f_1 + I$ *and* $f_2 + I$ *under the map* $\overline{\overline{\tau}}$ *gives us* $\mathcal{D}^{\perp}_{C_2((\mu^6,\omega))'} =_S \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & \omega & \overline{\omega} & \omega & 0 & \overline{\omega} & 1 \\ 0 & \overline{\omega} & \overline{\omega} & \overline{\omega} & 0 & \overline{\omega} & 0 \end{bmatrix} = \mathcal{D}_{C_2((\mu,\omega))}$. *As a consequence*

$$\mathcal{D}^{\perp}_{C_2((\mu^6,\omega))'} = \mathcal{D}_{C_2((\mu,\omega^2))}.$$

Therefore, the orthogonal of $\mathcal{D}$ *is the additive code*

$$\begin{aligned} \mathcal{D}^{\perp} = {} & \mathcal{D}_{\{(1,1)\}} \oplus \mathcal{D}_{C_2((\mu,1))} \oplus \mathcal{D}_{C_2((\mu^6,1))} \oplus \mathcal{I}_{C_4((1,\omega)} \oplus \mathcal{I}_{C_4((1,\omega^2)} \\ & \oplus \mathcal{D}_{C_2((\mu^6,\omega))} \oplus D_{C_2((\mu^6,\omega))} = \mathcal{D} \oplus \mathcal{I}_{C_4((1,\omega)} \oplus \mathcal{I}_{C_4((1,\omega^2)} \supseteq \mathcal{D}, \end{aligned}$$

and so the code is self-orthogonal.

5 Self-orthogonal and self-dual abelian codes

Lemma 4 *Let* $\mathcal{D} = \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C$ *be an additive abelian code in* $\mathcal{A}_4$ *and let* $\mathcal{D}^{\perp} = \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}^{\perp}_C$ *be its dual code. Then:*

1. $\mathcal{D}$ *is self-orthogonal if and only if for each* $C \in \mathcal{C}_2$, *if* $\mathcal{D}_C \neq 0$ *and* $\mathcal{D}_{C'} \neq 0$, *then* $\mathcal{D}_C =_S (f + I)$ *and* $\mathcal{D}_{C'} = \mathcal{O}(f + I)$, *with* $I \neq f + I$.
2. $\mathcal{D}$ *is self-dual if and only if it is self-orthogonal and for each* $C \in \mathcal{C}_2$ *such that* $\mathcal{D}_C = 0$, *then* $\mathcal{D}_{C'} = \mathcal{I}_{C'}$, *when* $C \in \mathcal{C}_2^o$ *(or* $\mathcal{D}_{C'} = \mathcal{I}_{C'_1} \oplus \mathcal{I}_{C'_2}$, *when* $C = C_1 \cup C_2 \in \mathcal{C}_2^e$*).*

Proof 1. *First of all notice that, for a code* $\mathcal{D}$ *the condition of self-orthogonality,* $\mathcal{D} \subseteq \mathcal{D}^{\perp}$ *is equivalent to* $\mathcal{D}_C \subseteq \mathcal{D}^{\perp}_C$ *for all* $C \in \mathcal{C}_2$. *This condition clearly holds for all* $C \in \mathcal{C}_2$ *such that* $\mathcal{D}_C = 0$. *If* $\mathcal{D}_C \neq 0$ *but* $\mathcal{D}_{C'} = 0$, *then* $\mathcal{D}^{\perp}_C = \mathcal{I}_C$, *when* $C \in \mathcal{C}_2^o$, *according to Theorem 3, and so the condition also holds. Finally, if* $\mathcal{D}_C \neq 0$ *and* $\mathcal{D}_{C'} \neq 0$, *then* $\mathcal{D}_C \neq \mathcal{I}_C$ *for the code to be self-orthogonal (since otherwise,* *from Theorem 3, $\mathcal{D}_{C'}^{\perp} = 0 \not\supseteq \mathcal{D}_{C'}$) and $\mathcal{D}_{C'} \neq \mathcal{I}_{C'}$ by the same argument. Hence $\mathcal{D}_C =_S (f+I)$ with $I \neq f+I$. Because $\mathcal{D}_{C'} \subseteq \mathcal{O}(f+I)$ and both sets are 1-dimensional $\mathcal{K}_C$ subspaces, we obtain the desired equality.*

2. *The code $\mathcal{D}$ is self-dual if and only if $\mathcal{D}_C = \mathcal{D}_C^{\perp}$ for all $C \in \mathcal{C}_2$. In particular it has to be self-orthogonal. For the classes $C \in \mathcal{C}_2$ such that $\mathcal{D}_C =_S (f+I)$ and $\mathcal{D}_{C'} = \mathcal{O}(f+I)$ (with $I \neq f+I$) the equality is true, whereas if $0 = \mathcal{D}_C = \mathcal{D}_C^{\perp}$, from Theorem 3, we must have $\mathcal{D}_{C'} = I_{C'}$, for the code to be self-dual. The case $C \in \mathcal{C}_2^e$ is similar.*

Now, we are able to describe the self-orthogonal and self-dual additive abelian codes in $\mathcal{A}_4$.

Theorem 4 *Let $\mathcal{D} = \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C$ be an additive abelian code in $\mathcal{A}_4$ and let $\mathcal{D}^{\perp} = \bigoplus_{C\in\mathcal{C}_2} \mathcal{D}_C^{\perp}$ be its dual code. Then, $\mathcal{D}$ is self-orthogonal (alt. $\mathcal{D}$ is self-dual) if and only if for each $C \in \mathcal{C}_2$ the following condition hold (alt. except those marked with an asterisk):*

1. *If $C \in \mathcal{C}_2^o$:*
   (a) *If $C = C_2((1,\ldots,1))$, then either*
      - *$\mathcal{D}_C = \{0\}$ $(*)$*
      - *or $\mathcal{D}_C$ is any $\mathcal{K}_C$-vector space of dimension 1.*

   (b) *In other case, either*
      i. *$\mathcal{D}_C = \{0\}$ and*
         - *$\mathcal{D}_{C'} = \mathcal{I}_{C'}$*
         - *or $\mathcal{D}_{C'}$ is any other $\mathcal{K}_{C'}$-vector subspace of $\overline{\mathcal{I}_{C'}\ (*)}$*

      ii. *or $\mathcal{D}_C =_S (f+I)$ with $f+I \neq I$, and $\mathcal{D}_{C'} =_S (\overline{\tilde{\tau}(g+I)})$, where $g+I \in \mathcal{I}_C$ is the multiplicative inverse of $f+I$ in the field $\mathcal{I}_C$.*
2. *If $C = C_1 \cup C_2 \in \mathcal{C}_2^e$:*
   (a) *If $C = C'$, then either*
      i. *$\mathcal{D}_C = \{0\}$ $(*)$,*

      ii. *or if $\overline{\mathcal{I}_{C_i}} = \mathcal{I}_{C_i}$ $(i = 1, 2)$, then*
         - *$\mathcal{D}_C =_S (e_{C_i} + I)$ with $i = 1, 2$*
         - *or $\mathcal{D}_C =_S (f_1 + \tilde{\tau}(f_1)z + I)$ where $z + I$ is a non-zero element of the subfield of $\mathcal{I}_{C_2}$ isomorphic to $\mathbb{F}_{2^{|C_1|}}$*

      iii. *or if $\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_2}$, then $\mathcal{D}_C =_S (f_1 + \tilde{\tau}(f_1)z + I)$ where $z + I$ is a non-zero element of $\mathcal{I}_{C_2}$ of order $2^{|C_1|} + 1$.*

   (b) *If $C \neq C'$, then either*
      i. *$\mathcal{D}_C = \{0\}$ and*
         - *$\mathcal{D}_{C'} = \mathcal{I}_{C'}$*
         - *or $\mathcal{D}_{C'}$ is any $\mathcal{K}_{C'}$-vector subspace of $\mathcal{I}_{C'}$ $(*)$,*

      ii. *or $\mathcal{D}_C =_S (e_{C_i} + I)$ $(i = 1, 2)$ and $\mathcal{D}_{C'} =_S (e_{C_i'} + I)$,*

      iii. *or $\mathcal{D}_C =_S (f_1 + f_2 + I)$ with $f_i + I \neq I$ for $i = 1, 2$, and $\mathcal{D}_{C'} =_S (\overline{\tilde{\tau}(g_1 + g_2 + I)})$, where $g_i + I \in \mathcal{I}_{C_i}$ is the multiplicative inverse of $f_i + I$ in the field $\mathcal{I}_{C_i}$ $(i = 1, 2)$.*

These possibilities for self-orthogonal (alt. self-dual) additive abelian codes are summarized in Table 2.

Proof 1. (a) *If $C = C_2((1,\ldots,1))$, then $C = C'$ and so, for the code to be self-orthogonal $\mathcal{D}_C = \mathcal{D}_{C'}$ must be a proper $\mathcal{K}_C$-vector subspace of $\mathcal{I}_C$ (according*

<table>
<tr><td colspan="3"></td><td>$\mathcal{D}_C$</td><td>$\mathcal{D}_{C'}$</td><td></td></tr>
<tr><td rowspan="8">$C \in \mathcal{C}_2^o$</td><td colspan="2" rowspan="2">$C_{(1,\dots,1)}$</td><td colspan="2">$\{0\}$</td><td>$*$</td></tr>
<tr><td colspan="2">${}_S(f+I)$</td><td></td></tr>
<tr><td colspan="2" rowspan="6">$C \neq C'$</td><td rowspan="3">$\{0\}$</td><td>$\{0\}$</td><td>$*$</td></tr>
<tr><td>${}_S(f+I)$</td><td>$*$</td></tr>
<tr><td>$\mathcal{I}_{C'}$</td><td></td></tr>
<tr><td rowspan="2">${}_S(f+I)$</td><td>$\{0\}$</td><td>$*$</td></tr>
<tr><td>${}_S(\overline{\tilde{\tau}(g+I)})$</td><td></td></tr>
<tr><td>$\mathcal{I}_C$</td><td>$\{0\}$</td><td></td></tr>
<tr><td rowspan="13">$C \in \mathcal{C}_2^e$</td><td rowspan="5">$C = C'$</td><td rowspan="3">$\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_1}$</td><td colspan="2">$\{0\}$</td><td>$*$</td></tr>
<tr><td colspan="2">${}_S(e_{C_i}+I)$</td><td></td></tr>
<tr><td colspan="2">${}_S(f_1+\tilde{\tau}(f_1)z+I)$</td><td></td></tr>
<tr><td rowspan="2">$\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_2}$</td><td colspan="2">$\{0\}$</td><td>$*$</td></tr>
<tr><td colspan="2">${}_S(f_1+\tilde{\tau}(f_1)z+I)$</td><td></td></tr>
<tr><td colspan="2" rowspan="8">$C \neq C'$</td><td rowspan="3">$\{0\}$</td><td>$\{0\}$</td><td>$*$</td></tr>
<tr><td>${}_S(f+I)$</td><td>$*$</td></tr>
<tr><td>$\mathcal{I}_{C'_1} \oplus \mathcal{I}_{C'_2}$</td><td></td></tr>
<tr><td rowspan="2">${}_S(e_{C_i}+I)$</td><td>$\{0\}$</td><td>$*$</td></tr>
<tr><td>${}_S(e_{C_{3-i}}+I)$</td><td></td></tr>
<tr><td rowspan="2">${}_S(f_1+f_2+I)$</td><td>$\{0\}$</td><td>$*$</td></tr>
<tr><td>${}_S(\overline{\tilde{\tau}(g_1+g_2+I)})$</td><td></td></tr>
<tr><td>$\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$</td><td>$\{0\}$</td><td></td></tr>
</table>

Table 2 Different possibilities on the summands for a code to be self-orthogonal or self-dual

to Lemma 4.1). The case $\mathcal{D}_C = \mathcal{D}_{C'} = \{0\}$ is allowed for self-orthogonality, but it is not acceptable for self-duality (according to Lemma 4.2). Finally, if $\mathcal{D}_C =_S (f+I)$, from Theorem 3 we know that $\mathcal{D}_C^{\perp} = \mathcal{O}(f+I) =_S (\overline{\tilde{\tau}(g+I)})$, where $g+I$ is the multiplicative inverse of $f+I$ in the field $\mathcal{I}_C$. Thus, ${}_S(f+I) =_S (\overline{\tilde{\tau}(g+I)})$ if and only if there exists $c+I \in S$ such that $(c+I)(f+I) = \overline{\tilde{\tau}(g+I)}$, if and only if $c+I = \overline{\tilde{\tau}(g+I)}(g+I) \in S$. The restriction of the ring automorphism $\bar{\cdot}$ to the ideal $\mathcal{I}_C$ is the identity, and so $c+I = \tilde{\tau}(g+I)(g+I) = \tilde{\tau}(c+I)$, i.e., $c+I \in S$ always.

(b) *In this case $C \neq C'$, and so self-orthogonality in the subcase i. (i.e., $\mathcal{D}_C = \{0\}$) is obvious (but self-duality is not possible unless $\mathcal{D}_{C'} = \mathcal{I}_{C'}$), according to Lemma 3. In the subcase ii. ($\mathcal{D}_C =_S (f+I)$) self-orthogonality is only true when $\mathcal{D}_{C'} =_S (\overline{\tilde{\tau}(g+I)})$, because of Theorem 3. Since $\tilde{\tau}$ and $\bar{\cdot}$ are commuting ring automorphisms of order at most 2, it follows that $\mathcal{D}_C =_S (f+I) =_S (\tilde{\tau}(\overline{\tilde{\tau}(f+I)})) = \mathcal{O}(\overline{\tilde{\tau}(g+I)})$ and thus the condition is also sufficient. Self-duality is always true in such a case.*

2. (a) *If $C = C' = C_1 \cup C_2$, the case $\mathcal{D}_C = \{0\}$ is possible if $\mathcal{D}$ is self-orthogonal, but not if it is self-dual (Lemma 4).*
If $C \in \mathcal{C}_2$, and $\overline{\mathcal{I}_C} = \mathcal{I}_C$, then the restriction of $\bar{\cdot}$ to $\mathcal{I}_C$ is the identity if and only if $C = C_2((1,\dots,1))$. In fact, in these conditions, if $f+I = \sum_\alpha f_\alpha X^\alpha + I \in \mathcal{I}_C$, then $\overline{X^\beta(f+I)} = X^\beta(f+I)$ for any index $\beta = (\beta_1,\dots,\beta_r)$. So, this implies that $f_{n-\alpha-\beta} = f_{\alpha-\beta}$ for all α and β. Taking $\alpha = \beta$ we have that $f_{n-2\beta} = f_0$ for all β. Since n_i is odd for $i = 1,\dots,r$, $f+I = f_0(\sum_\alpha X^\alpha + I)$ which is an element of $\mathcal{I}_C$ with $C = C_2((1,\dots,1))$.
Let us suppose that $\overline{\mathcal{I}_{C_i}} = \mathcal{I}_{C_i}$ for $i = 1,2$. Hence, $\overline{\mathcal{I}_C} = \mathcal{I}_C$ and the restriction $\bar{\cdot}|_{\mathcal{I}_{C_i}}$ is a non trivial field automorphism or order 2, i.e., $\overline{f_i+I} = f_i^{2^d} + I$,

where $d = |C_i|$, since $\mathcal{I}_{C_i} \cong \mathbb{F}_{4^{|C_i|}}$. If $\mathcal{D}_C =_S (f_i + I)$ ($i = 1$ or 2), then $\mathcal{O}(f_i+I) =_S (e_{C_i}+I)$, and so self-orthogonality implies $_S(f_i+I) =_S (e_{C_i}+I)$. In such a case $\mathcal{D}_C = \mathcal{D}_{C'}$, and the condition for self-duality if also satisfied. Otherwise, $\overline{\mathcal{D}_C} =_S (f_1+f_2+I)$ with $f_i+I \neq I$ ($i = 1,2$), and $\mathcal{O}(f_1+f_2+I) =_S (\tilde{\tau}(g_1 + g_2 + I)$, where $g_i + I$ is the multiplicative inverse of $f_i + I$ in the field $\mathcal{I}_{C_i}$. Therefore, the condition for self-orthogonality (and self-duality) holds if and only if there exists an element $c + I \in S$ such that

$$f_1 + f_2 + I = (c + I)(\overline{\tilde{\tau}(g_1)} + \overline{\tilde{\tau}(g_2)} + I) = (c + I)(\tilde{\tau}(g_1)^{2^d} + \tilde{\tau}(g_2)^{2^d} + I)$$

Then, the element $c + I \in S$ must verify the following condition

$$c + I = (f_1 + f_2 + I)(\tilde{\tau}(f_1)^{2^d} + \tilde{\tau}(f_2)^{2^d} + I) = f_1\tilde{\tau}(f_2)^{2^d} + f_2\tilde{\tau}(f_1)^{2^f} + I$$

Now, since $\tilde{\tau}(c + I) = c + I$, we arrive to these equations

$$\begin{cases} f_1\tilde{\tau}(f_2)^{2^d} + \tilde{\tau}(f_2)f_1^{2^d} + I = I \\ f_2\tilde{\tau}(f_1)^{2^d} + \tilde{\tau}(f_1)f_2^{2^d} + I = I \end{cases}$$

From the second equation, we obtain that $(\tilde{\tau}(f_1)g_2)^{2^d-1} + I) = e_{C_2} + I$, that is, $\tilde{\tau}(f_1)g_2 + I$ is a non-zero element of the subfield of $\mathcal{I}_{C_2}$ isomorphic to $\mathbb{F}_{2^d}$. So, we obtain $f_2 + I = \tilde{\tau}(f_1)z + I$. This solution also verifies the first equation, so the result follows.
Let us suppose that $\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_2}$. If $\mathcal{D}_C =_S (f_i + I)$ with $i = 1, 2$, $\mathcal{O}(f_i + I) =_S (e_{C_{3-i}} + I) \neq \mathcal{D}_C$, and so the code can not be self-orthogonal. Finally, we will consider $\mathcal{D}_C =_S (f_1 + f_2 + I)$. Since the restriction $\overline{\tilde{\tau}}|_{\mathcal{I}_{C_1}}$ (alt. $\overline{\tilde{\tau}}|_{\mathcal{I}_{C_2}}$) is a field automorphism of order 2, i.e., $\overline{\tilde{\tau}(f_i + I)} = f_i^{2^d} + I$, using the same argument of the case 2(a)ii, we arrive to the equations

$$\begin{cases} f_1^{2^d+1} + \tilde{\tau}(f_2)^{2^d+1} + I = I, \\ f_2^{2^d+1} + \tilde{\tau}(f_1)^{2^d+1} + I = I. \end{cases}$$

Solving the second equation we obtain $f_2 + I = \tilde{\tau}(f_1)z + I$, where $z + I$ is a non-zero element of $\mathcal{I}_{C_2}$ of order $2^d + 1$. This solution also satisfies the first equation, and the result follows.

(b) Let us now suppose that $C \neq C'$. The first case is similar to 1(b)i, where as the second one is similar to the first subcase of 2(a)ii. Finally, if $\overline{\mathcal{D}_C} =_S (f_1+f_2+I)$ with $f_i+I \neq I$ for $i = 1, 2$, then $\mathcal{O}(f_1+f_2+I) =_S (\overline{\tilde{\tau}(g_1 + g_2 + I)})$, where g_i+I is the multiplicative inverse of f_i+I ($i = 1, 2$). Hence, $\mathcal{D}_{C'} =_S (\tilde{\tau}(g_1 + g_2 + I))$ for the code to be self-orthogonal and self-dual.

Example 5 (Example 1 cont'd) The components of the self-orthogonal code $\mathcal{D}$ presented in the examples above fall in the following cases of Theorem 4:

- *$\mathcal{D}_{\{(1,1)\}}$ is case 1(a),*
- *$\mathcal{D}_{C_2((\mu,1))}$ and $\mathcal{D}_{C_2((\mu^6,1))}$ are case 1(b)ii,*
- *$\mathcal{D}_{C_2((1,\omega))}$ is case 2(a)i,*
- *and $\mathcal{D}_{C_2((\mu,\omega^2))}$ and $\mathcal{D}_{C_2((\mu^6,\omega))}$ are case 2(b)iii.*

Let us observe that this self-orthogonal code $\mathcal{D}$ allow us to construct, via [2][Theorem 2], a quantum-error-correcting code with parameters $[[21, 2, d]]$, where d is the smallest weight of codewords in $\mathcal{D}^{\perp} \setminus \mathcal{D}$. Sage computations [16] show that the actual distance of the quantum-error-correcting code is $d = 6$, i.e., it has the same distance as the best known code with the same parameters listed in [6].

The ring automorphism $\overline{\overline{\tau}}$ defines an equivalence relation over the set of 2-classes $\mathcal{C}_2$. Let us denote $\mathcal{B}$ the quotient set of $\mathcal{C}_2$ by this relation. Using this notation, the number of self-orthogonal and self-dual codes are given by the following result.

Corollary 2 *The number of additive abelian self-orthogonal (alt. self-dual) codes is given by Table 3.*

	Any	Generated by a single word
Self-orthogonal	$4 \prod_{\substack{C \in \mathcal{B} \\ C \neq C'}} (3 \cdot 2^{\lvert C \rvert} + 6) \prod_{\substack{C \in \mathcal{B} \\ C = C'}} (2^{\frac{\lvert C \rvert}{2}} + 2)$	$4 \prod_{\substack{C \in \mathcal{B} \\ C \neq C'}} (3 \cdot 2^{\lvert C \rvert} + 4) \prod_{\substack{C \in \mathcal{B} \\ C = C'}} (2^{\frac{\lvert C \rvert}{2}} + 2)$
Self-dual	$3 \prod_{\substack{C \in \mathcal{B} \\ C \neq C'}} (2^{\lvert C \rvert} + 3) \prod_{\substack{C \in \mathcal{B} \\ C = C'}} (2^{\frac{\lvert C \rvert}{2}} + 1)$	$3 \prod_{\substack{C \in \mathcal{B} \\ C \neq C'}} (2^{\lvert C \rvert} + 1) \prod_{\substack{C \in \mathcal{B} \\ C = C'}} (2^{\frac{\lvert C \rvert}{2}} + 1)$

Table 3 Number of self-orthogonal and self-dual codes

Proof *In Table 4 we count the number of codes from the possible choices in the entries of the table of Theorem 4 (see also Remark 7).*
In order to know the number of self-dual codes, we do no count rows marked with an asterisk. Finally, the code $\mathcal{D}$ is generated by a single word if and only if $\mathcal{D}_C$ is a $\mathcal{K}_C$-vector space of dimension 0 or 1 for all $C \in \mathcal{C}_2$, i.e., we do not count any row containing $\mathcal{I}_C$ or $\mathcal{I}_{C_1} \oplus \mathcal{I}_{C_2}$.

Acknowledgements *Edgar Martínez-Moro was partially funded by Spanish MCINN under projects MTM2007-64704 and MTM2010-21580-C02-02. A. Piñera-Nicolás and I. F. Rua were supported by MTM2010-18370-C04-01.*

<table>
<tr><th colspan="3"></th><th>$\mathcal{D}_C$</th><th>$\mathcal{D}_{C'}$</th><th>Total number</th><th></th></tr>
<tr><td rowspan="8">$C \in \mathcal{C}_2^o$</td><td colspan="2" rowspan="2">$C_{(1,\dots,1)}$</td><td colspan="2">1</td><td rowspan="2">4</td><td rowspan="2"></td></tr>
<tr><td colspan="2">$\frac{2^2-1}{2-1}$</td></tr>
<tr><td colspan="2" rowspan="6">$C \neq C'$</td><td rowspan="3">1</td><td>1</td><td rowspan="3">$2^{\lvert C\rvert}+3$</td><td rowspan="6">$3 \cdot 2^{\lvert C\rvert}+6$</td></tr>
<tr><td>$\frac{2^{\lvert C\rvert}-1}{2-1}$</td></tr>
<tr><td>1</td></tr>
<tr><td rowspan="2">$\frac{2^{\lvert C\rvert}-1}{2-1}$</td><td>1</td><td rowspan="2">$(2^{\lvert C\rvert}+1)\cdot 2$</td></tr>
<tr><td>1</td></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
<tr><td rowspan="13">$C \in \mathcal{C}_2^e$</td><td rowspan="5">$C = C'$</td><td rowspan="3">$\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_1}$</td><td colspan="2">1</td><td rowspan="3">$2^{\lvert C\rvert/2}+2$</td><td rowspan="5">$2^{\lvert C\rvert/2}+2$</td></tr>
<tr><td>2</td><td>1</td></tr>
<tr><td colspan="2">$2^{\lvert C\rvert/2}-1$</td></tr>
<tr><td rowspan="2">$\overline{\mathcal{I}_{C_1}} = \mathcal{I}_{C_2}$</td><td colspan="2">1</td><td rowspan="2">$2^{\lvert C\rvert/2}+2$</td></tr>
<tr><td colspan="2">$2^{\lvert C\rvert/2}+1$</td></tr>
<tr><td colspan="2" rowspan="8">$C \neq C'$</td><td rowspan="3">1</td><td>1</td><td rowspan="3">$2^{\lvert C\rvert}+3$</td><td rowspan="8">$3 \cdot 2^{\lvert C\rvert}+6$</td></tr>
<tr><td>$\frac{2^{\lvert C\rvert}-1}{2-1}$</td></tr>
<tr><td>1</td></tr>
<tr><td rowspan="2">2</td><td>1</td><td rowspan="2">4</td></tr>
<tr><td>1</td></tr>
<tr><td rowspan="2">$2^{\lvert C\rvert}-1$</td><td>1</td><td rowspan="2">$(2^{\lvert C\rvert}-1)\cdot 2$</td></tr>
<tr><td>1</td></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
</table>

Table 4 Total number of self-orthogonal and self-dual codes

References

1. *S. D. Berman. On the theory of group codes.* Cybernetics*, 3(1):25–31 (1969), 1969.*
2. *A. Calderbank, E. Rains, P. Shor, and N. Sloane. Quantum error correction via codes over GF(4).* IEEE Trans. Inform. Theory*, 44:1369–1387, 1998.*
3. *P. Charpin. Une généralisation de la construction de Berman des codes de Reed et Muller p-aires.* Comm. Algebra*, 16(11):2231–2246, 1988.*
4. *D. Cox, J. Little, and D. O'Shea.* Ideals, Varieties, and Algorithms*. Springer, New York, 2007.*
5. *B. Dey and B. Rajan. $\mathbb{F}_q$-linear cyclic codes over $\mathbb{F}_q^m$.* Des. Codes Cryptogr.*, 34:89–116, 2005.*
6. *M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at* `http://www.codetables.de`
7. *W. C. Huffman. Additive cyclic codes over $\mathbb{F}_4$.* Adv. Math. Commun.*, 1(4):427–459, 2007.*
8. *W. C. Huffman. Additive cyclic codes over $\mathbb{F}_4$.* Adv. Math. Commun.*, 2(3):309–343, 2008.*
9. *E. Martínez-Moro and I. F. Rúa. Multivariable codes over finite chain rings: serial codes.* SIAM J. Discrete Math.*, 20(4):947–959, 2006.*
10. *E. Martínez-Moro and I. F. Rúa. On repeated-root multivariable codes over a finite chain ring.* Des. Codes Cryptogr.*, 45:219–227, 2007.*
11. *W. W. Peterson and J. E. J. Weldon.* Error-correcting codes*. The M.I.T. Press, Cambridge, Mass.-London, second edition, 1972.*
12. *A. Poli. Important algebraic calculations for n-variables polynomial codes.* Discrete Math.*, 56(2-3):255–263, 1985.*
13. *A. Poli and L. Huguet.* Error correcting codes*. Prentice Hall International, Hemel Hempstead, 1992.*
14. *P. Shor. Scheme for reducing decoherence in quantum memory.* Phys. Rev. A*, 52, 1995.*
15. *A. Steane. Simple quantum error correcting codes.* Phys. Rev. Lett.*, 77:793–797, 1996.*
16. *W.A. Stein et al. Sage Mathematics Software (Version 3.0.1). The Sage Development Team, 2008.* `http://www.sagemath.org`