On cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes

Anuradha Sharma*

Center for Applied Mathematics,
IIIT Delhi,
New Delhi, India
Email: anuradha@iiitd.ac.in
*Corresponding author

Taranjot Kaur

Department of Mathematics,
IIT Delhi,
Hauz Khas, New Delhi, India
Email: taran.iit@gmail.com

Abstract: Let $\mathbb{F}_q$ denote the finite field of order q and characteristic p, n be a positive integer coprime to q and $t \geq 2$ be an integer satisfying $t \not\equiv 1(\text{mod } p)$. In this paper, we place a new trace bilinear form on $\mathbb{F}_{q^t}^n$, which is called the $*$ trace bilinear form and is a generalisation of the trace inner product when $q = t = 2$ and Hermitian trace inner product when q is even and $t = 2$. We observe that it is a non-degenerate, symmetric bilinear form on $\mathbb{F}_{q^t}^n$ for any prime power q and is alternating when q is even. We study dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n with respect to this bilinear form. We also explicitly determine bases of all the complementary-dual, self-orthogonal and self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n, and enumerate all the self-orthogonal and self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n. Besides this, by placing ordinary and Hermitian trace inner products on $\mathbb{F}_{q^2}^n$, we determine bases of all the complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n.

Keywords: sesquilinear forms; totally isotropic spaces; Witt index.
2000 Mathematics Subject Classification: 94B15

Reference to this paper should be made as follows: Sharma, A. and Kaur, T. (2017) 'On cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes', *Int. J. Information and Coding Theory*, Vol. 4, No. 1, pp.19–46.

Biographical notes: Anuradha Sharma received BSc with Honours in Mathematics, MSc and PhD in Mathematics from the Centre for Advanced Study in Mathematics, Panjab University, Chandigarh, India, in 2000, 2002 and 2006, respectively. She is an Associate Professor with the Centre for Applied Mathematics at Indraprastha Institute of Information Technology Delhi (IIIT-D), India. Prior to joining IIIT-D, she worked as an Assistant Professor at Indian Institute of Technology Delhi for around five and a half years and as an Assistant Professor at the Centre for Advanced Study in Mathematics, Panjab University, Chandigarh for around 3 years. Currently, she is working in algebraic coding theory. Her research interests include algebraic coding theory, number theory and algebra.

Taranjot Kaur received BSc (Hons.) and MSc (Hons.) in Mathematics from the Centre for Advanced Study in Mathematics at Panjab University, Chandigarh,

India, in 2010 and 2012, respectively. She is currently a Research Student in the Department of Mathematics at Indian Institute of Technology Delhi, India. She is working in the area of algebraic coding theory.

1 Introduction

Additive codes of length n over the finite field $\mathbb{F}_4$ are introduced and studied by Calderbank et al. (1998). In the same work, the problem of finding quantum error-correcting codes is related to the problem of finding self-orthogonal additive codes over $\mathbb{F}_4$ with respect to the trace inner product on $\mathbb{F}_4^n$. Later, this theory is generalised to additive codes over the finite field $\mathbb{F}_{p^2}$ by Rains (1999), where p is a prime. Additive codes over any arbitrary finite field are further studied by Bierbrauer and Edel (2000) using twisted BCH-codes. For any prime power q, self-orthogonal additive codes over $\mathbb{F}_{q^2}$ (with respect to the trace symplectic inner product) are related to q-ary quantum codes by Ashikhmin and Knill (2001), thereby generalising the work of Calderbank et al. (1998). A general theory for decomposing additive self-dual codes (with respect to the Hermitian trace inner product) over $\mathbb{F}_4$ is presented by Huffman (2007). Cyclic additive codes of odd length over $\mathbb{F}_4$ are further studied and enumerated by Huffman (2007a) by writing a canonical form decomposition of these codes. Besides this, self-orthogonal and self-dual cyclic additive codes of odd length n over $\mathbb{F}_4$ (with respect to the trace inner product on $\mathbb{F}_4^n$) are also enumerated. In another paper, this work is extended by Huffman (2008) for cyclic additive codes of even length over $\mathbb{F}_4$. A parametric description and enumeration of these codes are also given. In a related work, a transform domain characterisation of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes is obtained by Dey and Rajan (2005) using the discrete Fourier transform, where $t \geq 2$ is an integer. In the same work, the non-existence of self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of certain parameters is also established. Cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n coprime to q are further studied by Bierbrauer (2007) using the theory of twisted codes. The theory of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n with $\gcd(n, q) = 1$ is further developed by Bierbrauer (2012).

In order to further explore the properties of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes, the theory developed in Huffman (2007a) is further generalised by Huffman (2010). To be more precise, cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n are viewed as $\mathbb{F}_q[X]/\langle X^n - 1\rangle$-submodules of the quotient ring $\mathbb{F}_{q^t}[X]/\langle X^n - 1\rangle$, where $\gcd(n, q) = 1$ and $t \geq 2$ are an integer. Using this, the number of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n is determined and their dual codes with respect to the ordinary and Hermitian trace inner products on $\mathbb{F}_{q^t}^n$ are also studied. In addition to this, bases of all the self-orthogonal and self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes with respect to these two trace inner products are explicitly determined. Furthermore, for any integer $t \geq 2$, all the self-dual and self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n are enumerated with respect to these two bilinear forms. In a recent work, cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n are investigated by Cao and Gao (2015) using the theory of linear codes over finite chain rings, where $\gcd(n, q) \neq 1$.

Let q be a power of the prime p, n be a positive integer coprime to q, and $t \geq 2$ be an integer satisfying $t \not\equiv 1 (\text{mod } p)$. In this paper, a new trace bilinear form, denoted by $*$, is introduced and studied on $\mathbb{F}_{q^t}^n$, which coincides with the trace inner product considered by Calderbank et al. (1998) when $q = t = 2$ and Hermitian trace inner product considered by Ezerman et al. (2013) when q is even and $t = 2$ (see Remark 3.1). The dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes with respect to $*$ are also studied. Analogous to the class of complementary-dual cyclic codes studied by Massey (1992) and Yang and Massey (1994), we introduce and study complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes with respect $*$, ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^t}^n$. To be more precise, basis sets of all the complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes are explicitly determined with respect to $*$, ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^2}^n$. By placing $*$ trace bilinear form on $\mathbb{F}_{q^2}^n$, all the self-dual and self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes are explicitly determined in terms of their basis sets. All the self-dual and self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes are also enumerated for any integer $t \geq 2$ with respect to $*$. In a subsequent work, we shall enumerate all the complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n with respect to $*$, ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^t}^n$, where $t \geq 2$ is an integer.

This paper is structured as follows: In Section 2, we state some preliminaries that are needed to derive our main results. In Section 3, we define $*$ trace bilinear form $(\cdot,\cdot)_*$ on $\mathbb{F}_{q^t}^n$ and study its properties (Lemma 3.2). We also define a sesquilinear form $[\cdot,\cdot]_*$ on $\mathbb{F}_{q^t}[X]/\langle X^n-1\rangle$ and study its properties by relating it to $*$ trace bilinear form $(\cdot,\cdot)_*$ on $\mathbb{F}_{q^t}^n$ (Lemma 3.3). In Section 4, we determine bases of all the complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n with respect to $*$, ordinary and Hermitian trace bilinear forms (Theorem 4.2), and enumerate these three classes of codes (Theorem 4.3). Besides this, by placing $*$ trace bilinear form on $\mathbb{F}_{q^t}^n$, we explicitly determine bases of all the self-orthogonal and self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n when $t=2$ (Theorems 4.4 and 4.6) and enumerate these two classes of codes for any integer $t \geq 2$ satisfying $t \not\equiv 1 (\text{mod } p)$ (Theorems 4.5 and 4.7–4.9).

2 Some preliminaries

In this section, we state some preliminaries that are needed to derive our main results.

Throughout this paper, let q be a power of the prime p, $\mathbb{F}_q$ denote the finite field with q elements, n be a positive integer coprime to p and $t \geq 2$ be an integer. Let $\mathcal{R}_n^{(q)}$ and $\mathcal{R}_n^{(q^t)}$ denote the quotient rings $\mathbb{F}_q[X]/\langle X^n-1\rangle$ and $\mathbb{F}_{q^t}[X]/\langle X^n-1\rangle$, respectively, where X is an indeterminate over $\mathbb{F}_p$ and over any extension field of $\mathbb{F}_p$. We shall represent elements of the rings $\mathcal{R}_n^{(q)}$ and $\mathcal{R}_n^{(q^t)}$ by their representatives of degree strictly less than n in $\mathbb{F}_q[X]$ and $\mathbb{F}_{q^t}[X]$, respectively. As $\gcd(n,q)=1$, by Maschke's Theorem, both the rings $\mathcal{R}_n^{(q)}$ and $\mathcal{R}_n^{(q^t)}$ are semi-simple, and hence can be written as direct sums of minimal ideals, all of which are fields. More explicitly, if $\{\ell_0=0,\ell_1,\cdots,\ell_{s-1}\}$ is a complete set of representatives of q-cyclotomic cosets modulo n, then $X^n-1=m_0(X)m_1(X)\cdots m_{s-1}(X)$ is the factorisation of X^n-1 into monic irreducible polynomials over $\mathbb{F}_q$ with $m_i(X)=\prod\limits_{k\in C_{\ell_i}^{(q)}}(X-\eta^k)$ for $0\leq i\leq s-1$, where $C_{\ell_i}^{(q)}$ $(0\leq i\leq s-1)$ is the q-cyclotomic coset modulo n containing the integer ℓ_i and η is a primitive nth root of unity in an extension field of $\mathbb{F}_q$. Therefore if $\mathcal{K}_i$ is the ideal of $\mathcal{R}_n^{(q)}$ generated by the polynomial $(X^n-1)/m_i(X)$ for $0\leq i\leq s-1$, then it is easy to see that $\mathcal{R}_n^{(q)}=\mathcal{K}_0\oplus\mathcal{K}_1\oplus\cdots\oplus\mathcal{K}_{s-1}$, where $\mathcal{K}_i\mathcal{K}_j=\{0\}$ for all $i\neq j$ and $\mathcal{K}_i\simeq\mathbb{F}_{q^{d_i}}$ with d_i as the cardinality of $C_{\ell_i}^{(q)}$. Note that when n is even, there exists an integer $i^{\#}$ satisfying $0\leq i^{\#}\leq s-1$ and $C_{\ell_{i^{\#}}}^{(q)}=C_{\frac{n}{2}}^{(q)}=\{\frac{n}{2}\}$, as q is odd.

In order to write $\mathcal{R}_n^{(q^t)}$ as the direct sum of minimal ideals, we further factorise the polynomials $m_0(X),m_1(X),\cdots,m_{s-1}(X)$ into monic irreducible polynomials over $\mathbb{F}_{q^t}$. To do this, by Lemma 1 of Huffman (2010), we see that $C_{\ell_i}^{(q)}=C_{\ell_i}^{(q^t)}\cup C_{\ell_iq}^{(q^t)}\cup\cdots\cup C_{\ell_iq^{g_i-1}}^{(q^t)}$ with $g_i=\gcd(d_i,t)$ for $0\leq i\leq s-1$, which led to the following factorisation of $m_i(X)$ over $\mathbb{F}_{q^t}$: $m_i(X)=M_{i,0}(X)M_{i,1}(X)\cdots M_{i,g_i-1}(X)$, where $M_{i,j}(X)=\prod\limits_{k\in C^{(q^t)}_{\ell_i q^j}}(X-\eta^k)$ for $0\leq j\leq g_i-1$ with $0\leq i\leq s-1$. Therefore, if for each i and j, $\mathcal{I}_{i,j}$ is the ideal of $\mathcal{R}_n^{(q^t)}$ generated by $(X^n-1)/M_{i,j}(X)$, then one can show that $\mathcal{R}_n^{(q^t)}=\bigoplus\limits_{i=0}^{s-1}\bigoplus\limits_{j=0}^{g_i-1}\mathcal{I}_{i,j}$, where $\mathcal{I}_{i,j}\mathcal{I}_{i'j'}=\{0\}$ for $(i,j)\neq(i',j')$ and $\mathcal{I}_{i,j}\simeq\mathbb{F}_{q^{tD_i}}$ with $D_i=\frac{d_i}{g_i}$. Further, it is easy to see that $\mathcal{J}_i=\mathcal{I}_{i,0}\oplus\mathcal{I}_{i,1}\oplus\cdots\oplus\mathcal{I}_{i,g_i-1}$ is a vector space of dimension t over $\mathcal{K}_i$ for $0\leq i\leq s-1$.

In order to study the containment $\mathcal{R}_n^{(q)}\subset\mathcal{R}_n^{(q^t)}$, Huffman (2010) defined the ring automorphism $\tau_{q^u,w}:\mathcal{R}_n^{(q^r)}\to\mathcal{R}_n^{(q^r)}$ as $\tau_{q^u,w}\left(\sum\limits_{i=0}^{n-1}a_iX^i\right)=\sum\limits_{i=0}^{n-1}a_i^{q^u}X^{wi}$ for any integer $r\geq 1$, where u,w are integers satisfying $0\leq u\leq r$, $1\leq w\leq n-1$ and $\gcd(w,n)=1$. When $r=t$, by Lemma 2 of Huffman (2010), we see that $\tau_{q^u,w}$ permutes ideals $\mathcal{I}_{i,j}$'s of the ring $\mathcal{R}_n^{(q^t)}$.

Now an $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code $\mathcal{C}$ of length n is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^t}^n$. Further the code $\mathcal{C}$ is said to be cyclic if $(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$ implies that $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in\mathcal{C}$. Throughout this paper, we shall identify each vector $a=(a_0,a_1,\cdots,a_{n-1})\in\mathbb{F}_{q^t}^n$ with $a(X)=\sum\limits_{i=0}^{n-1}a_iX^i\in\mathcal{R}_n^{(q^t)}$. Under this identification, one can easily observe that the cyclic shift $\sigma(a)=(a_{n-1},a_0,a_1,\cdots,a_{n-2})$ of $a\in\mathbb{F}_{q^t}^n$ is identified with $Xa(X)\in\mathcal{R}_n^{(q^t)}$. Therefore every cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code of length n can be viewed as an $\mathcal{R}_n^{(q)}$-submodule of $\mathcal{R}_n^{(q^t)}$. Huffman (2010) studied dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n with respect forms, which are as defined below:

Let $\text{Tr}_{q,t}:\mathbb{F}_{q^t}\to\mathbb{F}_q$ be the trace map defined as $\text{Tr}_{q,t}(\alpha)=\sum\limits_{j=0}^{t-1}\alpha^{q^j}$ for each $\alpha\in\mathbb{F}_{q^t}$. It is well known that $\text{Tr}_{q,t}$ is an $\mathbb{F}_q$-linear, surjective map with kernel of size q^{t-1} (see Lidl and Niederreiter (1994, p.51)). Then for any integer $t\geq 2$, the ordinary trace inner product on $\mathbb{F}_{q^t}^n$ is a map $(\cdot,\cdot)_0:\mathbb{F}_{q^t}^n\times\mathbb{F}_{q^t}^n\to\mathbb{F}_q$, defined as

$$(a,b)_0=\sum_{j=0}^{n-1}\text{Tr}_{q,t}(a_jb_j)\ \text{ for }\ a=(a_0,a_1,\cdots,a_{n-1}),\ b=(b_0,b_1,\cdots,b_{n-1})\in\mathbb{F}_{q^t}^n,$$

while the ordinary trace sesquilinear form on $\mathcal{R}_n^{(q^t)}$ is a map $[\cdot,\cdot]_0:\mathcal{R}_n^{(q^t)}\times\mathcal{R}_n^{(q^t)}\to\mathcal{R}_n^{(q)}$, defined as

$$[a(X),b(X)]_0=\sum_{u=0}^{t-1}\tau_{q^u,1}\left(a(X)\tau_{1,-1}(b(X))\right)\ \text{ for }\ a(X),\ b(X)\in\mathcal{R}_n^{(q^t)}.$$

The Hermitian trace inner product on $\mathbb{F}_{q^t}^n$ is a generalisation of the trace inner product considered by Calderbank et al. (1998) and Rains (1999) on $\mathbb{F}_{q^2}^n$. It is defined only for even integers $t\geq 2$, which can be written as $t=2^ym$, where $y\geq 1$ and m are odd. It is easy to see that there exists an element $\gamma\in\mathbb{F}_{q^{2^y}}$ satisfying $\gamma+\gamma^{q^{2^{y-1}}}=0$. Then the Hermitian trace inner product on $\mathbb{F}_{q^t}^n$ is a map $(\cdot,\cdot)_\gamma:\mathbb{F}_{q^t}^n\times\mathbb{F}_{q^t}^n\to\mathbb{F}_q$, defined as

$$(a,b)_\gamma=\sum_{j=0}^{n-1}\text{Tr}_{q,t}(\gamma a_jb_j^{q^{t/2}})\ \text{ for }\ a=(a_0,a_1,\cdots,a_{n-1}),\ b=(b_0,b_1,\cdots,b_{n-1})\in\mathbb{F}_{q^t}^n,$$

while the Hermitian trace sesquilinear form on $\mathcal{R}_n^{(q^t)}$ is a map $[\cdot,\cdot]_\gamma : \mathcal{R}_n^{(q^t)} \times \mathcal{R}_n^{(q^t)} \to \mathcal{R}_n^{(q)}$, defined as

$$[a(X), b(X)]_\gamma = \sum_{u=0}^{t-1} \tau_{q^u,1}\left(\gamma a(X)\tau_{q^{t/2},-1}(b(X))\right) \text{ for } a(X),\ b(X) \in \mathcal{R}_n^{(q^t)}.$$

For more details, one may refer to Huffman (2010).

From now onwards, we will follow the same notations as in Section 2. In the following section, we shall introduce and study another generalisation of the trace inner product considered by Calderbank et al. (1998) when $q = t = 2$ and Hermitian trace inner product considered by Ezerman et al. (2013) when q is even and $t = 2$.

3 $*$-Trace sesquilinear forms on $\mathbb{F}_{q^t}^n$ and $\mathcal{R}_n^{(q^t)}$

In this section, we will define new sesquilinear forms on $\mathbb{F}_{q^t}^n$ and $\mathcal{R}_n^{(q^t)}$ for any integer $t \geq 2$ satisfying $t \not\equiv 1(\text{mod}\, p)$, and study their properties. For this, we need the following lemma:

Lemma 3.1: *Let $t \geq 2$ be an integer satisfying $t \not\equiv 1(\text{mod}\, p)$. Then the map $\phi : \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}$ defined as*

$$\phi(\alpha) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{t-1}} \textit{ for each } \alpha \in \mathbb{F}_{q^t},$$

is an $\mathbb{F}_q$-linear vector space automorphism.

Proof: To prove this, by Sylvester's law of nullity, it suffices to prove that ϕ is an injective $\mathbb{F}_q$-linear vector space homomorphism (see Hoffman and Kunze (1971, p.71)). Towards this, we first observe that ϕ is an $\mathbb{F}_q$-linear map. Next to prove that ϕ is an injective map, we will show that the kernel of ϕ is $\{0\}$. For this, we first note that $\phi(0) = 0$. Further, if α lies in the kernel of ϕ, then $\phi(\alpha) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{t-1}} = 0$, which gives $\phi(\alpha)^q = \alpha + \alpha^{q^2} + \cdots + \alpha^{q^{t-1}} = 0$. From this, we obtain $\phi(\alpha) - \phi(\alpha)^q = \alpha^q - \alpha = 0$, which gives $\alpha^{q^u} = \alpha$ for each integer u $(1 \leq u \leq t-1)$. This implies that $(t-1)\alpha = \phi(\alpha) = 0$, which holds only when $\alpha = 0$, as $t \not\equiv 1(\text{mod}\, p)$. This proves the lemma. □

Next we define a mapping $(\cdot,\cdot)_* : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \to \mathbb{F}_q$ as

$$(a,b)_* = \sum_{j=0}^{n-1} \text{Tr}_{q,t}(a_j\phi(b_j)) \text{ for all } a = (a_0, a_1, \cdots, a_{n-1}) \text{ and } b = (b_0, b_1, \cdots, b_{n-1}) \text{ in } \mathbb{F}_{q^t}^n.$$

It is easy to see that for all $a = (a_0, a_1, \cdots, a_{n-1})$ and $b = (b_0, b_1, \cdots, b_{n-1})$ in $\mathbb{F}_{q^t}^n$,

$$(a,b)_* = \sum_{j=0}^{n-1} \{\text{Tr}_{q,t}(a_j)\text{Tr}_{q,t}(b_j) - \text{Tr}_{q,t}(a_jb_j)\} = \sum_{j=0}^{n-1} \text{Tr}_{q,t}(a_j)\text{Tr}_{q,t}(b_j) - (a,b)_0. \quad (1)$$

In the following lemma, we prove that the mapping $(\cdot,\cdot)_*$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_{q^t}^n$ for any prime power q, and is alternating when q is even.

Lemma 3.2: *For $a, b, c \in \mathbb{F}_{q^t}^n$ and $\alpha \in \mathbb{F}_q$, the following hold:*

i $(a,b)_* \in \mathbb{F}_q$.

ii $(a, b+c)_* = (a,b)_* + (a,c)_*$ *and* $(a+b, c)_* = (a,c)_* + (b,c)_*$.

iii $(\alpha a, b)_* = (a, \alpha b)_* = \alpha(a,b)_*$.

iv $(\cdot,\cdot)_*$ *is symmetric.*

v $(\cdot,\cdot)_*$ *is non-degenerate.*

vi $(\cdot,\cdot)_*$ *is alternating when q is even.*

Proof: Parts (i)–(iv) follow immediately from (1) and using the fact that $\text{Tr}_{q,t}$ is an $\mathbb{F}_q$-linear map.

In order to prove (v), we see that as $(\cdot,\cdot)_*$ is symmetric, it is enough to show that if $(a,b)_* = 0$ for all $b \in \mathbb{F}_{q^t}^n$, then $a = 0$. Suppose, on the contrary, that there exists a non-zero vector $a = (a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_{q^t}^n$ such that $(a,b)_* = 0$ for all $b \in \mathbb{F}_{q^t}^n$. Let j $(0 \leq j \leq n-1)$ be an integer such that $a_j \neq 0$. Now as $\text{Tr}_{q,t}$ is an onto map, there exists $\theta \in \mathbb{F}_{q^t}$ such that $\text{Tr}_{q,t}(\theta) \neq 0$. Then for $b = (b_0, b_1, \cdots, b_{n-1})$ with $b_j = \phi^{-1}(\theta a_j^{-1})$ and $b_i = 0$ for all $i \neq j$, we get $(a,b)_* = \text{Tr}_{q,t}(\theta) \neq 0$, which is a contradiction.

To prove (vi), we assume that q is even. Then for each $a = (a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_{q^t}^n$, we have $(a,a)_* = \sum\limits_{j=0}^{n-1} \left\{\text{Tr}_{q,t}(a_j)^2 - \text{Tr}_{q,t}(a_j^2)\right\}$, by (1). Now as q is even, it is easy to see that $\text{Tr}_{q,t}(a_j)^2 = \text{Tr}_{q,t}(a_j^2)$ for $0 \leq j \leq n-1$, which implies that $(a,a)_* = 0$. □

Remark 3.1: When $t = 2$, we have $(a,b)_* = \sum\limits_{j=0}^{n-1} \text{Tr}_{q,2}(a_j b_j^q) = \sum\limits_{j=0}^{n-1} (a_j b_j^q + a_j^q b_j)$ for all $a = (a_0, a_1, \cdots, a_{n-1}), b = (b_0, b_1, \cdots, b_{n-1}) \in \mathbb{F}_{q^2}^n$. Therefore, $*$ trace bilinear form on $\mathbb{F}_{q^t}^n$ is a generalisation of the trace inner product considered by Calderbank et al. (1998) when $q = t = 2$ and Hermitian trace inner product considered by Ezerman et al. (2013) when q is even and $t = 2$.

Next we define a mapping $[\cdot,\cdot]_* : \mathcal{R}_n^{(q^t)} \times \mathcal{R}_n^{(q^t)} \to \mathcal{R}_n^{(q)}$ as follows:

$$[a(X), b(X)]_* = \sum_{u=0}^{t-1} \tau_{q^u,1}\big(a(X) \sum_{w=1}^{t-1} \tau_{q^w,-1}(b(X))\big) = \sum_{u=0}^{t-1}\sum_{w=1}^{t-1} \tau_{q^u,1}(a(X))\tau_{q^{u+w},-1}(b(X))$$

for all $a(X),\ b(X) \in \mathcal{R}_n^{(q^t)}$.

In the following lemma, we relate the mapping $[\cdot,\cdot]_*$ with the bilinear form $(\cdot,\cdot)_*$ on $\mathbb{F}_{q^t}^n$, and prove that it is a non-degenerate and Hermitian $\tau_{1,-1}$-sesquilinear form on $\mathcal{R}_n^{(q^t)}$.

Lemma 3.3: *For $a(X), b(X), c(X) \in \mathcal{R}_n^{(q^t)}$ and $f(X) \in \mathcal{R}_n^{(q)}$, the following hold:*

i $[a(X), b(X)]_* = \sum\limits_{k=0}^{n-1} \big(a, \sigma^k(b)\big)_* X^k$.

ii $[a(X),b(X)]_* \in \mathcal{R}_n^{(q)}$.

iii $[a(X),b(X)+c(X)]_* = [a(X),b(X)]_* + [a(X),c(X)]_*$ *and* $[a(X)+b(X),c(X)]_* = [a(X),c(X)]_* + [b(X),c(X)]_*$.

iv $[f(X)a(X),b(X)]_* = f(X)\,[a(X),b(X)]_*$ *and* $[a(X),f(X)b(X)]_* = \tau_{1,-1}\big(f(X)\big)\,[a(X),b(X)]_*$.

v $[a(X),b(X)]_* = \tau_{1,-1}\big([b(X),a(X)]_*\big)$.

vi $[\cdot,\cdot]_*$ *is non-degenerate.*

Proof: To prove this, we write $a(X)=a_0+a_1X+\cdots+a_{n-1}X^{n-1}$, $b(X)=b_0+b_1X+\cdots+b_{n-1}X^{n-1}$ and $c(X)=c_0+c_1X+\cdots+c_{n-1}X^{n-1}$. Let $a=(a_0,a_1,\cdots,a_{n-1})$, $b=(b_0,b_1,\cdots,b_{n-1})$ and $c=(c_0,c_1,\cdots,c_{n-1})$.

i By definition, we have

$$\begin{aligned}[a(X),b(X)]_* &= \sum_{u=0}^{t-1}\sum_{w=1}^{t-1}\tau_{q^u,1}\big(a(X)\big)\tau_{q^{u+w},-1}\big(b(X)\big)\\ &= \sum_{u=0}^{t-1}\sum_{w=1}^{t-1}\sum_{k=0}^{n-1}\Bigg(\sum_{\substack{i,j=0\\ i-j\equiv k(\text{mod } n)}}^{n-1} a_i^{q^u}b_j^{q^{u+w}}\Bigg)X^k,\end{aligned}$$

which clearly equals $(a,b)_*+(a,\sigma(b))_*X+\cdots+(a,\sigma^{n-1}(b))_*X^{n-1}$.

ii It follows from part (i) and Lemma 3.2(i).

iii Since $\tau_{q^u,1}$ and $\tau_{q^u,-1}$ are ring automorphisms for each integer $u\ge 0$, part (iii) follows.

iv As $f(X)\in\mathcal{R}_n^{(q)}$, one can observe that the ring automorphisms $\tau_{q^u,1}$ and $\tau_{q^u,-1}$ satisfy $\tau_{q^u,1}\big(f(X)\big)=f(X)$ and $\tau_{q^u,-1}\big(f(X)\big)=\tau_{1,-1}\big(f(X)\big)$ for each integer $u\ge 0$. From this, part (iv) follows immediately.

v By part (i), we have $[a(X),b(X)]_* = (a,b)_* + \big(a,\sigma(b)\big)_* X+\cdots+\big(a,\sigma^{n-1}(b)\big)_*X^{n-1}$. By Lemma 3.2(iv), we have $\big(a,\sigma^k(b)\big)_* = (\sigma^k(b),a)_*$ for $0\le k\le n-1$. Further for each k, we observe that $(\sigma^k(b),a)_*=(b,\sigma^{n-k}(a))_*$, from which we obtain

$$\begin{aligned}[a(X),b(X)]_* &= (b,a)_*+(b,\sigma^{n-1}(a))_*X+\cdots+(b,\sigma(a))_*X^{n-1}\\ &= \tau_{1,-1}\big((b,a)_*+(b,\sigma(a))_*X+\cdots+(b,\sigma^{n-1}(a))_*X^{n-1}\big)\\ &= \tau_{1,-1}\big([b(X),a(X)]_*\big),\end{aligned}$$

using part (i) again.

vi In order to prove (vi), we need to show that if $[a(X),b(X)]_*=0$ for all $b(X)\in\mathcal{R}_n^{(q^t)}$, then $a(X)=0$. Suppose, on the contrary, that $a(X)\neq 0$. Then there exists j $(0\le j\le n-1)$ such that $a_j\neq 0$. As $\text{Tr}_{q,t}$ is an onto map, there exists $\theta\in\mathbb{F}_{q^t}$ such that $\text{Tr}_{q,t}(\theta)\neq 0$. Then for $b(X)=\phi^{-1}(\theta a_j^{-1})X^j$, by part (i), we have $[a(X),b(X)]_*=(a,b)_*=\text{Tr}_{q,t}(\theta)\neq 0$, which is a contradiction. □

Now we proceed to study dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n with respect to the bilinear forms $(\cdot,\cdot)_0$, $(\cdot,\cdot)_\gamma$ and $(\cdot,\cdot)_*$ on $\mathbb{F}_{q^t}^n$.

4 Dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes

For $\delta \in \{*, 0, \gamma\}$, throughout this paper, let $\mathbb{T}_\delta$ be defined as

i the set of all integers $t \geq 2$ satisfying $t \not\equiv 1 (\text{mod } p)$ when $\delta = *$

ii the set of all integers $t \geq 2$ when $\delta = 0$

iii the set of all even integers $t \geq 2$ when $\delta = \gamma$.

Now for each $\delta \in \{*, 0, \gamma\}$ with $t \in \mathbb{T}_\delta$, the δ-dual code of $\mathcal{C}$ is defined as $\mathcal{C}^{\perp_\delta} = \{v \in \mathbb{F}_{q^t}^n : (v, c)_\delta = 0 \text{ for all } c \in \mathcal{C}\}$. It is easy to see that the dual code $\mathcal{C}^{\perp_\delta}$ is also an $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code of length n. Further, if the code $\mathcal{C}$ is cyclic, then its dual code $\mathcal{C}^{\perp_\delta}$ is also cyclic. From now onwards, we shall view cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n and their δ-dual codes as $\mathcal{R}_n^{(q)}$-submodules of $\mathcal{R}_n^{(q^t)}$. Furthermore, if $\mathcal{C} \subseteq \mathcal{R}_n^{(q^t)}$ is any cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code, then one can easily view its dual code $\mathcal{C}^{\perp_\delta} \subseteq \mathcal{R}_n^{(q^t)}$ as the dual code of $\mathcal{C}$ with respect to the sesquilinear form $[\cdot,\cdot]_\delta$ on $\mathcal{R}_n^{(q^t)}$ for each $\delta \in \{*, 0, \gamma\}$.

Now to study the properties of δ-dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n, we need to study actions of the ring automorphisms $\tau_{q^u,-1}$ $(0 \leq u \leq t-1)$ on the ideals $\mathcal{J}_i$ $(0 \leq i \leq s-1)$ of $\mathcal{R}_n^{(q^t)}$. For this, we observe that $C_{-\ell_0}^{(q)} = C_{\ell_0}^{(q)}$, and further for each i $(1 \leq i \leq s-1)$, there exists a unique integer i' $(1 \leq i' \leq s-1)$ satisfying $C_{-\ell_i}^{(q)} = C_{\ell_{i'}}^{(q)}$. This gives rise to a permutation μ of $\{0, 1, 2, \cdots, s-1\}$ defined by $C_{-\ell_i}^{(q)} = C_{\ell_{\mu(i)}}^{(q)}$ for $0 \leq i \leq s-1$. Note that $\mu(0) = 0$ and $\mu(\mu(i)) = i$ for $0 \leq i \leq s-1$. That is, μ is either the identity permutation or is a product of transpositions. When n is even, there exists an integer $i^\#$ $(0 \leq i^\# \leq s-1)$ satisfying $C_{\ell_{i^\#}}^{(q)} = C_{\frac{n}{2}}^{(q)} = \{\frac{n}{2}\}$, as q is odd. Note that $C_{-\ell_{i^\#}}^{(q)} = C_{\ell_{i^\#}}^{(q)}$ so that $\mu(i^\#) = i^\#$. Next we make the following observation:

Lemma 4.1: *Let u $(0 \leq u \leq t-1)$ be a fixed integer. Then we have $\tau_{q^u,-1}(\mathcal{J}_i) = \mathcal{J}_{\mu(i)}$ for $0 \leq i \leq s-1$.*

Proof: Working in a similar way as in Lemma 8 of Huffman (2010), the result follows. □

Huffman (2010) proved the following theorem for $\delta \in \{0, \gamma\}$ and we observe that it also holds for $\delta = *$. The proof, being similar to that of Huffman (2010, Theorem 7), is left to the reader.

Theorem 4.1: *Let $\mathcal{C}$ be a cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code of length n. For $\delta \in \{*, 0, \gamma\}$ with $t \in \mathbb{T}_\delta$, we have $\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{s-1}$ and $\mathcal{C}^{\perp_\delta} = \mathcal{C}_0^{(\delta)} \oplus \mathcal{C}_1^{(\delta)} \oplus \cdots \oplus \mathcal{C}_{s-1}^{(\delta)}$, where $\mathcal{C}_i = \mathcal{C} \cap \mathcal{J}_i$ and $\mathcal{C}_i^{(\delta)} = \mathcal{C}^{\perp_\delta} \cap \mathcal{J}_i$ for all $0 \leq i \leq s-1$. Furthermore, for each i, we have $\mathcal{C}_{\mu(i)}^{(\delta)} = \{a(X) \in \mathcal{J}_{\mu(i)} : [a(X), c(X)]_\delta = 0 \text{ for all } c(X) \in \mathcal{C}_i\}$ and $\dim_{\mathcal{K}_{\mu(i)}} \mathcal{C}_{\mu(i)}^{(\delta)} = t - \dim_{\mathcal{K}_i} \mathcal{C}_i$ for $0 \leq i \leq s-1$. (Throughout this paper, $\dim_K V$ denotes the dimension of a finite-dimensional vector space V over the field K.)*

Further, a cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code $\mathcal{C}$ of length n is said to be

- δ-complementary-dual if it satisfies $\mathcal{C} \cap \mathcal{C}^{\perp_\delta} = \{0\}$.
- δ-self-orthogonal if it satisfies $\mathcal{C} \subseteq \mathcal{C}^{\perp_\delta}$.
- δ-self-dual if it satisfies $\mathcal{C} = \mathcal{C}^{\perp_\delta}$.

The following lemma characterises all the δ-complementary-dual, δ-self-orthogonal and δ-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes.

Lemma 4.2: *For $\delta \in \{*, 0, \gamma\}$ with $t \in \mathbb{T}_\delta$, let $\mathcal{C}$ be a cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code of length n. Let us write $\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{s-1}$ and $\mathcal{C}^{\perp_\delta} = \mathcal{C}_0^{(\delta)} \oplus \mathcal{C}_1^{(\delta)} \oplus \cdots \oplus \mathcal{C}_{s-1}^{(\delta)}$, where $\mathcal{C}_i = \mathcal{C} \cap \mathcal{J}_i$ and $\mathcal{C}_i^{(\delta)} = \mathcal{C}^{\perp_\delta} \cap \mathcal{J}_i$ for all $0 \leq i \leq s-1$. Then*

i *the code $\mathcal{C}$ is δ-complementary-dual if and only if $\mathcal{C}_i \cap \mathcal{C}_i^{(\delta)} = \{0\}$ for all $0 \leq i \leq s-1$*

ii *the code $\mathcal{C}$ is δ-self-orthogonal if and only if $\mathcal{C}_i \subseteq \mathcal{C}_i^{(\delta)}$ for all $0 \leq i \leq s-1$*

iii *the code $\mathcal{C}$ is δ-self-dual if and only if $\mathcal{C}_i = \mathcal{C}_i^{(\delta)}$ for all $0 \leq i \leq s-1$.*

Proof: Proof is trivial. □

First of all, we will consider the case $t = 2$ and we will study δ-dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes for each $\delta \in \{*, 0, \gamma\}$. For this, we see that when $t = 2$, the minimal ideal $\mathcal{I}_{i,j}$ of $\mathcal{R}_n^{(q^2)}$ is the finite field of order q^{2D_i} for $0 \leq i \leq s-1$ and $0 \leq j \leq g_i - 1$, where $D_i = \frac{d_i}{g_i}$ with $g_i = \gcd(2, d_i)$. For $0 \leq i \leq s-1$, in view of Lemma 2 of Huffman (2010), we choose primitive elements $\rho_{i,0}(X), \rho_{i,1}(X), \cdots, \rho_{i,g_i-1}(X)$ of the finite fields $\mathcal{I}_{i,0}, \mathcal{I}_{i,1}, \cdots, \mathcal{I}_{i,g_i-1}$, respectively, satisfying $\tau_{q^j,1}\big(\rho_{i,0}(X)\big) = \rho_{i,j}(X)$ for all $0 \leq j \leq g_i - 1$. Let $e_{i,j}(X)$ be the multiplicative identity of $\mathcal{I}_{i,j}$ for each i and j. Recall that when n is even, there exists an integer $i^\#$ satisfying $0 \leq i^\# \leq s-1$ and $C_{\ell_{i^\#}}^{(q)} = C_{\frac{n}{2}}^{(q)} = \{\frac{n}{2}\}$, since q is odd. As $C_{-\ell_{i^\#}}^{(q)} = C_{\ell_{i^\#}}^{(q)} = \{\frac{n}{2}\}$, we have $\mu(i^\#) = i^\#$.

4.1 Determination of δ-complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes

In the following theorem, we explicitly determine bases of all the δ-complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n for each $\delta \in \{*, 0, \gamma\}$, provided $\gcd(n, q) = 1$.

Theorem 4.2: *Let $t = 2$, q be a power of the prime p and n be a positive integer with $\gcd(n, q) = 1$. Let $\mathcal{C}$ be a cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-code of length n. Let us write $\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{s-1}$ and $\mathcal{C}^{\perp_\delta} = \mathcal{C}_0^{(\delta)} \oplus \mathcal{C}_1^{(\delta)} \oplus \cdots \oplus \mathcal{C}_{s-1}^{(\delta)}$, where $\mathcal{C}_i = \mathcal{C} \cap \mathcal{J}_i$ and $\mathcal{C}_i^{(\delta)} = \mathcal{C}^{\perp_\delta} \cap \mathcal{J}_i$ for $0 \leq i \leq s-1$. Then $\mathcal{C}$ is δ-complementary-dual if and only if for each i ($0 \leq i \leq s-1$), the following hold:*

i *If $i = 0$ or $i = i^\#$ (provided n is even), then*

a *$\mathcal{C}_i = \{0\}$ or*

b *$\mathcal{C}_i = \mathcal{J}_i$ or*

c $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *with basis* $\{\rho_{i,0}(X)^k\}$, *where*

for $\delta = *:$ *k does not exist when q is even and* $0 \leq k \leq q$ *when q is odd.*

for $\delta = 0:$ $1 \leq k \leq q$ *when q is even,* $0 \leq k \leq q$ *when* $q \equiv 1\ (mod\ 4)$ *and* $0 \leq k \leq q$ *with* $k \not\equiv \frac{q+1}{4} (mod\ \frac{q+1}{2})$ *when* $q \equiv 3\ (mod\ 4)$.

for $\delta = \gamma:$ *k does not exist.*

ii *If* $i \notin \{0,\ i^{\#}\}$, $\mu(i) = i$ *and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,0}$, *then*

a $\mathcal{C}_i = \{0\}$ *or*

b $\mathcal{C}_i = \mathcal{J}_i$ *or*

c $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *with basis as follows:*

for $\delta = *:$ $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \leq k \leq q^{d_i} - 2$ *satisfies* $k \not\equiv 0$ $(mod\ q^{d_i/2} + 1)$ *when q is even and* $k \not\equiv \frac{q^{d_i/2}+1}{2}$ $(mod\ q^{d_i/2} + 1)$ *when q is odd.*

for $\delta = 0:$ $\{e_{i,0}(X)\}$ *or* $\{e_{i,1}(X)\}$ *or* $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \leq k \leq q^{d_i} - 2$ *satisfies* $k \not\equiv 0\ (mod\ q^{d_i/2} - 1)$ *when q is even and* $k \not\equiv \frac{q^{d_i/2}-1}{2}$ $(mod\ q^{d_i/2} - 1)$ *when q is odd.*

for $\delta = \gamma:$ $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \leq k \leq q^{d_i} - 2$ *satisfies* $k \not\equiv 0\ (mod\ q^{d_i/2} + 1)$.

iii *If* $i \notin \{0,\ i^{\#}\}$, $\mu(i) = i$ *and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,1}$, *then*

a $\mathcal{C}_i = \{0\}$ *or*

b $\mathcal{C}_i = \mathcal{J}_i$ *or*

c $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *with basis as follows:*

for $\delta = *:$ $\{e_{i,0}(X)\}$ *or* $\{e_{i,1}(X)\}$ *or* $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \leq k \leq q^{d_i} - 2$ *satisfies* $k \not\equiv 0\ (mod\ q^{d_i/2} - 1)$ *when q is even and* $k \not\equiv \frac{q^{d_i/2}-1}{2}$ $(mod\ q^{d_i/2} - 1)$ *when q is odd.*

for $\delta = 0:$ $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \leq k \leq q^{d_i} - 2$ *satisfies* $k \not\equiv 0\ (mod\ q^{d_i/2} + 1)$ *when q is even and* $k \not\equiv \frac{q^{d_i/2}+1}{2}$ $(mod\ q^{d_i/2} + 1)$ *when q is odd.*

for $\delta = \gamma:$ $\{e_{i,0}(X)\}$ *or* $\{e_{i,1}(X)\}$ *or* $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \leq k \leq q^{d_i} - 2$ *satisfies* $k \not\equiv 0\ (mod\ q^{d_i/2} - 1)$.

iv *When* $\mu(i) \neq i$, d_i *is even and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),0}$, *we have the following:*

a *If* $\mathcal{C}_i = \{0\}$, *then* $\mathcal{C}_{\mu(i)} = \{0\}$.

b *If* $\mathcal{C}_i = \mathcal{J}_i$, *then* $\mathcal{C}_{\mu(i)} = \mathcal{J}_{\mu(i)}$.

c *If $\mathcal{C}_i$ is a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ having basis $\{a(X)\}$, then $\mathcal{C}_{\mu(i)}$ is also a one-dimensional $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$ having basis $\{b(X)\}$, where*

for $\delta = *:$ $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,0}(X)$; $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,1}(X)$; *and* $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \leq k, k' \leq q^{d_i} - 2$ *satisfying* $k' \not\equiv k$ *(mod* $q^{d_i} - 1)$ *if q is even and* $k' \not\equiv k + \frac{q^{d_i}-1}{2}$ *(mod* $q^{d_i} - 1)$ *if q is odd.*

for $\delta = 0:$ $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,0}(X)$; $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,1}(X)$; $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \leq k, k' \leq q^{d_i} - 2$ *satisfying* $k' \not\equiv q^{d_i} - 1 - k$ *(mod* $q^{d_i} - 1)$ *if q is even and* $k' \not\equiv \frac{q^{d_i}-1}{2} - k$ *(mod* $q^{d_i} - 1)$ *if q is odd.*

for $\delta = \gamma:$ $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,0}(X)$; $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,1}(X)$; *and* $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \leq k, k' \leq q^{d_i} - 2$ *satisfying* $k' \neq k$.

v *When $\mu(i) \neq i$, d_i is even and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),1}$, we have the following:*

a *If $\mathcal{C}_i = \{0\}$, then $\mathcal{C}_{\mu(i)} = \{0\}$.*

b *If $\mathcal{C}_i = \mathcal{J}_i$, then $\mathcal{C}_{\mu(i)} = \mathcal{J}_{\mu(i)}$.*

c *If $\mathcal{C}_i$ is a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ having basis $\{a(X)\}$, then $\mathcal{C}_{\mu(i)}$ is also a one-dimensional $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$ having basis $\{b(X)\}$, where*

for $\delta = *:$ $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,0}(X)$; $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,1}(X)$; *and* $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \leq k, k' \leq q^{d_i} - 2$ *satisfying* $k' \not\equiv q^{d_i} - 1 - k$ *(mod* $q^{d_i} - 1)$ *if q is even and* $k' \not\equiv \frac{q^{d_i}-1}{2} - k$ *(mod* $q^{d_i} - 1)$ *if q is odd.*

for $\delta = 0:$ $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,0}(X)$; $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *with* $0 \leq k \leq q^{d_i} - 2$ *when* $a(X) = e_{i,1}(X)$; *and* $b(X) = e_{\mu(i),0}(X)$ *or* $b(X) = e_{\mu(i),1}(X)$ *or* $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with*

$0 \le k, k' \le q^{d_i} - 2$ satisfying $k' \not\equiv k \ (mod\ q^{d_i} - 1)$ if q is even and $k' \not\equiv \frac{q^{d_i}-1}{2} + k \ (mod\ q^{d_i} - 1)$ if q is odd.

for $\delta = \gamma$: *$b(X) = e_{\mu(i),0}(X)$ or $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ with $0 \le k \le q^{d_i} - 2$ when $a(X) = e_{i,0}(X)$; $b(X) = e_{\mu(i),1}(X)$ or $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ with $0 \le k \le q^{d_i} - 2$ when $a(X) = e_{i,1}(X)$; and $b(X) = e_{\mu(i),0}(X)$ or $b(X) = e_{\mu(i),1}(X)$ or $b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ when $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ with $0 \le k, k' \le q^{d_i} - 2$ satisfying $k' \not\equiv q^{d_i} - 1 - k \ (mod\ q^{d_i} - 1)$.*

vi *When $\mu(i) \ne i$ and d_i is odd, we have the following:*

a *If $\mathcal{C}_i = \{0\}$, then $\mathcal{C}_{\mu(i)} = \{0\}$.*

b *If $\mathcal{C}_i = \mathcal{J}_i$, then $\mathcal{C}_{\mu(i)} = \mathcal{J}_{\mu(i)}$.*

c *If $\mathcal{C}_i$ is a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ having basis $\{\rho_{i,0}(X)^k\}$, then $\mathcal{C}_{\mu(i)}$ is also a one-dimensional $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$ having basis $\{\rho_{\mu(i),0}(X)^{k'}\}$, where $0 \le k, k' \le q^{d_i}$ satisfy*

for $\delta = *$: *$k' \ne k$ if q is even and $k' \not\equiv k + \frac{q^{d_i}+1}{2} \ (mod\ q^{d_i} + 1)$ if q is odd.*

for $\delta = 0$: *$k' \not\equiv q^{d_i} + 1 - k \ (mod\ q^{d_i} + 1)$ if q is even and $k' \not\equiv \frac{q^{d_i}+1}{2} - k \ (mod\ q^{d_i} + 1)$ if q is odd.*

for $\delta = \gamma$: *$k' \ne k$.*

Proof: By Lemma 4.2(i), we see that the code $\mathcal{C}$ is δ-complementary-dual if and only if $\mathcal{C}_i \cap \mathcal{C}_i^{(\delta)} = \{0\}$ for $0 \le i \le s-1$. So for each i $(0 \le i \le s-1)$, we need to determine all $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying

$$\mathcal{C}_i \cap \mathcal{C}_i^{(\delta)} = \{0\}, \tag{2}$$

where $\dim_{\mathcal{K}_i}\mathcal{C}_i \le 2$ and $\dim_{\mathcal{K}_i}\mathcal{C}_i^{(\delta)} \le 2$ for each i.

When $\mu(i) = i$, by Theorem 4.1, we have $\dim_{\mathcal{K}_i}\mathcal{C}_i^{(\delta)} = 2 - \dim_{\mathcal{K}_i}\mathcal{C}_i$. From this, we see that $\mathcal{C}_i = \{0\}$ and $\mathcal{C}_i = \mathcal{J}_i$ satisfy (2). Further when $\dim_{\mathcal{K}_i}\mathcal{C}_i = 1$, we have $\dim_{\mathcal{K}_i}\mathcal{C}_i^{(\delta)} = 1$. As $\mathcal{C}_i \cap \mathcal{C}_i^{(\delta)}$ is a $\mathcal{K}_i$-subspace of $\mathcal{C}_i$ as well as $\mathcal{C}_i^{(\delta)}$, we observe that $\mathcal{C}_i$ will satisfy (2) if and only if $\mathcal{C}_i \ne \mathcal{C}_i^{(\delta)}$.

When $\mu(i) \ne i$, by Theorem 4.1, we have $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)}^{(\delta)} = 2 - \dim_{\mathcal{K}_i}\mathcal{C}_i$. Here we will determine the pairs $(\mathcal{C}_i, \mathcal{C}_{\mu(i)})$ satisfying

$$\mathcal{C}_i \cap \mathcal{C}_i^{(\delta)} = \{0\} \text{ and } \mathcal{C}_{\mu(i)} \cap \mathcal{C}_{\mu(i)}^{(\delta)} = \{0\}. \tag{3}$$

When $\mathcal{C}_i = \{0\}$, we have $\mathcal{C}_{\mu(i)}^{(\delta)} = \mathcal{J}_{\mu(i)}$. Here we observe that (3) will hold if and only if $\mathcal{C}_{\mu(i)} = \{0\}$, which gives $\mathcal{C}_i^{(\delta)} = \mathcal{J}_i$. When $\mathcal{C}_i = \mathcal{J}_i$, we have $\mathcal{C}_{\mu(i)}^{(\delta)} = \{0\}$. In this case, we note that (3) holds if and only if $\mathcal{C}_i^{(\delta)} = \{0\}$, which gives $\mathcal{C}_{\mu(i)} = \mathcal{J}_{\mu(i)}$. When $\dim_{\mathcal{K}_i}\mathcal{C}_i = 1$, we have $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)}^{(\delta)} = 1$. Here we assert that $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)} = 1$. This is because, if $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)} = 0$ or 2, then we have $\mathcal{C}_i^{(\delta)} = \mathcal{J}_i$ or $\{0\}$ in the respective cases, and hence (3) does not hold in both the cases. Therefore, in this case, we need to determine the pairs $(\mathcal{C}_i, \mathcal{C}_{\mu(i)})$ with $\mathcal{C}_i$ as a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ and $\mathcal{C}_{\mu(i)}$ as a one-dimensional $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$ satisfying $\mathcal{C}_i \neq \mathcal{C}_i^{(\delta)}$ and $\mathcal{C}_{\mu(i)} \neq \mathcal{C}_{\mu(i)}^{(\delta)}$.

From the above discussion, it follows that we need to determine all one-dimensional $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i \neq \mathcal{C}_i^{(\delta)}$ for $0 \leq i \leq s-1$. To do this, we shall first consider the case $\delta = *$.

i First let $i = 0$ or $i^{\#}$ (if n is even). Here we have $d_i = 1$, which gives $g_i = 1$ and $D_i = 1$ and so $\mathcal{J}_i = \mathcal{I}_{i,0} \simeq \mathbb{F}_{q^2}$ and $\mathcal{K}_i \simeq \mathbb{F}_q$. In this case, it is easy to observe that there are precisely $q+1$ distinct one-dimensional $\mathcal{K}_i$-subspaces of $\mathcal{J}_i$ having bases sets as $\{\rho_{i,0}(X)^k\}$ for $0 \leq k \leq q$. Here we assert that $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ holds for all k $(0 \leq k \leq q)$ when q is even and $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ does not hold for any k when q is odd. To prove this, we see that $\{\rho_{i,0}(X)^k\}$ $(0 \leq k \leq q)$ is a basis of $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ if and only if $\big[\rho_{i,0}(X)^k, \rho_{i,0}(X)^k\big]_* = 0$, by Theorem 4.1. That is, $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ holds if and only if $\big(\rho_{i,0}(X)^k\big)\tau_{q,-1}\big(\rho_{i,0}(X)^k\big) + \tau_{q,1}\big(\rho_{i,0}(X)^k\big)\tau_{1,-1}\big(\rho_{i,0}(X)^k\big)= 0$. Now by Lemma 11(i) and (ii) of Huffman (2010), we have $\tau_{1,-1}\big(\rho_{i,0}(X)\big) = \rho_{i,0}(X)$ and $\tau_{q,1}\big(\rho_{i,0}(X)\big) = \rho_{i,0}(X)^q$, which implies that $\tau_{q,-1}\big(\rho_{i,0}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(\rho_{i,0}(X)\big)\big) = \rho_{i,0}(X)^q$. This gives $\big(\rho_{i,0}(X)^k\big)\tau_{q,-1}\big(\rho_{i,0}(X)^k\big) + \tau_{q,1}\big(\rho_{i,0}(X)^k\big)\tau_{1,-1}\big(\rho_{i,0}(X)^k\big)= 2\rho_{i,0}(X)^{(q+1)k}$. From this, it follows that $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ if and only if $2\rho_{i,0}(X)^{(q+1)k} = 0$, which holds if and only if q is even. From this, part (i) follows.

When d_i is even, we have $g_i = 2$ and $D_i = d_i/2$. This implies that $\mathcal{J}_i = \mathcal{I}_{i,0} \oplus \mathcal{I}_{i,1}$ and $\mathcal{I}_{i,0} \simeq \mathcal{I}_{i,1} \simeq \mathcal{K}_i \simeq \mathbb{F}_{q^{d_i}}$. Here by Theorem 2 of Huffman (2010), it is easy to show that there are precisely $q^{d_i}+1$ distinct one-dimensional $\mathcal{K}_i$-subspaces of $\mathcal{J}_i$ having bases sets as $\{e_{i,0}(X)\}$, $\{e_{i,1}(X)\}$ and $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$ for $0 \leq k \leq q^{d_i}-2$. From now onwards, throughout the proof, we shall consider the subscript $j+1$ of $\mathcal{I}_{i,j+1}$ modulo 2.

ii Let $i \notin \{0,\ i^{\#}\}$ be such that $\mu(i) = i$ and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,0}$. In In this case, by Lemma 10(i) of Huffman (2010), we see that the integer d_i is even. Here we assert that $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ holds if and only if $\mathcal{C}_i$ has basis sets as $\{e_{i,0}(X)\}$, $\{e_{i,1}(X)\}$ and $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, where $0 \leq k \leq q^{d_i}-2$ satisfies $k \equiv 0 \pmod{q^{d_i/2}+1}$ when q is even and $k \equiv \frac{q^{d_i/2}+1}{2} \pmod{q^{d_i/2}+1}$ when q is odd. To prove this assertion, by Lemma 11(iii) of Huffman (2010), we see that for $j \in \{0,1\}$, $\tau_{1,-1}\big(\rho_{i,j}(X)\big) = \rho_{i,j}(X)^{q^{d_i/2}}$. Also we have $\tau_{q,1}(\rho_{i,j}(X)) = \rho_{i,j+1}(X)$ and $\tau_{q,1}(e_{i,j}(X)) = e_{i,j+1}(X)$. So we get $\tau_{q,-1}\big(\rho_{i,j}(X)\big) = \tau_{q,1}\ \big(\tau_{1,-1}\big(\rho_{i,j}(X)\big)\big) = \rho_{i,j+1}(X)^{q^{d_i/2}}$ and $\tau_{q,-1}\big(e_{i,j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(e_{i,j}(X)\big)\big) = e_{i,j+1}(X)$. In view of this, for $j \in \{0,1\}$, we observe that $[e_{i,j}(X), e_{i,j}(X)]_* = 0$, so by applying Theorem 4.1, we see that the subspace $\mathcal{C}_i$ with basis $\{e_{i,j}(X)\}$ satisfies $\mathcal{C}_i = \mathcal{C}_i^{(*)}$. Further, for $0 \leq k \leq q^{d_i}-2$, $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$ is a basis of $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ if and only if $\big[e_{i,0}(X) + \rho_{i,1}(X)^k, e_{i,0}(X) + \rho_{i,1}(X)^k\big]_* = 0$ by Theorem 4.1. This holds if and only if $\big(e_{i,0}(X) + \rho_{i,1}(X)^k\big)\tau_{q,-1}\big(e_{i,0}(X) + \rho_{i,1}(X)^k\big) + \tau_{q,1}\big(e_{i,0}(X) + \rho_{i,1}(X)^k\big)\tau_{1,-1}\big(e_{i,0}(X) + \rho_{i,1}(X)^k\big) = 0$ if and only if $\big(e_{i,0}(X) + \rho_{i,1}(X)^k\big)$ $\big(e_{i,1}(X) + \rho_{i,0}(X)^{kq^{d_i/2}}\big) + \big(e_{i,1}(X) + \rho_{i,0}(X)^k\big)\big(e_{i,0}(X) + \rho_{i,1}(X)^{kq^{d_i/2}}\big) = 0$

if and only if $\rho_{i,0}(X)^k + \rho_{i,0}(X)^{kq^{d_i/2}} = 0$ if and only if $k(q^{d_i/2} - 1) \equiv 0 \pmod{q^{d_i} - 1}$ when q is even and $k(q^{d_i/2} - 1) \equiv \frac{q^{d_i}-1}{2} \pmod{q^{d_i} - 1}$ when q is odd. From this, part (ii) follows.

iii Let $i \notin \{0, i^{\#}\}$ be such that $\mu(i) = i$ and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,1}$. In this case also, by Lemma 10(i) of Huffman (2010), we note that the integer d_i is even. We also note that $\tau_{1,-1}(\mathcal{I}_{i,1}) = \mathcal{I}_{i,0}$. Further, by Lemma 2 of Huffman (2010), we have $\tau_{q,1}(\mathcal{I}_{i,j}) = \mathcal{I}_{i,j+1}$ for $j \in \{0, 1\}$. From this, we obtain $\tau_{q,-1}(\mathcal{I}_{i,j}) = \mathcal{I}_{i,j}$ for $j \in \{0, 1\}$. Now by Lemma 11(iv) of Huffman (2010), we have $\tau_{q,-1}\big(\rho_{i,j}(X)\big) = \rho_{i,j}(X)^{q^{d_i/2}}$ and $\tau_{q,-1}\big(e_{i,j}(X)\big) = e_{i,j}(X)$. As $\tau_{q^2,1} = \tau_{1,1}$, we see that $\tau_{1,-1}\big(\rho_{i,j}(X)\big) = \tau_{q,1}\big(\tau_{q,-1}\big(\rho_{i,j}(X)\big)\big) = \rho_{i,j+1}(X)^{q^{d_i/2}}$ for $j \in \{0, 1\}$ and $\tau_{1,-1}\big(e_{i,j}(X)\big) = e_{i,j+1}(X)$. From this, we see that $[e_{i,j}(X), e_{i,j}(X)]_* \neq 0$ for $j \in \{0, 1\}$, which implies that the subspace $\mathcal{C}_i$ with basis $\{e_{i,j}(X)\}$ does not satisfy $\mathcal{C}_i = \mathcal{C}_i^{(*)}$. Further, working in a similar way as in part (ii), one can prove the desired result for the subspace $\mathcal{C}_i$ with basis $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, where $0 \leq k \leq q^{d_i} - 2$.

iv Let $\mu(i) \neq i$, d_i be even and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),0}$. Here we observe that for $j \in \{0, 1\}$, $\tau_{1,-1}(\mathcal{I}_{i,j}) = \mathcal{I}_{\mu(i),j}$, which gives $\tau_{1,-1}\big(\mathcal{I}_{\mu(i),j}\big) = \mathcal{I}_{i,j}$. From this, we get $\tau_{1,-1}\big(\rho_{i,j}(X)\big) = \rho_{\mu(i),j}(X)$ and $\tau_{1,-1}\big(e_{i,j}(X)\big) = e_{\mu(i),j}(X)$ for $j \in \{0, 1\}$. Further, by applying Lemma 2 of Huffman (2010), for $j \in \{0, 1\}$, we have $\tau_{q,1}\big(e_{i,j}(X)\big) = e_{i,j+1}(X)$, $\tau_{q,1}\big(e_{\mu(i),j}(X)\big) = e_{\mu(i),j+1}(X)$ and $\tau_{q,1}\big(\rho_{i,j}(X)\big) = \rho_{i,j+1}(X)$, $\tau_{q,1}\big(\rho_{\mu(i),j}(X)\big) = \rho_{\mu(i),j+1}(X)$ by our choice of identity elements $e_{i,j}(X)$'s and primitive elements $\rho_{i,j}(X)$'s. From this, we get $\tau_{q,-1}\big(\rho_{i,j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(\rho_{i,j}(X)\big)\big) = \rho_{\mu(i),j+1}(X)$ and $\tau_{q,-1}\big(\rho_{\mu(i),j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(\rho_{\mu(i),j}(X)\big)\big) = \rho_{i,j+1}(X)$. Besides this, we have $\tau_{q,-1}\big(e_{i,j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(e_{i,j}(X)\big)\big) = e_{\mu(i),j+1}(X)$ and $\tau_{q,-1}\big(e_{\mu(i),j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(e_{\mu(i),j}(X)\big)\big) = e_{i,j+1}(X)$. Using this, it is easy to observe that $\big[e_{\mu(i),j}(X), e_{i,j}(X)\big]_* = 0$, $[e_{\mu(i),j+1}(X), e_{i,j}(X)]_* \neq 0$ and $\big[e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k, e_{i,j}(X)\big]_* \neq 0$ for $j \in \{0, 1\}$. This, by Theorem 4.1, implies that if the subspace $\mathcal{C}_i$ has basis $\{e_{i,j}(X)\}$, then the subspace $\mathcal{C}_{\mu(i)}^{(*)}$ has basis $\{e_{\mu(i),j}(X)\}$. Since the subspace $\mathcal{C}_{\mu(i)}$ has to satisfy (3), its basis set has the following possible choices: $\{e_{\mu(i),j+1}(X)\}$ and $\{e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k\}$, where $0 \leq k \leq q^{d_i} - 2$. We next observe that if $\mathcal{C}_{\mu(i)}$ has basis $\{e_{\mu(i),j+1}(X)\}$, then $\mathcal{C}_i^{(*)}$ has basis $\{e_{i,j+1}(X)\}$ and this choice satisfies (3). On the other hand, if $\mathcal{C}_{\mu(i)}$ has basis $\{e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k\}$, then $\mathcal{C}_i^{(*)}$ has basis $\{e_{i,0}(X) + \rho_{i,1}(X)^{k'}\}$, where $k' \equiv k \pmod{q^{d_i} - 1}$ when q is even and $k' \equiv\ k + \frac{q^{d_i}-1}{2} \pmod{q^{d_i} - 1}$ when q is odd. Note that in this case also, (3) holds. Further working in a similar way as above, one can show that if $\mathcal{C}_i$ has basis $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$ for $0 \leq k \leq q^{d_i} - 2$, then $\{e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^\ell\}$ is a basis of $\mathcal{C}_{\mu(i)}^{(*)}$, where $\ell \equiv k \pmod{q^{d_i} - 1}$ if q is even and $\ell \equiv k + \frac{q^{d_i}-1}{2} \pmod{q^{d_i} - 1}$ if q is odd. We next observe that (3) holds if the subspace $\mathcal{C}_{\mu(i)}$ has basis sets as $\{e_{\mu(i),j}(X)\}$ or $\{e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^m\}$ for each $j \in \{0, 1\}$, where $m \not\equiv \ell \pmod{q^{d_i} - 1}$ when q is even and $m \not\equiv \ell + \frac{q^{d_i}-1}{2} \pmod{q^{d_i} - 1}$ when q is odd. These two possible choices for basis of $\mathcal{C}_{\mu(i)}$ give rise to the following choices for basis of $\mathcal{C}_i^{(*)}$ in the respective cases: $\{e_{i,j+1}(X)\}$ and $\{e_{i,0}(X)+\rho_{i,1}(X)^u\}$, where $u \equiv m$ (mod $q^{d_i}-1$) when q is even and $u \equiv m + \frac{q^{d_i}-1}{2}$ (mod $q^{d_i}-1$) when q is odd. One can easily verify that in all these cases, (3) holds. This proves (iv).

v Let $\mu(i) \neq i$, d_i be even and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),1}$. Here we note that $\tau_{1,-1}(\mathcal{I}_{i,j}) = \mathcal{I}_{\mu(i),j+1}$ for $j \in \{0,1\}$. Next by Lemma 2 of Huffman (2010), we have $\tau_{q,1}(\mathcal{I}_{i,j}) = \mathcal{I}_{i,j+1}$ for $j \in \{0,1\}$. This implies that $\tau_{1,-1}\big(\rho_{i,j}(X)\big) = \rho_{\mu(i),j+1}(X)$, $\tau_{1,-1}\big(e_{i,j}(X)\big) = e_{\mu(i),j+1}(X)$, $\tau_{q,1}\big(\rho_{i,j}(X)\big) = \rho_{i,j+1}(X)$, $\tau_{q,1}\big(e_{i,j}(X)\big) = e_{i,j+1}(X)$, $\tau_{q,1}\big(\rho_{\mu(i),j}(X)\big) = \rho_{\mu(i),j+1}(X)$ and $\tau_{q,1}\big(e_{\mu(i),j}(X)\big) = e_{\mu(i),j+1}(X)$. From this, it follows that $\tau_{q,-1}\big(\rho_{i,j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(\rho_{i,j}(X)\big)\big) = \rho_{\mu(i),j}(X)$ and $\tau_{q,-1}\big(\rho_{\mu(i),j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(\rho_{\mu(i),j}(X)\big)\big) = \rho_{i,j}(X)$. Also we have $\tau_{q,-1}\big(e_{i,j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(e_{i,j}(X)\big)\big) = e_{\mu(i),j}(X)$ and $\tau_{q,-1}\big(e_{\mu(i),j}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(e_{\mu(i),j}(X)\big)\big) = e_{i,j}(X)$. Now working in a similar way as in part (iv), part (v) follows.

vi Finally, we assume that $\mu(i) \neq i$ and d_i are odd. Here we have $g_i = 1$, $\mathcal{J}_i = \mathcal{I}_{i,0} \simeq \mathbb{F}_{q^{2d_i}}$ and $\mathcal{K}_i \simeq \mathbb{F}_{q^{d_i}}$. In this case, we observe that there are precisely $q^{d_i}+1$ distinct one-dimensional $\mathcal{K}_i$-subspaces of $\mathcal{J}_i$ having basis sets as $\{\rho_{i,0}(X)^k\}$, where $0 \leq k \leq q^{d_i}$. Further, it is easy to show that if, for $0 \leq k \leq q^{d_i}$, the set $\{\rho_{i,0}(X)^k\}$ is a basis of $\mathcal{C}_i$, then $\{\rho_{\mu(i),0}(X)^\ell\}$ is a basis of $\mathcal{C}^{(*)}_{\mu(i)}$, where $0 \leq \ell \leq q^{d_i}$ is an integer satisfying $\ell \equiv k$ (mod $q^{d_i}+1$) when q is even and $\ell \equiv k + \frac{q^{d_i}+1}{2}$ (mod $q^{d_i}+1$) when q is odd. To prove this, we observe that $\tau_{q,1}$ is an automorphism of $\mathcal{J}_i$ of order 2, so we have $\tau_{q,1}\big(\rho_{i,0}(X)\big) = \rho_{i,0}(X)^{q^{d_i}}$ and $\tau_{q,1}\big(e_{i,0}(X)\big) = e_{i,0}(X)$. Further by applying Lemma 2 of Huffman (2010), we get $\tau_{1,-1}\big(\rho_{i,0}(X)\big) = \rho_{\mu(i),0}(X)$ and $\tau_{1,-1}\big(e_{i,0}(X)\big) = e_{\mu(i),0}(X)$. This gives $\tau_{q,-1}\big(\rho_{i,0}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(\rho_{i,0}(X)\big)\big) = \rho_{\mu(i),0}(X)^{q^{d_i}}$ and $\tau_{q,-1}\big(e_{i,0}(X)\big) = \tau_{q,1}\big(\tau_{1,-1}\big(e_{i,0}(X)\big)\big) = e_{\mu(i),0}(X)$. Now working in a similar manner as in part (iv), the result follows.

For $\delta \in \{0,\gamma\}$, working in a similar way as above, the desired result follows. □

In the following theorem, we enumerate all the δ-complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n for $\delta \in \{*,0,\gamma\}$, provided $\gcd(n,q)=1$. For this, throughout this paper, let $\mathfrak{F}$ be the set consisting of all the fixed points of μ excluding 0 and $i^{\#}$ (if n is even) and $\mathfrak{M}$ be the set containing one element from each of the transpositions in μ.

Theorem 4.3: *Let $t=2$, q be a power of the prime p and n be a positive integer coprime to q. For $\delta \in \{*,0,\gamma\}$, let N be the number of distinct δ-complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n.*

i *When $\delta = *$, we have $N = A\prod_{i\in\mathfrak{F}}(q^{d_i}-q^{d_i/2}+2)\prod_{h\in\mathfrak{M}}(q^{2d_h}+q^{d_h}+2)$, where $A=2$ if q is even and $A=(q+3)^{\gcd(n,2)}$ if q is odd.*

ii *When $\delta = 0$, we have $N = A\prod_{i\in\mathfrak{F}}(q^{d_i}-q^{d_i/2}+2)\prod_{h\in\mathfrak{M}}(q^{2d_h}+q^{d_h}+2)$, where $A=q+2$ if q is even, $A=(q+3)^{\gcd(n,2)}$ if $q \equiv 1$ (mod 4) and $A=(q+1)^{\gcd(n,2)}$ if $q \equiv 3$ (mod 4).*

iii *When* $\delta = \gamma$, *we have* $N = A \prod_{i \in \mathfrak{F}} (q^{d_i} - q^{d_i/2} + 2) \prod_{h \in \mathfrak{M}} (q^{2d_h} + q^{d_h} + 2)$, *where* $A = 2$ *if* n *is odd and* $A = 4$ *if* n *is even.*

Proof: For $i \in \mathfrak{F} \cup \{0, i^{\#}\}$, let N_i be the number of distinct $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i \cap \mathcal{C}_i^{(\delta)} = \{0\}$. For $h \in \mathfrak{M}$, let N_h be the number of distinct pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$ with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h \cap \mathcal{C}_h^{(\delta)} = \{0\}$ and $\mathcal{C}_{\mu(h)} \cap \mathcal{C}_{\mu(h)}^{(\delta)} = \{0\}$. Then in view of Lemma 4.2(i), we see that the number N of distinct δ-complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n is given by

$$N = \prod_{i=0}^{s-1} N_i = \begin{cases} N_0 \prod\limits_{i \in \mathfrak{F}} N_i \prod\limits_{h \in \mathfrak{M}} N_h & \text{if } n \text{ is odd;} \\ N_0 N_{i^{\#}} \prod\limits_{i \in \mathfrak{F}} N_i \prod\limits_{h \in \mathfrak{M}} N_h & \text{if } n \text{ is even.} \end{cases}$$

Now using Theorem 4.2, the desired result follows. □

4.2 Determination of $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes

In the following theorem, we explicitly determine bases of all the $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n, provided $\gcd(n, q) = 1$.

Theorem 4.4: *Let* $t = 2$, q *be a power of the prime* p *and* n *be a positive integer coprime to* q. *Let* $\mathcal{C}$ *be a cyclic* $\mathbb{F}_q$*-linear* $\mathbb{F}_{q^2}$*-code of length* n. *Let us write* $\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{s-1}$ *and* $\mathcal{C}^{\perp_*} = \mathcal{C}_0^{(*)} \oplus \mathcal{C}_1^{(*)} \oplus \cdots \oplus \mathcal{C}_{s-1}^{(*)}$, *where* $\mathcal{C}_i = \mathcal{C} \cap \mathcal{J}_i$ *and* $\mathcal{C}_i^{(*)} = \mathcal{C}^{\perp_*} \cap \mathcal{J}_i$ *for all* $0 \le i \le s-1$. *Then* $\mathcal{C}$ *is* $*$*-self-orthogonal if and only if for each* i *(*$0 \le i \le s-1$*), the following hold:*

i *If* $i = 0$ *or* $i = i^{\#}$ *(provided* n *is even), then*

a $\mathcal{C}_i = \{0\}$ *or*

b $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis* $\{\rho_{i,0}(X)^k\}$, *where*
for q even: $0 \le k \le q$.
for q odd: k does not exist.

ii *If* $i \notin \{0, i^{\#}\}$, $\mu(i) = i$ *and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,0}$, *then*

a $\mathcal{C}_i = \{0\}$ *or*

b $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis as follows:*
for q even: $\{e_{i,0}(X)\}$ *or* $\{e_{i,1}(X)\}$ *or* $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \le k \le q^{d_i} - 2$ *satisfies* $k \equiv 0 \ (\text{mod}\ q^{d_i/2} + 1)$.
for q odd: $\{e_{i,0}(X)\}$ *or* $\{e_{i,1}(X)\}$ *or* $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, *where* $0 \le k \le q^{d_i} - 2$ *satisfies* $k \equiv \frac{q^{d_i/2}+1}{2} \ (\text{mod}\ q^{d_i/2} + 1)$.

iii *If* $i \notin \{0, i^{\#}\}$, $\mu(i) = i$ *and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,1}$, *then*

a $\mathcal{C}_i = \{0\}$ *or*

b $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis* $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$ *with* $0 \leq k \leq q^{d_i} - 2$ *satisfying*
for q even: $k \equiv 0$ *(mod* $q^{d_i/2} - 1)$.
for q odd: $k \equiv \frac{q^{d_i/2}-1}{2}$ *(mod* $q^{d_i/2} - 1)$.

iv *When* $\mu(i) \neq i$, d_i *is even and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),0}$, *we have the following:*

a *If* $\mathcal{C}_i = \{0\}$, *then* $\mathcal{C}_{\mu(i)} \subseteq \mathcal{J}_{\mu(i)}$.

b *If* $\mathcal{C}_i = \mathcal{J}_i$, *then* $\mathcal{C}_{\mu(i)} = \{0\}$.

c *If* $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis* $\{a(X)\}$, *then either* $\mathcal{C}_{\mu(i)} = \{0\}$ *or* $\mathcal{C}_{\mu(i)}$ *is a one-dimensional* $\mathcal{K}_{\mu(i)}$*-subspace of* $\mathcal{J}_{\mu(i)}$ *having basis* $\{b(X)\}$, *where* $b(X) = e_{\mu(i),0}(X)$ *when* $a(X) = e_{i,0}(X)$;
$b(X) = e_{\mu(i),1}(X)$ *when* $a(X) = e_{i,1}(X)$;
$b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \leq k, k' \leq q^{d_i} - 2$ *satisfying*
for q even: $k' = k$.
for q odd: $k' \equiv k + \frac{q^{d_i}-1}{2}$ *(mod* $q^{d_i} - 1)$.

v *When* $\mu(i) \neq i$, d_i *is even and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),1}$, *we have the following:*

a *If* $\mathcal{C}_i = \{0\}$, *then* $\mathcal{C}_{\mu(i)} \subseteq \mathcal{J}_{\mu(i)}$.

b *If* $\mathcal{C}_i = \mathcal{J}_i$, *then* $\mathcal{C}_{\mu(i)} = \{0\}$.

c *If* $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis* $\{a(X)\}$, *then either* $\mathcal{C}_{\mu(i)} = \{0\}$ *or* $\mathcal{C}_{\mu(i)}$ *is a one-dimensional* $\mathcal{K}_{\mu(i)}$*-subspace of* $\mathcal{J}_{\mu(i)}$ *having basis* $\{b(X)\}$, *where*
$b(X) = e_{\mu(i),1}(X)$ *when* $a(X) = e_{i,0}(X)$;
$b(X) = e_{\mu(i),0}(X)$ *when* $a(X) = e_{i,1}(X)$;
$b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \leq k, k' \leq q^{d_i} - 2$ *satisfying*
for q even: $k' \equiv q^{d_i} - 1 - k$ *(mod* $q^{d_i} - 1)$.
for q odd: $k' \equiv \frac{q^{d_i}-1}{2} - k$ *(mod* $q^{d_i} - 1)$.

vi *When* $\mu(i) \neq i$ *and* d_i *is odd, we have the following:*

a *If* $\mathcal{C}_i = \{0\}$, *then* $\mathcal{C}_{\mu(i)} \subseteq \mathcal{J}_{\mu(i)}$.

b *If* $\mathcal{C}_i = \mathcal{J}_i$, *then* $\mathcal{C}_{\mu(i)} = \{0\}$.

c *If* $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis* $\{\rho_{i,0}(X)^k\}$ *with* $0 \leq k \leq q^{d_i}$, *then either* $\mathcal{C}_{\mu(i)} = \{0\}$ *or* $\mathcal{C}_{\mu(i)}$ *is a one-dimensional* $\mathcal{K}_{\mu(i)}$*-subspace of* $\mathcal{J}_{\mu(i)}$ *having basis* $\{\rho_{\mu(i),0}(X)^{k'}\}$ *with* $0 \leq k' \leq q^{d_i}$ *satisfying*
for q even: $k' = k$.
for q odd: $k' \equiv k + \frac{q^{d_i}+1}{2}$ *(mod* $q^{d_i} + 1)$.

Proof: By Lemma 4.2(ii), we see that $\mathcal{C}$ is $*$-self-orthogonal if and only if $\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}$ for all $0 \leq i \leq s-1$. So for each i $(0 \leq i \leq s-1)$, we need to determine all $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying

$$\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}, \tag{4}$$

where $\dim_{\mathcal{K}_i}\mathcal{C}_i \leq 2$ and $\dim_{\mathcal{K}_i}\mathcal{C}_i^{(*)} \leq 2$ for each i. It is clear that $\mathcal{C}_i = \{0\}$ satisfies (4).

First suppose that i is an integer satisfying $0 \leq i \leq s-1$ and $\mu(i) = i$. Here we observe that when $\mathcal{C}_i = \mathcal{J}_i$, we have $\mathcal{C}_i^{(*)} = \{0\}$ and so (4) is not satisfied. Further, by Theorem 4.1, we have $\dim_{\mathcal{K}_i}\mathcal{C}_i^{(*)} = 2 - \dim_{\mathcal{K}_i}\mathcal{C}_i$. From this, we see that when $\dim_{\mathcal{K}_i}\mathcal{C}_i = 1$, we have $\dim_{\mathcal{K}_i}\mathcal{C}_i^{(*)} = 1$ and so $\mathcal{C}_i$ satisfies (4) if and only if $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ holds.

Next suppose that i is an integer satisfying $0 \leq i \leq s-1$ and $\mu(i) \neq i$. Here we have $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)}^{(*)} = 2 - \dim_{\mathcal{K}_i}\mathcal{C}_i$. Here we need to determine the pairs $(\mathcal{C}_i, \mathcal{C}_{\mu(i)})$ with $\mathcal{C}_i$ as a $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ and $\mathcal{C}_{\mu(i)}$ as a $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$ satisfying

$$\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)} \text{ and } \mathcal{C}_{\mu(i)} \subseteq \mathcal{C}_{\mu(i)}^{(*)}. \tag{5}$$

In this case, when $\mathcal{C}_i = \{0\}$, we have $\mathcal{C}_{\mu(i)}^{(*)} = \mathcal{J}_{\mu(i)}$ and so (5) holds if and only if $\mathcal{C}_{\mu(i)}$ is any $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$. When $\mathcal{C}_i = \mathcal{J}_i$, we have $\mathcal{C}_{\mu(i)}^{(*)} = \{0\}$. In this case, (5) holds if and only if $\mathcal{C}_{\mu(i)} = \{0\}$. When $\dim_{\mathcal{K}_i}\mathcal{C}_i = 1$, we have $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)}^{(*)} = 1$. Here (5) holds if and only if either $\mathcal{C}_{\mu(i)} = \{0\}$ or $\mathcal{C}_{\mu(i)}$ is a one-dimensional $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$ satisfying $\mathcal{C}_{\mu(i)} = \mathcal{C}_{\mu(i)}^{(*)}$. Now it remains to determine all one-dimensional $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ for $0 \leq i \leq s-1$, which can be determined working in a similar manner as in Theorem 4.2. □

In the following theorem, we enumerate all the $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n. For this, we recall that $\mathfrak{F}$ is the set consisting of all the fixed points of μ excluding 0 and $i^{\#}$ (if n is even) and $\mathfrak{M}$ is the set containing exactly one element from each of the transpositions in μ.

Theorem 4.5: *Let $t = 2$, q be a power of the prime p and n be a positive integer coprime to q.*

i *The number of distinct $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n is given by $\mathfrak{A}\prod_{i\in\mathfrak{F}}(q^{d_i/2}+2)\prod_{h\in\mathfrak{M}}(3q^{d_h}+6)$, where $\mathfrak{A} = q+2$ if q is even and $\mathfrak{A} = 1$ if q is odd.*

ii *The number of distinct $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n generated by a single codeword is given by $\mathbb{A}\prod_{i\in\mathfrak{F}}(q^{d_i/2}+2)\prod_{h\in\mathfrak{M}}(3q^{d_h}+4)$, where $\mathbb{A} = q+2$ if q is even and $\mathbb{A} = 1$ if q is odd.*

Proof: i For $i \in \mathfrak{F} \cup \{0, i^{\#}\}$, let M_i be the number of distinct $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}$. For $h \in \mathfrak{M}$, let M_h be the number of distinct pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$

with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h \subseteq \mathcal{C}_h^{(*)}$ and $\mathcal{C}_{\mu(h)} \subseteq \mathcal{C}_{\mu(h)}^{(*)}$. Then in view of Lemma 4.2(ii), we see that the number M of distinct $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n is given by

$$M = \prod_{i=0}^{s-1} M_i = \begin{cases} M_0 \prod\limits_{i \in \mathfrak{F}} M_i \prod\limits_{h \in \mathfrak{M}} M_h & \text{if } n \text{ is odd;} \\ M_0 M_{i^\#} \prod\limits_{i \in \mathfrak{F}} M_i \prod\limits_{h \in \mathfrak{M}} M_h & \text{if } n \text{ is even.} \end{cases}$$

Now using Theorem 4.4, the result follows.

ii By Lemma 6 of Huffman (2010), we see that every cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-code can be generated by a single codeword provided $\dim_{\mathcal{K}_i} \mathcal{C}_i \leq 1$ with equality holding for at least one i, which implies that $\mathcal{C}_i \neq \mathcal{J}_i$ for $0 \leq i \leq s-1$. Now working as in part (i) and applying Theorem 4.4, part (ii) follows. □

4.3 Determination of $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes

In the following theorem, we determine bases of all the $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n when q is an even prime power and establish the non-existence of such codes when q is an odd prime power, provided $\gcd(n, q) = 1$.

Theorem 4.6: *Let $t = 2$, q be a power of the prime p and n be a positive integer coprime to q. Let $\mathcal{C}$ be a cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-code of length n. Let $\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{s-1}$ and $\mathcal{C}^{\perp_*} = \mathcal{C}_0^{(*)} \oplus \mathcal{C}_1^{(*)} \oplus \cdots \oplus \mathcal{C}_{s-1}^{(*)}$, where $\mathcal{C}_i = \mathcal{C} \cap \mathcal{J}_i$ and $\mathcal{C}_i^{(*)} = \mathcal{C}^{\perp_*} \cap \mathcal{J}_i$ for all $0 \leq i \leq s-1$.*
When q is an odd prime power, there does not exist any $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-code of length n.
When q is an even prime power, the code $\mathcal{C}$ is $*$-self-dual if and only if for each i $(0 \leq i \leq s-1)$, the following hold:

i *If $i = 0$, then $\mathcal{C}_i$ is a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ having basis $\{\rho_{i,0}(X)^k\}$, where $0 \leq k \leq q$.*

ii *If $1 \leq i \leq s-1$ is such that $\mu(i) = i$ and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,0}$, then $\mathcal{C}_i$ is a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ having basis $\{e_{i,0}(X)\}$ or $\{e_{i,1}(X)\}$ or $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, where $0 \leq k \leq q^{d_i} - 2$ satisfies $k \equiv 0$ (mod $q^{d_i/2} + 1$).*

iii *If $1 \leq i \leq s-1$ is such that $\mu(i) = i$ and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{i,1}$, then $\mathcal{C}_i$ is a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ having basis $\{e_{i,0}(X) + \rho_{i,1}(X)^k\}$, where $0 \leq k \leq q^{d_i} - 2$ satisfies $k \equiv 0$ (mod $q^{d_i/2} - 1$).*

iv *When $\mu(i) \neq i$, d_i is even and $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),0}$, we have the following:*

a *If $\mathcal{C}_i = \{0\}$, then $\mathcal{C}_{\mu(i)} = \mathcal{J}_{\mu(i)}$.*

b *If $\mathcal{C}_i = \mathcal{J}_i$, then $\mathcal{C}_{\mu(i)} = \{0\}$.*

c *If $\mathcal{C}_i$ is a one-dimensional $\mathcal{K}_i$-subspace of $\mathcal{J}_i$ having basis $\{a(X)\}$, then $\mathcal{C}_{\mu(i)}$ is also a one-dimensional $\mathcal{K}_{\mu(i)}$-subspace of $\mathcal{J}_{\mu(i)}$ with basis $\{b(X)\}$, where*
$b(X) = e_{\mu(i),0}(X)$ when $a(X) = e_{i,0}(X)$;
$b(X) = e_{\mu(i),1}(X)$ when $a(X) = e_{i,1}(X)$; and

$b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^k$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \le k \le q^{d_i} - 2$.

v *When* $\mu(i) \neq i$, d_i *is even and* $\tau_{1,-1}(\mathcal{I}_{i,0}) = \mathcal{I}_{\mu(i),1}$, *we have the following:*

a *If* $\mathcal{C}_i = \{0\}$, *then* $\mathcal{C}_{\mu(i)} = \mathcal{J}_{\mu(i)}$.

b *If* $\mathcal{C}_i = \mathcal{J}_i$, *then* $\mathcal{C}_{\mu(i)} = \{0\}$.

c *If* $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis* $\{a(X)\}$, *then* $\mathcal{C}_{\mu(i)}$ *is also a one-dimensional* $\mathcal{K}_{\mu(i)}$*-subspace of* $\mathcal{J}_{\mu(i)}$ *with basis* $\{b(X)\}$, *where*
$b(X) = e_{\mu(i),1}(X)$ *when* $a(X) = e_{i,0}(X)$;
$b(X) = e_{\mu(i),0}(X)$ *when* $a(X) = e_{i,1}(X)$;
$b(X) = e_{\mu(i),0}(X) + \rho_{\mu(i),1}(X)^{k'}$ *when* $a(X) = e_{i,0}(X) + \rho_{i,1}(X)^k$ *with* $0 \le k, k' \le q^{d_i} - 2$ *satisfying* $k' \equiv q^{d_i} - 1 - k \ (mod\ q^{d_i} - 1)$.

vi *When* $\mu(i) \neq i$ *and* d_i *is odd, we have the following:*

a *If* $\mathcal{C}_i = \{0\}$, *then* $\mathcal{C}_{\mu(i)} = \mathcal{J}_{\mu(i)}$.

b *If* $\mathcal{C}_i = \mathcal{J}_i$, *then* $\mathcal{C}_{\mu(i)} = \{0\}$.

c *If* $\mathcal{C}_i$ *is a one-dimensional* $\mathcal{K}_i$*-subspace of* $\mathcal{J}_i$ *having basis* $\{\rho_{i,0}(X)^k\}$ *with* $0 \le k \le q^{d_i}$, *then* $\mathcal{C}_{\mu(i)}$ *is also a one-dimensional* $\mathcal{K}_{\mu(i)}$*-subspace of* $\mathcal{J}_{\mu(i)}$ *with basis* $\{\rho_{\mu(i),0}(X)^k\}$.

Proof: In view of Lemma 4.2(iii), we see that the code $\mathcal{C}$ is $*$-self-dual if and only if $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ for $0 \le i \le s-1$. Further, by Theorem 4.1, we have $\dim_{\mathcal{K}_i}\mathcal{C}_i + \dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)}^{(*)} = 2$ for all $0 \le i \le s-1$. From this, we see that $\dim_{\mathcal{K}_i}\mathcal{C}_i = 1$ for all i satisfying $\mu(i) = i$, while both the dimensions $\dim_{\mathcal{K}_i}\mathcal{C}_i$ and $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)}$ are at most 2 when $\mu(i) \neq i$.

Now by Theorem 4.2(i), we see that when q is odd, there does not exist any one-dimensional $\mathcal{K}_i$-subspace $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ for $i = 0$ or $i = i^{\#}$ (if n is even). From this, it follows that when q is an odd prime power, there does not exist any $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-code.

Next let q be an even prime power. Here we must have $\dim_{\mathcal{K}_i}\mathcal{C}_i = 1$ for all i satisfying $\mu(i) = i$ and both $\dim_{\mathcal{K}_i}\mathcal{C}_i$ and $\dim_{\mathcal{K}_{\mu(i)}}\mathcal{C}_{\mu(i)}$ are at most 2 when $\mu(i) \neq i$. Now working in a similar way as in Theorem 4.2, the result follows immediately. □

In the following theorem, we will count all the $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n provided $\gcd(n, q) = 1$.

Theorem 4.7: *Let* $t = 2$, q *be a power of the prime* p *and* n *be a positive integer coprime to* q.

i *When* q *is odd, there does not exist any* $*$*-self-dual cyclic* $\mathbb{F}_q$*-linear* $\mathbb{F}_{q^2}$*-code of length* n. *When* q *is even, there are precisely* $(q+1)\prod\limits_{i\in\mathfrak{F}}(q^{d_i/2}+1)\prod\limits_{h\in\mathfrak{M}}(q^{d_h}+3)$ *distinct* $*$*-self-dual cyclic* $\mathbb{F}_q$*-linear* $\mathbb{F}_{q^2}$*-codes of length* n.

ii *When* q *is odd, there does not exist any* $*$*-self-dual cyclic* $\mathbb{F}_q$*-linear* $\mathbb{F}_{q^2}$*-code of length* n *generated by a single codeword. When* q *is even, the number of distinct*

$*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n generated by a single codeword is given by $(q+1)\prod\limits_{i\in\mathfrak{F}}(q^{d_i/2}+1)\prod\limits_{h\in\mathfrak{M}}(q^{d_h}+1)$.

Proof: i For $i \in \mathfrak{F}\cup\{0, i^{\#}\}$, let $\hat{M}_i$ be the number of distinct $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$. For $h \in \mathfrak{M}$, let $\hat{M}_h$ be the number of distinct pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$ with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h = \mathcal{C}_h^{(*)}$ and $\mathcal{C}_{\mu(h)} = \mathcal{C}_{\mu(h)}^{(*)}$. Then in view of Lemma 4.2(iii), we see that the number $\hat{M}$ of distinct $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes of length n is given by

$$\hat{M} = \prod_{i=0}^{s-1}\hat{M}_i = \begin{cases} \hat{M}_0 \prod\limits_{i\in\mathfrak{F}}\hat{M}_i \prod\limits_{h\in\mathfrak{M}}\hat{M}_h & \text{if } n \text{ is odd;} \\ \hat{M}_0\hat{M}_{i^{\#}} \prod\limits_{i\in\mathfrak{F}}\hat{M}_i \prod\limits_{h\in\mathfrak{M}}\hat{M}_h & \text{if } n \text{ is even.} \end{cases}$$

Now using Theorem 4.6, the result follows.

ii By Lemma 6 of Huffman (2010), we see that every cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-code can be generated by a single codeword provided $\dim_{\mathcal{K}_i}\mathcal{C}_i \leq 1$ with equality holding for at least one i, which implies that $\mathcal{C}_i \neq \mathcal{J}_i$ for $0 \leq i \leq s-1$. Now using Theorem 4.6, the desired result follows.

□

4.4 Enumeration of $*$-self-orthogonal and $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes

In this section, we assume that $t \geq 3$ is an integer satisfying $t \not\equiv 1(\text{mod } p)$. Here we will enumerate all the $*$-self-orthogonal and $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n, where $\gcd(n, q) = 1$.

First of all, we proceed to enumerate all the $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n. For this, let $\mathcal{C}$ be a cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code of length n. Let us write $\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{s-1}$ and $\mathcal{C}^{\perp_*} = \mathcal{C}_0^{(*)} \oplus \mathcal{C}_1^{(*)} \oplus \cdots \oplus \mathcal{C}_{s-1}^{(*)}$, where $\mathcal{C}_i = \mathcal{C} \cap \mathcal{J}_i$ and $\mathcal{C}_i^{(*)} = \mathcal{C}^{\perp_*} \cap \mathcal{J}_i$ for all $0 \leq i \leq s-1$. Then by Lemma 4.2(ii), we see that $\mathcal{C}$ is $*$-self-orthogonal if and only if $\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}$ for all $0 \leq i \leq s-1$. Further, for $i \in \mathfrak{F}\cup\{0, i^{\#}\}$, let $\hat{N}_i$ denote the number of $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}$. For $h \in \mathfrak{M}$, let $\hat{N}_h$ denote the number of distinct pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$ with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h \subseteq \mathcal{C}_h^{(*)}$ and $\mathcal{C}_{\mu(h)} \subseteq \mathcal{C}_{\mu(h)}^{(*)}$. Then by Lemma 4.2(ii), the total number $\hat{N}$ of distinct $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n is given by

$$\hat{N} = \begin{cases} \hat{N}_0\hat{N}_{i^{\#}} \prod\limits_{i\in\mathfrak{F}}\hat{N}_i \prod\limits_{h\in\mathfrak{M}}\hat{N}_h & \text{if } n \text{ is even;} \\ \hat{N}_0 \prod\limits_{i\in\mathfrak{F}}\hat{N}_i \prod\limits_{h\in\mathfrak{M}}\hat{N}_h & \text{if } n \text{ is odd.} \end{cases} \tag{6}$$

In the following theorem, we enumerate all the $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n, provided $\gcd(n, q) = 1$.

Theorem 4.8: *Let q be a power of the prime p, n be a positive integer coprime to q and $t \geq 3$ be an integer satisfying $t \not\equiv 1(mod\ p)$. Then the number $\hat{N}$ of distinct $*$-self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n is given by*

i
$$\left(\sum_{k=0}^{t/2}\begin{bmatrix} t/2 \\ k \end{bmatrix}_q \prod_{j=0}^{k-1}(q^{\frac{t-2j}{2}}+1)\right)\prod_{i\in\mathfrak{F}}\left(\sum_{r=0}^{t/2}\begin{bmatrix} t/2 \\ r \end{bmatrix}_{q^{d_i}}\prod_{\ell=0}^{r-1}\left(q^{\frac{d_i(t-2\ell-1)}{2}}+1\right)\right)$$
$$\prod_{h\in\mathfrak{M}}\left(\sum_{u=0}^{t}\begin{bmatrix} t \\ u \end{bmatrix}_{q^{d_h}}\sum_{b=0}^{t-u}\begin{bmatrix} t-u \\ b \end{bmatrix}_{q^{d_h}}\right)$$
when both q, t are even.

ii
$$A^{gcd(n,2)}\prod_{i\in\mathfrak{F}}\left(\sum_{r=0}^{(t-1)/2}\begin{bmatrix} (t-1)/2 \\ r \end{bmatrix}_{q^{d_i}}\prod_{\ell=0}^{r-1}\left(q^{\frac{d_i(t-2\ell)}{2}}+1\right)\right)$$
$$\prod_{h\in\mathfrak{M}}\left(\sum_{u=0}^{t}\begin{bmatrix} t \\ u \end{bmatrix}_{q^{d_h}}\sum_{b=0}^{t-u}\begin{bmatrix} t-u \\ b \end{bmatrix}_{q^{d_h}}\right), \textit{ where}$$
$$A=\sum_{k=0}^{(t-1)/2}\begin{bmatrix} (t-1)/2 \\ k \end{bmatrix}_q\prod_{j=0}^{k-1}\left(q^{\frac{t-2j-1}{2}}+1\right) \textit{ when both } q, t \textit{ are odd.}$$

iii
$$A^{gcd(n,2)}\prod_{i\in\mathfrak{F}}\left(\sum_{r=0}^{t/2}\begin{bmatrix} t/2 \\ r \end{bmatrix}_{q^{d_i}}\prod_{\ell=0}^{r-1}\left(q^{\frac{d_i(t-2\ell-1)}{2}}+1\right)\right)$$
$$\prod_{h\in\mathfrak{M}}\left(\sum_{u=0}^{t}\begin{bmatrix} t \\ u \end{bmatrix}_{q^{d_h}}\sum_{b=0}^{t-u}\begin{bmatrix} t-u \\ b \end{bmatrix}_{q^{d_h}}\right), \textit{ where}$$
$$A=\sum_{k=0}^{t/2}\begin{bmatrix} t/2 \\ k \end{bmatrix}_q\prod_{j=0}^{k-1}\left(q^{\frac{t-2j-2}{2}}+1\right) \textit{ when } q\equiv 3(mod\ 4) \textit{ and } t\equiv 2(mod\ 4).$$

iv
$$A^{gcd(n,2)}\prod_{i\in\mathfrak{F}}\left(\sum_{r=0}^{t/2}\begin{bmatrix} t/2 \\ r \end{bmatrix}_{q^{d_i}}\prod_{\ell=0}^{r-1}\left(q^{\frac{d_i(t-2\ell-1)}{2}}+1\right)\right)$$
$$\prod_{h\in\mathfrak{M}}\left(\sum_{u=0}^{t}\begin{bmatrix} t \\ u \end{bmatrix}_{q^{d_h}}\sum_{b=0}^{t-u}\begin{bmatrix} t-u \\ b \end{bmatrix}_{q^{d_h}}\right), \textit{ where}$$
$$A=\sum_{k=0}^{(t-2)/2}\begin{bmatrix} (t-2)/2 \\ k \end{bmatrix}_q\prod_{j=0}^{k-1}\left(q^{\frac{t-2j}{2}}+1\right) \textit{ when } q\equiv 3(mod\ 4) \textit{ and } t\equiv 0(mod\ 4)$$
or $q \equiv 1(mod\ 4)$ and t is even.

In order to prove this theorem, let $[\cdot,\cdot]_* \upharpoonright_{\mathcal{J}_i\times\mathcal{J}_i}$ denote the restriction of the sesquilinear form $[\cdot,\cdot]_*$ to $\mathcal{J}_i\times\mathcal{J}_i$ for $0\leq i\leq s-1$. By Lemma 3.3(v), it is clear that the sesquilinear form $[\cdot,\cdot]_* \upharpoonright_{\mathcal{J}_i\times\mathcal{J}_i}$ is reflexive for each i. Further, we observe the following:

Lemma 4.3: *Let $0\leq i\leq s-1$ be an integer. Then the sesquilinear form $[\cdot,\cdot]_* \upharpoonright_{\mathcal{J}_i\times\mathcal{J}_i}$ is non-degenerate if and only if $\mu(i)=i$ if and only if $i\in\mathfrak{F}\cup\{0\}$ or $i\in\mathfrak{F}\cup\{0,i^{\#}\}$*

accordingly as n is odd or even. Furthermore, for all i $(0 \leq i \leq s-1)$ satisfying $\mu(i) = i$, the sesquilinear form $[\cdot,\cdot]_* \restriction_{\mathcal{J}_i \times \mathcal{J}_i}$ is Hermitian if $i \in \mathfrak{F}$ and is symmetric otherwise.

Proof: Working in a similar manner as in Lemma 13 of Huffman (2010) and using Lemma 3.3(v), the result follows. □

In the following lemma, we will determine the numbers $\hat{N}_i$ for all i satisfying $0 \leq i \leq s-1$ and $\mu(i) = i$.

Lemma 4.4: *Let $t \geq 3$ be an integer satisfying $t \not\equiv 1(mod\ p)$ and i $(0 \leq i \leq s-1)$ be an integer satisfying $\mu(i) = i$. Then the following hold:*

i *For $i \in \mathfrak{F}$, we have*
$$\hat{N}_i = \begin{cases} \displaystyle\sum_{k=0}^{t/2} \begin{bmatrix} t/2 \\ k \end{bmatrix}_{q^{d_i}} \prod_{\ell=0}^{k-1} \big(q^{\frac{d_i(t-2\ell-1)}{2}} + 1\big) & \text{if } t \text{ is even;} \\ \displaystyle\sum_{k=0}^{(t-1)/2} \begin{bmatrix} (t-1)/2 \\ k \end{bmatrix}_{q^{d_i}} \prod_{\ell=0}^{k-1} \big(q^{\frac{d_i(t-2\ell)}{2}} + 1\big) & \text{if } t \text{ is odd.} \end{cases}$$

ii *For $i = 0$ or $i = i^{\#}$ (provided n is even), we have*

$$\hat{N}_i = \begin{cases} \displaystyle\sum_{k=0}^{(t-1)/2} \begin{bmatrix} (t-1)/2 \\ k \end{bmatrix}_q \prod_{j=0}^{k-1} \big(q^{\frac{t-2j-1}{2}} + 1\big) & \text{if } q \text{ is odd and } t \text{ is odd;} \\ \displaystyle\sum_{k=0}^{t/2} \begin{bmatrix} t/2 \\ k \end{bmatrix}_q \prod_{j=0}^{k-1} \big(q^{\frac{t-2j-2}{2}} + 1\big) & \text{if } q \equiv 3(mod\ 4) \text{ and } t \equiv 2(mod\ 4); \\ \displaystyle\sum_{k=0}^{(t-2)/2} \begin{bmatrix} (t-2)/2 \\ k \end{bmatrix}_q \prod_{j=0}^{k-1} \big(q^{\frac{t-2j}{2}} + 1\big) & \text{if } q \equiv 3(mod\ 4) \text{ and } t \equiv 0(mod\ 4) \\ & \text{or } q \equiv 1(mod\ 4) \text{ and } t \text{ is even;} \\ \displaystyle\sum_{k=0}^{t/2} \begin{bmatrix} t/2 \\ k \end{bmatrix}_q \prod_{j=0}^{k-1} \big(q^{\frac{t-2j}{2}} + 1\big) & \text{if } q \text{ is even and } t \text{ is even.} \end{cases}$$

Proof: For $0 \leq i \leq s-1$ and $\mu(i) = i$, we recall that the number $\hat{N}_i$ equals the number of distinct $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}$.

i When $i \in \mathfrak{F}$, by Lemma 4.3, we see that $[\cdot,\cdot]_* \restriction_{\mathcal{J}_i \times \mathcal{J}_i}$ is a non-degenerate, reflexive and Hermitian sesquilinear form. Therefore $(\mathcal{J}_i, [\cdot,\cdot]_* \restriction_{\mathcal{J}_i \times \mathcal{J}_i})$ is a unitary space having dimension t over $\mathcal{K}_i \simeq \mathbb{F}_{q^{d_i}}$. By Taylor (1992, p.116), the Witt index m of $\mathcal{J}_i$ is given by

$$m = \begin{cases} \frac{t}{2} & \text{if } t \text{ is even;} \\ \frac{t-1}{2} & \text{if } t \text{ is odd.} \end{cases}$$

In this case, from Lemma 10(i) of Huffman (2010), we note that d_i is an even integer. Now by Exercise 11.3 of Taylor (1992, p.174), for $0 \leq k \leq m$, the number of distinct

k-dimensional $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}$ (or equivalently the number of distinct k-dimensional totally isotropic $\mathcal{K}_i$-subspaces of $\mathcal{J}_i$) is given by $\begin{bmatrix} m \\ k \end{bmatrix}_{q^{d_i}} \prod\limits_{j=0}^{k-1} \left(q^{d_i(m-\epsilon-j)}+1\right)$, where $\epsilon = 1/2$ if t is even and $\epsilon = -1/2$ if t is odd. From this, part (i) follows.

ii Let $i = 0$ or $i \in \{0, i^{\#}\}$ accordingly as n is odd or even. By Lemma 4.3, we see that $[\cdot,\cdot]_* \restriction_{\mathcal{J}_i \times \mathcal{J}_i}$ is a non-degenerate, reflexive and symmetric sesquilinear form. Here we will consider the following two cases separately: I. q is odd and II. q is even.

Case I. Let q be odd. In this case, $d_i = 1$ and so $\mathcal{K}_i \simeq \mathbb{F}_q$. Here it is easy to see that the map $Q_i : \mathcal{J}_i \to \mathcal{K}_i$, defined as $Q_i\big(u(X)\big) = \frac{1}{2}\left[u(X), u(X)\right]_*$ for all $u(X) \in \mathcal{J}_i$, is a quadratic map on $\mathcal{J}_i$. That is, $(\mathcal{J}_i, Q_i)$ is a non-degenerate quadratic space having dimension t over $\mathcal{K}_i$. Further, working in a similar manner as in the discussion of Theorem 16 of Huffman (2010), the Witt index m of the quadratic space $(\mathcal{J}_i, Q_i)$ is given by

$$m = \begin{cases} \frac{t-1}{2} \text{ if } t \text{ is odd;} \\ \frac{t-2}{2} \text{ if } t \text{ is even and } q \equiv 1 \pmod 4 \text{ or } t \equiv 0 \pmod 4 \text{ and } q \equiv 3 \pmod 4; \\ \frac{t}{2} \text{ if } t \equiv 2 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

Further, using Exercise 11.3 of Taylor (1992, p.174), we see that for $0 \leq k \leq m$, the number of distinct k-dimensional $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i \subseteq \mathcal{C}_i^{(*)}$ (or equivalently, the number of k-dimensional totally singular $\mathcal{K}_i$-subspaces of $\mathcal{J}_i$) is given by $\begin{bmatrix} m \\ k \end{bmatrix}_q \prod\limits_{j=0}^{k-1} \left(q^{d_i(m-\epsilon-j)}+1\right)$, where m is the Witt index of $\mathcal{J}_i$ and $\epsilon = 2m - t + 1$. From this, we get the desired result.

Case II. Let q be even. In this case, n must be odd and $i = 0$. Further, as $t \not\equiv 1 (\text{mod } p)$, the integer t must be even. By Huffman (2010, p.264), we see that $\mathcal{J}_0 = \{ah(X) : a \in \mathbb{F}_{q^t}\} \simeq \mathbb{F}_{q^t}$ and $\mathcal{K}_0 = \{\alpha h(X) : \alpha \in \mathbb{F}_q\} \simeq \mathbb{F}_q$, where $h(X) = (1 + X + X^2 + \cdots + X^{n-1})$. We next observe that $[ah(X), bh(X)]_* = \text{Tr}_{q,t}\big(a\phi(b)\big)h(X)$ for all $ah(X), bh(X) \in \mathcal{J}_0$. Since $h(X) \neq 0$, we observe that if the vectors $ah(X), bh(X) \in \mathcal{J}_0$ are orthogonal with respect to $[\cdot,\cdot]_* \restriction_{\mathcal{J}_0 \times \mathcal{J}_0}$, then the corresponding vectors $a, b \in \mathbb{F}_{q^t}$ are orthogonal with respect to $(\cdot,\cdot)_*$ on $\mathbb{F}_{q^t}$ and vice versa. So the number of distinct $\mathcal{K}_0$-subspaces $\mathcal{C}_0$ of $\mathcal{J}_0$ satisfying $\mathcal{C}_0 \subseteq \mathcal{C}_0^{(*)}$ is equal to the total number of totally isotropic $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^t}$ with respect to $(\cdot,\cdot)_*$. Further, by Lemma 3.2, we see that $(\cdot,\cdot)_*$ is a non-degenerate, reflexive and alternating bilinear form on $\mathbb{F}_{q^t}$, i.e., $(\mathbb{F}_{q^t}, (\cdot,\cdot)_*)$ is a symplectic space having dimension t over $\mathbb{F}_q$ and the Witt index of $\mathbb{F}_{q^t}$ is $\frac{t}{2}$. Now by using Exercise 11.3 of Taylor (1992, p.174), for $0 \leq k \leq \frac{t}{2}$, the number of distinct k-dimensional totally isotropic $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^t}$ is given by $\begin{bmatrix} t/2 \\ k \end{bmatrix}_q \prod\limits_{j=0}^{k-1} \left(q^{\frac{t-2j}{2}}+1\right)$, from which the desired result follows immediately. □

In the following lemma, we consider the case $h \in \mathfrak{M}$ and count the pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$ with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h \subseteq \mathcal{C}_h^{(*)}$ and $\mathcal{C}_{\mu(h)} \subseteq \mathcal{C}_{\mu(h)}^{(*)}$.

Lemma 4.5: *For $h \in \mathfrak{M}$, the number $\hat{N}_h$ of distinct pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$ with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h \subseteq \mathcal{C}_h^{(*)}$ and $\mathcal{C}_{\mu(h)} \subseteq \mathcal{C}_{\mu(h)}^{(*)}$ is given by $\hat{N}_h = \sum_{k=0}^{t} \begin{bmatrix} t \\ k \end{bmatrix}_{q^{d_h}} \sum_{j=0}^{t-k} \begin{bmatrix} t-k \\ j \end{bmatrix}_{q^{d_h}}$.*

Proof: Its proof is similar to that of Lemma 12 of Huffman (2010). □

Proof of Theorem 4.8: It follows immediately from Lemmas 4.4 and 4.5, and using (6). □

Next we proceed to count all the $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n. For all i satisfying $0 \leq i \leq s-1$ and $\mu(i) = i$, let $\widetilde{N}_i$ denote the number of $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$. For $h \in \mathfrak{M}$, let $\widetilde{N}_h$ denote the number of pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$ with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h = \mathcal{C}_h^{(*)}$ and $\mathcal{C}_{\mu(h)} = \mathcal{C}_{\mu(h)}^{(*)}$. Then by Lemma 4.2(iii), the total number of $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n is given by

$$\widetilde{N} = \begin{cases} \widetilde{N}_0 \widetilde{N}_{i\#} \prod\limits_{i \in \mathfrak{F}} \widetilde{N}_i \prod\limits_{h \in \mathfrak{M}} \widetilde{N}_h & \text{if } n \text{ is even;} \\ \widetilde{N}_0 \prod\limits_{i \in \mathfrak{F}} \widetilde{N}_i \prod\limits_{h \in \mathfrak{M}} \widetilde{N}_h & \text{if } n \text{ is odd.} \end{cases} \tag{7}$$

In the following theorem, we enumerate all the $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n, provided $\gcd(n, q) = 1$.

Theorem 4.9: *Let q be a power of the prime p, n be a positive integer coprime to q and $t \geq 3$ be an integer satisfying $t \not\equiv 1(mod\ p)$.*

i *When t is odd or $q \equiv 3(mod\ 4)$ and $t \equiv 0(mod\ 4)$ or $q \equiv 1(mod\ 4)$ and t is even, there does not exist any $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-code of length n.*

ii *When $q \equiv 3(mod\ 4)$ and $t \equiv 2(mod\ 4)$, the number $\widetilde{N}$ of distinct $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n is given by*

$$\widetilde{N} = a^{gcd(n,2)} \prod_{i \in \mathfrak{F}} \left(\prod_{j=0}^{(t-2)/2} \left(q^{\frac{d_i(t-2j-1)}{2}} + 1 \right) \right) \prod_{h \in \mathfrak{M}} \left(\sum_{k=0}^{t} \begin{bmatrix} t \\ k \end{bmatrix}_{q^{d_h}} \right),$$

$$\textit{where } a = \prod_{\ell=0}^{(t-2)/2} \left(q^{\frac{t-2\ell-2}{2}} + 1 \right).$$

iii *When both t and q are even, the number $\widetilde{N}$ of distinct $*$-self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length n is given by*

$$\widetilde{N} = \prod_{j=0}^{(t-2)/2} \left(q^{\frac{t-2j}{2}} + 1 \right) \prod_{i \in \mathfrak{F}} \left(\prod_{j=0}^{(t-2)/2} \left(q^{\frac{d_i(t-2j-1)}{2}} + 1 \right) \right) \prod_{h \in \mathfrak{M}} \left(\sum_{k=0}^{t} \begin{bmatrix} t \\ k \end{bmatrix}_{q^{d_h}} \right).$$

In order to prove this theorem, we need to prove the following two lemmas:

Lemma 4.6: *Let q be a power of the prime p, n be a positive integer coprime to q and $t \geq 3$ be an integer satisfying $t \not\equiv 1(mod\, p)$. Let i be an integer satisfying $0 \leq i \leq s-1$ and $\mu(i) = i$.*

i *If $i \in \mathfrak{F}$, then we have*

$$\widetilde{N}_i = \begin{cases} \prod\limits_{\ell=0}^{(t-2)/2} \left(q^{\frac{d_i(t-2\ell-1)}{2}} + 1\right) & \textit{if } t \textit{ is even}; \\ 0 & \textit{if } t \textit{ is odd.} \end{cases}$$

ii *If $i = 0$ or $i = i^{\#}$ (provided n is even), then we have*

$$\widetilde{N}_i = \begin{cases} \prod\limits_{j=0}^{(t-2)/2} \left(q^{\frac{t-2j-2}{2}} + 1\right) & \textit{if } q \equiv 3(mod\, 4) \textit{ and } t \equiv 2(mod\, 4); \\ 0 & \textit{if } q \equiv 3(mod\, 4) \textit{ and } t \equiv 0(mod\, 4) \textit{ or } q \equiv 1(mod\, 4) \\ & \textit{and } t \textit{ is even or } t \textit{ is odd}; \\ \prod\limits_{j=0}^{(t-2)/2} \left(q^{\frac{t-2j}{2}} + 1\right) & \textit{if both } q \textit{ and } t \textit{ are even.} \end{cases}$$

Proof: For all i satisfying $0 \leq i \leq s-1$ and $\mu(i) = i$, the number $\widetilde{N}_i$ equals the number of $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$. Further, by Theorem 4.1, we see that if the $\mathcal{K}_i$-dimension of $\mathcal{C}_i$ is k_i, then the $\mathcal{K}_i$-dimension of $\mathcal{C}_i^{(*)} = \mathcal{C}_{\mu(i)}^{(*)}$ is $t - k_i$, as $\mu(i) = i$. This implies that $k_i = t - k_i$ for all i satisfying $\mu(i) = i$. From this, it follows that there does not exist any $\mathcal{K}_i$-subspace $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ when t is odd and the dimension of the $\mathcal{K}_i$-subspace $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$ must be $\frac{t}{2}$ when t is even. Therefore $\widetilde{N}_i = 0$ when t is odd. So from now onwards, we assume that t is an even integer. In this case, if there exists a $\mathcal{K}_i$-subspace $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$, then $\dim_{\mathcal{K}_i} \mathcal{C}_i = \frac{t}{2}$.

i First let $i \in \mathfrak{F}$. Here by Lemma 4.3, we see that $[\cdot,\cdot]_* \restriction_{\mathcal{J}_i \times \mathcal{J}_i}$ is a non-degenerate, reflexive and Hermitian sesquilinear form. Therefore $\left(\mathcal{J}_i, [\cdot,\cdot]_* \restriction_{\mathcal{J}_i \times \mathcal{J}_i}\right)$ is a unitary space having dimension t over $\mathcal{K}_i \simeq \mathbb{F}_{q^{d_i}}$. So it suffices to count all the $\frac{t}{2}$-dimensional $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$, which equals the number of distinct totally isotropic $\frac{t}{2}$-dimensional $\mathcal{K}_i$-subspaces of $\mathcal{J}_i$. By Taylor (1992, p.116), as t is even, the Witt index m of $\mathcal{J}_i$ is $\frac{t}{2}$. By Lemma 10(i) of Huffman (2010), we also note that d_i is an even integer. Now using Exercise 11.3 of Taylor (1992, p.174), we see that the number of distinct $\frac{t}{2}$-dimensional totally isotropic $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ is given by $\begin{bmatrix} t/2 \\ t/2 \end{bmatrix}_{q^{d_i}} \prod\limits_{j=0}^{(t-2)/2} \left(q^{\frac{d_i(t-2j-1)}{2}} + 1\right)$.

ii Next let $i = 0$ or $i \in \{0, i^{\#}\}$ accordingly as n is odd or even. Here we will consider the following two cases separately: I. q is odd and II. q is even.

Case I. Let q be odd. In this case, we have $d_i = 1$, which implies that $\mathcal{K}_i \simeq \mathbb{F}_q$. It is easy to see that the map $Q_i : \mathcal{J}_i \to \mathcal{K}_i$, defined as $Q_i\big(u(X)\big) = \frac{1}{2}\left[u(X), u(X)\right]_*$ for all $u(X) \in \mathcal{J}_i$, is a quadratic map on $\mathcal{J}_i$. That is, $(\mathcal{J}_i, Q_i)$ is a non-degenerate quadratic space having dimension t over $\mathcal{K}_i$. So it suffices to count all the $\frac{t}{2}$-dimensional $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ satisfying $\mathcal{C}_i = \mathcal{C}_i^{(*)}$, that is, we need to enumerate all the totally singular $\frac{t}{2}$-dimensional $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$. Now working in a similar manner as in the discussion of Theorem 16 of Huffman (2010), we see that the Witt index m of $(\mathcal{J}_i, Q_i)$ is given by

$$m = \begin{cases} \frac{t-2}{2} & \text{if } t \text{ is even and } q \equiv 1 \pmod 4 \text{ or } t \equiv 0 \pmod 4 \text{ and } q \equiv 3 \pmod 4; \\ \frac{t}{2} & \text{if } t \equiv 2 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

Now as the Witt index m is equal to the dimension of a maximal totally singular $\mathcal{K}_i$-subspace of $\mathcal{J}_i$, we must have $\widetilde{N}_i = 0$ when t is even and $q \equiv 1 \pmod 4$ or $t \equiv 0 \pmod 4$ and $q \equiv 3 \pmod 4$. On the other other hand, when $t \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$, using Exercise 11.3 of Taylor (1992, p.174), we see that the number of $\frac{t}{2}$-dimensional totally singular $\mathcal{K}_i$-subspaces $\mathcal{C}_i$ of $\mathcal{J}_i$ is given by

$$\begin{bmatrix} t/2 \\ t/2 \end{bmatrix}_q \prod_{j=0}^{(t-2)/2} \left(q^{\frac{t-2j-2}{2}} + 1\right), \text{ which equals } \prod_{j=0}^{(t-2)/2} \left(q^{\frac{t-2j-2}{2}} + 1\right).$$

Case II. Next let q be even. In this case, n must be odd and $i = 0$. Here also, working as in Lemma 4.4(ii), we see that the total number of totally isotropic $\frac{t}{2}$-dimensional $\mathcal{K}_0$-subspaces $\mathcal{J}_0$ is same as the number of distinct totally isotropic $\frac{t}{2}$-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^t}$ with respect to $(\cdot,\cdot)_*$. Further, by Lemma 3.2, we see that $(\cdot,\cdot)_*$ is a non-degenerate, reflexive and alternating bilinear form on $\mathbb{F}_{q^t}$, i.e., $(\mathbb{F}_{q^t}, (\cdot,\cdot)_*)$ is a symplectic space having dimension t over $\mathbb{F}_q$ and the Witt index of $\mathbb{F}_{q^t}$ is $\frac{t}{2}$. Now using Exercise 11.3 of Taylor (1992, p.174), we see that the number of distinct totally isotropic $\frac{t}{2}$-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^t}$ is given by

$$\begin{bmatrix} t/2 \\ t/2 \end{bmatrix}_q \prod_{j=0}^{(t-2)/2} \left(q^{\frac{t-2j}{2}} + 1\right) = \prod_{j=0}^{(t-2)/2} \left(q^{\frac{t-2j}{2}} + 1\right).$$ □

Lemma 4.7: *Let q be a power of the prime p, n be a positive integer coprime to q and $t \geq 3$ be an integer satisfying $t \not\equiv 1 (mod\ p)$. For $h \in \mathfrak{M}$, we have* $\widetilde{N}_h = \sum_{k=0}^{t} \begin{bmatrix} t \\ k \end{bmatrix}_{q^{d_h}}$.

Proof: For each $h \in \mathfrak{M}$, the number $\widetilde{N}_h$ equals the number of distinct pairs $(\mathcal{C}_h, \mathcal{C}_{\mu(h)})$ with $\mathcal{C}_h$ as a $\mathcal{K}_h$-subspace of $\mathcal{J}_h$ and $\mathcal{C}_{\mu(h)}$ as a $\mathcal{K}_{\mu(h)}$-subspace of $\mathcal{J}_{\mu(h)}$ satisfying $\mathcal{C}_h = \mathcal{C}_h^{(*)}$ and $\mathcal{C}_{\mu(h)} = \mathcal{C}_{\mu(h)}^{(*)}$. Now for a given $\mathcal{K}_h$-subspace $\mathcal{C}_h$ of $\mathcal{J}_h$, by Theorem 4.1, we have $\mathcal{C}_{\mu(h)}^{(*)} = \{a(X) \in \mathcal{J}_{\mu(h)} : [a(X), c(X)]_* = 0 \text{ for all } c(X) \in \mathcal{C}_h\}$ and thus $\mathcal{C}_{\mu(h)} = \mathcal{C}_{\mu(h)}^{(*)}$ can be uniquely determined for a given choice of $\mathcal{C}_h$. In view of this, we observe that the number $\widetilde{N}_h$ equals the number of $\mathcal{K}_h$-subspaces of $\mathcal{J}_h$. Now as $\dim_{\mathcal{K}_h} \mathcal{J}_h = t$ and $\mathcal{K}_h$ is the finite field of order q^{d_h}, using Lemma 4 of Huffman (2010), we see that the number of k-dimensional $\mathcal{K}_h$-subspaces of $\mathcal{J}_h$ is given by $\begin{bmatrix} t \\ k \end{bmatrix}_{q^{d_h}}$ for each k $(0 \leq k \leq t)$. From this, we obtain $\widetilde{N}_h = \sum_{k=0}^{t} \begin{bmatrix} t \\ k \end{bmatrix}_{q^{d_h}}$. □

Proof of Theorem 4.9: It follows immediately from Lemmas 4.6 and 4.7, and using (7). □

Acknowledgements

Research support by DST India, under the grant SERB/F/3551/2012-13, is gratefully acknowledged. Research support by NBHM, India, is gratefully acknowledged.

References

Ashikhmin, A. and Knill, E. (2001) 'Nonbinary quantum stabilizer codes', *IEEE Transactions on Information Theory*, Vol. 47, No. 7, pp.3065–3072.

Bierbrauer, J. and Edel, Y. (2000) 'Quantum twisted codes', *Journal of Combinatorial Designs*, Vol. 8, No. 3, pp.174–188.

Bierbrauer, J. (2007) 'Cyclic additive and quantum stabilizer codes', *Lecture Notes in Computer Science,* Vol. 4547, pp.276–283.

Bierbrauer, J. (2012) 'Cyclic additive codes', *Journal of Algebra*, Vol. 372, pp.661–672.

Calderbank, A.R., Rains, E.M., Shor, P.M. and Sloane, N.J.A. (1998) 'Quantum error correction via codes over GF(4)', *IEEE Transactions on Information Theory*, Vol. 44, No. 4, pp.1369–1387.

Cao, Y. and Gao, Y. (2015) 'Repeated root cyclic $\mathbb{F}_q$-linear codes over $\mathbb{F}_{q^\ell}$', *Finite Fields and its Application*, Vol. 31, pp.202–227.

Dey, B.K. and Rajan, B.S. (2005) '$\mathbb{F}_q$-linear cyclic codes over $\mathbb{F}_{q^m}$: DFT approch', *Designs, Codes and Cryptography*, Vol. 34, No. 1, pp.89–116.

Ezerman, M.F., Jitman, S., Ling, S. and Pasechnik, D.V. (2013) 'CSS-like constructions of asymmetric quantum codes', *IEEE Transactions on Information Theory*, Vol. 59, No. 10, pp.6732–6754.

Hoffmann, K. and Kunze, R. (1971) *Linear Algebra*, 2nd ed., Prentice-Hall, New Jersey.

Huffman, W.C. (2007) 'Additive self-dual codes over $\mathbb{F}_4$ with an automorphism of odd prime order', *Advances in Mathematics of Communications*, Vol. 1, No. 3, pp.357–398.

Huffman, W.C. (2007a) 'Additive cyclic codes over $\mathbb{F}_4$', *Advances in Mathematics of Communications*, Vol. 1, No. 4, pp.429–461.

Huffman, W.C. (2008) 'Additive cyclic codes over $\mathbb{F}_4$ of even length', *Advances in Mathematics of Communications*, Vol. 2, No. 3, pp.309–343.

Huffman, W.C. (2010) 'Cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes', *International Journal of Information and Coding Theory*, Vol. 1, No. 3, pp.249–284.

Lidl, R. and Niederreiter, H. (1994) *Introduction to Finite Fields and their Applications*, Cambridge University Press, Cambridge.

Massey, J.L. (1992) 'Linear codes with complementary duals', *Discrete Mathematics*, Vol. 106–107, pp.337–342.

Rains, E.M. (1999) 'Nonbinary quantum codes', *IEEE Transactions on Information Theory*, Vol. 45, No. 6, pp.1827–1832.

Taylor, D.E. (1992) *The Geometry of the Classical Groups*, Heldermann Verlag, Germany.

Yang, X. and Massey, J.L. (1994) 'The condition for a cyclic code to have a complementary dual', *Discrete Mathematics*, Vol. 126, pp.391–393.