HAL open science

Additive complementary dual codes over F 4

Minjia Shi, Na Liu, Jon-Lark Kim, Patrick Solé

▶ **To cite this version:**

Minjia Shi, Na Liu, Jon-Lark Kim, Patrick Solé. Additive complementary dual codes over F 4. Finite Fields and Their Applications, In press. hal-03789248

HAL Id: hal-03789248

https://hal.science/hal-03789248v1

Submitted on 27 Sep 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Additive complementary dual codes over $\mathbb{F}_4$

Minjia Shi · Na Liu · Jon-Lark Kim · Patrick Solé

Abstract A linear code is linear complementary dual (LCD) if it meets its dual trivially. LCD codes have been a hot topic recently due to Boolean masking application in the security of embarked electronics (Carlet and Guilley, 2014). Additive codes over $\mathbb{F}_4$ are $\mathbb{F}_4$-codes that are stable by codeword addition but not necessarily by scalar multiplication. An additive code over $\mathbb{F}_4$ is additive complementary dual (ACD) if it meets its dual trivially. The aim of this research is to study such codes which meet their dual trivially. All the techniques and problems used to study LCD codes are potentially relevant to ACD codes. Interesting constructions of ACD codes from binary codes are given with respect to the trace Hermitian and trace Euclidean inner product. The former product is relevant to quantum codes.

Keywords Additive code, finite field, LCD code

Mathematics Subject Classification: Primary 94 B05, Secondary 16 L 30.

This research is supported by National Natural Science Foundation of China (12071001), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20).

M. Shi
Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China.
E-mail: smjwcl.good@163.com

Na Liu
School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China.
E-mail: naliu1177@163.com

Jon-Lark Kim
Department of Mathematics, Sogang University, Seoul, South Korea
E-mail: jlkim@sogang.ac.kr

P. Solé
Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France
E-mail: sole@enst.fr

1 Introduction

To begin with, let us recall some basic definitions. A *linear* $[n, k]$ *code* over a finite field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The set of vectors orthogonal to $\mathcal{C}$ under the usual inner product is the *dual* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$. A linear code $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^\perp$, and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. On the other hand, a linear code $\mathcal{C}$ is an *LCD code* (linear complementary dual code) if $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. In particular, $\mathcal{C}$ is a *binary LCD code* if $\mathcal{C}$ is a binary linear code satisfying $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$.

Massey [14] introduced the notion of LCD codes in order to provide an optimum linear coding solution for the two-user binary adder channel. In a later work [15], he also showed that there exist asymptotically good LCD codes. Furthermore, Sendrier showed that LCD codes meet the asymptotic Gilbert-Varshamov bound in [17].

In 2014, Carlet and Guilley [3] introduced several constructions of LCD codes and investigated an application of LCD codes against Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA). Recall from [3] that SCA consists in passively recording some leakage that is the source of information to retrieve the key, and that FIA consist in actively perturbating the device so as to obtain exploitable differences at the output.

In the approach of [3], the direct sum $\mathcal{C} \oplus \mathcal{C}^\perp = \mathbb{F}_q^n$ is essential, and the minimum distance of $\mathcal{C}$ (resp. $\mathcal{C}^\perp$) acts as a performance criterion for SCA (resp. FIA). Since this model does not use the linearity of $\mathcal{C}$ but only its additivity, it makes sense to study additive complementary dual (ACD) codes over finite fields or finite rings. Moreover, since linear codes are additive codes, LCD codes are ACD. Furthermore, Guilley [8] reported to us that the application of ACD codes to security still makes sense. This motivates the current study.

In the same spirit, Shi et al. [18] studied ACD codes over a noncommutative non-unital ring E with four elements recently. Nevertheless, little is known about a general theory of ACD codes over $\mathbb{F}_4$. All the techniques and problems used to study LCD codes [6] are potentially relevant to ACD codes. Interesting constructions of ACD codes from binary codes are given with respect to two trace inner products: the trace Euclidean inner product, and the trace Hermition inner product, familiar since the studies of quantum codes [2]. We have also constructed ACD $(6, 2^5, 4)$, $(35, 2^7, 26)$, and $(96, 2^7, 72)$ codes over $\mathbb{F}_4$ under the trace Euclidean inner product, all of which have more codewords than optimal LCD $[6, 2, 4]$, $[35, 3, 26]$, and $[96, 3, 72]$ codes over $\mathbb{F}_4$, respectively.

Our paper consists of five sections. Section 2 recalls basic definitions and notations from additive codes under the two inner products. Section 3 discusses ACD codes with respect to the trace Hermitian inner product. Section 4 discusses ACD codes with with respect to the trace Euclidean inner product. Section 5 concludes the article.

2 Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ denote the finite field of order 2 and 4 respectively, where $\bar{\omega} = \omega^2 = \omega + 1$, $\omega^3 = 1$.

An *additive code* $\mathcal{C}$ *over* $\mathbb{F}_4$ *of length* n is an additive subgroup of $\mathbb{F}_4^n$. As $\mathcal{C}$ is a free $\mathbb{F}_2$-module, it has size 2^k for some $0 \leq k \leq 2n$. We call $\mathcal{C}$ an $(n, 2^k)$ code. It

has a basis, as a $\mathbb{F}_2$-module, consisting of k basis vectors. Interest in additive codes over $\mathbb{F}_4$ has arisen because of their correspondence to quantum codes as described in [2]. There is a natural inner product on the additive codes arising from the trace map. The *trace* map $\mathrm{Tr} : \mathbb{F}_4 \to \mathbb{F}_2$ is given by

$$\mathrm{Tr}(x) = x + x^2.$$

In particular $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$ and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\overline{\omega}) = 1$. The *conjugate* of $x \in \mathbb{F}_4$, denoted $\overline{x}$, is the image of x under the Frobenius automorphism; in other words, $\overline{0} = 0$, $\overline{1} = 1$, and $\overline{\overline{\omega}} = \omega$.

Definition 1 A *generator matrix of an $(n, 2^k)$ additive code $\mathcal{C}$ over $\mathbb{F}_4$* is a $k \times n$ matrix G with entries in $\mathbb{F}_4$ such that $\mathcal{C} = \{\mathbf{u}G : \ \mathbf{u} \in \mathbb{F}_2^k\}$. Note that G has 2-rank k.

As usual, the *weight* $\mathrm{wt}(\mathbf{c})$ of $\mathbf{c} \in \mathcal{C}$ is the number of nonzero components of $\mathbf{c}$. The minimum weight d of $\mathcal{C}$ is the smallest weight of any nonzero codeword in $\mathcal{C}$. If $\mathcal{C}$ is an $(n, 2^k)$ additive code of minimum weight d, $\mathcal{C}$ is called an $(n, 2^k, d)$ code.

Example 1 Let $\mathcal{G}_6$ be the $[6, 3, 4]$ *hexacode* whose generator matrix as a linear $\mathbb{F}_4$-code is

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

This is also an additive code; thinking of $\mathcal{G}_6$ as an additive code, it has generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \\ \omega & 0 & 0 & \omega & \overline{\omega} & \overline{\omega} \\ 0 & \omega & 0 & \overline{\omega} & \omega & \overline{\omega} \\ 0 & 0 & \omega & \overline{\omega} & \overline{\omega} & \omega \end{bmatrix}.$$

For $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_4^n$, we define the Hermitian inner product, the trace Hermitian inner product and the trace Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$ as follows:

$$(i)\ \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i \overline{y}_i, \ (ii)\ \mathbf{x} \star \mathbf{y} = \sum_{i=1}^{n} \mathrm{Tr}(x_i \overline{y}_i), \ (iii)\ \mathbf{x} \diamond \mathbf{y} = \sum_{i=1}^{n} \mathrm{Tr}(x_i y_i).$$

If $\mathcal{C}$ is an $(n, 2^k)$ additive code, the dual of $\mathcal{C}$ with respect to the Hermitian inner product, the trace Hermitian inner product and the trace Euclidean inner product are defined as follows:

$$\mathcal{C}^{\perp_{\mathrm{H}}} = \{u \in \mathbb{F}_4^n : u \cdot v = 0 \ for \ all \ v \in \mathcal{C}\},$$

$$\mathcal{C}^{\perp_{\mathrm{TrH}}} = \{u \in \mathbb{F}_4^n : u \star v = 0 \ for \ all \ v \in \mathcal{C}\},$$

$$\mathcal{C}^{\perp_{\mathrm{TrE}}} = \{u \in \mathbb{F}_4^n : u \diamond v = 0 \ for \ all \ v \in \mathcal{C}\}.$$

Obviously, $\mathcal{C}^{\perp_{\mathrm{H}}}$, $\mathcal{C}^{\perp_{\mathrm{TrH}}}$ and $\mathcal{C}^{\perp_{\mathrm{TrE}}}$ are $(n, 2^{2n-k})$ additive codes. If, in addition, $\mathcal{C}$ is linear, we say $\mathcal{C}$ is *linear complementary dual with respect to the Hermitian inner product (or quaternary Hermitian LCD)* if $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{H}}} = \{\mathbf{0}\}$. If $\mathcal{C}$ is additive, we say $\mathcal{C}$ is *additive complementary dual (ACD) with respect to the trace Hermitian inner product* if $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{TrH}}} = \{\mathbf{0}\}$, and $\mathcal{C}$ is *additive complementary dual (ACD) with respect to the trace Euclidean inner product* if $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{TrE}}} = \{\mathbf{0}\}$.

3 ACD codes with respect to the trace Hermitian inner product ⋆

We have a criteria for ACD codes in terms of a generator matrix as follows.

Theorem 1 ([4, Proposition 1], [15, Proposition 1]) *Let G be a generator matrix for an $[n,k]$ linear code $\mathcal{C}$ over a field. Then $\mathcal{C}$ is a Euclidean (resp. a Hermitian) LCD code if and only if, the $k \times k$ matrix GG^T (resp. $G\bar{G}^T$) is invertible.*

Theorem 2 ([1]) *Let $\mathcal{C}$ be an additive $(n, 2^k)$ code over $\mathbb{F}_4$ with generator matrix G. Then $\mathcal{C}$ is ACD with respect to the trace Hermitian inner product if and only if $G \star G = G\bar{G}^T + \bar{G}G^T$ is invertible.*

The following lemma is straightforward from the definition of the inner products.

Lemma 1 ([5, Lemma 2.1]) *Assume $\mathcal{C}$ is a linear code over $\mathbb{F}_4$. Then $\mathcal{C}^{\perp_{\mathrm{TrH}}}$ is equal to the dual of $\mathcal{C}$ with respect to the Hermitian inner product. Similarly, $\mathcal{C}^{\perp_{\mathrm{TrE}}}$ is equal to the dual of $\mathcal{C}$ with respect to the Euclidean inner product.*

Corollary 1 *Any Hermitian LCD $[n,k,d]$ code $\mathcal{C}$ over $\mathbb{F}_4$ is an ACD $(n, 2^{2k}, d)$ code over $\mathbb{F}_4$ with respect to the trace Hermitian inner product.*

Proof Suppose that $\mathcal{C}$ is a Hermitian LCD code over $\mathbb{F}_4$. Then $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{H}}} = \{\mathbf{0}\}$. By Lemma 1, $\mathcal{C}^{\perp_{\mathrm{H}}} = \mathcal{C}^{\perp_{\mathrm{TrH}}}$. Thus, $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{TrH}}} = \{\mathbf{0}\}$, which means that $\mathcal{C}$ is ACD with respect to the trace Hermitian inner product. The parameters of $\mathcal{C}$ over $\mathbb{F}_4$ are obvious.

Corollary 2 *Suppose $\mathcal{C}_2$ is a binary LCD $[n,k,d]$ code with generator matrix G_2. Let $\mathcal{C}_2^4$ be a linear code over $\mathbb{F}_4$ with generator matrix G_2. Then by regarding $\mathcal{C}_2^4$ as an additive code over $\mathbb{F}_4$, $\mathcal{C}_2^4$ is an ACD $(n, 2^{2k}, d)$ code with respect to the trace Hermitian inner product.*

Proof Let G_2 be a generator matrix for $\mathcal{C}_2$. Then, by Theorem 1, $G_2G_2^T$ is invertible over $\mathbb{F}_2$. Since $G_2 = \bar{G}_2$, $G_2\bar{G}_2{}^T$ is invertible over $\mathbb{F}_4$. Hence, by Theorem 1, $\mathcal{C}_2^4$ as a linear code over $\mathbb{F}_4$ is an Hermitian LCD $[n,k,d]$ code over $\mathbb{F}_4$. Therefore, by Corollary 1, $\mathcal{C}_2^4$ is an ACD $(n, 2^{2k}, d)$ code with respect to the trace Hermitian inner product.

Lemma 2 ([10]) *If A is a symmetric integral matrix with zero diagonal, then 2-rank(A) is even.*

Proof We give a detailed proof here since the proof in [10] is concise. Recall that a principal submatrix of a square matrix A is the matrix obtained by deleting any m rows and the corresponding m columns.

Let A' be a non-singular principal submatrix of A such that 2-rank(A) = 2-rank(A'). Then A' is also symmetric integral with zero diagonal. We may assume that $A' \equiv B \pmod 2$ for some skew symmetric integral matrix B. Over $\mathbb{Z}$, any skew symmetric matrix B of odd order has determinant 0 (since $B = -B^T$ implies that $\det(B) = -\det(B^T) = -\det(B)$, hence $\det(B) = 0$). So, if 2-rank (A') is odd, then $\det(A') \equiv \det(B) \equiv 0 \pmod 2$. This is a contradiction since A' has a full rank, that is, $\det(A') \not\equiv 0 \pmod 2$. Thus 2-rank (A') is even. Therefore, 2-rank (A) is even.

Theorem 3 *If $\mathcal{C}$ is a trace Hermitian ACD $(n, 2^k)$ code over $\mathbb{F}_4$ with generator matrix G, then k is even.*

Proof Let $A = G \star G = G\bar{G}^T + \bar{G}G^T$. Then A is a $k \times k$ symmetric integral matrix with zero diagonal. Since $\mathcal{C}$ is ACD, the 2-rank of A must be k by Theorem 2. By Lemma 2, k is even.

Lemma 3 *Let $\mathcal{C}$ and $\mathcal{D}$ are two binary $[n, k_1]$ and $[n, k_2]$ linear codes. If $\mathcal{C}_4 = a\mathcal{C} + b\mathcal{D}$, where $a \neq b$ and $a, b \in \mathbb{F}_4 \setminus \{0\}$, then $\mathcal{C}_4^{\perp_{\mathrm{TrH}}} = a\mathcal{D}^\perp + b\mathcal{C}^\perp$.*

Proof Let $\mathbf{u} \in a\mathcal{D}^\perp + b\mathcal{C}^\perp$; then there exist $\mathbf{d}' \in \mathcal{D}^\perp$ and $\mathbf{c}' \in \mathcal{C}^\perp$ such that $\mathbf{u} = a\mathbf{d}' + b\mathbf{c}'$. For $\mathbf{v} = a\mathbf{c} + b\mathbf{d} \in \mathcal{C}_4$, where $\mathbf{c} \in \mathcal{C}$ and $\mathbf{d} \in \mathcal{D}$, we have

$$\begin{aligned}
\mathbf{u} \star \mathbf{v} &= (a\mathbf{d}' + b\mathbf{c}') \star (a\mathbf{c} + b\mathbf{d}) \\
&= (a\mathbf{d}' + b\mathbf{c}') \cdot (\bar{a}\mathbf{c} + \bar{b}\mathbf{d}) + (\bar{a}\mathbf{d}' + \bar{b}\mathbf{c}') \cdot (a\mathbf{c} + b\mathbf{d}) \\
&= a\bar{a}\mathbf{d}' \cdot \mathbf{c} + a\bar{b}\mathbf{d}' \cdot \mathbf{d} + b\bar{a}\mathbf{c}' \cdot \mathbf{c} + b\bar{b}\mathbf{c}' \cdot \mathbf{d} + \bar{a}a\mathbf{d}' \cdot \mathbf{c} + \bar{a}b\mathbf{d}' \cdot \mathbf{d} + \bar{b}a\mathbf{c}' \cdot \mathbf{c} + \bar{b}b\mathbf{c}' \cdot \mathbf{d} \\
&= (a\bar{b} + \bar{a}b)\mathbf{d}' \cdot \mathbf{d} + (b\bar{a} + \bar{b}a)\mathbf{c}' \cdot \mathbf{c} \\
&= 0.
\end{aligned}$$

Hence, $a\mathcal{D}^\perp + b\mathcal{C}^\perp \subseteq \mathcal{C}_4^{\perp_{\mathrm{TrH}}}$.

Since $a \neq b$, $|\mathcal{C}_4| = |\mathcal{C}||\mathcal{D}| = 2^{k_1} \cdot 2^{k_2} = 2^{k_1+k_2}$, then $\mathcal{C}_4^{\perp_{\mathrm{TrH}}} = \frac{2^{2n}}{|\mathcal{C}_4|} = 2^{2n-(k_1+k_2)} = 2^{2n-k_1-k_2}$. And $|a\mathcal{D}^\perp + b\mathcal{C}^\perp| = 2^{n-k_1} \cdot 2^{n-k_2} = 2^{2n-k_1-k_2}$. Therefore, $\mathcal{C}_4^{\perp_{\mathrm{TrH}}} = a\mathcal{D}^\perp + b\mathcal{C}^\perp$.

Proposition 1 *If $\mathcal{C}$ is a self-dual $[2n, n]$ binary code, let $\mathcal{D}$ be a binary linear code and $\mathbb{F}_2^{2n} = \mathcal{C} \oplus \mathcal{D}$, then $\mathcal{C}_4 = a\mathcal{C} + b\mathcal{D}$ is an ACD $(2n, 2^{2n})$ code over $\mathbb{F}_4$ with respect to the trace Hermitian inner product, where $a \neq b$ and $a, b \in \mathbb{F}_4 \setminus \{0\}$.*

Proof Since $\mathcal{C}$ is self-dual, $\mathcal{C} = \mathcal{C}^\perp$. By $\mathbb{F}_2^{2n} = \mathcal{C} \oplus \mathcal{D}$, we know that

$$\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\},\ \mathcal{C}^\perp \cap \mathcal{D}^\perp = (\mathcal{C} \oplus \mathcal{D})^\perp = (\mathbb{F}_2^{2n})^\perp = \{\mathbf{0}\},$$

then $\mathcal{C} \cap \mathcal{D}^\perp = \{\mathbf{0}\}$. By Lemma 3, $\mathcal{C}_4^{\perp_{\mathrm{TrH}}} = a\mathcal{D}^\perp + b\mathcal{C}^\perp = a\mathcal{D}^\perp + b\mathcal{C}$.

If there exists $\mathbf{0} \neq \mathbf{v} \in \mathcal{C}_4 \cap \mathcal{C}_4^{\perp_{\mathrm{TrH}}}$, then there are $\mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{D}$, and $\mathbf{c}, \mathbf{d}$ are nonzero such that $\mathbf{v} = a\mathbf{c} + b\mathbf{d}$. Similarly, there are $\mathbf{c}' \in \mathcal{D}^\perp$, $\mathbf{d}' \in \mathcal{C}$, and $\mathbf{c}', \mathbf{d}'$are nonzero such that $\mathbf{v} = a\mathbf{c}' + b\mathbf{d}'$. Hence we have $a\mathbf{c} + b\mathbf{d} = a\mathbf{c}' + b\mathbf{d}'$, which implies that $\mathbf{c} = \mathbf{c}', \mathbf{d} = \mathbf{d}'$. Then we have $\mathbf{c} \in \mathcal{C} \cap \mathcal{D}^\perp$, $\mathbf{d} \in \mathcal{D} \cap \mathcal{C}$, where $\mathbf{c}, \mathbf{d}$ are nonzero, which is a contradiction. Therefore, $\mathcal{C}_4$ is an ACD code.

Corollary 3 *Suppose that $\mathcal{C}$ is a self-dual $[2n, n]$ binary code and $\mathcal{D}$ is a binary linear code such that $\mathbb{F}_2^{2n} = \mathcal{C} \oplus \mathcal{D}$. Let $\mathcal{C}_4 = a\mathcal{C} + b\mathcal{D}$. Then its minimum distance $d(\mathcal{C}_4)$ is equal to $\min\{d(\mathcal{C}), d(\mathcal{D})\}$.*

Proof Obviously, we have $d(\mathcal{C}_4) \leq \min\{d(\mathcal{C}), d(\mathcal{D})\}$. On the other hand, for any nonzero codeword $a\mathbf{u} + b\mathbf{v} \in \mathcal{C}_4$ with $\mathbf{u} \in \mathcal{C}$ and $\mathbf{v} \in \mathcal{D}$, since $a, b \in \mathbb{F}_4 \setminus \{0\}$ and $a \neq b$, $\mathrm{wt}(a\mathbf{u} + b\mathbf{v}) \geq \max\{\mathrm{wt}(a\mathbf{u}), \mathrm{wt}(b\mathbf{v})\} \geq \min\{d(\mathcal{C}), d(\mathcal{D})\}$. Therefore, $d(\mathcal{C}_4) = \min\{d(\mathcal{C}), d(\mathcal{D})\}$.

Remark 1 Proposition 1 shows that we can get ACD codes over $\mathbb{F}_4$ from binary linear self-dual codes.

Example 2 Let $\mathcal{C}$ be a binary $[4,2,2]$ code with generator matrix G_1 of the form

$$G_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Let $\mathcal{D}$ be a binary $[4,2,2]$ code with generator matrix G_2 of the form

$$G_2 = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

It is easy to check that $\mathcal{C}$ is self-dual and $\mathbb{F}_2^4 = \mathcal{C} \oplus \mathcal{D}$. By Proposition 1, $\mathcal{C}_4 = \mathcal{C} + \omega\mathcal{D}$ is an $(4, 2^4, 2)$ ACD code over $\mathbb{F}_4$ with generator matrix G of the form

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ \omega & \omega & 0 & \omega \\ 0 & \omega & \omega & \omega \end{bmatrix}.$$

4 ACD codes with respect to the trace Euclidean inner product ⋄

In this section, we construct ACD codes with respect to the trace Euclidean inner product.

Lemma 4 *Any Euclidean LCD $[n,k,d]$ code $\mathcal{C}$ over $\mathbb{F}_4$ is an ACD $(n, 2^{2k}, d)$ code over $\mathbb{F}_4$ with respect to the trace Euclidean inner product.*

Proof Suppose that $\mathcal{C}$ is an Euclidean LCD code over $\mathbb{F}_4$. Then $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{E}}} = \{\mathbf{0}\}$, where $\mathcal{C}^{\perp_{\mathrm{E}}}$ denotes the dual of $\mathcal{C}$ under the Euclidean inner product. By Lemma 1, $\mathcal{C}^{\perp_{\mathrm{E}}} = \mathcal{C}^{\perp_{\mathrm{TrE}}}$. Thus, $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{TrE}}} = \{\mathbf{0}\}$, which means that $\mathcal{C}$ is ACD with respect to the trace Euclidean inner product. The parameters of $\mathcal{C}$ over $\mathbb{F}_4$ are obvious.

We want a characterization of an ACD code with respect to the Euclidean inner product in terms of its generator matrix. We follow the idea from [1].

Definition 2 ([1]) Let V be an inner product space over a field $\mathbb{F}_q$. An $\mathbb{F}_q$-linear map $T : V \to V$ is called an $\mathbb{F}_q$-orthogonal projection with respect to the prescribed inner product $< \cdot, \cdot >$ if
(i) $T^2 = T$, and
(ii) $< \mathbf{u}, \mathbf{v} >= 0$ for all $\mathbf{u} \in \mathrm{Im}(T)$ and $\mathbf{v} \in \mathrm{Ker}(T)$.

Lemma 5 *Using the notation of Definition 2, if $\langle \cdot, \cdot \rangle$ is nondegenerate, then $\mathrm{Ker}(T)$ is the dual of $\mathrm{Im}(T)$ under $\langle \cdot, \cdot \rangle$.*

Proof From basic linear algebra, $\dim_{\mathbb{F}_q}(\mathrm{Ker}(T)) = \dim_{\mathbb{F}_q}(V) - \dim_{\mathbb{F}_q}(\mathrm{Im}(T))$. Let $\mathcal{D}$ be the dual of $\mathrm{Im}(T)$ under $\langle \cdot, \cdot \rangle$. As $\langle \cdot, \cdot \rangle$ is nondegenerate, $\dim_{\mathbb{F}_q}(\mathcal{D}) = \dim_{\mathbb{F}_q}(V) - \dim_{\mathbb{F}_q}(\mathrm{Im}(T))$. Thus $\mathrm{Ker}(T)$ and $\mathcal{D}$ have the same dimension. By part (ii) of Definition 2, $\mathrm{Ker}(T) \subseteq \mathcal{D}$. As $\mathrm{Ker}(T)$ and $\mathcal{D}$ have the same dimension, they are equal.

Lemma 6 *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_4$ and let $T : \mathbb{F}_4^n \to \mathbb{F}_4^n$ be an $\mathbb{F}_4$-linear map. Then T is an $\mathbb{F}_4$-orthogonal projection with respect to the trace Euclidean inner product onto $\mathcal{C}$ if and only if*

$$T(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & if\ \boldsymbol{v} \in \mathcal{C} \\ \boldsymbol{0} & if\ \boldsymbol{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}. \end{cases}$$

Proof Suppose that $T : \mathbb{F}_4^n \to \mathbb{F}_4^n$ is an $\mathbb{F}_4-$orthogonal projection with respect to the trace Euclidean inner product onto $\mathcal{C}$. Let $\mathbf{v} \in \mathcal{C} = \mathrm{Im}(T)$. Then there exists $\mathbf{x} \in \mathbb{F}_4^n$ such that $\mathbf{v} = T(\mathbf{x})$. So $\mathbf{v} = T(\mathbf{x}) = T^2(\mathbf{x}) = T(T(\mathbf{x})) = T(\mathbf{v})$. Now let $\mathbf{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}$; then $T(\mathbf{v}) = \mathbf{0}$ by Lemma 5.

Conversely, assume that

$$T(\mathbf{v}) = \begin{cases} \mathbf{v} & if\ \mathbf{v} \in \mathcal{C} \\ \mathbf{0} & if\ \mathbf{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}. \end{cases}$$

Since T is a function, $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{TrE}}} = \{\mathbf{0}\}$ implying $\mathbb{F}_4^n = \mathcal{C} \oplus \mathcal{C}^{\perp_{\mathrm{TrE}}}$. If $\mathbf{v} \in \mathcal{C}$, $T^2(\mathbf{v}) = T(T(\mathbf{v})) = T(\mathbf{v}) = \mathbf{v}$; if $\mathbf{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}$, $T^2(\mathbf{v}) = T(T(\mathbf{v})) = T(\mathbf{0}) = \mathbf{0} = T(\mathbf{v})$. So $T^2 = T$ on $\mathcal{C}$ and on $\mathcal{C}^{\perp_{\mathrm{TrE}}}$, and hence on $\mathcal{C} \oplus \mathcal{C}^{\perp_{\mathrm{TrE}}} = \mathbb{F}_4^n$ by linearity, verifying part (i) of Definition 2. Also $\mathrm{Im}(T) = \mathcal{C}$. As in the proof of Lemma 5, $\dim_{\mathbb{F}_4}(\mathcal{C}^{\perp_{\mathrm{TrE}}}) = \dim_{\mathbb{F}_4}(\mathrm{Ker}(T))$. As $T(\mathbf{v}) = \mathbf{0}$ for $\mathbf{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}$, $\mathcal{C}^{\perp_{\mathrm{TrE}}} \subseteq \mathrm{Ker}(T)$ imply $\mathcal{C}^{\perp_{\mathrm{TrE}}} = \mathrm{Ker}(T)$, verifying part (ii) of Definition 2.

Lemma 7 *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_4$. Then $\mathcal{C}$ is ACD with respect to the trace Euclidean inner product if and only if there exists an $\mathbb{F}_4$-orthogonal projection with respect to the trace Euclidean inner product from $\mathbb{F}_4^n$ onto $\mathcal{C}$.*

Proof Let $T_{\mathcal{C}}$ is an $\mathbb{F}_4$-orthogonal projection with respect to the trace Euclidean inner product from $\mathbb{F}_4^n$ onto $\mathcal{C}$. By Lemma 6, it follows that,

$$T_{\mathcal{C}}(\mathbf{v}) = \begin{cases} \mathbf{v} & if\ \mathbf{v} \in \mathcal{C} \\ \mathbf{0} & if\ \mathbf{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}. \end{cases}$$

Assume that $\mathcal{C}$ is not ACD with respect to the trace Euclidean inner product. Then there exists $\mathbf{u} \neq \mathbf{0}$ such that $\mathbf{u} \in \mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{TrE}}}$. Hence, $\mathbf{u} = T_{\mathcal{C}}(\mathbf{u}) = \mathbf{0}$, which is a contradiction. Therefore, $\mathcal{C}$ is ACD with respect to the trace Euclidean inner product

Conversely, assume that $\mathcal{C}$ is ACD with respect to the trace Euclidean inner product. Let $\mathbf{v} \in \mathbb{F}_4^n$, then there exists a unique pair $\mathbf{u} \in \mathcal{C}$ and $\mathbf{w} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}$ such that $\mathbf{v} = \mathbf{u} + \mathbf{w}$. Defined a map $T_{\mathcal{C}} : \mathbb{F}_4^n \to \mathbb{F}_4^n$ by $T_{\mathcal{C}}(\mathbf{v}) = \mathbf{u}$. Clearly, $T_{\mathcal{C}}$ is an $\mathbb{F}_4$-linear map such that:

$$T_{\mathcal{C}}(\mathbf{v}) = \begin{cases} \mathbf{v} & if\ \mathbf{v} \in \mathcal{C} \\ \mathbf{0} & if\ \mathbf{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}. \end{cases}$$

Hence, by Lemma 6, $T_{\mathcal{C}}$ is an $\mathbb{F}_4$-orthogonal projection with respect to the trace Euclidean inner product from $\mathbb{F}_4^n$ onto $\mathcal{C}$.

Theorem 4 *Let $\mathcal{C}$ be an additive $(n, 2^k)$ code over $\mathbb{F}_4$ with generator matrix G. Then $\mathcal{C}$ is ACD with respect to the trace Euclidean inner product if and only if $G \diamond G = GG^T + \bar{G}\bar{G}^T$ is invertible. Moreover, in this case the map $T_{\mathcal{C}}(\boldsymbol{v}) = \mathrm{Tr}(\boldsymbol{v}G^T)(GG^T + \bar{G}\bar{G}^T)^{-1}G$ is an $\mathbb{F}_4$-orthogonal projection with respect to the trace Euclidean inner product from $\mathbb{F}_4^n$ onto $\mathcal{C}$, where for $\mathbf{v} \in \mathbb{F}_4^n$, $\mathrm{Tr}(\mathbf{v}G^T) = \mathbf{v}G^T + \bar{\mathbf{v}}\bar{G}^T$.*

Proof Assume $\mathrm{Tr}(GG^T) = GG^T + \bar{G}\bar{G}^T$ is not invertible. Since $\mathrm{Tr}(GG^T)$ is a $k \times k$ matrix, we have $\mathrm{rank}(\mathrm{Tr}(GG^T) < k$. Hence

$$k = \mathrm{null}(\mathrm{Tr}(GG^T)) + \mathrm{rank}(\mathrm{Tr}(GG^T)) < \mathrm{null}(\mathrm{Tr}(GG^T)) + k,$$

then $\mathrm{null}(\mathrm{Tr}(GG^T)) > k - k = 0$. So there exists $\mathbf{u} \in \mathrm{Ker}(\mathrm{Tr}(GG^T)) \setminus \{\mathbf{0}\} \subseteq \mathbb{F}_2^k$ such that $\mathbf{u}\mathrm{Tr}(GG^T) = \mathbf{0}$ and $\mathbf{u}G \in \mathcal{C} \setminus \{\mathbf{0}\}$. We have,

$$\mathbf{0} \neq \mathbf{u} \in \mathrm{Ker}(\mathrm{Tr}(GG^T)) = \mathbf{u}GG^T + \mathbf{u}\bar{G}\bar{G}^T = (\mathbf{u}G)G^T + (\bar{\mathbf{u}}\bar{G})\bar{G}^T$$

Hence, $\mathbf{u}G$ is also a vector in $\mathcal{C}^{\perp_{\mathrm{TrE}}}$; i.e., $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{TrE}}} \neq \{\mathbf{0}\}$. Therefore, $\mathcal{C}$ is not ACD with respect to the trace Euclidean inner product.

Conversely, assume that $GG^T + \bar{G}\bar{G}^T$ is invertible. Let $T_{\mathcal{C}} : \mathbb{F}_4^n \to \mathcal{C}$ be defined by

$$T_{\mathcal{C}}(\mathbf{v}) = \mathrm{Tr}(\mathbf{v}G^T)(GG^T + \bar{G}\bar{G}^T)^{-1}G.$$

Let $\mathbf{v} \in \mathbb{F}_4^n$. If $\mathbf{v} \in \mathcal{C}$, then there exists $\mathbf{u} \in \mathbb{F}_2^k$ such that $\mathbf{v} = \mathbf{u}G$; hence,

$$\begin{aligned}
T_{\mathcal{C}}(\mathbf{v}) &= \mathrm{Tr}(\mathbf{v}G^T)(GG^T + \bar{G}\bar{G}^T)^{-1}G \\
&= \mathrm{Tr}(\mathbf{u}GG^T)(GG^T + \bar{G}\bar{G}^T)^{-1}G \\
&= (\mathbf{u}GG^T + \bar{\mathbf{u}}\bar{G}\bar{G}^T)(GG^T + \bar{G}\bar{G}^T)^{-1}G \\
&= \mathbf{u}(GG^T + \bar{G}\bar{G}^T)(GG^T + \bar{G}\bar{G}^T)^{-1}G \\
&= \mathbf{u}I_kG \\
&= \mathbf{u}G \\
&= \mathbf{v},
\end{aligned}$$

Assume that $\mathbf{v} \in \mathcal{C}^{\perp_{\mathrm{TrE}}}$. Then $\mathrm{Tr}(\mathbf{v}G^T) = \mathbf{0}$, and

$$T_{\mathcal{C}}(\mathbf{v}) = \mathrm{Tr}(\mathbf{v}G^T)(GG + \bar{G}\bar{G}^T)^{-1}G = \mathbf{0}(GG^T + \bar{G}\bar{G}^T)^{-1}G = \mathbf{0}.$$

Hence by Lemma 6, $T_{\mathcal{C}}$ is an $\mathbb{F}_4$-orthogonal projection with respect to the trace Euclidean inner product from $\mathbb{F}_4^n$ onto $\mathcal{C}$. By Lemma 7, $\mathcal{C}$ is an ACD code with respect to the trace Euclidean inner product.

Corollary 4 *If $\mathcal{C}$ and $\mathcal{D}$ are two binary LCD $[n, k_1]$ and $[n, k_2]$ codes respectively, then $\mathcal{C}_4 = \omega\mathcal{C} + \omega^2\mathcal{D}$ is an ACD $(n, 2^{k_1+k_2})$ code over $\mathbb{F}_4$ with respect to the trace Euclidean inner product.*

Proof Since $\mathcal{C}$ and $\mathcal{D}$ are LCD codes, we have $\mathcal{C} \cap \mathcal{C}^{\perp} = \{\mathbf{0}\}, \mathcal{D} \cap \mathcal{D}^{\perp} = \{\mathbf{0}\}$. Furthermore, since $\{\omega, \omega^2\}$ is a trace orthogonal basis in $\mathbb{F}_4$, we have $\mathcal{C}_4^{\perp_{\mathrm{TrE}}} = \omega\mathcal{C}^{\perp} + \omega^2\mathcal{D}^{\perp}$. We need to prove that $\mathcal{C}_4 \cap \mathcal{C}_4^{\perp_{\mathrm{TrE}}} = \{\mathbf{0}\}$. If there exists $\mathbf{0} \neq \mathbf{v} \in \mathcal{C}_4 \cap \mathcal{C}_4^{\perp_{\mathrm{TrE}}}$, then there are $\mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{D}$, and $\mathbf{c}, \mathbf{d}$ are nonzero such that $\mathbf{v} = \omega\mathbf{c} + \omega^2\mathbf{d}$. Similarly, there are $\mathbf{c}' \in \mathcal{C}^{\perp}$, $\mathbf{d}' \in \mathcal{D}^{\perp}$, and $\mathbf{c}', \mathbf{d}'$ are nonzero such that $\mathbf{v} = \omega\mathbf{c}' + \omega^2\mathbf{d}'$. Hence we have $\omega\mathbf{c} + \omega^2\mathbf{d} = \omega\mathbf{c}' + \omega^2\mathbf{d}'$, which implies that $\mathbf{c} = \mathbf{c}', \mathbf{d} = \mathbf{d}'$. Then we have $\mathbf{c} \in \mathcal{C} \cap \mathcal{C}^{\perp}$, $\mathbf{d} \in \mathcal{D} \cap \mathcal{D}^{\perp}$, where $\mathbf{c}, \mathbf{d}$ are nonzero, which is a contradiction. Therefore, $\mathcal{C}_4$ is an ACD code. Clearly, the $\mathbb{F}_2$-rank of $\mathcal{C}_4$ is $k_1 + k_2$.

Corollary 5 *Let $\mathcal{C}_1$ be a binary $[2n, k]$ code with generator matrix $G_1 = [A|B]$, where A and B are $k \times n$ matrices. Let $\mathcal{C}_2$ be an additive code with generator matrix $G = \omega A + \omega^2 B$. Then $\mathcal{C}_2$ is an ACD $(n, 2^k)$ code over $\mathbb{F}_4$ with respect to the trace Euclidean inner product if and only if $\mathcal{C}_1$ is a binary $[2n, k]$ LCD code.*

Proof Suppose that $\mathcal{C}_1$ is a binary LCD code. Then, by Theorem 1, $[A|B][A|B]^T = AA^T + BB^T$ is invertible over $\mathbb{F}_2$. We also have

$$\begin{aligned} G \diamond G &= (\omega A + \omega^2 B)(\omega A^T + \omega^2 B^T) + (\overline{\omega} A + \overline{\omega^2} B)(\overline{\omega} A^T + \overline{\omega^2} B^T) \\ &= (\omega^2 + \omega) AA^T + (\omega + \omega^2) BB^T \\ &= AA^T + BB^T; \end{aligned}$$

hence $G \diamond G = [A|B][A|B]^T$ is invertible over $\mathbb{F}_4$. Therefore, by Theorem 4, $\mathcal{C}_2$ is ACD with respect to the trace Euclidean inner product. Clearly, the $\mathbb{F}_2$-rank of $\mathcal{C}_2$ is k.

Conversely, if $\mathcal{C}_2$ is ACD with respect to the trace Euclidean inner product, then we reverse the above proof to show that $\mathcal{C}_1$ is a binary LCD code.

Example 3 Let $\mathcal{C}_1$ be a binary $[12, 6, 4]$ code with the generator matrix $G_1 = [A|B]$ of the form

$$G_1 = \left[\begin{array}{cccccc|cccccc} 1&0&0&0&0&0&0&1&1&1&0&0 \\ 0&1&0&0&0&0&1&1&0&1&1&0 \\ 0&0&1&0&0&0&1&0&1&0&1&1 \\ 0&0&0&1&0&0&1&1&0&1&0&1 \\ 0&0&0&0&1&0&0&1&1&0&1&1 \\ 0&0&0&0&0&1&0&0&1&1&1&0 \end{array}\right].$$

It is easy to check that $\mathcal{C}_1$ is a binary LCD code. By Corollary 5 $\mathcal{C}_2$ is a $(6, 2^6, 4)$ ACD code with generator matrix G

$$G = \begin{bmatrix} \omega & \omega^2 & \omega^2 & \omega^2 & 0 & 0 \\ \omega^2 & 1 & 0 & \omega^2 & \omega^2 & 0 \\ \omega^2 & 0 & 1 & 0 & \omega^2 & \omega^2 \\ \omega^2 & \omega^2 & 0 & 1 & 0 & \omega^2 \\ 0 & \omega^2 & \omega^2 & 0 & 1 & \omega^2 \\ 0 & 0 & \omega^2 & \omega^2 & \omega^2 & \omega \end{bmatrix}.$$

Corollary 6 *Let $\mathcal{C}$ be an $(n, 2^k)$ additive conjucyclic code with generator matrix G over $\mathbb{F}_4$, and form the binary code*

$$\mathcal{C}' = \{ Tr(\omega \boldsymbol{u}) | Tr(\overline{\omega} \boldsymbol{u}) : \boldsymbol{u} \in \mathcal{C} \},$$

where the trace is applied componentwise and the vertical bar denotes concatenation. Then $\mathcal{C}'$ is a binary cyclic code of length $2n$ with generator matrix $G' = [\omega G + \bar{\omega}\bar{G} | \bar{\omega} G + \omega \bar{G}]$, which is LCD if and only if $\mathcal{C}$ is ACD with respect to the trace Euclidean inner product.

Proof Suppose that $\mathcal{C}$ is an ACD code with respect to the trace Euclidean inner product. Then $G \diamond G = GG^T + \bar{G}\bar{G}^T$ is invertible. And $\mathcal{C}'$ is a binary cyclic code with generator matrix G'. Hence:

$$\begin{aligned} G'G'^T &= (\omega G + \bar{\omega}\bar{G})(\omega G^T + \bar{\omega}\bar{G}^T) + (\bar{\omega}G + \omega\bar{G})(\bar{\omega}G^T + \omega\bar{G}^T) \\ &= \omega^2 GG^T + G\bar{G}^T + \bar{G}G^T + \omega\bar{G}\bar{G}^T + \omega GG^T + G\bar{G}^T + \bar{G}G^T + \omega^2\bar{G}\bar{G}^T \\ &= GG^T + \bar{G}\bar{G}^T. \end{aligned}$$

Therefore, $\mathcal{C}'$ is a binary LCD code.

Conversely, if $\mathcal{C}'$ is a binary LCD code, then we reverse the above proof to show that $\mathcal{C}$ is an ACD code with respect to the trace Euclidean inner product.

Remark 2 As a natural question, one can ask whether there is an ACD $(n, 2^{k^*}, d^*)$ code over $\mathbb{F}_4$ under the trace Euclidean inner product which satisfies $k^* > 2k$ and $d^* = d$, given an optimal linear LCD $[n, k, d]$ code over $\mathbb{F}_4$ under the Euclidean inner product. In what follows, we give several examples with the above conditions. This implies that ACD codes over $\mathbb{F}_4$ are sometimes better than LCD codes over $\mathbb{F}_4$.

Example 4 By Grassl's table [7], there is an Euclidean optimal $[6, 2, 4]$ code over $\mathbb{F}_4$. One can also find an optimal LCD $[6, 2, 4]$ code $\mathcal{K}_1$ over $\mathbb{F}_4$ with generator matrix K_1 under the Euclidean inner product.

$$K_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & \omega \\ 0 & 1 & \omega & \omega & \omega^2 & \omega \end{bmatrix},$$

By a random search, we have constructed an ACD $(6, 2^5, 4)$ code $\mathcal{K}_{2,1}$ over $\mathbb{F}_4$ with generator matrix $K_{2,1}$ under the trace Euclidean inner product as follows. Note that $\mathcal{K}_{2,1}$ has double codewords than $\mathcal{K}_1$ although both have the same length and minimum weight.

$$K_{2,1} = \begin{bmatrix} 1 & 0 & \omega & 1 & \omega^2 & \omega \\ \omega & 0 & \omega & \omega^2 & 1 & \omega^2 \\ 0 & 1 & 0 & 1 & \omega & \omega \\ 0 & \omega & \omega & \omega & \omega & \omega \\ 0 & 0 & 1 & \omega & 1 & \omega \end{bmatrix}.$$

The weight distribution of $\mathcal{K}_{2,1}$ is $A_0 = 1, A_4 = 17, A_5 = 8, A_6 = 6$ and the order of the permutation automorphism group of $\mathcal{K}_{2,1}$ is 4.

We have also found two more inequivalent ACD $(6, 2^5, 4)$ codes denoted by $\mathcal{K}_{2,2}$ and $\mathcal{K}_{2,3}$ with generator matrices $K_{2,2}$ and $K_{2,3}$, respectively. The weight distributions and the orders of the permutation automorphism groups of these codes are displayed in Table 1.

$$K_{2,2} = \begin{bmatrix} 1 & 0 & \omega & \omega^2 & \omega^2 & 0 \\ \omega & 0 & 0 & \omega & 1 & \omega^2 \\ 0 & 1 & 0 & 1 & 1 & \omega \\ 0 & \omega & 0 & \omega & \omega & 1 \\ 0 & 0 & \omega^2 & \omega^2 & 1 & 1 \end{bmatrix}, \quad K_{2,3} = \begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega^2 \\ \omega & 0 & \omega & \omega^2 & \omega^2 & \omega^2 \\ 0 & 1 & 0 & 1 & \omega^2 & 1 \\ 0 & \omega & \omega & 1 & \omega & 0 \\ 0 & 0 & \omega^2 & \omega & \omega^2 & \omega \end{bmatrix}.$$

Example 5 It is well known [4] that linear $[n, k, d]$ codes over $\mathbb{F}_4$ are equivalent to LCD $[n, k, d]$ codes under the Euclidean inner product. For $n = 35$ and 96 with $k = 3$, there are optimal linear $[35, 3, 26]$, $[96, 3, 72]$ codes over $\mathbb{F}_4$ [7], which implies that there are optimal LCD $[35, 3, 26]$, $[96, 3, 72]$ codes over $\mathbb{F}_4$. Guo el al. [9] constructed better additive $(35, 2^7, 26)$ and $(96, 2^7, 72)$ codes over $\mathbb{F}_4$ with generator matrices $G_{7,35}$ and $G_{7,96}$, respectively. However, these are not ACD codes under the trace Euclidean inner product. By multiplying some columns of $G_{7,35}$ and $G_{7,96}$ by nonzero elements of $\mathbb{F}_4$, we have constructed an ACD $(35, 2^7, 26)$ code $\mathcal{K}_3$ and an ACD $(96, 2^7, 72)$ code $\mathcal{K}_4$ over $\mathbb{F}_4$ with generator matrices K_3 and K_4, respectively under the trace Euclidean inner product. The weight distributions and the orders of the permutation automorphism groups of these codes are displayed in Table 1.

$$K_3 = \begin{bmatrix}
1&0&\omega&\omega^2&0&\omega&\omega^2&0&1&\omega^2&\omega^2&1&0&\omega&\omega^2&\omega&0&0&\omega&\omega^2&1&\omega&\omega^2&1&1&\omega^2&\omega&0&\omega^2&\omega&0&0&\omega&\omega^2&1\\
\omega&0&\omega&1&\omega^2&1&1&0&\omega&0&1&\omega^2&1&\omega^2&1&\omega^2&1&0&\omega&0&\omega&\omega^2&1&\omega^2&\omega&0&\omega&0&0&\omega&0&1&\omega^2&1&\omega^2\\
0&1&\omega&0&\omega&\omega^2&1&0&1&\omega&0&\omega^2&\omega&1&0&1&\omega&0&\omega^2&\omega&1&0&1&\omega&0&\omega^2&\omega&1&\omega^2&\omega&1&\omega^2&0&1&\omega\\
0&\omega&0&\omega&\omega&\omega&\omega^2&0&\omega&0&1&\omega^2&1&\omega^2&0&\omega&0&1&\omega^2&1&\omega^2&0&\omega&0&1&\omega^2&1&\omega^2&\omega&0&\omega&\omega^2&1&\omega^2&1\\
0&0&1&1&1&\omega^2&\omega^2&0&0&1&\omega^2&\omega&\omega&\omega^2&0&0&1&\omega^2&\omega&\omega&\omega^2&0&0&1&\omega^2&\omega&\omega&\omega^2&1&1&0&\omega&\omega^2&\omega^2&\omega\\
0&0&0&0&0&0&0&1&1&1&1&1&1&1&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&1&1&1&1&1&1&1&\omega&\omega&\omega&\omega&\omega&\omega&\omega
\end{bmatrix}.$$

$$K_4 = \begin{bmatrix} A_1 & A_2 & A_3 \end{bmatrix},$$

where

$$A_1 = \begin{bmatrix}
1&0&0&1&\omega^2&1&1&\omega&\omega&0&0&\omega^2&\omega^2&1&1&\omega&\omega&0&0&\omega^2&\omega^2&1&1&\omega&0&\omega^2&\omega^2&\omega&\omega&1&1&0\\
\omega&0&1&1&1&\omega&0&1&\omega^2&0&\omega&\omega^2&1&\omega&0&1&\omega^2&0&\omega&\omega^2&1&\omega&0&1&0&1&\omega&0&\omega^2&\omega&1&\omega^2\\
0&1&0&1&\omega&\omega^2&\omega&1&0&1&0&\omega^2&\omega&\omega^2&\omega&1&0&1&0&\omega^2&\omega&\omega^2&\omega&1&0&\omega&0&1&\omega^2&1&\omega^2&\omega\\
0&\omega&1&\omega&1&\omega^2&\omega^2&0&0&\omega&\omega&1&1&\omega^2&\omega^2&0&0&\omega&\omega&1&1&\omega^2&\omega^2&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0\\
0&0&\omega&\omega^2&1&1&\omega&\omega^2&0&0&\omega^2&\omega&1&1&\omega&\omega^2&0&0&\omega^2&\omega&1&1&\omega&\omega^2&0&0&1&\omega^2&\omega&\omega&\omega^2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&\omega&\omega&\omega&\omega&\omega&\omega&\omega\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\omega&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2
\end{bmatrix},$$

$$A_2 = \begin{bmatrix}
0&\omega^2&\omega^2&\omega&\omega&1&1&0&\omega&1&1&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0&0&\omega^2&\omega^2&\omega&1&\omega&\omega&\omega^2&\omega^2&0&0&1\\
0&1&\omega&0&\omega^2&\omega&1&\omega^2&\omega^2&\omega&1&\omega^2&0&1&\omega&0&\omega^2&\omega&1&\omega^2&0&1&\omega&0&\omega&\omega^2&0&\omega&1&0&\omega^2&1\\
0&\omega&0&1&\omega^2&1&\omega^2&\omega&0&\omega&0&1&\omega^2&1&\omega^2&\omega&0&\omega&0&1&\omega^2&1&\omega^2&\omega&0&\omega&0&1&\omega^2&1&\omega^2&\omega\\
0&\omega^2&\omega^2&\omega&\omega&1&1&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0\\
0&0&1&\omega^2&\omega&\omega&\omega^2&1&0&0&1&\omega^2&\omega&\omega&\omega^2&1&0&0&1&\omega^2&\omega&\omega&\omega^2&1&0&0&1&\omega^2&\omega&\omega&\omega^2&1\\
\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&1&1&1&1&1&1&1&1\\
\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&\omega&\omega&\omega&\omega&\omega&\omega&\omega
\end{bmatrix},$$

$$A_3 = \begin{bmatrix}
1&\omega&\omega&\omega^2&\omega^2&0&0&1&1&\omega&\omega&\omega^2&\omega^2&0&0&1&\omega^2&0&0&1&1&\omega&\omega&\omega^2&\omega^2&0&0&1&1&\omega&\omega&\omega^2\\
\omega&\omega^2&0&\omega&1&0&\omega^2&1&\omega&\omega^2&0&\omega&1&0&\omega^2&1&\omega&\omega^2&0&\omega&1&0&\omega^2&1&\omega&\omega^2&0&\omega&1&0&\omega^2&1\\
0&\omega&0&1&\omega^2&1&\omega^2&\omega&0&\omega&0&1&\omega^2&1&\omega^2&\omega&\omega&0&\omega&\omega^2&1&\omega^2&1&0&\omega&0&\omega&\omega^2&1&\omega^2&1&0\\
0&\omega^2&\omega^2&\omega&\omega&1&1&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0&0&\omega^2&\omega^2&\omega&\omega&1&1&0\\
0&0&1&\omega^2&\omega&\omega&\omega^2&1&0&0&1&\omega^2&\omega&\omega&\omega^2&1&1&1&0&\omega&\omega^2&\omega^2&\omega&0&1&1&0&\omega&\omega^2&\omega^2&\omega&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega\\
\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2&\omega^2
\end{bmatrix}.$$

Table 1: Weight distribution and permutation automorphism group order $|\mathrm{PAut}(\mathcal{C})|$ for our ACD codes $\mathcal{C}$ over $\mathbb{F}_4$

code $\mathcal{C}$	parameters	weight distribution	$\lvert\mathrm{PAut}(\mathcal{C})\rvert$
$\mathcal{K}_{2,1}$	$(6, 2^5, 4)$	$A_0 = 1, A_4 = 17, A_5 = 8, A_6 = 6$	4
$\mathcal{K}_{2,2}$	$(6, 2^5, 4)$	$A_0 = 1, A_4 = 17, A_5 = 8, A_6 = 6$	1
$\mathcal{K}_{2,3}$	$(6, 2^5, 4)$	$A_0 = 1, A_4 = 15, A_5 = 12, A_6 = 4$	1
$\mathcal{K}_3$	$(35, 2^7, 26)$	$A_0 = 1, A_{26} = 105, A_{28} = 15, A_{30} = 7$	84
$\mathcal{K}_4$	$(96, 2^7, 72)$	$A_0 = 1, A_{72} = 118, A_{80} = 9$	$2^{44} \cdot 3^{17} \cdot 7$

5 Conclusion

In this paper, we have studied ACD codes over $\mathbb{F}_4$ with respect to the trace Hermitian inner product and the trace Euclidean inner product. Interesting constructions of ACD codes from binary codes are given with respect to the both inner products. As a good motivation of ACD codes, we have also constructed several ACD $(n, 2^{2k+1}, d)$ codes over $\mathbb{F}_4$ under the trace Euclidean inner product which are better than optimal Euclidean LCD $[n, k, d]$ codes over $\mathbb{F}_4$.

Acknowledgement

We want to thank the referees for their careful reading and constructive comments. This paper has been greatly improved.

References

1. Boonniyom K., Jitman S.: Complementary dual subfield linear codes over finite fields. Thai Journal of Mathematics Special issue ICMSA2015, 133-152 (2016).
2. Calderbank A. R., Rains E. M., Shor P. W., and Sloane N. J. A.: Quantum error correction via codes over $\mathbb{F}_4$, IEEE Trans. Inform. Theory. **44**, 1369–1387 (1998).
3. Carlet C., Guilley S.: Complementary dual codes for counter-measures to side-channel attacks. Coding Theory and Applications. Raquel Pinto, Paula Rocha-Malonek, Paolo Vettori eds, Springer, CIMSMS, **3**, 97–105 (2015).
4. Carlet C., Mesnager S., Tang C., Qi Y., Pellikaan, R.: Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. IEEE Trans. Inform. Theory. **64**(4), 3010-3017 (2018).
5. Dougherty S. T., Kim J.-L., Lee N.: Additive self-dual codes over finite fields of even order. Bull. Korean Math. **55**(2), 341-357 (2018).
6. Dougherty S. T., Kim J.-L., Ozkaya B., Sok L., Solé P.: The combinatorics of LCD codes, linear programming bound and orthogonal matrices. Int. J. Inf. Coding Theory. **4**(2/3), 116-128 (2017).
7. Grassl M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de` Accessed on 2022-07-01.
8. Guilley S.: a personal communication on July 15, (2021).
9. Guo, L. B., Liu, Y., Lu, L.D., Li, R. H.: On construction of good quaternary additive codes. **12** 03013, (2017).
10. Haemers W. H., Peeters M. J. P., van Rijckevorsel J. M.: Binary codes of strongly regular graphs. Des. Codes Cryptogr. **17**, 187-209 (1999).
11. Huffman W. C.: Additive cyclic codes over $\mathbb{F}_4$. Adv. in Math. Commun. **1**(4), 427-459 (2007).
12. Huffman W. C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, (2003).
13. MacWilliams F. J., Sloane N. J. A.: The theory of error-correcting codes. North-Holland, Amsterdam, (1977).
14. Massey J. L.: Reversible codes. Inf. Control. **7**(3), 369-380 (1964).
15. Massey J. L.: Linear codes with complementary duals. Discret. Math. **106-107**, 337-342 (1992).
16. Rains E., Sloane N. J. A.: Self-dual codes, in: V. S. Pless, W. C. Huffman (Eds.), Handbook of Coding Theory, Elsevier. Amsterdam. The Netherlands, (1998).
17. Sendrier N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discret. Math. **285**(1), 345–347 (2004).
18. Shi M., Li S., Kim J.-L., Solé P.: LCD and ACD codes over a noncom mutative non-unital ring with four elements. Cryptogr. Commun. (2021), https://doi.org/10.1007/s12095-021-00545-4.