# A NEW CONCATENATED TYPE CONSTRUCTION FOR LCD CODES AND ISOMETRY CODES

CLAUDE CARLET, CEM GÜNERI, FERRUH ÖZBUDAK AND PATRICK SOLÉ

Abstract. We give a new concatenated type construction for linear codes with complementary dual (LCD) over small finite fields. In this construction we need a special class of inner codes that we call *isometry codes*. Our construction generalizes a recent construction in [1] and [5] and it allows us to construct LCD codes with improved parameters directly.

*Keywords*: LCD code, concatenation, isometry code

*Mathematics Subject Classification:* 94B05, 11T71.

## 1. Introduction

Linear codes with complementary duals (LCD) are linear codes whose intersection with their dual is trivial. This concept was introduced by Massey [6]. Recently the first author and Guilley [1] investigated an interesting application of binary LCD codes against side-channel attacks and fault injection attacks and presented several constructions of LCD codes.

This has started an interest in several newer constructions of LCD codes over arbitrary finite fields, see for example [2, 4, 5, 9]. These constructions either use special classes of linear codes like quasi-cyclic codes or they construct LCD codes over large finite fields compared to their length. In classical coding theory an efficient method for constructing long codes over small finite fields is the method of concatenation. It uses codes over a large finite field (outer codes) with minimum distance $D$ and suitable inner codes with minimum distance $d$ and produces linear codes over the corresponding small field of minimum distance having a guaranteed lower bound of $dD$. There is only one analog of this construction for LCD codes, which is in [1, Proposition 3] and [5, Theorem 5.2]. However this construction works only if the small field $\mathbb{F}_q$ and the large field $\mathbb{F}_{q^k}$ satisfy

- $q$ is even or
- $q$ is odd and $k$ is odd.

Moreover the corresponding inner code has parameters $[k, k, 1]$ and the guaranteed minimum distance is just $D$ if the starting LCD code (outer code) over the large field $\mathbb{F}_{q^k}$ has minimum distance $D$.

Department of Mathematics, University of Paris VIII and University of Paris XIII, UMR 7539, CNRS, France, e-mail: claude.carlet@univ-paris8.fr.

Sabancı University, FENS, 34956 İstanbul, Turkey, email: guneri@sabanciuniv.edu.

Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, email: ozbudak@metu.edu.tr.

CNRS/LAGA, University of Paris VIII, 93 526 Saint-Denis, France, email: sole@enst.fr.

In this paper we introduce a new class of codes that we call *isometry codes*. These codes are defined for any $\mathbb{F}_q$ and have parameters $[n,k,d]$ with $d \geqslant 2$. We prove that using isometry codes as inner codes in the concatenation gives LCD codes in the small finite field if we start with LCD codes (outer codes) over a large finite field (see Theorem 3.1 below). This allows us to construct LCD codes with larger guaranteed minimum distance over arbitrary finite fields. We also provide some direct improvements of the results given in [4, Table 2].

The rest of the paper is organized as follows. We introduce isometry codes in Section 2. We give our construction in Section 3. We give some applications and numerical results in Section 4.

## 2. Isometry Codes

Let $q$ be a prime power and $2 \leqslant k \leqslant n$ be integers. The *trace* of $\alpha \in \mathbb{F}_{q^k}$ over $\mathbb{F}_q$ is defined as

$$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{k-1} \alpha^{q^i} = \alpha + \alpha^q + \cdots + \alpha^{q^{k-1}}.$$

From now on, we denote $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha)$ by $\mathrm{Tr}(\alpha)$. Let $\{e_1,\ldots,e_k\} \subseteq \mathbb{F}_q^k$. Assume that $(e_1,\ldots,e_k)$ is an ordered basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Recall that $(e'_1,\ldots,e'_k)$ is the dual basis of $(e_1,\ldots,e_k)$ if

$$\mathrm{Tr}(e_i e'_j) = \delta_{ij}$$

for $1 \leqslant i,j \leqslant k$. There exists a uniquely determined dual basis for any basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Recall that $(e_1,\ldots,e_k)$ is called a *self-dual basis* of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ if $(e_1,\ldots,e_k) = (e'_1,\ldots,e'_k)$. Note that there exists a self-dual basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ if and only if (see, for example, [8])

- $q$ is even or
- $q$ is odd and $k$ is odd.

**Definition 2.1.** Let $(e_1,\ldots,e_k)$ be an ordered basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. An $\mathbb{F}_q$-linear map $\pi : \mathbb{F}_{q^k} \to \mathbb{F}_q^n$ is called an *isometry with respect to* $(e_1,\ldots,e_k)$ if

$$\pi(e_i) \cdot \pi(e'_j) = \delta_{ij}$$

for $1 \leqslant i,j \leqslant k$ where the inner product is the Euclidean inner product in $\mathbb{F}_q^n$. Here $(e'_1,\ldots,e'_k)$ is the dual basis of $(e_1,\ldots,e_k)$. The image $\pi(\mathbb{F}_{q^k})$ is called an *isometry code* with respect to $(e_1,\ldots,e_k)$.

**Remark 2.2.** Note that an isometry code $\pi(\mathbb{F}_{q^k})$ with respect to $(e_1,\ldots,e_k)$ is a linear $[n,k]$ code over $\mathbb{F}_q$. Indeed, $\{\pi(e_1),\pi(e_2),\ldots,\pi(e_k)\}$ is linearly independent over $\mathbb{F}_q$: If $a_1,a_2,\ldots,a_k \in \mathbb{F}_q$ with $a_1\pi(e_1) + a_2\pi(e_2) + \cdots + a_k\pi(e_k) = 0$, then multiplying the vectors with $\pi(e'_1)$ in both sides we obtain that

$$a_1\pi(e'_1)\cdot\pi(e_1) + a_2\pi(e'_1)\cdot\pi(e_2) + \cdots + a_k\pi(e'_1)\cdot\pi(e_k) = a_1 = 0.$$

Similarly, $a_2 = a_3 = \cdots = a_k = 0$, which shows that the dimension of $\pi(\mathbb{F}_{q^k})$ is $k$ over $\mathbb{F}_q$.

Next we give some simple examples.

**Example 2.1.** *If $k = n$ and $(e_1, \ldots, e_k)$ is a self-dual basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, then the map*

$$\begin{aligned}\pi :&\mathbb{F}_{q^k} \to \mathbb{F}_q^k \\ &u \longmapsto \pi(u) = (\mathrm{Tr}(e_1u), \mathrm{Tr}(e_2u), \ldots, \mathrm{Tr}(e_ku))\end{aligned}$$

*is an isometry with respect to $(e_1, \ldots, e_k)$ obviously. The corresponding isometry code $\pi(\mathbb{F}_{q^k})$ is a linear $[k, k, 1]$ code over $\mathbb{F}_q$.*

**Example 2.2.** *We have confirmed the following results by MAGMA.*

- *If $k = 2, n = 3$ and $q = 2$, then there are 6 distinct isometries $\pi : \mathbb{F}_{q^2} \to \mathbb{F}_q^3$ for each basis $(e_1, e_2)$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.*
- *If $k = 2, n = 4$ and $q = 2$, then there are 32 distinct isometries $\pi : \mathbb{F}_{q^2} \to \mathbb{F}_q^4$ for each basis $(e_1, e_2)$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.*
- *If $k = 3, n = 4$ and $q = 2$, then there are 48 distinct isometries $\pi : \mathbb{F}_{q^3} \to \mathbb{F}_q^4$ for each basis $(e_1, e_2, e_3)$ of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$.*
- *If $k = 2, n = 2$ and $q = 3$, then there is no isometry $\pi : \mathbb{F}_{q^2} \to \mathbb{F}_q^2$ for any basis $(e_1, e_2)$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.*
- *If $k = 2, n = 3$ and $q = 3$, then there are 24 distinct isometries $\pi : \mathbb{F}_{q^2} \to \mathbb{F}_q^3$ for each basis $(e_1, e_2)$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.*
- *If $k = 2, n = 4$ and $q = 3$, then there are 288 distinct isometries $\pi : \mathbb{F}_{q^2} \to \mathbb{F}_q^4$ for each basis $(e_1, e_2)$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.*

**Definition 2.3.** Let $2 \leqslant k \leqslant n$ be integers. Assume that there exists an isometry $\pi : \mathbb{F}_{q^k} \to \mathbb{F}_q^n$ with respect to at least one basis $(e_1, \ldots, e_k)$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Let $d_{\max-isometry}(q; [n, k])$ be the largest minimum distance of all isometry codes $\pi(\mathbb{F}_{q^k}) \subseteq \mathbb{F}_q^n$ among all basis $(e_1, \ldots, e_k)$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Assume that there is no isometry $\pi(\mathbb{F}_{q^k}) \subseteq \mathbb{F}_q^n$ with respect to any basis $(e_1, \ldots, e_k)$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Then we define $d_{\max-isometry}(q; [n, k]) = 0$ by convention.

The following examples are interesting and they give reasoning for Definition 2.3.

**Example 2.3.** $d_{\max-isometry}(q; [4, 2]) = 2$ *for $q = 2$. For example,*

$$\begin{aligned}\pi_1 :&\mathbb{F}_{q^2} \to \mathbb{F}_q^4 \\ &u \longmapsto \pi(u) = (\mathrm{Tr}(w^2u), \mathrm{Tr}(w^2u), \mathrm{Tr}(wu), \mathrm{Tr}(w^2u))\end{aligned}$$

*is an isometry with respect to $(1, w)$ and $\pi_1(\mathbb{F}_{q^2})$ is a linear $[4, 2, 1]$ code over $\mathbb{F}_2$. However,*

$$\begin{aligned}\pi_2 :&\mathbb{F}_{q^2} \to \mathbb{F}_q^4 \\ &u \longmapsto \pi(u) = (\mathrm{Tr}(wu), \mathrm{Tr}(w^2u), \mathrm{Tr}(u), \mathrm{Tr}(u))\end{aligned}$$

*is an isometry with respect to $(1, w)$ and $\pi_2(\mathbb{F}_{q^2})$ is a linear $[4, 2, 2]$ code over $\mathbb{F}_2$. Here $w$ is the primitive element of $\mathbb{F}_{2^2}$ satisfying $w^2 + w + 1 = 0$. Note that a code over $\mathbb{F}_2$ with parameters $[4, 2, 2]$ is optimal.*

**Example 2.4.** $d_{\max -isometry}(q;[5,3]) = 2$ *for* $q = 2$. *For example,*

$$\begin{aligned}\pi_1 :&\mathbb{F}_{q^3} \to \mathbb{F}_q^5\\ &u \longmapsto \pi(u) = (\mathrm{Tr}(w^6u), \mathrm{Tr}(w^5u), \mathrm{Tr}(w^6u), \mathrm{Tr}(w^6u), \mathrm{Tr}(w^3u))\end{aligned}$$

*is an isometry with respect to* $(1, w, w^2)$ *and* $\pi_1(\mathbb{F}_{q^3})$ *is a linear* $[5, 3, 1]$ *code over* $\mathbb{F}_2$. *However,*

$$\begin{aligned}\pi_2 :&\mathbb{F}_{q^3} \to \mathbb{F}_q^5\\ &u \longmapsto \pi(u) = (\mathrm{Tr}(w^3u), \mathrm{Tr}(w^5u), \mathrm{Tr}(w^6u), \mathrm{Tr}(u), \mathrm{Tr}(u))\end{aligned}$$

*is an isometry with respect to* $(1, w, w^2)$ *and* $\pi_2(\mathbb{F}_{q^3})$ *is a linear* $[5, 3, 2]$ *code over* $\mathbb{F}_2$. *Here* $w$ *is the primitive element of* $\mathbb{F}_{2^2}$ *satisfying* $w^3 + w + 1 = 0$. *Note that a code over* $\mathbb{F}_2$ *with parameters* $[5, 3, 2]$ *is optimal.*

## 3. A New Concatenated Type Construction

In this section we give our construction.

Let $2 \leqslant k \leqslant n$ be integers and $\mathbb{F}_q$ be a finite field such that

$$d_{\max -isometry}(q;[n,k]) \geqslant 1.$$

Let $\pi : \mathbb{F}_{q^k} \to \mathbb{F}_q^n$ be an isometry with respect to a basis $(e_1, \ldots, e_k)$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ such that $\pi(\mathbb{F}_{q^k})$ is an $\mathbb{F}_q$-linear code of length $n$, dimension $k$ and minimum distance $d_{\max -isometry}(q;[n,k])$.

Let $C \subseteq \mathbb{F}_{q^k}^s$ be a linear code over $\mathbb{F}_{q^k}$ with parameters $[s, t, d(C)]$. Let $\pi : \mathbb{F}_{q^k}^s \to \mathbb{F}_q^{ns}$ be the $\mathbb{F}_q$-linear map defined as

$$\begin{aligned}\pi^{\otimes s} :&\mathbb{F}_{q^k}^s \to \mathbb{F}_q^{ns}\\ &(\alpha_1, \alpha_2, \ldots, \alpha_s) \longmapsto [\pi(\alpha_1), \pi(\alpha_2), \ldots, \pi(\alpha_s)]\end{aligned}$$

where $\mathbb{F}_q^{ns}$ is identified with $n \times s$ matrices over $\mathbb{F}_q$ and $\pi(\alpha_i)$ corresponds to the $i$-th column of length $s$ over $\mathbb{F}_q$.

**Theorem 3.1.** *If* $C$ *is an LCD code over* $\mathbb{F}_{q^k}$ *with parameters* $[s, t, d(C)]$, *then* $\pi^{\otimes s}(C)$ *is an LCD code over* $\mathbb{F}_q$ *with parameters* $[sn, tk, d(C)d_{\max -isometry}(q;[n,k])]$.

**Remark 3.2.** This construction is the same with the one of [1, Proposition 3] and [5, Theorem 5.2] if $k = n$ and $\pi$ is the obvious isometry corresponding to self-dual bases as in Example 2.1. Note that $d_{\max -isometry}(q;[n,k]) = 1$ in this case. Our construction is new and effective especially when $d_{\max -isometry}(q;[n,k]) \geqslant 2$ as in Examples 2.3 and 2.4.

**Proof.** We use some methods of Chen-Ling-Xing in [3]. Let $E = \pi(\mathbb{F}_{q^k})$ and $E^\perp$ be its dual in $\mathbb{F}_{q^n}$. Note that $E$ is a linear $[n, k]_q$ code and $E^\perp$ is a linear $[n, n-k]_q$ code. For $1 \leqslant i \leqslant s$ let $E_i = E$ and $E_i^\perp = E^\perp$. Note that

$$E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp \subseteq \mathbb{F}_q^{sn}$$

is an $\mathbb{F}_q$-linear code with parameters $[sn, s(n-k)]_q$. We note that $\pi^{\otimes s}(\mathbb{F}_{q^k}) \perp (E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp)$ trivially as

$$[\pi(\alpha_1), \pi(\alpha_2), \ldots, \pi(\alpha_s)] \cdot [b_1, b_2, \ldots, b_s] = \pi(\alpha_1) \cdot b_1 + \pi(\alpha_2) \cdot b_2 + \cdots + \pi(\alpha_s) \cdot b_s = 0$$

if $\pi(\alpha_1) \perp b_1, \pi(\alpha_2) \perp b_2, \ldots, \pi(\alpha_s) \perp b_s$. Hence,

$$\pi^{\otimes s}(C) \perp (E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp). \tag{1}$$

Moreover, $\pi(\mathbb{F}_{q^k}) \cap E^\perp = \{0\}$. Indeed, let $\beta \in \mathbb{F}_{q^k}$ with $\pi(\beta) \perp E$, or equivalently

$$\pi(\beta) \cdot \pi(e_i) = 0 \tag{2}$$

for $1 \leqslant i \leqslant k$. Let $(e_1', e_2', \ldots, e_k')$ be the dual basis for the basis $(e_1, e_2, \ldots, e_k)$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Let $\beta = b_1 e_1' + \cdots + b_k e_k'$ with $b_1, \ldots, b_k \in \mathbb{F}_q$. Then by (1) we have

$$(\pi(e_1')b_1 + \pi(e_2')b_2 + \cdots + \pi(e_k')b_k) \cdot \pi(e_1) = 0,$$

which implies that $b_1 = 0$ as $\pi$ is an isometry and hence $\pi(e_i') \cdot \pi(e_1) = \delta_{1i}$. Similarly $b_2 = \ldots = b_k = 0$ and hence $\beta = 0$. Therefore, $\pi^{\otimes s}(\mathbb{F}_{q^k}) \cap (E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp) = \{0\}$ and in particular

$$\pi^{\otimes s}(C^\perp) \cap (E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp) = \{0\}. \tag{3}$$

To show that $\pi^{\otimes s}(C)$ is LCD, we observe that it is enough to prove

$$\pi^{\otimes s}(C^\perp) \perp \pi^{\otimes s}(C). \tag{4}$$

Indeed the dimension of the dual of $\pi^{\otimes s}(C)$ is

$$sn - tk = \dim(\pi^{\otimes s}(C^\perp)) + \dim(E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp)$$

as $\dim(\pi^{\otimes s}(C^\perp)) = k(s-t)$ and $\dim(E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp) = s(n-k)$. Using (1), (3) and (4) we conclude that the dual of $\pi^{\otimes s}(C)$ is $(E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp) \oplus \pi^{\otimes s}(C^\perp)$. As $\pi^{\otimes s}(C) \cap (E_1^\perp \times E_2^\perp \times \cdots \times E_s^\perp) = \{0\}$ and $C \cap C^\perp = \{0\}$, we conclude that $\pi^{\otimes s}(C)$ is $LCD$. Indeed if $\underline{a} \in \pi^{\otimes s}(C) \cap \pi^{\otimes s}(C)^\perp = \pi^{\otimes s}(C) \cap \pi^{\otimes s}(C^\perp)$, then there exists $\underline{\alpha} \in C \cap C^\perp$ such that $\underline{a} = \pi^{\otimes s}(\underline{\alpha})$. As $C$ is LCD we obtain that $\underline{\alpha} = 0$ and hence $\underline{a} = 0$.

Now we prove (4). Let $(\alpha_1, \ldots, \alpha_s) \in \mathbb{F}_{q^k}^s$ and $(\beta_1, \ldots, \beta_s) \in \mathbb{F}_{q^k}^s$ such that $(\alpha_1, \ldots, \alpha_s) \cdot (\beta_1, \ldots, \beta_s) = 0$. For $1 \leqslant l \leqslant s$ and $1 \leqslant i, j \leqslant k$, let $a_l^i, b_l^j \in \mathbb{F}_q$ such that

$$\alpha_l = \sum_{i=1}^{k} a_l^i e_i \text{ and } \beta_l = \sum_{j=1}^{k} b_l^j e_j'.$$

Hence we have that

$$\sum_{l=1}^{s} \sum_{i=1}^{k} \sum_{j=1}^{k} a_l^i b_l^j e_i e_j' = 0.$$

Taking the trace of both sides we obtain that

$$\sum_{l=1}^{s} \sum_{i=1}^{k} \sum_{j=1}^{k} a_l^i b_l^j = 0 \tag{5}$$

as $\mathrm{Tr}(e_i e'_j) = 0$ for $1 \leqslant i, j \leqslant k$. We will show that

$$\pi^{\otimes s}(\alpha_1, \ldots, \alpha_s) \cdot \pi^{\otimes s}(\beta_1, \ldots, \beta_s) = \sum_{l=1}^{s} \pi(\alpha_l) \cdot \pi(\beta_l) = 0 \tag{6}$$

which implies (4). We have $\pi(\alpha_l) = \sum_{i=1}^{k} a_l^i \pi(e_i)$ and $\pi(\beta_l) = \sum_{j=1}^{k} b_l^j \pi(e'_j)$ for $1 \leqslant l \leqslant s$. Hence

$$\sum_{l=1}^{s} \pi(\alpha_l) \cdot \pi(\beta_l) = \sum_{l=1}^{s} \sum_{i=1}^{k} \sum_{j=1}^{k} a_l^i b_l^j \pi(e_i) \cdot \pi(e'_j) = \sum_{l=1}^{s} \sum_{i=1}^{k} a_l^i b_l^i$$

which follows from the isometry property that $\pi(e_i) \cdot \pi(e'_j) = \delta_{ij}$ for $1 \leqslant i, j \leqslant k$. Using (5) and (6), we complete the proof.

□

Next we give a direct generalization of Theorem 3.1 which would be useful in some applications as it would cover a wider range of parameters. Let $s \geqslant 2$ be an integer and for $1 \leqslant i \leqslant s$, assume that $\pi_i : \mathbb{F}_{q^k} \to \mathbb{F}_q^{n_i}$ are isometries with respect to the same basis $(e_1, \ldots, e_k)$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Let us note that the $n_i$'s need not be the same.

For each $i$, let $E_i := \pi_i(\mathbb{F}_{q^k})$ be the corresponding isometry code over $\mathbb{F}_q$ with length $n_i$, dimension $k$ and minimum distance $d_{\max-isometry}(q, [n_i, k])$. Consider the $\mathbb{F}_q$-linear injection

$$\begin{array}{rccc} \pi & : & \mathbb{F}_{q^k}^s & \to & \mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_s} \\ & & (\alpha_1, \alpha_2, \ldots, \alpha_s) & \mapsto & [\pi_1(\alpha_1), \ldots, \pi_s(\alpha_s)]. \end{array}$$

The following is a direct generalization of Theorem 3.1.

**Theorem 3.3.** *If $C$ is an LCD code over $\mathbb{F}_{q^k}$ with parameters $[s, t, d(C)]$, then $\pi(C)$ is an LCD code over $\mathbb{F}_q$ of length $n_1 + \cdots + n_s$ and dimension $tk$. The minimum distance of $\pi(C)$ is at least*

$$\min \left\{ \sum_{i \in I} d_{\max-isometry}(q; [n_i, k]) : \ I \subseteq \{1, \ldots, s\}, \ |I| = d(C) \right\}.$$

## 4. Numerical Results

In this section we directly improve some parameters in [4, Table 2] using Examples 2.3 and 2.4. We also provide some numerical results on the parameters of isometry codes.

The following examples give improvements on [4, Table 2].

**Example 4.1.** *There exists and optimal (maximum distance separable) LCD code $C$ with parameters $[4, 2, 3]$ over $\mathbb{F}_4$ (see for example [7]). Recall that $\pi_2(\mathbb{F}_4)$ is an isometry code given explicitly in Example 2.3 with parameters $[4, 2, 2]$ over $\mathbb{F}_2$. Hence using Theorem 3.1 we obtain an LCD code with parameters $[16, 4, 6]$ over $\mathbb{F}_2$. This is an improvement compared to* [4, Table 2]*, as the corresponding LCD code in* [4, Table 2] *has parameters $[16, 2, 6]$ over $\mathbb{F}_2$.*

**Example 4.2.** *There exists and optimal (maximum distance separable) LCD code $C_1$ with parameters $[4, 2, 3]$ over $\mathbb{F}_8$ (see for example [7]). Recall that $\pi_2(\mathbb{F}_8)$ is an isometry code given explicitly in Example 2.4 with parameters $[5, 3, 2]$ over $\mathbb{F}_2$. Hence using Theorem 3.1 and $C_1$ we obtain an LCD code with parameters $[20, 6, 6]$ over $\mathbb{F}_2$. This is an improvement compared*

*to* [4, Table 2]*, as the corresponding LCD code in* [4, Table 2] *has parameters* $[20, 6, 6]$ *over* $\mathbb{F}_2$*.*

*Similarly there exists and optimal (maximum distance separable) LCD code* $C_2$ *with parameters* $[4, 3, 2]$ *over* $\mathbb{F}_8$*. In the same way using* $C_2$ *instead of* $C_1$ *we obtain an LCD code with parameters* $[20, 9, 4]$ *over* $\mathbb{F}_2$*. This is an improvement compared to* [4, Table 2]*, as the corresponding LCD code in* [4, Table 2] *has parameters* $[20, 8, 4]$ *over* $\mathbb{F}_2$*.*

Finally we give some numerical results that we obtained using MAGMA on the values of $d_{\max-isometry}(q; [n, k])$ for some small values of $n$ and $k$ for $q = 2$ and $q = 3$.

Table 1: Parameters of Some Isometry Codes for $q = 2$

| $[n, k]$ | $d_{\max-isometry}(q; [n, k])$ |
|---|---|
| $[2, 2]$ | 1 |
| $[3, 2]$ | 1 |
| $[4, 2]$ | 2 |
| $[5, 2]$ | 2 |
| $[6, 2]$ | 3 |
| $[3, 3]$ | 1 |
| $[4, 3]$ | 1 |
| $[5, 3]$ | 2 |
| $[6, 3]$ | 2 |

Table 2: Parameters of Some Isometry Codes for $q = 3$

| $[n, k]$ | $d_{\max-isometry}(q; [n, k])$ |
|---|---|
| $[2, 2]$ | 0 |
| $[3, 2]$ | 1 |
| $[4, 2]$ | 2 |
| $[5, 2]$ | 3 |
| $[6, 2]$ | 3 |
| $[3, 3]$ | 1 |
| $[4, 3]$ | 2 |
| $[5, 3]$ | 2 |

Note that in Table 1, the isometry codes with $[n, k] \in \{[4, 2], [5, 3]\}$ over $\mathbb{F}_2$ are optimal (maximum distance separable). Similarly in Table 2, the isometry codes with $[n, k] \in \{[5, 2], [4, 3], [5, 3]\}$ over $\mathbb{F}_3$ are optimal (maximum distance separable).

## 5. Acknowledgments

Authors are supported by the project SECODE in the framework of Chist-Era-Net. This paper has been written during and after a one-week research group meeting at CIRM-Luminy, titled "On Linear Complementary Dual Codes". We thank CIRM for hospitality and ideal research environment provided. Güneri and Özbudak are supported by the TÜBİTAK project

215E200, which is associated with SECODE project in the scope of the CHIST-ERA Program. Carlet and Solé are also supported by the SECODE Project.

## References

[1] C. Carlet, and S. Guilley. Complementary Dual Codes for Counter-measures to Side-Channel Attacks. Post-proceedings of the 4th International Castle Meeting, Palme Castle, Portugal, September 15-18, 2014, published by the journal Advances in Mathematics of Communications. 10(1) pp. 131-150, 2016. A preliminary version has appeared in the proceedings published by CIM Series in Mathematical Sciences, Vol. 3, 2015.

[2] C. Carlet, S. Mesnager, C. Tang and Y. Qi. Euclidean and Hermitian LCD MDS codes arXiv preprint arXiv: 1702.08033v2.

[3] H. Chen, S. Ling, and C. Xing. Asymptotically Good Quantum Codes Exceeding the Ashikhmin-Litsyn-Tsfasman bound. IEEE Transactions on Information Theory. 47(5): pp. 2055-2058, 2001.

[4] S. T. Dougherty, J-L. Kim, B. Özkaya, L. Sok and P. Solé. The Combinatorics of LCD Codes: Linear programming bound and orthogonal matrices. International Journal of Information and Coding Theory. 4 (2/3): pp. 116-128, 2017.

[5] C. Güneri, B. Özkaya, and P. Solé. Quasi-Cyclic Complementary Dual Code. Finite Fields and Their Applications, 42, pp. 67-80, 2016.

[6] J. L Massey. Linear Codes with Complementary Duals. Discrete Mathematics. 106/107: pp. 333-342, 1992.

[7] L. F. Jin Construction of MDS Codes with Complementary Dual. IEEE Transactions on Information Theory. 63(5): pp. 2843-2847, 2016.

[8] G.Seroussi, and A. Lempel. Factorization of Symmetric Matrices and Trace-Orthogonal Bases in Finite Fields. SIAM Journal on Computing. 9(4): pp. 758-767, 1980.

[9] L. Sok, M. Shi and P. Solé. Constructions of Optimal LCD codes over Large Finite Fields. arXiv preprint arXiv: 1704.0483v1.