

1 **SCALAR PRODUCTS AND LEFT LCD CODES**

2 NABIL BENNENI AND ANDRÉ LEROY

ABSTRACT. In this article, we introduce new scalar products over finite rings via additive isomorphisms. This allows us to define new notions of right (respectively left) orthogonal codes, that are not necessarily linear. This leads to definitions of right (resp. left) dual codes and left LCD codes similar to the classical LCD codes. Furthermore, we provide necessary and sufficient conditions for the existence of these codes.

3 **Key words:** Scalar products, right and left dual codes, left-LCD codes.

4 **MSC 2020:** 94B05, 16S50.

5 1. INTRODUCTION

6 Linear complementary dual codes (LCD) were initially introduced by Massey [4]
7 in 1992, with the intention of using them for the so-called two-user binary adder
8 channel. Massey proved that the use of an LCD code solves some of the decodability
9 difficulties. LCD codes play an important role in practical applications in particular,
10 against side-channel and fault injection attacks; for more details cf. [1].

11 In this paper, we focus on the class of left LCD codes (left Complementary Dual
12 codes) which is important because of their connection with quantum error correction
13 and quantum computing [5].

14 Skew triangular matrix rings presented in [3] gave us the opportunity to create new
15 dot products, which is extremely beneficial for creating left and right dual codes
16 different from the classic dual codes. In addition, we stipulated that the codes must
17 be left-LCD codes (left-linear Complementary Dual codes).

18 This paper is organized as follows. In Section 2, we define a new product on a
19 matrix ring $M_n(R)$ via the action of an automorphism $\theta \in Aut(R)$. This was
20 inspired by [3] where a similar construction was defined on upper triangular matrix
21 rings. We also introduce new dot products and their left and right orthogonality
22 relations. We characterize self-dual codes with respect to this new dot product. We
23 study the connections between some subsets of R^n arising from these definitions.
24 In Section 3, we study a necessary and sufficient condition for a left linear code to
25 be a left LCD code (left linear Complementary Dual codes). We give examples of
26 the best known left LCD codes obtained in this way using \mathbb{F}_4 , \mathbb{F}_8 , \mathbb{F}_9 or \mathbb{F}_{16} for R
27 and the Frobenius automorphism for θ .

2. NEW PRODUCTS VIA ADDITIVE ISOMORPHISMS

1

2 We will define a new product on a matrix ring $M_n(R)$ via the action of an
 3 automorphism $\theta \in \text{Aut}(R)$. Let us start with a very general statement.

Lemma 2.1. *Let $R, +, \cdot$ be a ring and $S, +$ be an additive, abelian group such that $\varphi : R, + \rightarrow S, +$ is an isomorphism of additive groups. Then the following multiplication $*$ gives S a ring structure.*

$$\text{For } s_1, s_2 \in S, s_1 * s_2 = \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_2))$$

4 The map $\varphi : R \rightarrow S$ is therefore a ring isomorphism.

5 *Proof.* Let $R, +, \cdot$ be a ring and $S, +$ be an additive (=abelian) group such that
 6 $\varphi : R, + \rightarrow S, +$ is an isomorphism of additive groups. By definition, we have
 7 $s_1 * s_2 = \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_2))$. We compute

$$\begin{aligned} s_1 * (s_2 * s_3) &= \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_2 * s_3)) \\ &= \varphi(\varphi^{-1}(s_1)\varphi^{-1}(\varphi(\varphi^{-1}(s_2)\varphi^{-1}(s_3)))) \\ &= \varphi(\varphi^{-1}(s_1)(\varphi^{-1}(s_2)\varphi^{-1}(s_3))) \\ &= \varphi((\varphi^{-1}(s_1)\varphi^{-1}(s_2))\varphi^{-1}(s_3)) \\ &= (s_1 * s_2) * s_3. \end{aligned}$$

8

$$\begin{aligned} s_1 * (s_2 + s_3) &= \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_2 + s_3)) \\ &= \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_2) + \varphi^{-1}(s_1)\varphi^{-1}(s_3)) \\ &= \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_2)) + \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_3)) \\ &= s_1 * s_2 + s_1 * s_3. \end{aligned}$$

9

$$\begin{aligned} s_1 * \varphi(1_R) &= \varphi(\varphi^{-1}(s_1)\varphi^{-1}(\varphi(1))) \\ &= \varphi(\varphi^{-1}(s_1)1) = s_1. \end{aligned}$$

10

$$\begin{aligned} \varphi(r_1 r_2) &= \varphi(\varphi^{-1}(s_1)\varphi^{-1}(s_2)) \\ &= s_1 * s_2 = \varphi(r_1)\varphi(r_2). \end{aligned}$$

11

□

12 Before coming to the main focus of our paper, let us apply this lemma and give
 13 an example:

14 **Example 2.2.** (1) Consider $\mathbb{Z}/n\mathbb{Z}$ and let $m \in \{1, \dots, n\}$ be such that m and
 15 n are coprime. The map $\varphi : \mathbb{Z}/n\mathbb{Z}, + \rightarrow \mathbb{Z}/n\mathbb{Z}, +$ defined by $\varphi(1 + n\mathbb{Z}) =$
 16 $m + n\mathbb{Z}$ is an isomorphism of additive structure. This gives a new ring
 17 structure on $\mathbb{Z}/n\mathbb{Z}$ where the unity will be $m + n\mathbb{Z}$.

1 (2) Consider $\mathbb{Z}/8\mathbb{Z}$ and the map $\varphi : \mathbb{Z}/8\mathbb{Z}, +, * \longrightarrow \mathbb{Z}/8\mathbb{Z}, +, *$ defined by
2 $\varphi(\mathbb{Z}/8\mathbb{Z}) = 3 \times (\mathbb{Z}/8\mathbb{Z})$. $\bar{2} * \bar{3} = \varphi(\varphi^{-1}(\bar{2})\varphi^{-1}(\bar{3})) = \varphi(\bar{6}\bar{1}) = 2$.
3 $I(\mathbb{Z}/8\mathbb{Z}) = 2 \cdot (\mathbb{Z}/8\mathbb{Z})$, $\varphi(I(\mathbb{Z}/8\mathbb{Z})) = \varphi(2 \cdot (\mathbb{Z}/8\mathbb{Z})) = \varphi(\bar{2}) * \mathbb{Z}/8\mathbb{Z} =$
4 $(\bar{6} * (\mathbb{Z}/8\mathbb{Z}))$.

5 We can apply this lemma to a matrix ring $M_n(R)$ and an automorphism θ of R , +
6 (not necessarily a ring automorphism). We get an additive isomorphism, denoted
7 $\varphi : M_n(R) \longrightarrow M_n(R)$, by setting, for $A = (A_{ij}) \in M_n(R)$, $\varphi(A)_{ij} = \theta^{i-1}(A_{ij})$.
8 From φ we can create a new product on $M_n(R)$. We describe this product in
9 Theorem 2.3.

Theorem 2.3. *Let $\theta \in \text{Aut}(R)$, and φ the map defined above. Then the product $*$
defined on $M_n(R), +$ satisfies, for $A = (a_{ij})$ and $B = (b_{ij})$ we have*

$$(A * B)_{ij} = \sum_{k=1}^n a_{ik}\theta^{i-k}(b_{kj})$$

10 *Proof.* For $1 \leq i, j \leq n$, we compute:

$$\begin{aligned} (A * B)_{ij} &= \varphi(\varphi^{-1}(A)\varphi^{-1}(B))_{ij} = \theta^{i-1}((\varphi^{-1}(A)\varphi^{-1}(B))_{ij}) \\ &= \theta^{i-1}\left(\sum_k \varphi^{-1}(A)_{ik}\varphi^{-1}(B)_{kj}\right) \\ &= \sum_k \theta^{i-1}(\theta^{1-i}(A_{ik})\theta^{1-k}(B_{kj})) \\ &= \sum_k A_{ik}\theta^{i-k}(B_{kj}). \end{aligned}$$

11 This concludes the proof. □

12 **Example 2.4.** *We define the additive map φ by:*

$$\begin{aligned} \varphi : M_2(R) &\longrightarrow M_2(R) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix}; \end{aligned}$$

13

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &= \varphi(\varphi^{-1}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\varphi^{-1}\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right)) \\ &= \varphi\left(\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}\right) \\ &= \varphi\left(\begin{pmatrix} aa' + cb' & ac' + cd' \\ ba' + db' & bc' + dd' \end{pmatrix}\right) \\ &= \begin{pmatrix} aa' + cb' & ba' + db' \\ ac' + cd' & bc' + dd' \end{pmatrix}. \end{aligned}$$

1 **Example 2.5.** We define the additive map φ by:

$$\begin{aligned} \varphi : M_2(R) &\longrightarrow M_2(R) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} b & c \\ d & a \end{pmatrix}; \end{aligned}$$

2

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &= \varphi(\varphi^{-1}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\varphi^{-1}\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right)) \\ &= \varphi\left(\begin{pmatrix} d & a \\ b & c \end{pmatrix} \begin{pmatrix} d' & a' \\ b' & c' \end{pmatrix}\right). \\ &= \varphi\left(\begin{pmatrix} dd' + ab' & da' + ac' \\ bd' + cb' & ba' + cc' \end{pmatrix}\right) \\ &= \begin{pmatrix} da' + ac' & bd' + cb' \\ ba' + cc' & dd' + cb' \end{pmatrix}. \end{aligned}$$

3 The map $\varphi : M_n(R), \cdot \longrightarrow M_n(R), *$ gives an isomorphism of rings (see Lemma
4 2.1). This new product structure restricted to the subring of upper triangular
5 matrices over a finite field F with the Frobenius map was already used in Habibi
6 et al [3]. The next proposition is a particular case of Lemma 2.1.

7 **Proposition 2.6.** Let $\varphi : M_n(R), \cdot \longrightarrow M_n(R), *$ be the map define by $\varphi(a_{ij}) =$
8 $\theta^{i-1}(a_{ij})$. Then φ is an isomorphism of rings.

9 **Corollary 2.7.** The inverse of a matrix $A \in M_n(R), *$ is the matrix $\varphi(B) \in$
10 $M_n(R), *$ where B is the usual inverse of $\varphi^{-1}(A)$.

11 *Proof.* Suppose that $\varphi^{-1}(A)B = I_n$, then $A * \varphi(B) = \varphi(\varphi^{-1}(A)B) = \varphi(I_n) = I_n,$
12 as desired. \square

13 In order to introduce a scalar product related to the new product of matrices,
14 we are forced to generalize the above construction as follows.

Let R be a ring, and for any $n, k \in \mathbb{N}$, suppose we have an additive isomorphism

$$\varphi_{n,k} : M_{n,k}(R), + \longrightarrow M_{n,k}(R), +.$$

15 Now, if $A \in M_{n,k}(R)$ and $B \in M_{k,l}(R)$ we define

- 16 (a) $A \circ B = \varphi_{n,l}^{-1}(\varphi_{n,k}(A)\varphi_{k,l}(B)).$
17 (b) $A * B = \varphi_{n,l}(\varphi_{n,k}^{-1}(A)\varphi_{k,l}^{-1}(B)).$

There are many ways of defining the additive maps $\varphi_{n,k}$ in general. For instance,
we could use any permutation of the nk entries of the matrices in $M_{n,k}(R)$. In this
paper, we will consider an automorphism θ of the ring R and construct an additive
map $\varphi_{n,k}$ as follows:

$$\varphi_{n,k}(A)_{ij} = (\theta^{i-1}(a_{i,j})) \quad \text{where } A = (a_{i,j}) \in M_{n,k}(R).$$

18 With these notations we have:

1 **Lemma 2.8.** *Let R be a ring, $A \in M_{n,k}(R), B \in M_{k,l}(R)$ and $\theta \in \text{Aut}(R)$. With*
2 *the above notations we have:*

3 (1) $(A \circ B)_{i,j} = \sum_r A_{ir} \theta^{r-i}(B_{r,j})$

4 (2) $(A * B)_{i,j} = \sum_r A_{ir} \theta^{i-r}(B_{r,j})$.

5 (3) *If $n = k$ the map $\varphi : M_n(R), +, \cdot \longrightarrow M_n(R), +, *$ defined by $\varphi((A_{ij})) =$
6 $((\theta^{i-1})(A_{ij}))$ is a ring homomorphism.*

7 *In (1) and (2) above, these products are additive on both variables but are linear*
8 *only on the left.*

9 *Proof.* We have

$$\begin{aligned} (A \circ B)_{ij} &= \varphi_{n,l}^{-1}((\varphi_{n,k}(A)\varphi_{k,l}(B)))_{ij} \\ &= \theta^{1-i}(\sum_s \varphi_{n,k}(A)_{is} \varphi_{kl}(B)_{sj}) \\ &= \theta^{1-i}(\sum_s \theta^{i-1}(A_{is}) \theta^{s-1}(B_{sj})) \\ &= \sum_s A_{is} \theta^{s-i}(B_{sj}). \end{aligned}$$

10 A similar computation gives the second formula.

11 (3) is left to the reader. □

12 Let us remark that in the above definitions of the maps $\varphi_{n,k}$ the indices n, k just
13 fix the size of the matrices we are working with. In the sequel we will just write φ
14 and drop the indices.

We denote by R^n the space of rows $M_{1,n}(R)$ and by nR the space of columns
 $M_{n,1}(R)$. For $x \in R^n$, we denote $x^t \in {}^nR$ the transpose of x . If we consider $\varphi_{1,n}$
and $\varphi_{n,1}$, \circ and $*$ give two scalar products i.e. biadditive maps from $R^n \times {}^nR$ into
 R . More explicitly we have, for $a, b \in R^n$ we have:

$$a \circ b^t = \varphi_{1,1}^{-1}(\varphi_{1,n}(a)\varphi_{n,1}(b^t)) \quad \text{and} \quad a * b^t = \varphi_{1,1}(\varphi_{1,n}^{-1}(a)\varphi_{n,1}^{-1}(b^t)).$$

In general, these scalar products are neither R -linear nor symmetric in the sense
that, in general, for $a, b \in R^n$ $a \circ b^t \neq b \circ a^t$ and $a * b^t \neq b * a^t$. Note that the
orthogonality with respect to these scalar products is not the same as the classical
orthogonality. Similarly, the orthogonalities for both the operations \circ and $*$ are
different. Let $C \subseteq R^n$, we define

$${}^{\perp} * C = \{x \in R^n \mid x * c^t = 0, \forall c \in C\} \quad \text{and} \quad C^{*\perp} = \{x \in R^n \mid c * x^t = 0, \forall c \in C\}$$

$${}^{\perp} \circ C = \{x \in R^n \mid x \circ c^t = 0, \forall c \in C\} \quad \text{and} \quad C^{\circ\perp} = \{x \in R^n \mid c \circ x^t = 0, \forall c \in C\}$$

15 **Remarks 2.9.** *We usually take $\varphi_{1,1} = \text{Id}$. In these cases*

16 (1) *if $\varphi_{1,n}$ is a left linear map from $R_R^n \longrightarrow R_R^n$. Then scalar products given*
17 *by $*$ and \circ are left linear but just additive on the right.*

18 (2) *if $\varphi_{1,n}$ is a right linear map from $R_R^n \longrightarrow R_R^n$. Then scalar products given*
19 *by $*$ and \circ are right linear but only additive on the left.*

- 1 (3) If $\varphi_{1,n}$ and $\varphi_{n,1}$ are the identity maps (on R^n and nR respectively) then $*$
2 is the usual scalar product.
3 (4) If $\varphi_{1,n}$ is the identity and for any $(b_1, \dots, b_n) \in R^n$, $\varphi_{1,n}((b_1, \dots, b_n)^t) =$
4 $(b_1^*, \dots, b_n^*)^t$ where $*$ is an involution on R , then $*$ is an Hermitian product.

5 **Proposition 2.10.** Let $C \subseteq R^n$, we have:

- 6 (1) $C^{*,\perp} = (\varphi_{n,1}(\varphi_{1,n}^{-1}(C)^\perp))^t$.
7 (2) $\varphi_{1,n}^{-1}({}^\perp C) = \varphi_{n,1}^{-1}(C^t)^\perp$.
8 (3) ${}^\perp C = \varphi_{1,n}^{-1}(\varphi_{n,1}(C^t)^\perp)$.
9 (4) $C^{\circ\perp} = \varphi_{n,1}^{-1}(\varphi_{1,n}(C)^\perp)$.

Proof. (1) Let the maps

$$\varphi_{1,n} : M_{1,n}(R) \rightarrow M_{1,n}(R) ; \varphi_{n,1} : M_{n,1}(R) \rightarrow M_{n,1}(R) \text{ and } \varphi_{1,1} = Id.$$

10

$$\begin{aligned} C^{*\perp} &= \{x \in R^n \mid \varphi_{1,1}(\varphi_{1,n}^{-1}(c)\varphi_{n,1}^{-1}(x^t)) = 0, \forall c \in C\} \\ &= \{x \in R^n \mid \varphi_{1,1}(y\varphi_{n,1}^{-1}(x^t)) = 0, \forall y \in \varphi_{1,n}^{-1}(C)\} \\ &= \{x \in R^n \mid \varphi_{1,n}^{-1}(C)\varphi_{n,1}^{-1}(x^t) = 0\} \\ &= (\varphi_{n,1}(\varphi_{1,n}^{-1}(C)^\perp))^t. \end{aligned}$$

11 Hence the result.

12 (2) This is left to the reader.

13 (3) We compute:

$$\begin{aligned} {}^\perp C &= \{x \in R^n \mid x \circ c^t = 0, \forall c \in C\} \\ &= \{x \in R^n \mid \varphi_{1,1}^{-1}(\varphi_{1,n}(x)\varphi_{n,1}(c^t)) = 0\} \\ &= \{\varphi_{1,n}^{-1}(x) \mid \varphi_{n,1}(c^t) = 0\} \\ &= \varphi_{n,1}^{-1}(\varphi_{n,1}(C^t)^\perp). \end{aligned}$$

14 (4) This is left to the reader. □

15 Similar results hold for the other scalar products. Thanks to this proposition we
16 can characterize self-duality with respect to $*$ via usual orthogonality.

17 **Corollary 2.11.** A code C is a self-dual code for $*$ (i.e. $C = C^{*\perp}$) if and only
18 $\varphi_{n,1}^{-1}(C^t) = \varphi_{1,n}^{-1}(C)^\perp$. Similarly if $C = {}^\perp C$, then we have $\varphi_{1,n}(C) = \varphi_{n,1}(C^t)^\perp$.

19 Similar results hold for the other scalar products.

20 **Examples 2.12.** The map $\varphi_{1,3} : M_{1,3}(R) \rightarrow M_{1,3}(R)$, $\varphi_{1,3}(a_1, a_2, a_3) = (\lambda a_3, a_1, a_2)$,
21 where $\lambda \in R$ and $\varphi_{3,1}(b_1, b_2, b_3)^t = (b_2, b_1, b_3)^t$. The scalar product for $*$ given by
22 $(a_1, a_2, a_3) * (b_1, b_2, b_3)^t = (\lambda a_3, a_1, a_2) \cdot (b_2, b_1, b_3)^t = \lambda a_3 b_2 + a_1 b_2 + a_2 b_3$
23 Let $R = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ with $\alpha^2 + \alpha + 1 = 0$, $\lambda = \alpha$ and $C = \langle (1, 0, 1), (\alpha, 1, 0) \rangle$.
24 Then $(C)^{*,\perp} = \{(x, \alpha^2 x, \alpha x) \mid x \in \mathbb{F}_4\}$.

1 Let θ be an automorphism of R . For $n \geq 1$, $a = (a_1, \dots, a_n) \in R^n$, and $b =$
2 $(b_1, \dots, b_n) \in R^n$, we define $\varphi_{1,n}(a) = a$ and $\varphi_{n,1}(b^t) = (b_1, \theta(b_2), \dots, \theta^{n-1}(b_n))^t$.
3 Explicitly we have $a * b^t = \sum_r a_r \theta^{r-1}(b_r)$ and $a \circ b^t = \sum_r a_r \theta^{1-r}(b_r)$.

4 **Proposition 2.13.** *Let C be a subset of R^n . We have:*

- 5 (1) ${}^{\perp}C$ is always an R -submodule of R^n and $C^{*\perp}$ is always additive subgroup
6 of R^n .
7 (2) Let $x, y \in R^n$, we have $x * y^t = x \cdot \varphi(y)$, where \cdot stands for the usual dot
8 product.
9 (3) We have $C \subseteq {}^{\perp}{}^{\perp}C$ and $C \subseteq ({}^{\perp}C^t)^{\perp}$.
10 (3') We have $C \subseteq {}^{\perp\circ}C$ and $C \subseteq ({}^{\perp\circ}C^t)^{\perp}$.
11 (4) We have ${}^{\perp}C = \varphi(C^t)^{\perp}$ and $C^{\perp} = \varphi(C^{*\perp})$.
12 (4') We have ${}^{\perp\circ}C = \varphi(C^t)^{\perp}$ and $C^{\perp} = \varphi(C^{\circ\perp})$.

13 *Proof.* (1). These properties are direct consequences of the definitions.

14 (2). Let $x, y \in R^n$, we have $x * y^t = \sum_{i=1}^n x_i \theta^{i-1}(y_i) = (x_1, \dots, x_n) \varphi((y_1, \dots, y_n)^t)$.

15 (3). Let $(x_1, \dots, x_n) \in C^{*\perp}$ then for any $c = (c_1, \dots, c_n) \in C$, we have $c *$
16 $(x_1, \dots, x_n)^t = 0$, i.e. $\sum c_i \theta^{i-1}(x_i) = 0$, i.e. $(c_1, \dots, c_n) \in {}^{\perp,*} \{(x_1, \dots, x_n)\}$, this
17 gives the first inclusion. The second is obtained similarly.

18 (3'),(4) and (4') are obtained similarly. \square

19 Let us remark that all the assertions of the above Proposition 2.13, except (2),
20 are valid in the general setting of $*$ and \circ .

21

22 3. LEFT LCD CODES AND APPLICATIONS

23 In this section, we fix $\theta \in \text{Aut}(R)$. We will use the $*$ multiplication for matrices
24 as defined in Lemma 2.8. Analogues of the results that we will obtain are also true
25 for the \circ multiplication. We give the definition of a $*$ -LCD code and a necessary
26 and sufficient condition for a code is a $*$ -LCD code.

27 **Definition 3.1.** *A left linear code C is $*$ -LCD if $C \cap C^{*\perp} = \{0\}$ ($C \cap {}^{\perp,*}C = \{0\}$).*

28 If C is a left linear code, we can define it via a set of row bases $\{c_1, \dots, c_k\} \subseteq R^n$.
29 So if H is the $k \times n$ matrix defined by these vectors, we have that $C = R^k H$. Since
30 the map φ is a bijection, we can also define the code C by $C = R^k * G$ for a matrix
31 $G \in M_{k,n}(R)$.

32 **Lemma 3.2.** *Let R be a commutative ring, $y \in R^k$ and $G \in M_{k,n}(R)$, we have*
33 $(y * G)^t = \varphi(G)^t * \varphi^{-1}(y^t)$.

34 *Proof.* We compute $(y * G)^t = (y \varphi(G))^t = \varphi(G)^t y^t = \varphi(G)^t \varphi(\varphi^{-1}(y^t))$
35 $= \varphi(G)^t * \varphi^{-1}(y^t)$. This concludes the proof. \square

36 **Theorem 3.3.** *Let R be a commutative field and $G \in M_{k,n}(R)$. The code $C =$
37 $R^k * G$ is a left $*$ -LCD code if and only if $G * \varphi(G)^t \in M_n(R)$ is invertible.*

1 *Proof.* Assume that the matrix $G * \varphi(G)^t \in M_n(R)$ is invertible, and let $\mathit{mathbfc} \in$
2 $C \cap^{\perp,*} C$. There exists $u \in R^k$ such that $\mathit{mathbfc} = u * G$. Since $\mathit{mathbfc} \in^{\perp,*} C$,
3 we have that for every $y \in R^k$, $\mathit{mathbfc} * (y * G)^t = 0$. We thus get that $0 =$
4 $(u * G) * (y * G)^t$. The above lemma then gives $0 = u * G * \varphi(G)^t * \varphi^{-1}(y^t)$. Since
5 $y \in R^k$, our assumption gives that $u = 0$ and hence $c = 0$. Conversely, let us show
6 that if $C \cap^{\perp,*} C = \{0\}$ then $G * \varphi(G)^t$ is invertible. Assume to the contrary that
7 $G * \varphi(G)^t$ is not invertible and let $v \in R^k$ be such that $v * G * \varphi(G)^t = 0$. For any
8 $e = e' * G \in C$, we have $v * G * e^t = v * G * (e' * G)^t * = v * G * \varphi(G)^t * \varphi^{-1}(e'^t) = 0$.
9 We thus have that $v * G \in C \cap^{\perp,*} C$, a contradiction. \square

10 **Remarks 3.4.** The above result has analogues in all the three remaining orthogo-
11 nals viz. $C^{*,\perp}, \perp, \circ C$ and $C^{\circ,\perp}$. Notice that for the right orthogonals $C^{*,\perp}, C^{\circ,\perp}$ we
12 have to use a right linear code C defined by a matrix $H \in M_{n,k}(R)$, i.e. $C = HR^k$.

13 **3.1. Results and computation.** In this subsection, we present examples of good
14 left LCD codes and dual code $C^{\perp,*}$ form the from Theorem 3.3 and Proposition
15 2.10 ($\varphi^{-1}(C^{\perp}) = C^{*\perp}$) over $(GF(4))$, $(GF(8))$, $(GF(9))$ and $(GF(16))$. These
16 codes (left LCD) are either optimal or have the same parameters as best known
17 linear codes available in the database [2].

18
19

20 4. ACKNOWLEDGEMENT

21 This work was supported by The International Mathematical Union (IMU Abel
22 Visiting Scholar Program 2024). We would like to thank Professor Steven Dougherty
23 for correcting misprints in a previous version of this paper.

24 REFERENCES

- 25 [1] C. Carlet and S. Guilley. Complementary dual codes for counter-measures to side-channel
26 attacks. In ICMCTA, pages 97-105. Springer, 2014.
27 [2] M. Grassl. Code tables: Bounds on the parameters of codes.
28 [3] M. Habibi, A. Moussavi, and A. Alhevaz. On skew triangular matrix rings. In Algebra Col-
29 loquium, World Scientic, volume 22, pages 271-280., 2015.
30 [4] J. L. Massey. Linear codes with complementary duals. Discrete Mathematics, 106:337-
31 342,1992.
32 [5] Calderbank, A Robert and Rains, Eric M and Shor, Peter M and Sloane, Neil JA, IEEE
33 Transactions on Information Theory,44, 4,1369–1387, 1998.

34 USTHB, FACULTÉ DE MATHÉMATIQUES, LABORATOIRE ATN,, BP 32 EL ALIA BAB EZZOUAR
35 ALGIERS ALGERIA, EMAIL: NABIL.BENNENI@GMAIL.COM

36 UNIV. ARTOIS, UR 2462, LABORATOIRE DE MATHÉMATIQUES DE LENS (LML), F-62300 LENS,
37 FRANCE, EMAIL: ANDRE.LEROY@UNIV-ARTOIS.FR

TABLE 1. Examples of best known and optimal left-LCD codes over $GF(4)$ and $GF(8)$

Generator Matrix	$[n, k, d]_q$	Type of Codes
$\begin{pmatrix} 1 & 0 & 0 & 0 & w^5 & w^2 & 1 \\ 0 & 1 & 0 & 0 & w^2 & w^2 & 1 \\ 0 & 0 & 1 & 0 & w^4 & w^6 & w^6 \\ 0 & 0 & 0 & 1 & w^6 & 1 & w^6 \end{pmatrix}$	$[7, 4, 4]_8$	$C^{\perp,*}$ Left-LCD
$\begin{pmatrix} 1 & 0 & 0 & 0 & w^2 & 0 & w^2 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & w^2 & w & w^2 \\ 0 & 0 & 0 & 1 & 0 & w^2 & 1 \end{pmatrix}$	$[7, 4, 3]_4$	$C^{\perp,*}$ Left-LCD
$\begin{pmatrix} 1 & 0 & 0 & w^2 & w^2 & w^2 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & w^2 & w^2 & w^2 \end{pmatrix}$	$[7, 3, 4]_4$	${}^{\perp}C$
$\begin{pmatrix} 1 & 0 & 0 & w^2 & w^2 & w^3 & w^5 & w^6 & w^4 & w \\ 0 & 1 & 0 & w^5 & w^4 & w^2 & w & w^4 & w^3 & w^6 \\ 0 & 0 & 1 & w & w^5 & w^6 & w^6 & w^4 & w & w^4 \end{pmatrix}$	$[10, 3, 8]_8$	$C^{\perp,*}$ Left-LCD
$\begin{pmatrix} 1 & 0 & 0 & w^3 & w^3 & w^2 & w^6 \\ 0 & 1 & 0 & w^4 & w^5 & 1 & w^2 \\ 0 & 0 & 1 & w^4 & w^4 & w^4 & w^4 \end{pmatrix}$	$[7, 3, 4]_8$	${}^{\perp}C$
$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & w^2 & 1 & 1 & w^2 & w \\ 0 & 1 & 0 & 0 & 0 & 0 & w^2 & w & 0 & w & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & w^2 & w^2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & w & w^2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & w^2 & 0 & 0 & 1 & w^2 \\ 0 & 0 & 0 & 0 & 0 & 1 & w^2 & w^2 & w & 1 & w^2 \end{pmatrix}$	$[11, 6, 4]_4$	$C^{\perp,*}$ Left-LCD
$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & w & 1 & w^2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & w^2 & 0 & 1 & w^2 & w^2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & w & 1 & w & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & w & 0 & w^2 & w^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & w & w^2 \end{pmatrix}$	$[11, 6, 4]_4$	${}^{\perp}C$

TABLE 2. Examples of best known and optimal Left LCD codes over $GF(9)$ and $GF(16)$

Generator Matrix																			$[n, k, d]_q$
$\begin{pmatrix} 1 & 0 & 0 & 0 & w^7 & 0 & w & w^5 & w & 2 & w^3 & w^3 & w^3 & w^3 & 0 & 1 & w^2 & w^3 & 1 \\ 0 & 1 & 0 & 0 & w^6 & 0 & w^2 & w^3 & w^2 & 0 & w^6 & w^2 & w & 1 & w^5 & w^3 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 2 & w^3 & 0 & w^5 & w^3 & 0 & w^3 & 1 & 2 & w^6 & w^6 & w^5 & w^5 \\ 0 & 0 & 0 & 1 & w^5 & 0 & w^3 & w^2 & w & w^3 & 1 & w^2 & w^7 & w^2 & w^3 & 2 & w^5 & w^3 & w^7 \\ 0 & 0 & 0 & 0 & 0 & 1 & w^7 & 2 & w^2 & w^3 & 1 & w^7 & w^5 & w^5 & w & w^6 & w^7 & w & w \end{pmatrix}$																			$[19, 5, 12]_9$
$\begin{pmatrix} 1 & 0 & 0 & 0 & w^7 & 0 & w & w^5 & w & 2 & w^3 & w^3 & w^3 & w^3 & 0 & 1 & w^2 & w^3 & 1 \\ 0 & 1 & 0 & 0 & w^2 & 0 & w^6 & w & w^6 & 0 & w^2 & w^6 & w^3 & 1 & w^7 & w & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 2 & w^3 & 0 & w^5 & w^3 & 0 & w^3 & 1 & 2 & w^6 & w^5 & w^5 \end{pmatrix}$																			$[19, 3, 13]_9$
$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & w^7 & 2 & w^2 & w^3 & 1 & w^7 & w^5 & w^5 & w & w^6 & w^7 & w & w \\ 0 & 1 & 0 & 0 & w^5 & 0 & w^3 & w^7 & w^3 & 2 & w & w & w & w & 0 & 1 & w^6 & w & 1 \\ 0 & 0 & 1 & 0 & w^2 & 0 & w^2 & w^3 & w^2 & 0 & w^6 & w^2 & w & 1 & w^5 & w^3 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 & w & 0 & w^7 & w^w & 0 & w^2 & 1 & 2 & w^2 & w^2 & w^7 & w^7 \\ 0 & 0 & 0 & 0 & w^5 & 0 & w^3 & w^2 & w & w^3 & 1 & w^2 & w^7 & w^2 & w^3 & 2 & w^5 & w^3 & w^7 \end{pmatrix}$																			$[19, 5]_9$
$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & w^{10} & w^4 & w^6 & w^4 & w^{13} & w & w^9 & w^{13} & w^5 & 1 & & \\ 0 & 1 & 0 & 0 & 0 & 0 & w^{12} & w^{10} & w^9 & w^{11} & w^{11} & w^{12} & w^2 & w^{13} & w^{12} & w^{12} & w^{12} & & \\ 0 & 0 & 1 & 0 & 0 & 0 & w^{14} & w^7 & w^8 & w^9 & w^{10} & w & w^{10} & w^5 & w^{12} & 1 & w & & \\ 0 & 0 & 0 & 1 & 0 & 0 & w^3 & w^3 & w^9 & w^{12} & w^6 & w^3 & w^2 & w^3 & 1 & w^3 & 1 & & \\ 0 & 0 & 0 & 0 & 1 & 0 & w^5 & w^2 & w^{12} & w^5 & w^{10} & w^{12} & w^4 & w^6 & w^9 & w^{10} & w^{12} & & \\ 0 & 0 & 0 & 0 & 0 & 1 & w^{10} & 1 & w^{10} & w^5 & w^{10} & 1 & w^{10} & 1 & w^5 & 1 & 1 & & \end{pmatrix}$																			$[17, 6, 10]_{16}$