IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 18, 2021, accepted March 2, 2021, date of publication March 8, 2021, date of current version March 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3064503

Hermitian Rank Metric Codes and Duality

JAVIER DE LA CRUZ[1], JORGE ROBINSON EVILLA[1,2], AND FERRUH ÖZBUDAK[3]

[1]Departamento de Matemáticas y Estadística, Universidad del Norte, Barranquilla 081007, Colombia
[2]Departamento de Matemáticas, Universidad del Atlántico, Barranquilla 081007, Colombia
[3]Department of Mathematics, Institute of Applied Mathematics, Middle East Technical University, 06800 Ankara, Turkey

Corresponding author: Ferruh Özbudak (ozbudak@metu.edu.tr)

This work was supported in part by the Ministerio de Ciencia, Tecnología e Innovación (Minciencias) under Project 121571250178.

ABSTRACT In this paper we define and study rank metric codes endowed with a Hermitian form. We analyze the duality for $\mathbb{F}_{q^2}$-linear matrix codes in the ambient space $(\mathbb{F}_{q^2})_{n,m}$ and for both $\mathbb{F}_{q^2}$-additive codes and $\mathbb{F}_{q^{2m}}$-linear codes in the ambient space $\mathbb{F}^n_{q^{2m}}$. Similarly, as in the Euclidean case we establish a relationship between the duality of these families of codes. For this we introduce the concept of q^m-duality between bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and prove that a q^m-self dual basis exists if and only if m is an odd integer. We obtain connections on the dual codes in $\mathbb{F}^n_{q^{2m}}$ and $(\mathbb{F}_{q^2})_{n,m}$ with the corresponding inner products. In particular, we study Hermitian linear complementary dual, Hermitian self-dual and Hermitian self-orthogonal codes in $\mathbb{F}^n_{q^{2m}}$ and $(\mathbb{F}_{q^2})_{n,m}$. Furthermore, we present connections between Hermitian $\mathbb{F}_{q^2}$-additive codes and Euclidean $\mathbb{F}_{q^2}$-additive codes in $\mathbb{F}^n_{q^{2m}}$.

INDEX TERMS Rank metric codes, additive rank metric codes, Hermitian rank metric codes.

I. INTRODUCTION

Rank metric codes were introduced by Delsarte (1978) as a q-analogue of coding theory [13]. Due to their applications in cryptography and in network error correction ([30], [31]), there is a great interest in studying their general properties and their connections with other topics [1], [4], [9]–[11], [24], [26], [27], [29].

In the matrix representation linear rank metric codes are $\mathbb{F}_Q$-linear subspaces of the ambient space $V = (\mathbb{F}_Q)_{n,m}$, where Q is a prime power and the weight of an element $A \in (\mathbb{F}_Q)_{n,m}$ is defined as the rank of the matrix. In the vector representation, rank metric codes are $\mathbb{F}_{Q^m}$-linear subspaces of the ambient space $U = \mathbb{F}^n_{Q^m}$, where the weight of a vector $v \in \mathbb{F}^n_{Q^m}$ is defined as the maximal number of coordinates of v which are linearly independent over $\mathbb{F}_Q$.

It is well known that using an invertible isometry $\lambda_{\mathcal{B}} : U \longrightarrow V$, any $\mathbb{F}_{Q^m}$-linear code $C \leq U$ can be considered as an $\mathbb{F}_Q$-linear matrix code $\mathcal{C} \leq V$, called the code associated to the code C, which shares the same rank properties as C (see Definition 3). However, conversely given an $\mathbb{F}_Q$-linear code $\mathcal{C}$ in V, we only obtain $\mathbb{F}_Q$-linearity, i.e. an $\mathbb{F}_Q$-additive rank metric code C in the space U. Therefore, the Hermitian forms we define on V and U are over $\mathbb{F}_Q$. Furthermore, we define a Hermitian form on U over $\mathbb{F}_{Q^m}$ and show their relationship with those defined over $\mathbb{F}_Q$.

Classical additive codes of length n over $\mathbb{F}_4$ are subgroups under addition of $\mathbb{F}^n_4$ and were first introduced in [5] because of their connection to quantum codes. Specifically the authors in [5] transform the problem of finding quantum error-correcting codes into the problem of finding additive codes over $\mathbb{F}_4$ which are self-orthogonal with respect to a certain trace inner product. The author of [8] classified additive codes over $\mathbb{F}_9$ that are self-dual with respect to the Hermitian trace inner product, which in quantum information theory correspond to ternary quantum error-correcting codes. Additive codes were generalized and studied in [3], [16], [19], [20].

Additive codes and self-duality are also considered in the ambient space of matrices endowed with the rank metric (see, for example, [22], [25], [26]). They have potential applications not only in network coding, combinatorics and cryptography but also in code-based cryptography (and hence post-quantum cryptography).

Duality in coding theory is an interesting notion with many applications. Recently codes having trivial intersections with their duals, in particular linear complementary dual codes, are shown to be interesting also for some side-channel attacks in cryptography [6].

The paper is structured as follows. In Section 2 we collect preliminaries on σ-sesquilinear forms, Hermitian forms and

The associate editor coordinating the review of this manuscript and approving it for publication was Cesar Vargas-Rosales.

Euclidean forms. In Section 3 we define Hermitian $\mathbb{F}_{q^2}$-linear rank metric codes in the ambient space $(\mathbb{F}_{q^2})_{n,m}$ and analyze some properties such as the MacWilliams Identities. The main contributions of our paper are given in Sections 4 and 5. We obtain some connections on additive codes and their dual codes in the ambient spaces $\mathbb{F}^n_{q^{2m}}$ and $(\mathbb{F}_{q^2})_{n,m}$ together with corresponding Hermitian inner products. In Section 4 we define Hermitian $\mathbb{F}_{q^{2m}}$-linear and $\mathbb{F}_{q^2}$-additive rank metric codes in the ambient space $\mathbb{F}^n_{q^{2m}}$. In order to analyze the duality of these families of codes we introduce the concept of q^m-duality for two bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. We prove that a q^m-self-dual basis exists if and only if m is an odd integer. Additionally, we establish a relationship between the theory of the duality for the spaces $(\mathbb{F}_{q^2})_{n,m}$ and $\mathbb{F}^n_{q^{2m}}$ (see Theorem 3). Due to this result, the MacWillams Identities are valid for Hermitian codes of $\mathbb{F}^n_{q^{2m}}$. We state results on Hermitian linear complementary dual codes, self-dual codes and self-orthogonal codes. Finally, in Section 5 we present connections between Hermitian $\mathbb{F}_{q^2}$-additive codes and Euclidean $\mathbb{F}_{q^2}$-additive codes in $\mathbb{F}^n_{q^{2m}}$.

II. BASIC FACTS ON σ-SESQUILINEAR, EUCLIDEAN AND HERMITIAN FORMS

Let $\mathbb{K}$ be a finite field, $\mathbb{F}$ an extension of $\mathbb{K}$, $\sigma \in \mathrm{Aut}(\mathbb{K})$ and V a finite-dimensional $\mathbb{F}$-vector space. A σ-sesquilinear form on V over $\mathbb{K}$ is a map $\langle \cdot, \cdot \rangle : V \times V \longrightarrow \mathbb{K}$ such that if $x, y, z \in V$ and $\alpha \in \mathbb{K}$, then $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$, $\langle x, y + z\rangle = \langle x, y\rangle + \langle x, z\rangle$, $\langle \alpha x, y\rangle = \alpha\langle x, y\rangle$ and $\langle x, \alpha y\rangle = \sigma(\alpha)\langle x, y\rangle$. In addition, if $\mathrm{ord}(\sigma) = 2$ and $\sigma(\langle x, y\rangle) = \langle y, x\rangle$, then the form is called a Hermitian form. In the case $\mathrm{ord}(\sigma) = 1$ and $\langle x, y\rangle = \langle y, x\rangle$ the form is called a Euclidean form. A σ-sesquilinear form with the property that $\langle x, y\rangle = 0 \iff \langle y, x\rangle = 0$ is called reflexive. Clearly, Hermitian and Euclidean forms are reflexive. A σ-sesquilinear form is called non-degenerate if $\langle x, y\rangle = 0$ for all $y \in V$ implies $x = 0$.

For any $\mathbb{F}$-linear vector subspace $W \leq V$, the *dual space* of W with respect to a reflexive σ-sesquilinear form $\langle \cdot, \cdot \rangle$, denoted by $W^{\perp}$, is

$$W^{\perp} := \{v \in V : \langle v, W\rangle = 0\}.$$

In this case we say that W is *self-orthogonal* if $W \subseteq W^{\perp}$ and *self-dual* if $W = W^{\perp}$. It is well known that if $\langle \cdot, \cdot \rangle$ is non-degenerate and reflexive, then $\dim_{\mathbb{K}}(W^{\perp}) = \dim_{\mathbb{K}}(V) - \dim_{\mathbb{K}}(W)$ and $(W^{\perp})^{\perp} = W$.

The radical of a reflexive σ-sesquilinear form $\langle \cdot, \cdot \rangle$ on V is the $\mathbb{F}$-vector space

$$\mathrm{rad}(\langle \cdot, \cdot \rangle) = \{x \in V : \langle x, y\rangle = 0 \text{ for all } y \in V\}.$$

Clearly a reflexive σ-sesquilinear form is non-degenerate if and only if its radical is trivial.

If $\mathcal{B} = \{\beta_1, \ldots, \beta_m\}$ is a basis of V over $\mathbb{K}$ and if $\langle \cdot, \cdot \rangle$ is a σ-sesquilinear form on V, then

$$\begin{aligned}\langle x, y\rangle &= \langle \sum_{i=1}^{m} x_i\beta_i, \sum_{j=1}^{m} y_j\beta_j\rangle \\ &= \sum_{i=1}^{m} x_i \sum_{j=1}^{m} \langle \beta_i, \beta_j\rangle\sigma(y_j) \\ &= \overline{x}G_{\mathcal{B}}\sigma(\overline{y})^t,\end{aligned}$$

where $\overline{x} = (x_1, \ldots, x_m)$, $\overline{y} = (y_1, \ldots, y_m) \in \mathbb{K}^m$ and $\sigma(\overline{y}) := (\sigma(y_1), \ldots, \sigma(y_m)) \in \mathbb{K}^m$. The matrix $G_{\mathcal{B}} = (\langle \beta_i, \beta_j\rangle) \in (\mathbb{K})_m$ is called the Gram matrix of $\langle \cdot, \cdot \rangle$ with respect to the basis $\mathcal{B}$.

Symmetric matrices $A \in (\mathbb{K})_m$ and $B \in (\mathbb{K})_m$ are said to be *conjunctive* if there exists a non-singular matrix $P \in \mathrm{GL}_m(\mathbb{K})$ such that $B = P^tAP$. Two Euclidean forms are *equivalent* if and only if their Gram matrices are conjunctive. We shall use the following well-known lemma.

Lemma 1: Let char($\mathbb{K}$) be an odd integer and let $A \in (\mathbb{K})_m$ be a non-singular symmetric matrix. Then A and I_m are conjunctive or A and $J = diag(1, \ldots, 1, a)$ are conjunctive, where a is an arbitrary non-square in $\mathbb{K}$.

Proof: If $\mathrm{char}(\mathbb{K})$ is odd, then there are exactly two equivalence classes of non-degenerate Euclidean forms on $\mathbb{K}^m$, represented by the matrices I_m and J (see [2]). □

It is well known that if $\mathbb{K}_0$ is the field of fixed points of σ and $\mathrm{ord}(\sigma) = 2$, then $(\mathbb{K} : \mathbb{K}_0) = 2$. Therefore $|\mathbb{K}| = |\mathbb{K}_0|^2 = q^2$ for some q prime power and $\sigma(x) = x^q$ for all $x \in \mathbb{K}$. Let $\mathbb{K} = \mathbb{F}_{q^2}$ and let $x^* := x^q$ be the conjugate of $x \in \mathbb{F}_{q^2}$. For a matrix $A \in (\mathbb{F}_{q^2})_m$, write $A^{(q)}$ for the matrix obtained from A by conjugation of each entry. We define the *conjugate* of A, denoted by A^*, as the transpose of the matrix $A^{(q)}$ i.e. $A^* = (A^{(q)})^t$. A matrix $A \in (\mathbb{F}_{q^2})_m$ is *Hermitian* if $A^* = A$.

It is easy to verify that $\langle \cdot, \cdot \rangle$ is Hermitian if and only if its Gram matrix $G_{\mathcal{B}}$ is Hermitian. Therefore there exists an one-to-one correspondence between the set of Hermitian matrices in $(\mathbb{F}_{q^2})_m$ and the set of Hermitian forms on V. Notice that $\langle \cdot, \cdot \rangle$ is a non-degenerate Hermitian form if and only if its Gram matrix $G_{\mathcal{B}}$ is non-singular in $(\mathbb{F}_{q^2})_m$ and Hermitian.

Hermitian matrices $A \in (\mathbb{F}_{q^2})_m$ and $B \in (\mathbb{F}_{q^2})_m$ are said to be *conjunctive* if there exists a non-singular matrix $P \in \mathrm{GL}_m(\mathbb{F}_{q^2})$ such that $B = P^*AP$. Two Hermitian forms are *equivalent* if and only if their Gram matrices are conjunctive.

The following lemma is crucial for the proof of Theorem 2.

Lemma 2:

1) *Let $A \in (\mathbb{F}_{q^2})_m$. Then A^*A is a Hermitian matrix with* $\det(A^*A) = \det(A)^{q+1} =: \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\det(A))$.
2) *Let $A \in (\mathbb{F}_{q^2})_m$ be a non-singular Hermitian matrix. Then A and I_m are conjunctive.*

Proof:

1) Let $A = (a_{ij}) \in (\mathbb{F}_{q^2})_m$. Since

$$\begin{aligned}\det(A^{(q)}) &= \sum_{\sigma \in \mathrm{Sym}(m)} \mathrm{sgn}(\sigma) \prod_{i=1}^{m} a^q_{i,\sigma(i)} \\ &= \left(\sum_{\sigma \in \mathrm{Sym}(m)} \mathrm{sgn}(\sigma) \prod_{i=1}^{m} a_{i,\sigma(i)} \right)^q \\ &= [\det(A)]^q,\end{aligned}$$

we have $\det(A^*) = \det(A^{(q)}) = [\det(A)]^q$.

2) See [18, Lemma 2.3].

□

III. HERMITIAN $\mathbb{F}_{q^2}$-LINEAR RANK METRIC CODES

Let $(\mathbb{F}_{q^2})_{n,m}$ be the $\mathbb{F}_{q^2}$-vector space of matrices over $\mathbb{F}_{q^2}$ of type (n, m). On $(\mathbb{F}_{q^2})_{n,m}$ we define the so-called rank metric distance by $\mathrm{d}(A, B) := rank(A - B)$ for $A, B \in (\mathbb{F}_{q^2})_{n,m}$.

A t-dimensional $\mathbb{F}_{q^2}$-subspace $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ endowed with the metric d is called an $\mathbb{F}_{q^2}$*-linear rank metric* code with minimum distance $\mathrm{d}(\mathcal{C}) := \min\{\mathrm{d}(A, B) \mid A \neq B \in \mathcal{C}\}$. Clearly, the minimum distance of a code $\mathcal{C} \neq \{0\}$ is also

$$d(\mathcal{C}) := \min\{rank(A) : A \in \mathcal{C},\ A \neq 0\}.$$

The *trace Hermitian inner product* of two matrices $A = (a_{ij}) \in (\mathbb{F}_{q^2})_{n,m}$ and $B = (b_{ij}) \in (\mathbb{F}_{q^2})_{n,m}$, is defined by $\langle A, B\rangle_H = \mathrm{Tr}(A(B^t)^{(q)})$, where Tr denotes the trace of the matrix and B^t the transpose of B. It is easy to verify that $\langle\cdot,\cdot\rangle_H$ is a non-degenerate Hermitian form. The dual of the code $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ with respect to this form is denoted by $\mathcal{C}^{\perp_H}$. Since $\langle\cdot,\cdot\rangle_H$ is non-degenerate and reflexive, we have $\dim_{\mathbb{F}_{q^2}}(\mathcal{C}^{\perp_H}) = nm - \dim_{\mathbb{F}_{q^2}}(\mathcal{C})$ and $(\mathcal{C}^{\perp_H})^{\perp_H} = \mathcal{C}$.

A *Hermitian rank metric* $\mathbb{F}_{q^2}$*-linear code* is a rank metric code $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ equipped with the Hermitian form $\langle\cdot,\cdot\rangle_H$.

The *ordinary trace inner product* of two matrices $A = (a_{ij}) \in (\mathbb{F}_{q^2})_{n,m}$ and $B = (b_{ij}) \in (\mathbb{F}_{q^2})_{n,m}$, is defined by $\langle A, B\rangle_E = \mathrm{Tr}(A(B^t))$ and the dual of the code $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ with respect to this Euclidean form is denoted by $\mathcal{C}^{\perp_E}$.

Remark 1: Throughout the paper, we always assume $2 \leq n \leq m$.

Similarly, as in classical coding theory, the rank distribution of $\mathcal{C}$ is the collection $A_0(\mathcal{C}), \ldots, A_n(\mathcal{C})$, where $A_i(\mathcal{C}) := |\{A \in \mathcal{C} : rank(A) = i\}|$ for $i \in \{0, \ldots, n\}$.

In [13] Delsarte established a bound for the minimum rank distance of a code similar to the Singleton bound for Hamming distance:

Theorem 1: (Rank Singleton bound) *Let* $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ *be an* $\mathbb{F}_{q^2}$*-linear code of dimension t with minimum distance d. Then we have*

$$d \leq n - t/m + 1.$$

Rank metric codes meeting the Singleton bound are called *Maximum Rank Distance* (MRD) codes. Delsarte was the first who proved in [13] the existence of $\mathbb{F}_{q^2}$-linear MRD codes.

Using the MacWilliams Identities for the Euclidean form we can prove the following lemma.

Lemma 3: Let $\mathcal{C}$ *and* $\mathcal{D}$ *be two t-dimensional rank metric codes in* $(\mathbb{F}_Q)_{n,m}$ *with the same rank distribution. Then* $\mathcal{C}^{\perp_E}$ *and* $\mathcal{D}^{\perp_E}$ *have the same rank distribution.*

Proof: Let $(A_i(\mathcal{C}))_{0\leq i\leq n}$ and $(A_i(\mathcal{D}))_{0\leq i\leq n}$ be the rank distribution of $\mathcal{C}$ and $\mathcal{D}$, respectively and let $A_i(\mathcal{C}) = A_i(\mathcal{D})$ for all $i \in \{0, \ldots, n\}$. For any integer $0 \leq r \leq n$, we have $\sum_{i=0}^{n-r}\begin{bmatrix} n-i \\ r \end{bmatrix}A_i(\mathcal{C}) = Q^{t-mr}\left(\sum_{j=0}^{r-1}\begin{bmatrix} n-j \\ r-j \end{bmatrix}B_j(\mathcal{C}^{\perp_E}) + B_r(\mathcal{C}^{\perp_E})\right)$. Assume

$$B_j(\mathcal{C}^{\perp_E}) = B_j(\mathcal{D}^{\perp_E})$$

for $j < r$. Then

$$\sum_{i=0}^{n-r}\begin{bmatrix} n-i \\ r \end{bmatrix}A_i(\mathcal{D}) = Q^{t-mr}\left(\sum_{j=0}^{r-1}\begin{bmatrix} n-j \\ r-j \end{bmatrix}B_j(\mathcal{D}^{\perp_E}) + B_r(\mathcal{C}^{\perp_E})\right)$$

and we have $B_r(\mathcal{C}^{\perp_E}) = B_r(\mathcal{D}^{\perp_E})$. □

Remark 2: Let $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ *be an* $\mathbb{F}_{q^2}$*-linear rank code. Since* $\mathcal{C}$ *and* $\mathcal{C}^{(q)}$ *have the same rank distribution and* $\mathcal{C}^{\perp_H} = (\mathcal{C}^{(q)})^{\perp_E}$*, we get by Lemma 3 that* $\mathcal{C}^{\perp_E}$ *and* $\mathcal{C}^{\perp_H}$ *have the same rank distribution.*

By the previous remark the MacWilliams Identities are also valid for Hermitian rank metric codes. We state this direct consequence in the following corollary, which would be useful for some applications.

Corollary 1: (Hermitian MacWilliams Identities) *Let* $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ *be an* $\mathbb{F}_{q^2}$*-linear Hermitian rank code of dimension t. Let* $(A_i)_{0\leq i\leq n}$ *and* $(B_i)_{0\leq i\leq n}$ *be the rank distribution of* $\mathcal{C}$ *and* $\mathcal{C}^{\perp_H}$*, respectively. For any integer* $0 \leq r \leq n$*, we have*

$$\sum_{i=0}^{n-r}\begin{bmatrix} n-i \\ r \end{bmatrix}A_i(\mathcal{C}) = (q^2)^{t-mr}\sum_{j=0}^{r}\begin{bmatrix} n-j \\ r-j \end{bmatrix}B_j(\mathcal{C}^{\perp_H}).$$

Remark 3: Note that if $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ *is an MRD code, then by Remark 2 we have that* $\mathcal{C}^{\perp_H}$ *is also an MRD code.*

IV. HERMITIAN $\mathbb{F}_{q^2}$-ADDITIVE AND $\mathbb{F}_{q^{2m}}$-LINEAR RANK METRIC CODES

The field $\mathbb{F}_{q^{2m}}$ may be viewed as an m-dimensional vector space over $\mathbb{F}_{q^2}$. The *rank* of a vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^{2m}}^n$ is defined as the maximum number of coordinates in v that are linearly independent over $\mathbb{F}_{q^2}$, i.e. $rank(v) := \dim_{\mathbb{F}_{q^2}}\langle v_1, \ldots, v_n\rangle$. Then we have a rank metric distance given by $\mathrm{d}(v, u) = rank(v - u)$ for $v, u \in \mathbb{F}_{q^{2m}}^n$. A $\mathbb{F}_{q^{2m}}$-linear subspace $C \leq \mathbb{F}_{q^{2m}}^n$ of dimension k endowed with this metric is called a $\mathbb{F}_{q^{2m}}$*-linear rank metric* $[n, k]$ code.

On the other hand, a $\mathbb{F}_{q^2}$-additive code $C \subseteq \mathbb{F}_{q^{2m}}^n$ of dimension t over $\mathbb{F}_{q^2}$ endowed with the rank metric is called a $\mathbb{F}_{q^2}$*-additive rank metric* $[nm, t]$ code. In this case the dimension of C over $\mathbb{F}_{q^{2m}}$ is defined as the number k such that $(q^{2m})^k = |C|$. Note that k is not necessarily an integer and $k = \frac{t}{m}$.

The *minimum distance* of a rank metric code $C \neq \{0\}$, denoted by $d(C)$, is the smallest rank distance between any pair of distinct codewords. If $C \leq \mathbb{F}_{q^{2m}}^n$ is an $\mathbb{F}_{q^2}$-additive code of dimension t over $\mathbb{F}_{q^2}$ with minimum distance d, then $d \leq n - t/m + 1$. In particular if $C \leq \mathbb{F}_{q^{2m}}^n$ is an $\mathbb{F}_{q^{2m}}$-linear code of dimension k, then $d \leq n - k + 1$. $\mathbb{F}_{q^2}$-additive or $\mathbb{F}_{q^{2m}}$-linear rank metric codes meeting this bound are equally called Maximum Rank Distance (MRD) codes.

Given a vector $v = (v_1, \dots, v_n) \in \mathbb{F}_{q^{2m}}^n$ we denote by $M_k(v) \in (\mathbb{F}_{q^{2m}})_{k,n}$ the matrix

$$M_k(v) = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1^{[1]_{q^2}} & v_2^{[1]_{q^2}} & \dots & v_n^{[1]_{q^2}} \\ & & \vdots & \\ v_1^{[k-1]_{q^2}} & v_2^{[k-1]_{q^2}} & \dots & v_n^{[k-1]_{q^2}} \end{pmatrix}, \quad (1)$$

where $[i]_{q^2} := (q^2)^i$.

Gabidulin showed in [14] that if $v_1, \dots, v_n$ are linearly independent over $\mathbb{F}_{q^2}$, then the $\mathbb{F}_{q^{2m}}$-linear code $C \leq \mathbb{F}_{q^{2m}}^n$ generated by the matrix $M_k(v_1, \dots, v_n)$ is a k-dimensional MRD code and we call it the *Gabidulin code $\mathcal{G}_k(v)$ generated by $M_k(v_1, \dots, v_n)$.*

In $\mathbb{F}_{q^{2m}}^n$ we can define two different inner products: The ordinary Hermitian inner product $\langle \cdot, \cdot \rangle_H$ and the trace inner product $\langle \cdot, \cdot \rangle_{TH}$. More precisely we have.

Definition 1: For $v = (v_1, \dots, v_n)$, $u = (u_1, \dots, u_n) \in \mathbb{F}_{q^{2m}}^n$ we define

1) *$\langle v, u \rangle_H = \sum_{i=1}^n v_i u_i^{q^m} \in \mathbb{F}_{q^{2m}}$ (ordinary Hermitian inner product)*
2) *$\langle v, u \rangle_{TH} = \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}} \left(\sum_{i=1}^n v_i u_i^{q^m} \right) \in \mathbb{F}_{q^2}$ (trace Hermitian inner product).*

Lemma 4: The following facts hold.

1) *The map $\langle \cdot, \cdot \rangle_H$ is a Hermitian non-degenerate form.*
2) *If m is a odd integer, then the map $\langle \cdot, \cdot \rangle_{TH}$ is a Hermitian non-degenerate form. Otherwise, $\langle \cdot, \cdot \rangle_{TH}$ is a Euclidean form.*

Proof:

1) Let $\sigma : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ be the automorphism of $\mathbb{F}_{q^2}$ defined by $\sigma(\alpha) := \alpha^{q^m}$ for all $\alpha \in \mathbb{F}_{q^2}$ and $\widehat{\sigma}$ the extension of σ over the field $\mathbb{F}_{q^{2m}}$. It is easy to verify that $\langle \cdot, \cdot \rangle_H$ is a $\widehat{\sigma}$-sesquilinear non-degenerate form. Moreover $\widehat{\sigma}$ is the Frobenius automorphism of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$, which is an involution.
2) Without difficulty we see that $\langle \cdot, \cdot \rangle_{TH}$ is a σ-sesquilinear form, where $\sigma : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ is the automorphism of $\mathbb{F}_{q^2}$ defined by $\sigma(\alpha) := \alpha^{q^m}$ for all $\alpha \in \mathbb{F}_{q^2}$. We prove that $\langle \cdot, \cdot \rangle_{TH}$ is also non-degenerate. Let $u \in \mathbb{F}_{q^{2m}}^n$ and $\langle v, u \rangle_{TH} = 0$ for all $v \in \mathbb{F}_{q^{2m}}^n$. Suppose that $u \neq 0$ with $u_j \neq 0$ for a some $j \in \{1, \dots, n\}$. Then we have that $u_j^{q^m} \neq 0$. Since $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}$ is a non-zero map and $\mathbb{F}_{q^{2m}} = \{z u_j^{q^m} : z \in \mathbb{F}_{q^{2m}}\}$, there exists $z u_j^{q^m} \in \mathbb{F}_{q^{2m}}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(z u_j^{q^m}) \neq 0$. Let $v \in \mathbb{F}_{q^{2m}}^n$ with $v_j = z u_j^{q^m}$ and $v_i = 0$ for all $i \neq j$. Then, $\langle v, u \rangle_{TH} = \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(z u_j^{q^m}) \neq 0$, a contradiction.
On the other hand, if m is an odd integer, then for all $x \in \mathbb{F}_{q^2}$ we have $x^{q^m - q} = x^{q(q^{m-1}-1)} = x^{q(q^2-1)s} = 1$, where $s \in \mathbb{N}$, since $m-1$ is even and $q^2 - 1 | q^{m-1} - 1$. Hence $\sigma(\alpha) = \alpha^{q^m} = \alpha^q$ for all $\alpha \in \mathbb{F}_{q^2}$ and $\mathrm{ord}(\sigma) = 2$. As $\langle v, u \rangle_{TH} = \sigma(\langle u, v \rangle_{TH})$ the form is Hermitian. In the case that m is even, then $\mathrm{ord}(\sigma) = 1$.

□

A *Hermitian $\mathbb{F}_{q^2}$-additive code* (*Hermitian $\mathbb{F}_{q^{2m}}$-linear code*) is an $\mathbb{F}_{q^2}$-additive ($\mathbb{F}_{q^{2m}}$-linear) rank metric code $C \leq \mathbb{F}_{q^{2m}}^n$ equipped with the Hermitian form $\langle \cdot, \cdot \rangle_{TH}$ ($\langle \cdot, \cdot \rangle_H$). We denoted by $C^{\perp_{TH}}$ and $C^{\perp_H}$ the dual code of C with respect to the trace Hermitian inner product and to the ordinary Hermitian inner product respectively.

Lemma 5: Let C be a subset of $\mathbb{F}_{q^{2m}}^n$. Then we have

1) *$C^{\perp_H}$ is an $\mathbb{F}_{q^2}$-vector subspace of $C^{\perp_{TH}}$.*
2) *If C is an $\mathbb{F}_{q^2}$-additive code, then $\dim_{\mathbb{F}_{q^2}}(C^{\perp_{TH}}) = nm - \dim_{\mathbb{F}_{q^2}}(C)$. Similarly, if C is an $\mathbb{F}_{q^{2m}}$-linear code, then $\dim_{\mathbb{F}_{q^{2m}}}(C^{\perp_H}) = n - \dim_{\mathbb{F}_{q^{2m}}}(C)$.*
3) *If C is an $\mathbb{F}_{q^{2m}}$-linear code, then $C^{\perp_H} = C^{\perp_{TH}}$.*

Proof: The proof of part 1 and part 2 is immediate. By part 1 we have that $C^{\perp_H} \subseteq C^{\perp_{TH}}$. On the other hand, by part 2 we have

$$\begin{aligned} \dim_{\mathbb{F}_{q^2}}(C^{\perp_H}) &= m \cdot \dim_{\mathbb{F}_{q^{2m}}}(C^{\perp_H}) = m(n - \dim_{\mathbb{F}_{q^{2m}}}(C)) \\ &= mn - \dim_{\mathbb{F}_{q^2}}(C) = \dim_{\mathbb{F}_{q^2}}(C^{\perp_{TH}}), \end{aligned}$$

so part 3 follows. □

Remark 4:

1) *Note that the map $\langle \cdot, \cdot \rangle : \mathbb{F}_{q^{2m}} \times \mathbb{F}_{q^{2m}} \longrightarrow \mathbb{F}_{q^2}$ defined as $\langle a, b \rangle := \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(a b^{q^m})$ is a non-degenerated σ-sesquilinear form, where $\sigma(\alpha) = \alpha^{q^m}$ for all $\alpha \in \mathbb{F}_{q^2}$. Therefore, if $\mathcal{B}$ is a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and $G_{\mathcal{B}}$ is the Gram matrix of $\langle \cdot, \cdot \rangle$, then $G_{\mathcal{B}}$ is nonsingular in $(\mathbb{F}_{q^2})_m$. In particular, if m is an odd integer, then the map $\langle \cdot, \cdot \rangle$ is a Hermitian form, since $\sigma(\alpha) = \alpha^{q^m} = \alpha^q$ for all $\alpha \in \mathbb{F}_{q^2}$. For m an even integer, $\langle \cdot, \cdot \rangle$ is a Euclidean form.*
2) *Moreover, note that if $v = (v_1, \dots, v_n)$, $u = (u_1, \dots, u_n) \in \mathbb{F}_{q^{2m}}^n$, then*

$$\langle v, u \rangle_{TH} = \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\langle v, u \rangle_H) = \sum_{i=1}^n \langle v_i, u_i \rangle.$$

Definition 2: Let $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ and $\mathcal{B}' = \{\beta'_1, \dots, \beta'_m\}$ be two bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. If $\langle \beta'_i, \beta_j \rangle = \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\beta'_i \beta_j^{q^m}) = \delta_{ij}$ for all $i, j \in \{1, \dots, m\}$, then the bases $\mathcal{B}$ and $\mathcal{B}'$ are said to be q^m-dual to each other. Moreover, a basis $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ is called a q^m-self-dual basis if $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\beta_i \beta_j^{q^m}) = \delta_{ij}$, for all $i, j \in \{1, \dots, m\}$.

Remember that bases $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ and $\mathcal{B}^* = \{\beta_1^*, \dots, \beta_m^*\}$ are said dual if $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\beta_i^* \beta_j) = \delta_{ij}$ for all $i, j \in \{1, \dots, m\}$. In the case that $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\beta_i \beta_j) = \delta_{ij}$ for all $i, j \in \{1, \dots, m\}$ we say that $\mathcal{B}$ is self-dual. It is well known that any basis $\mathcal{B}$ of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ has a dual basis $\mathcal{B}^*$ which is unique. This result also holds for q^m-duality. In fact, if $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ is a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$, then the unique dual basis $\mathcal{B}' = \{\beta'_1, \dots, \beta'_m\}$ to the basis $\mathcal{B}^{q^m} := \{\beta_1^{q^m}, \dots, \beta_m^{q^m}\}$ is q^m-dual to $\mathcal{B}$.

Lemma 6: Let $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ be a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$, $G_{\mathcal{B}}$ the Gram matrix of the σ-sesquilinear form $\langle a, b \rangle := \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(a b^{q^m})$ with respect to the basis $\mathcal{B}$, where $\sigma(\alpha) = \alpha^{q^m}$ for all $\alpha \in \mathbb{F}_{q^2}$ and let $M_k(v) \in (\mathbb{F}_{q^{2m}})_{k,n}$ the matrix (1) *for all vectors* $v=(v_1,\dots,v_n)\in\mathbb{F}_{q^{2m}}^n$ *and* $1\leq k\leq n$. *Then we have:*

1) $G_{\mathcal{B}}=M_m(\overline{\mathcal{B}})^*M_m(\overline{\mathcal{B}})$.
2) *The basis* $\mathcal{B}=\{\beta_1,\dots,\beta_m\}$ *is a* q^m*-self-dual basis of* $\mathbb{F}_{q^{2m}}$ *over* $\mathbb{F}_{q^2}$ *if and only if* $M_m(\overline{\mathcal{B}})^*M_m(\overline{\mathcal{B}})=I_m$, *where* $\overline{\mathcal{B}}:=(\beta_1,\dots,\beta_m)\in\mathbb{F}_{q^{2m}}^m$.
3) $[\det(M_m(\overline{\mathcal{B}}))]^{q^2}=(-1)^{m-1}\det(M_m(\overline{\mathcal{B}}))$.

Proof:

1) Let $S:=M_m(\overline{\mathcal{B}})^*M_m(\overline{\mathcal{B}})$. If we denote the entry of matrix S at position (i,j) by s_{ij}, then

$$\begin{aligned}s_{ij}&=\sum_{k=1}^{m}(\beta_i^{[k-1]_{q^2}})^{q^m}\beta_j^{[k-1]_{q^2}}\\&=\sum_{k=1}^{m}(\beta_i^{q^m}\beta_j)^{[k-1]_{q^2}}\\&=\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\beta_i^{q^m}\beta_j).\end{aligned}$$

2) The statement follows from part 1.
3) From the proof of Lemma 2 we know that $[\det(M_m(\overline{\mathcal{B}}))]^{q^2}=\det\left(M_m(\overline{\mathcal{B}})^{(q^2)}\right)$. Furthermore

$$\det\left(M_m(\overline{\mathcal{B}})^{(q^2)}\right)=\begin{vmatrix}\beta_1^{[1]_{q^2}}&\beta_2^{[1]_{q^2}}&\dots&\beta_m^{[1]_{q^2}}\\\vdots&\vdots&\vdots&\vdots\\\beta_1^{[m-1]_{q^2}}&\beta_2^{[m-1]_{q^2}}&\dots&\beta_m^{[m-1]_{q^2}}\\\beta_1&\beta_2&\dots&\beta_m\end{vmatrix}\tag{2}$$

and

$$\det(M_m(\overline{\mathcal{B}}))=\begin{vmatrix}\beta_1&\beta_2&\dots&\beta_m\\\beta_1^{[1]_{q^2}}&\beta_2^{[1]_{q^2}}&\dots&\beta_m^{[1]_{q^2}}\\\vdots&\vdots&\vdots&\vdots\\\beta_1^{[m-1]_{q^2}}&\beta_2^{[m-1]_{q^2}}&\dots&\beta_m^{[m-1]_{q^2}}\end{vmatrix}.$$

By swapping the last row of (2) $(m-1)$-times, we get $\det\left(M_m(\overline{\mathcal{B}})^{(q^2)}\right)=(-1)^{m-1}\det(M_m(\overline{\mathcal{B}}))$.

□

Let $\mathcal{B}=\{\beta_1,\dots,\beta_m\}$ be a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and $v=(v_1,\dots,v_n)\in\mathbb{F}_{q^{2m}}^n$. If $v_i=\sum_{j=1}^{m}\lambda_{ij}\beta_j$, where $\lambda_{ij}\in\mathbb{F}_{q^2}$ and $1\leq i\leq n$, the *associated matrix* of v with respect to the basis $\mathcal{B}$, is defined as $\lambda_{\mathcal{B}}(v):=(\lambda_{ij})_{n,m}\in(\mathbb{F}_{q^2})_{n,m}$. Note $v=\overline{\mathcal{B}}\lambda_{\mathcal{B}}(v)^T$, for all $v=(v_1,\dots,v_n)\in\mathbb{F}_{q^{2m}}^n$, where $\overline{\mathcal{B}}:=(\beta_1,\dots,\beta_m)\in\mathbb{F}_{q^{2m}}^m$. Therefore $\lambda_{\mathcal{B}}(v)^{(q^m)}=\lambda_{\mathcal{B}^{(q^m)}}(v^{(q^m)})$. The map $\mathbb{F}_{q^{2m}}^n\ni v\longmapsto\lambda_{\mathcal{B}}(v)\in(\mathbb{F}_{q^2})_{n,m}$ is an invertible $\mathbb{F}_{q^2}$-linear transformation and an invertible isometry i.e. $d(v,u)=d(\lambda_{\mathcal{B}}(v),\lambda_{\mathcal{B}}(u))$ for all $v,u\in\mathbb{F}_{q^{2m}}^n$.

Lemma 7: Let $\mathcal{B}=\{\beta_1,\dots,\beta_m\}$ *and* $\mathcal{B}'=\{\beta_1',\dots,\beta_m'\}$ *be two* q^m*-self-dual bases of* $\mathbb{F}_{q^{2m}}$ *over* $\mathbb{F}_{q^2}$. *If* $a=\sum_{i=1}^m x_i\beta_i'$, $b=\sum_{j=1}^m y_j\beta_j\in\mathbb{F}_{q^{2m}}$, *where* $(x_1,\dots,x_m)$, $(y_1,\dots,y_m)\in\mathbb{F}_{q^2}^m$, *then* $\langle a,b\rangle=\sum_{k=1}^m x_ky_k^{q^m}$.

Proof:

$$\begin{aligned}\langle a,b\rangle&=\langle\sum_{i=1}^{m}x_i\beta_i',\sum_{j=1}^{m}y_j\beta_j\rangle\\&=\sum_{i=1}^{m}\sum_{j=1}^{m}a_ib_j^{q^m}\langle\beta_i',\beta_j\rangle=\sum_{k=1}^{m}x_ky_k^{q^m}.\end{aligned}$$

□

It is well known that a dual basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ always exits, but a self-dual basis exits if and only if q^2 is even or both q^2 and m are odd (see [21]). With respect to the existence of a q^m-dual basis we have the following result.

Theorem 2: There exists a q^m*-self-dual basis of* $\mathbb{F}_{q^{2m}}$ *over* $\mathbb{F}_{q^2}$ *if and only if* m *is an odd integer.*

Proof: Let m be an odd integer and let $\mathcal{A}=\{\alpha_1,\dots,\alpha_m\}$ be a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. Moreover, let $G_{\mathcal{A}}$ be the Gram matrix with respect to the basis $\mathcal{A}$ of the σ-sesquilinear form $\langle a,b\rangle:=\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(ab^{q^m})$, where $\sigma(\alpha)=\alpha^{q^m}$ for all $\alpha\in\mathbb{F}_{q^2}$. By Remark 4 (1) we know that $G_{\mathcal{A}}$ is a nonsingular Hermitian matrix in $(\mathbb{F}_{q^2})_m$. Therefore by Lemma 2 (2) there exists a nonsingular matrix $H=(h_{ij})_m\in(\mathbb{F}_{q^2})_m$ such that $H^*G_{\mathcal{A}}H=I_m$. Define $\beta_j=\sum_{i=1}^m\alpha_ih_{ij}$ for $j=1,\dots,m$. We can prove that $\mathcal{B}=\{\beta_1,\dots,\beta_m\}$ is a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and $M_m(\overline{\mathcal{B}})=M_m(\overline{\mathcal{A}})H$, where $\overline{\mathcal{A}}:=(\alpha_1,\dots,\alpha_m)\in\mathbb{F}_{q^{2m}}^m$ and $\overline{\mathcal{B}}:=(\beta_1,\dots,\beta_m)\in\mathbb{F}_{q^{2m}}^m$. By Lemma 6 (1) we know that $G_{\mathcal{A}}=M_m(\overline{\mathcal{A}})^*M_m(\overline{\mathcal{A}})$, therefore

$$\begin{aligned}(M_m(\overline{\mathcal{B}}))^*M_m(\overline{\mathcal{B}})&=H^*(M_m(\overline{\mathcal{A}}))^*M_m(\overline{\mathcal{A}})H\\&=H^*G_{\mathcal{A}}H=I_m.\end{aligned}$$

Hence by Lemma 6 (2), $\mathcal{B}$ is a q^m-self-dual basis.

On the other hand, let m be an even integer and let $\mathrm{char}(\mathbb{F}_{q^2})$ be an odd integer. Suppose that there exists a q^m-self-dual basis $\mathcal{B}=\{\beta_1,\dots,\beta_m\}$. If $\mathcal{A}=\{\alpha_1,\dots,\alpha_m\}$ is also a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and $\beta_j=\sum_{i=1}^m\alpha_is_{ij}$, where $s_{ij}\in\mathbb{F}_{q^2}$, for $j\in\{1,\dots,m\}$, then we have

$$\begin{aligned}\delta_{ij}&=\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\beta_i\beta_j^{q^m})\\&=\sum_{k=1}^{m}\sum_{l=1}^{m}s_{ki}\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\alpha_k\alpha_l^{q^m})s_{lj}^{q^m}.\end{aligned}$$

Since $x^{q^m}=x$ for all $x\in\mathbb{F}_{q^2}$, we have $\delta_{ij}=\sum_{k=1}^m\sum_{l=1}^m s_{ki}\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\alpha_k\alpha_l^{q^m})s_{lj}$. Therefore $I_m=S^tG_{\mathcal{A}}S$, where $S:=(s_{ij})_m\in\mathrm{GL}_m(\mathbb{F}_{q^2})$. Thus $\det(G_{\mathcal{A}})\in(\mathbb{F}_{q^2}^{\times})^2$. By Lemma 1 and Remark 4 (1), we can also argue in the reverse direction. Hence there exists a q^m-self-dual basis $\mathcal{B}$ if and only if there exists a basis $\mathcal{A}$ such that $\det(G_{\mathcal{A}})\in(\mathbb{F}_{q^2}^{\times})^2$. By Lemma 6 (1) we have $G_{\mathcal{A}}=M_m(\overline{\mathcal{A}})^*M_m(\overline{\mathcal{A}})$.

Therefore by Lemma 2 (1), we have $\det(G_{\mathcal{A}}) = [\det(M_m(\overline{\mathcal{A}}))]^{q^m+1}$. We know that

$$\begin{aligned}[\det(M_m(\overline{\mathcal{A}}))]^{q^2} &= (-1)^{m-1}\det(M_m(\overline{\mathcal{A}}))\\ &= -\det(M_m(\overline{\mathcal{A}}))\\ &\neq \det(M_m(\overline{\mathcal{A}})),\end{aligned}$$

i.e. $y := \det(M_m(\overline{\mathcal{A}})) \notin \mathbb{F}_{q^2}$. If there exits $x \in \mathbb{F}_{q^2}^{\times}$ such that $y^{q^{m+1}} = x^2$, then

$$y = (y^{q^{m+1}})^{q^{m-1}} = (x^2)^{q^{m-1}} \in \mathbb{F}_{q^2},$$

a contradiction.

Finally, let m be an even integer and let $\operatorname{char}(\mathbb{F}_{q^2})$ be an even integer. Then for all basis $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ we have that the entries of the main diagonal of the Gram matrix $G_{\mathcal{B}}$ are zero. Indeed, let $x_i := \beta_i^{q^m+1}$ for all $i = 1, \dots, m$. Since $x_i^{q^m-1} = 1$, we have that $x_i \in \mathbb{F}_{q^m}$. Therefore $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^m}}(x_i) = 2x = 0$. As m is an even integer, then $\mathbb{F}_{q^2}$ is a subfield of $\mathbb{F}_{q^m}$. Hence for the transitive property of the trace we have

$$\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(x_i) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^2}}(\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^m}}(x_i)) = 0.$$

□

Definition 3: If $C \leq \mathbb{F}_{q^{2m}}^n$ is a Hermitian $\mathbb{F}_{q^2}$-additive or $\mathbb{F}_{q^{2m}}$-linear rank metric code, then we define the $\mathbb{F}_{q^2}$-linear Hermitian code associated to the code C with respect to the basis $\mathcal{B}$ as

$$\lambda_{\mathcal{B}}(C) = \{\lambda_{\mathcal{B}}(v) : v \in C\} \leq (\mathbb{F}_{q^2})_{n,m}.$$

Since $\lambda_{\mathcal{B}}$ is an invertible isometry, then $d(C) = d(\lambda_{\mathcal{B}}(C))$ and $A_i(\lambda_{\mathcal{B}}(C)) = A_i(C)$ for $i = 1, \dots, n$. Moreover, $\lambda_{\mathcal{B}}$ is an invertible $\mathbb{F}_{q^2}$-linear transformation, therefore we have $\dim_{\mathbb{F}_{q^2}}(\lambda_{\mathcal{B}}(C)) = \dim_{\mathbb{F}_{q^2}}(C)$ for all $\mathbb{F}_{q^2}$-additive rank metric code C. In particular, $\dim_{\mathbb{F}_{q^2}}(\lambda_{\mathcal{B}}(C)) = m \cdot \dim_{\mathbb{F}_{q^{2m}}}(C) = \dim_{\mathbb{F}_{q^2}}(C)$ for an $\mathbb{F}_{q^{2m}}$-linear rank metric code C.

Remark 5: Using $\lambda_{\mathcal{B}}$ we can see that every $\mathbb{F}_{q^2}$-additive code or $\mathbb{F}_{q^{2m}}$-linear code can be seen as an $\mathbb{F}_{q^2}$-linear matrix code. In general not every $\mathbb{F}_{q^2}$-linear matrix code $\mathcal{C} \leq (\mathbb{F}_{q^2})_{n,m}$ arises from an $\mathbb{F}_{q^{2m}}$-linear code, for example when $(q^{2m}-1) \nmid A_i(\mathcal{C})$ for all $i = 1, \dots, n$. However, there is always an $\mathbb{F}_{q^2}$-additive code $C \leq \mathbb{F}_{q^{2m}}^n$ such that $\lambda_{\mathcal{B}}(C) = \mathcal{C}$.

An interesting question is how $\lambda_{\mathcal{B}}$ behaves in relation to the duality defined with the Hermitian form. Indeed, if we can prove that there is an invertible isometry $\varphi : \mathbb{F}_{q^{2m}}^n \longrightarrow (\mathbb{F}_{q^2})_{n,m}$ such that $\varphi(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_H}$, then the Hermitian $\mathbb{F}_{q^2}$-additive codes satisfy the MacWilliams Identities (in particular the $\mathbb{F}_{q^{2m}}$-linear codes). The reason is that, in this case, we have $B_i(C^{\perp_{TH}}) = B_i(\varphi(C^{\perp_{TH}})) = B_i(\lambda_{\mathcal{B}}(C)^{\perp_H})$ for all $i = 0, \dots, n$ and since $A_i(C) = A_i(\lambda_{\beta}(C))$ for all $i = 0, \dots, n$, we would be able to apply Corollary 1, which is valid for $\mathbb{F}_{q^2}$-linear matrix codes. Theorem 3 (1) shows that for an odd integer m given a basis $\mathcal{B}$ of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$, the map $v \longmapsto \lambda_{\mathcal{B}'}(v)$ where $\mathcal{B}'$ is a basis q^m-dual to $\mathcal{B}$ is the desired invertible isometry. In fact, if m is an odd integer, then $\lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_H}$.

Proposition 1: Let $\mathcal{B}$ and $\mathcal{B}'$ be q^m-dual bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and $v, u \in \mathbb{F}_{q^{2m}}^n$.

1) *If m is an odd integer, then $\langle v, u\rangle_{TH} =: \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\langle v, u\rangle_H) = \langle \lambda_{\mathcal{B}'}(v), \lambda_{\mathcal{B}}(u)\rangle_H$.*
2) *If m is an even integer, then $\langle v, u\rangle_{TH} =: \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\langle v, u\rangle_H) = \langle \lambda_{\mathcal{B}'}(v), \lambda_{\mathcal{B}}(u)\rangle_E$.*

Proof: Let $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ and $\mathcal{B}' = \{\beta_1', \dots, \beta_m'\}$ be two q^m-dual bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. Let $v, u \in \mathbb{F}_{q^{2m}}^n$ such that $(x_{ij}) = \lambda_{\mathcal{B}'}(v)$ and $(y_{ij}) = \lambda_{\mathcal{B}}(u)$ i.e. $v_i = \sum_{j=1}^m x_{ij}\beta_j'$ and $u_i = \sum_{k=1}^m y_{ik}\beta_k$.

Then by Remark 4 (2) and Lemma 7 we have

$$\begin{aligned}\langle v, u\rangle_{TH} &= \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\langle v, u\rangle_H) = \sum_{i=1}^{n}\langle v_i, u_i\rangle\\ &= \sum_{i=1}^{n}\sum_{l=1}^{m} x_{il}y_{il}^{q^m} = \mathrm{Tr}\left(\lambda_{\mathcal{B}'}(v)\left(\lambda_{\mathcal{B}}(u)^t\right)^{q^m}\right).\end{aligned}$$

If m is an odd integer, then $\left(\lambda_{\mathcal{B}}(u)^t\right)^{q^m} = \left(\lambda_{\mathcal{B}}(u)^t\right)^q$. For m an even integer we have $\left(\lambda_{\mathcal{B}}(u)^t\right)^{q^m} = \lambda_{\mathcal{B}}(u)^t$.

□

The following result was independently established in [15], [17], [27] for Euclidean rank metric codes and dual bases. Now we show a version for Hermitian rank metric codes and q^m-dual bases.

Theorem 3: Let $C \leq \mathbb{F}_{q^{2m}}^n$ be an $\mathbb{F}_{q^2}$-additive code, $\mathcal{B}$ and $\mathcal{B}'$ q^m-dual bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. Then the following hold:

1) *If m is an odd integer, then*

$$\lambda_{\mathcal{B}'}(C^{\perp_H}) \leq \lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_H}.$$

In particular, if $C \leq \mathbb{F}_{q^{2m}}^n$ is an $\mathbb{F}_{q^{2m}}$-linear code, we have

$$\lambda_{\mathcal{B}'}(C^{\perp_H}) = \lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_H}.$$

2) *If m is an even integer, then*

$$\lambda_{\mathcal{B}'}(C^{\perp_H}) \leq \lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_E}.$$

In particular, if $C \leq \mathbb{F}_{q^{2m}}^n$ is an $\mathbb{F}_{q^{2m}}$-linear code, we have

$$\lambda_{\mathcal{B}'}(C^{\perp_H}) = \lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_E}.$$

Proof: Let $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ and $\mathcal{B}' = \{\beta_1', \dots, \beta_m'\}$ be two q^m-dual bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. By Lemma 5 (1) it is clear that $\lambda_{\mathcal{B}'}(C^{\perp_H}) \leq \lambda_{\mathcal{B}'}(C^{\perp_{TH}})$ for all $\mathbb{F}_{q^2}$-additive code C. Suppose $\lambda_{\mathcal{B}'}(v) \in \lambda_{\mathcal{B}'}(C^{\perp_{TH}})$ and $\lambda_{\mathcal{B}}(u) \in \lambda_{\mathcal{B}}(C)$, where $v \in C^{\perp_{TH}}$ and $u \in C$. By Proposition 1 (1) we have

$$\langle \lambda_{\mathcal{B}'}(v), \lambda_{\mathcal{B}}(u)\rangle_H = \langle v, u\rangle_{TH} = 0.$$

Therefore $\lambda_{\mathcal{B}'}(C^{\perp_{TH}}) \leq \lambda_{\mathcal{B}}(C)^{\perp_H}$. By Lemma 5 (2) we have $\dim_{\mathbb{F}_{q^2}} \lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \dim_{\mathbb{F}_{q^2}}(\lambda_{\mathcal{B}}(C)^{\perp_H})$. Hence $\lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_H}$.

Similarly, by Proposition 1 (2) we have

$$\langle \lambda_{\mathcal{B}'}(v), \lambda_{\mathcal{B}}(u)\rangle_E = \langle v, u\rangle_{TH} = 0.$$

Therefore $\lambda_{\mathcal{B}'}(C^{\perp_{TH}}) \le \lambda_{\mathcal{B}}(C)^{\perp_E}$. Since

$$\begin{aligned}\dim_{\mathbb{F}_{q^2}}(\lambda_{\mathcal{B}}(C)^{\perp_E}) &= nm - \dim_{\mathbb{F}_{q^2}} \lambda_{\mathcal{B}}(C)\\ &= nm - \dim_{\mathbb{F}_{q^2}}(C)\\ &= \dim_{\mathbb{F}_{q^2}} \lambda_{\mathcal{B}'}(C^{\perp_{TH}}),\end{aligned}$$

we have $\lambda_{\mathcal{B}'}(C^{\perp_{TH}}) = \lambda_{\mathcal{B}}(C)^{\perp_E}$.

In particular, if C is an $\mathbb{F}_{q^{2m}}$-linear code, then by Lemma 5 (3) we have $\lambda_{\mathcal{B}'}(C^{\perp_H}) = \lambda_{\mathcal{B}'}(C^{\perp_{TH}})$. Hence parts 1 and 2 are complete. □

Corollary 2: Let $(A_i)_{0\le i\le n}$ and $(B_i)_{0\le i\le n}$ be the rank distribution of an $\mathbb{F}_{q^2}$-additive ($\mathbb{F}_{q^{2m}}$-linear) rank metric code $C \le \mathbb{F}_{q^{2m}}^n$ and $C^{\perp_{TH}}$ ($C^{\perp_H}$), respectively. For any integer $0 \le r \le n$, we have

$$\sum_{i=0}^{n-r}\begin{bmatrix}n-i\\ r\end{bmatrix}A_i = \frac{|C|}{q^{2mr}}\sum_{j=0}^{r}\begin{bmatrix}n-j\\ r-j\end{bmatrix}B_j,$$

which we call the Hermitian MacWilliams Identities.

Proof: Let m be an odd integer. By Theorem 3 (1) we have $B_i(C^{\perp_{TH}}) = B_i(\lambda_{\mathcal{B}'}(C^{\perp_{TH}}))$ $= B_i(\lambda_{\mathcal{B}}(C)^{\perp_H})$ for all $i = 0, \dots, n$. Moreover $A_i(C) = A_i(\lambda_{\beta}(C))$ for all $i = 0, \dots, n$, therefore by Corollary 1 we are done. On the other hand, let m be an even integer. By Theorem 3 (2) we have $B_i(C^{\perp_{TH}}) = B_i(\lambda_{\mathcal{B}'}(C^{\perp_{TH}})) = B_i(\lambda_{\mathcal{B}}(C)^{\perp_E})$ for all $i = 0, \dots, n$. But $B_i(\lambda_{\mathcal{B}}(C)^{\perp_E}) = B_i(\lambda_{\mathcal{B}}(C)^{\perp_H})$ by Remark 2. Again by Corollary 1 the sentence follows. □

Example 1: A classical linear code $C \le \mathbb{K}^n$ is called linear complementary dual, or shortly an LCD code, if $\mathbb{K}^n = C \oplus C^{\perp_E}$ [23]. Classical LCD codes are of particular interest because the class of LCD codes is asymptotically good [23] and achieves the Gilbert-Varshamov bound [28]. Furthermore the codes play a crucial role in information protection [6]. A $\mathbb{F}_{q^m}$-linear rank metric code $C \le \mathbb{F}_{q^{2m}}^n$ is called a rank Hermitian LCD code (rank metric code with Hermitian complementary dual) if $C \oplus C^{\perp_H} = \mathbb{F}_{q^{2m}}^n$. In [12] the authors investigate and characterize ideals in the group algebra $\mathbb{K}G$ which have complementary duals, i.e., ideals C in $\mathbb{K}G$ that satisfy $\mathbb{K}G = C \oplus C^{\perp_E}$. Similarly as in the Euclidean case, we can prove that $C \le \mathbb{F}_{q^{2m}}^n$ is a Hermitian LCD code if and only if GG^* is nonsingular, where $G \in (\mathbb{F}_{q^{2m}})_{k,n}$ is a generator matrix of C. Additionally, we say that an $\mathbb{F}_{q^2}$-linear rank metric matrix code $\mathcal{C} \le (\mathbb{F}_{q^2})_{n,m}$ is a rank Hermitian LCD code if $\mathcal{C} \oplus \mathcal{C}^{\perp_H} = (\mathbb{F}_{q^2})_{n,m}$. If m is an odd integer and $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ is a q^m-self-dual basis, then, by applying Theorem 3 (1), we see that $C \le \mathbb{F}_{q^{2m}}^n$ is a rank Hermitian LCD code if and only if $\lambda_{\mathcal{B}}(C)$ is a rank Hermitian LCD code. Moreover, by Lemma 6 (1), $M_m(\overline{\mathcal{B}})^* M_m(\overline{\mathcal{B}}) = I_m$. Therefore $\mathcal{G}_k(\overline{\mathcal{B}})$ is an MRD LCD code.

Example 2: Let $\alpha \in \mathbb{F}_{q^{2m}}$. Then the map $\Upsilon_\alpha : \mathbb{F}_{q^{2m}} \longmapsto \mathbb{F}_{q^{2m}}$ defined by $\Upsilon_\alpha(x) = \alpha x$ for all $x \in \mathbb{F}_{q^{2m}}$ is an $\mathbb{F}_{q^2}$-linear transformation. We have that the associated basis of Υ_α with respect to the basis $\mathcal{B}$ is $\lambda_{\mathcal{B}}(\alpha\overline{\mathcal{B}})$. Moreover we can prove that $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\alpha) = \mathrm{Tr}(\lambda_{\mathcal{B}}(\alpha\overline{\mathcal{B}}))$ for all $\alpha \in \mathbb{F}_{q^{2m}}$, actually this is a usual alternative definition for the trace of an element α (see [7]). Let m be an odd integer and let $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ a q^m-self-dual basis. We know that if $C \le \mathbb{F}_{q^{2m}}^m$, then $I_m \in \lambda_{\mathcal{B}}(C) \iff \overline{\mathcal{B}} \in C$. Therefore, if $C := \mathcal{G}_1(\overline{\mathcal{B}})$, by Theorem 3 (1) we have

$$\begin{aligned}\overline{\mathcal{B}} \in C^{\perp_H} &\iff I_m \in \lambda_{\mathcal{B}}(C^{\perp_H}) = \lambda_{\mathcal{B}}(C)^{\perp_H}\\ &\iff \mathrm{Tr}(\lambda_{\mathcal{B}}(\alpha\overline{\mathcal{B}})) = 0\\ &\iff \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}(\alpha) = 0\end{aligned}$$

for all $\alpha \in \mathbb{F}_{q^{2m}}$. Hence $\overline{\mathcal{B}} \notin \mathcal{G}_1(\overline{\mathcal{B}})^{\perp_H}$ and $I_m \notin \lambda_{\mathcal{B}}(\mathcal{G}_1(\overline{\mathcal{B}}))^{\perp_H}$ i.e. $\mathcal{G}_1(\overline{\mathcal{B}})$ and $\lambda_{\mathcal{B}}(\mathcal{G}_1(\overline{\mathcal{B}}))$ are not self-orthogonal codes.

In the rest of this section we present a connection of certain Hermitian LCD, Hermitian self-dual and Hermitian self-orthogonal codes in the ambient spaces $\mathbb{F}_{q^{2m}}^n$ and $(\mathbb{F}_{q^2})_{n,m}$. We start with a simple lemma.

Lemma 8: Let $C \le \mathbb{F}_{q^{2m}}^n$ be an $\mathbb{F}_{q^{2m}}$-linear code. Then we have the following:

1) *C is Hermitian LCD if and only if C is trace Hermitian LCD.*
2) *C is Hermitian self-dual if and only if C is trace Hermitian self-dual.*
3) *C is Hermitian self-orthogonal if and only if C is trace Hermitian self-orthogonal.*

Proof: The results follow immediately using Lemma 5 item 3. □

Now we give our connection for m is odd.

Theorem 4: Let $m \ge 1$ be an odd integer. Let $C \le \mathbb{F}_{q^{2m}}^n$ be an $\mathbb{F}_{q^{2m}}$-linear code. Let $\mathcal{B}$ be an q^m-self dual basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. Then the following hold:

1) *$\lambda_{\mathcal{B}}(C)$ is Hermitian LCD $\iff$ C is Hermitian LCD $\iff$ C is trace Hermitian LCD.*
2) *$\lambda_{\mathcal{B}}(C)$ is Hermitian self-dual $\iff$ C is Hermitian self-dual $\iff$ C is trace Hermitian self-dual.*
3) *$\lambda_{\mathcal{B}}(C)$ is Hermitian self-orthogonal $\iff$ C is Hermitian self-orthogonal $\iff$ C is trace Hermitian self-orthogonal.*

Proof: As $\mathcal{B}$ is q^m-self-dual basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$, using Theorem 3 we have

$$\lambda_{\mathcal{B}}(C^{\perp_H}) = \lambda_{\mathcal{B}}(C)^{\perp_H}.$$

Hence we obtain that

$$\lambda_{\mathcal{B}}(C)^{\perp_H} \cap \lambda_{\mathcal{B}}(C) = \lambda_{\mathcal{B}}\left(C^{\perp_H}\right) \cap \lambda_{\mathcal{B}}(C) = \lambda_{\mathcal{B}}\left(C^{\perp_H} \cap C\right).$$

This completes the proof that $\lambda_{\mathcal{B}}(C)$ is Hermitian LCD (respectively Hermitian self-dual and Hermitian self-orthogonal) if and only if C is Hermitian LCD (resp. Hermitian self-dual and Hermitian self-orthogonal). The part corresponding to trace Hermitian follows from Lemma 8. □

V. CONNECTIONS WITH EUCLIDEAN $\mathbb{F}_{q^2}$-ADDITIVE CODES

In this section we present connections between Hermitian $\mathbb{F}_{q^2}$-additive codes and Euclidean $\mathbb{F}_{q^2}$-additive codes in $\mathbb{F}_{q^{2m}}^n$. The following result is elementary but crucial for this section.

Lemma 9: Let C be an $\mathbb{F}_{q^2}$-additive rank metric codes in $\mathbb{F}^n_{q^{2m}}$. Then $C^{(q^m)}$ is an $\mathbb{F}_{q^2}$-additive rank metric code and C and $C^{(q^m)}$ have the same rank distribution.

Proof: $A_i(C) = A_i(\lambda_{\mathcal{B}}(C)) = A_i(\lambda_{\mathcal{B}}(C)^{(q^m)})$, for all $i = 0, \ldots, n$. Since $\lambda_{\mathcal{B}}(C)^{(q^m)} = \lambda_{\mathcal{B}^{(q^m)}}(C^{(q^m)})$, we have $A_i(C) = A_i(\lambda_{\mathcal{B}^{(q^m)}}(C^{(q^m)})) = A_i(\lambda_{\mathcal{B}}(C^{(q^m)})) = A_i(C^{(q^m)})$, for all $i = 0, \ldots, n$.

□

Remark 6: If C and D are two $\mathbb{F}_{q^{2m}}$-linear rank metric codes in $\mathbb{F}^n_{q^{2m}}$ with the same rank distribution, then $C^{\perp_E}$ and $D^{\perp_E}$ have the same rank distribution. Indeed, if $A_i(C) = A_i(D)$ for all $i = 0, \ldots, n$, then $A_i(\lambda_{\mathcal{B}}(C)) = A_i(\lambda_{\mathcal{B}}(D))$. By Lemma 3 we have $B_i(\lambda_{\mathcal{B}}(C)^{\perp_E}) = B_i(\lambda_{\mathcal{B}}(D)^{\perp_E})$ for all $i = 0, \ldots, n$. Since $\lambda_{\mathcal{B}}(C')^{\perp_E}$ and $C'^{\perp_E}$ have the same rank distribution for all $\mathbb{F}_{q^{2m}}$-linear code $C' \leq \mathbb{F}^n_{q^{2m}}$, we have $B_i(C^{\perp_E}) = B_i(D^{\perp_E})$ for all $i = 0, \ldots, n$. On the other hand, by Lemma 9 we have that C and $C^{(q^m)}$ have the same rank distribution. Moreover $C^{\perp_H} = (C^{(q^m)})^{\perp_E}$. Therefore $C^{\perp_E}$ and $C^{\perp_H}$ have the same rank distribution. Hence the MacWilliams Identities are valid for $\mathbb{F}_{q^{2m}}$-linear Hermitian rank metric codes as the Corollary 2 also shows.

In order to establish similar results to those given in Lemma 3, Remark 2 and Remark 6, for $\mathbb{F}_{q^2}$-additive codes in $\mathbb{F}^n_{q^{2m}}$, we define a new inner product, the trace Euclidean product $\langle \cdot, \cdot \rangle_{TE}$.

Definition 4: We define the trace Euclidean inner product of $v = (v_1, \ldots, v_n) \in \mathbb{F}^n_{q^{2m}}$ and $u = (u_1, \ldots, u_n) \in \mathbb{F}^n_{q^{2m}}$ as

$$\langle v, u \rangle_{TE} = \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}} \left(\sum_{i=1}^{n} v_i u_i \right) \in \mathbb{F}_{q^2}.$$

The trace Euclidean product $\langle \cdot, \cdot \rangle_{TE}$ gives rise to a non-degenerated Euclidean form. Moreover, we have the following result, whose proof is similar to that of Theorem 3.

Theorem 5: Let $C \leq \mathbb{F}^n_{q^{2m}}$ be an $\mathbb{F}_{q^2}$-additive code, $\mathcal{B}$ and $\mathcal{B}^*$ dual bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. The following hold:

$$\lambda_{\mathcal{B}^*}(C^{\perp_E}) \leq \lambda_{\mathcal{B}^*}(C^{\perp_{TE}}) = \lambda_{\mathcal{B}}(C)^{\perp_E}.$$

In particular, if $C \leq \mathbb{F}^n_{q^{2m}}$ is an $\mathbb{F}_{q^{2m}}$-linear code, we have

$$\lambda_{\mathcal{B}^*}(C^{\perp_E}) = \lambda_{\mathcal{B}^*}(C^{\perp_{TE}}) = \lambda_{\mathcal{B}}(C)^{\perp_E}.$$

Corollary 3: Let C and D be two rank $\mathbb{F}_{q^2}$-additive rank metric codes in $\mathbb{F}^n_{q^{2m}}$ with the same rank distribution. Then $\mathcal{C}^{\perp_{TE}}$ and $\mathcal{D}^{\perp_{TE}}$ have the same rank distribution.

Proof: Let $A_i(C) = A_i(D)$ for all $i = 0, \ldots, n$. Then $A_i(\lambda_{\mathcal{B}}(C)) = A_i(C) = A_i(D) = A_i(\lambda_{\mathcal{B}}(D))$. Therefore by Lemma 3 we have $B_i(\lambda_{\mathcal{B}}(C)^{\perp_E}) = B_i(\lambda_{\mathcal{B}}(D)^{\perp_E})$. Moreover, by Theorem 5 we have $B_i(C^{\perp_{TE}}) = B_i(\lambda_{\mathcal{B}^*}(C^{\perp_{TE}})) = B_i(\lambda_{\mathcal{B}}(C)^{\perp_E})$ for all $i = 0, \ldots, n$. Similarly $B_i(D^{\perp_{TE}}) = B_i(\lambda_{\mathcal{B}}(D)^{\perp_E})$ for all $i = 0, \ldots, n$.

□

Remark 7: Let $C \leq \mathbb{F}^n_{q^{2m}}$ an $\mathbb{F}_{q^2}$-additive code. Since C and $C^{(q^m)}$ have the same rank distribution and $C^{\perp_{TH}} = (C^{(q^m)})^{\perp_{TE}}$, then by Corollary 3, $C^{\perp_{TE}}$ and $C^{\perp_{TH}}$ have the same rank distribution. In particular, the MacWilliams Identities are valid for $\mathbb{F}_{q^2}$-linear Hermitian rank metric codes as we already know from Corollary 2.

VI. CONCLUSION

In this paper we study $\mathbb{F}_{q^2}$-additive and $\mathbb{F}_{q^{2m}}$-linear codes in the ambient spaces $\mathbb{F}^n_{q^{2m}}$ and $(\mathbb{F}_{q^2})_{n,m}$ endowed with Hermitian forms and suitable rank metrics. We extend many results for such codes in the literature obtained for Euclidean forms to Hermitian forms. In order to study the dual codes with respect to Hermitian forms, we introduce the concept of a q^m-self dual basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and we completely characterize them. We obtain many connections in between these codes in the ambient spaces $\mathbb{F}^n_{q^{2m}}$ and $(\mathbb{F}_{q^2})_{n,m}$ and their Hermitian duals. As consequences, we obtain results on Hermitian LCD, self-dual and self-orthogonal codes in both of these ambient spaces. Furthermore we obtain Hermitian MacWilliams Identities for $\mathbb{F}_{q^2}$-additive and $\mathbb{F}_{q^{2m}}$-linear codes endowed with Hermitian form in these ambient spaces.

For future studies, it would be interesting to construct optimal Hermitian LCD and self-dual codes in $\mathbb{F}^n_{q^{2m}}$ and $(\mathbb{F}_{q^2})_{n,m}$ with the corresponding rank metrics systematically for nontrivial parameters. These codes have potential applications in many areas including network coding, symmetric cryptography, and code-based cryptography. Hence it is worth finding fast decoding algorithms for these codes. Also it natural to expect designs of countermeasure protocols for side-channel attacks on cryptographic systems using these rank metric codes, which require further investigation.

ACKNOWLEDGMENT

Javier de la Cruz was with the University of Magdeburg. The authors are very grateful to Wolfgang Willems for the valuable discussions.

REFERENCES

[1] F. Arias, J. de la Cruz, J. Rosenthal, and W. Willems, "On q-analog Steiner systems of rank metric codes," *Discrete Math.*, vol. 341, no. 10, pp. 2729–2734, Oct. 2018.

[2] E. Artin, *Geometric Algebra*. New York, NY, USA: Interscience, 1957.

[3] J. Bierbrauer, "Cyclic additive and quantum stabilizer codes," in *Proc. 1st Int. Workshop, WAIFI*, in Lecture Notes in Computer Science, vol. 4547, C. Carlet and B. Sunar, Eds., Madrid, Spain, Jun. 2007, pp. 276–283.

[4] E. Byrne and A. Ravagnani, "An Assmus–Mattson theorem for rank metric codes," *SIAM J. Discrete Math.*, vol. 33, no. 3, pp. 1242–1260, Jan. 2019.

[5] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via over $GF(4)$," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[6] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," *Adv. Math. Commun.*, vol. 10, no. 1, pp. 131–150, Mar. 2016.

[7] B. Conrad. *Norm and Trace*. Accessed: Sep. 15, 2020. [Online]. Available: http://math.stanford.edu/conrad/210BPage/handouts/normtrace.pdf

[8] L. E. Danielsen, "On the classification of hermitian self-dual additive codes over $GF(9)$," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5500–5511, Aug. 2012.

[9] J. de la Cruz, "On dually almost MRD codes," *Finite Fields Their Appl.*, vol. 53, pp. 1–20, Sep. 2018.

[10] J. de la Cruz, E. Gorla, H. H. López, and A. Ravagnani, "Weight distribution of rank-metric codes," *Des., Codes Cryptogr.*, vol. 86, no. 1, pp. 1–16, Jan. 2018.

[11] W. Willems, A. Wassermann, M. Kiermaier, and J. D. L. Cruz, "Algebraic structures of MRD codes," *Adv. Math. Commun.*, vol. 10, no. 3, pp. 499–510, Aug. 2016.

[12] J. de la Cruz and W. Willems, "On group codes with complementary duals," *Des., Codes Cryptogr.*, vol. 86, no. 9, pp. 2065–2073, Sep. 2018.

[13] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Combinat. Theory A*, vol. 25, no. 3, pp. 226–241, Nov. 1978.

[14] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inf. Transmiss.*, vol. 21, no. 1, pp. 3–16, 1985.

[15] M. Gadouleau and Z. Yan, "Properties of rank metric codes," 2007, *arXiv:cs/0702077*. [Online]. Available: https://arxiv.org/abs/cs/0702077

[16] C. Güneri, F. Özbudak, and F. Özdemir, "Hasse–Weil bound for additive cyclic codes," *Des., Codes Cryptogr.*, vol. 82, nos. 1–2, pp. 249–263, Jan. 2017.

[17] D. Grant and M. K. Varanasi, "Duality theory for space-time codes over finite fields," *Adv. Math. Commun.*, vol. 2, no. 1, pp. 35–54, 2005.

[18] R. M. Guralnick, "On the singular value decomposition over finite fields and orbits of GU×GU," 2018, *arXiv:1805.06999*. [Online]. Available: http://arxiv.org/abs/1805.06999

[19] W. C. Huffman, "Cyclic $\mathbb{F}_q$-linear F_{q^t}-codes," *Int. J. Inf. Coding Theory*, vol. 1, no. 3, pp. 249–284, 2010.

[20] W. C. Huffman, "On theory of $\mathbb{F}_q$-linear F_{q^t}-codes," *Adv. Math. Commun.*, vol. 7, no. 3, pp. 349–378, 2013.

[21] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM J. Comput.*, vol. 9, no. 4, pp. 758–767, Nov. 1980.

[22] W. K. Kadir and C. Li, "On decoding additive generalized twisted Gabidulin codes," *Cryptogr. Commun.*, vol. 12, no. 5, pp. 987–1009, Sep. 2020.

[23] J. L. Massey, "Linear codes with complementary duals," *Discrete Math.*, vols. 106–107, pp. 337–342, Sep. 1992.

[24] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal, "On the genericity of maximum rank distance and Gabidulin codes," *Des., Codes Cryptogr.*, vol. 86, no. 2, pp. 341–363, Feb. 2018.

[25] K. Otal and F. Özbudak, "Additive rank metric codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 164–168, Jan. 2017.

[26] K. Otal, F. Özbudak, and W. Willems, "Self-duality of generalized twisted Gabidulin codes," *Adv. Math. Commun.*, vol. 12, no. 4, pp. 707–721, 2018.

[27] A. Ravagnani, "Rank-metric codes and their duality theory," *Des., Codes Cryptogr.*, vol. 80, no. 1, pp. 197–216, Jul. 2016.

[28] N. Sendrier, "Linear codes with complementary duals meet the Gilbert–Varshamov bound," *Discrete Math.*, vol. 285, pp. 345–347, Aug. 2004.

[29] J. Sheekey, "A new family of linear maximum rank distance codes," *Adv. Math. Commun.*, vol. 10, no. 3, pp. 475–488, Aug. 2016.

[30] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5479–5490, Dec. 2009.

[31] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.

JAVIER DE LA CRUZ received the M.Sc. degree in mathematics from Universidad Nacional, Medellín, Colombia, in 2007, and the Ph.D. degree in mathematics from the University of Magdeburg, Germany, in 2012. From 2004 to 2008 and since 2012, he has been with the Department of Mathematics, Universidad del Norte, Barranquilla, Colombia. In 2016, he held a postdoctoral position with the University of Zurich, for one year. His primary research interest includes algebraic coding theory.

JORGE ROBINSON EVILLA received the M.Sc. degree in mathematics from Universidad Nacional, Medellín, Colombia, in 2007. He is currently pursuing the Ph.D. degree with Universidad del Norte. Since 2008, he has been with the Department of mathematics, Universidad del Atlántico. He is also a part-time Lecturer with Universidad del Norte. His primary research interest includes algebraic coding theory.

FERRUH ÖZBUDAK received the B.S. degree in electrical and electronics engineering and the Ph.D. degree in mathematics from Bilkent University, Ankara, Turkey, in 1993 and 1997, respectively. He is currently a Professor with Middle East Technical University, Ankara. His research interests include algebraic curves, codes, sequences, cryptography, finite fields, and finite rings.