Galois Hull Dimensions of Gabidulin Codes

Habibal Islam
School of Computer Science
University of St.Gallen
St. Gallen, Switzerland
habibal.islam@unisg.ch

Anna-Lena Horlemann
School of Computer Science
University of St.Gallen
St. Gallen, Switzerland
anna-lena.horlemann@unisg.ch

Abstract—For a prime power $q$, an integer $m$ and $0 \leq e \leq m - 1$ we study the $e$-Galois hull dimension of Gabidulin codes $G_k(\alpha)$ of length $m$ and dimension $k$ over $\mathbb{F}_{q^m}$. Using a self-dual basis $\alpha$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we first explicitly compute the hull dimension of $G_k(\alpha)$. Then a necessary and sufficient condition of $G_k(\alpha)$ to be linear complementary dual (LCD), self-orthogonal and self-dual will be provided. We prove the existence of $e$-Galois (where $e = \frac{m}{2}$) self-dual Gabidulin codes of length $m$ for even $q$, which is in contrast to the known fact that Euclidean self-dual Gabidulin codes do not exist for even $q$. As an application, we construct two classes of MDS entangled-assisted quantum error-correcting codes (MDS EAQECCs) whose parameters have more flexibility compared to known codes in this context.

Index Terms—Gabidulin code, Galois inner product, self-orthogonal code, LCD code, entangled-assisted quantum error-correcting code

I. INTRODUCTION

For a linear code $C$, the hull is defined by $\text{hull}(C) = C \cap C^\perp$, where $C^\perp$ is the dual code of $C$. The hull investigation is important for many reasons, for instance, codes having $\text{hull}(C) = \{0\}$ are said to be linear complementary dual (LCD) codes, introduced by Massey [26], and can be applied for preventing popular cryptographic attacks such as side channel and fault-injection attacks [4]. Codes satisfying $\text{hull}(C) = C$ (resp. $C^\perp$) are known as self-orthogonal (resp. dual-containing), in particular, codes having $\text{hull}(C) = C = C^\perp$ are called self-dual. These codes have some interesting applications in secret-sharing schemes and quantum coding, see [8], [19], [20]. Besides, the notion of hull dimension can be successfully applied for constructing quantum error-correcting codes [14], [23], [25], [35], and determining the computational complexity of algorithms for finding automorphism groups [21], or checking the equivalence (permutation) of two linear codes [22], [31]. Several studies on the hull dimension under popular inner products (e.g., Euclidean, Hermitian, etc.) can be found in the literature [11]. The $e$-Galois inner product (which generalizes both the Euclidean and the Hermitian) over $\mathbb{F}_{q^m}$ where $0 \leq e \leq m - 1$ has been introduced by Fan and Zhang in 2017 [9]. This inner product can also be applied for constructing quantum codes. However, so far there are only few studies on the $e$-Galois hull dimension (of generalized Reed-Solomon codes) and their application in quantum codes [2], [3], [10].

H. Islam is supported by the International Postdoctoral Fellowship (IPF) of the University of St.Gallen, Switzerland.

A special class of maximum distance separable (MDS) codes, called Gabidulin codes was introduced in [12]. Detailed surveys of Gabidulin codes and their (Euclidean/Hermitian) duality can be found in [6], [7], [15], [18], [29], [33]. Here, we investigate the $e$-Galois hull dimension of Gabidulin codes, in particular, by using a self-dual basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we obtain a necessary and sufficient condition for these codes to be LCD, self-orthogonal and self-dual. Unlike Euclidean self-dual Gabidulin codes [27], for $e = m/2$ we show that $e$-Galois self-dual Gabidulin codes exist for even $q$. Furthermore, we can construct MDS codes in $\mathbb{F}_{q^m}^m$ (whose $e$-Galois hull dimensions are calculated explicitly) of dimension $k > \lfloor \frac{p^e+m}{p+1} \rfloor$, where $p$ is the characteristic of the field, which was proposed as an open problem in [2], [3], [10]. At the end, using the $e$-Galois hull dimensions we obtain some classes of MDS entangled-assisted quantum error-correcting codes (MDS EAQECCs), among which some have dimensions $k > \lfloor \frac{p^e+m}{p+1} \rfloor$, and are hence not included in the codes that appeared in [2], [3], [10].

II. PRELIMINARIES

Let $q$ be a prime power and $\mathbb{F}_{q^m}$ be a field of order $q^m$. Let the elements of $\alpha = (\alpha_1, \ldots, \alpha_m)$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and denote by $\alpha^g := (\alpha_1^g, \ldots, \alpha_m^g)$ the coordinate-wise application of the Frobenius map. The Gabidulin code $G_k(\alpha)$ of length $m$ and dimension $k$ is defined by the generator matrix

$$G = \begin{pmatrix}
\alpha \\
\alpha^g \\
\alpha^{g^2} \\
\vdots \\
\alpha^{g^{k-1}}
\end{pmatrix}, \tag{1}
$$

see [12]. The Gabidulin code $G_k(\alpha)$ can also be defined as an evaluation code of linearized polynomials with evaluation points $\{\alpha_1, \ldots, \alpha_m\}$. It is a maximum rank distance (MRD) code, and hence also an MDS code, i.e., it has minimum Hamming distance $d = m - k + 1$. For more details on Gabidulin codes see [12], [24], [32].

Let $0 \leq e \leq m - 1$ and $x = (x_0, x_1, \ldots, x_{m-1})$, $y = (y_0, y_1, \ldots, y_{m-1}) \in \mathbb{F}_{q^m}^m$, we recall from [9] that the $e$-Galois inner product is defined by

$$x \cdot_e y := \sum_{i=0}^{m-1} x_i y_i^e.$$
For \( e = 0 \), it is the Euclidean and for \( e = \frac{m}{2} \) (when \( m \) is even), it is equivalent to the Hermitian inner product.

For a Gabidulin code \( G_k(\alpha) \) of length \( m \) over \( \mathbb{F}_{q^m} \), the \( e \)-Galois dual is defined by
\[
G_k(\alpha)^{⊥_e} := \{ x \in \mathbb{F}_{q^m}^m : x \cdot y = 0 \text{ for all } y \in G_k(\alpha) \}.
\]
Further, \( G_k(\alpha) \) is said to be self-orthogonal (resp. self-dual) if \( G_k(\alpha) \subseteq G_k(\alpha)^{⊥_e} \) (resp. \( G_k(\alpha) = G_k(\alpha)^{⊥_e} \)).

Let \( \alpha = \{ \alpha_1, \cdots, \alpha_m \} \) and \( \beta = \{ \beta_1, \cdots, \beta_m \} \) be two bases of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \). Then \( \beta \) is said to be a dual (orthogonal) basis of \( \alpha \) if \( Tr(\alpha_i \beta_j) = \delta_{ij} \), where \( Tr : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q \) is the usual trace function. When \( \alpha = \beta \), we call \( \alpha \) a self-dual basis.

Self-dual bases do not exist generally, the necessary and sufficient condition for their existence is given by the next result.

**Lemma II.1.** [30, 36] The vector space \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \) has a self-dual basis if and only if \( q \) and \( m \) both are odd.

We recall from [13, page 22-24] that for a Gabidulin code \( G_k(\alpha) \) of length \( m \), whose generator matrix is given by (1), there is a unique basis \( \beta = (\beta_1, \beta_2, \cdots, \beta_m) \) such that the transpose of the Moore matrix
\[
B = \begin{pmatrix}
\beta \\
\beta q \\
\vdots \\
\beta q^{m-1}
\end{pmatrix}
\]
is the inverse to the \( m \times m \) generator matrix \( G \) (in the form of (1)) of \( G_m(\alpha) \). Therefore, \( GB^T = B^T G = I \). Note that \( B^T G = I \) is the matrix representation of the original definition of dual basis given above, i.e., \( \beta \) is the dual basis to \( \alpha \). This dual basis defines a parity check matrix (i.e., a generator matrix of the Euclidean dual code) of \( G_k(\alpha) \) as
\[
H = \begin{pmatrix}
\beta^k \\
\beta^{k+1} \\
\vdots \\
\beta^{q^m-1}
\end{pmatrix}.
\]
Using the matrix \( H \) we now compute the generator matrix for \( G_k(\alpha)^{⊥_e} \) in the following.

**Theorem II.2.** Let \( G_k(\alpha) \) be a Gabidulin code of length \( m \) and dimension \( k \). Let \( \beta \) be the dual basis to \( \alpha \). Then a generator matrix of \( G_k(\alpha)^{⊥_e} \) is given by
\[
G_k(\alpha)^{⊥_e} = \begin{pmatrix}
\beta^{q^{k-e}} \\
\beta^{q^{k+e+1}} \\
\vdots \\
\beta^{q^{m-e-1}}
\end{pmatrix} = H^{t^{m-e}} = H^T = 0.
\]

**Proof.** We have
\[
G \cdot (G_k(\alpha)^{⊥_e})^T = G \cdot ((H^{t^{m-e}})^T)^T = G \cdot H^T = 0.
\]
Since \( G_k^{⊥_e} \) is the generator matrix of the Gabidulin code \( G_{m-k}(\beta^{q^{k-e}}) \), it has full rank and the statement follows.

### III. HULL DIMENSION OF \( G_k(\alpha) \)

Recall that the \( e \)-Galois hull of \( G_k(\alpha) \) is defined by \( \text{Hull}_e(G_k(\alpha)) = G_k(\alpha) \cap G_k(\alpha)^{⊥_e} \). Clearly, \( \text{Hull}_e(G_k(\alpha)) \) is a subspace of both \( G_k(\alpha) \) and \( G_k(\alpha)^{⊥_e} \). Therefore, \( G_k(\alpha) \) is LCD if and only if \( \dim (\text{Hull}_e(G_k(\alpha))) = 0 \), and self-orthogonal if and only if \( \dim (\text{Hull}_e(G_k(\alpha))) = \dim (G_k(\alpha)) = k \). In the following we compute the hull dimension of Gabidulin codes.

**Theorem III.1.** Let \( \alpha \) be a self-dual basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \), and \( G_k(\alpha) \) be aGabidulin code of length \( m \) and dimension \( k \). Then
\[
\dim (\text{Hull}_e(G_k(\alpha))) = \begin{cases} 
\min(m-k,e) & \text{if } 0 \leq e \leq k \\
\min(m-e,k) & \text{if } k+1 \leq e \leq m-1
\end{cases}
\]

**Proof.** Let \( 0 \leq e \leq k \). Thus \( q^{k-e} \geq q^0 \) and hence
\[
 \text{rk} \left( \begin{pmatrix} G_k & \alpha \\ \alpha q & \alpha q^{q^k-1} \\ \vdots & \vdots \\ \alpha q^{q^{m-e-2}} & \alpha q^{q^{m-e-2}} \\ \alpha q^{q^{m-e-1}} & \alpha q^{q^{m-e}} \end{pmatrix} \right) = \text{rk} \left( \begin{pmatrix} \alpha \\ \alpha q \\ \vdots \\ \alpha q^{q^{m-k-1}+1} \\ \alpha q^{q^{m-k}+1} \\ \vdots \\ \alpha q^{q^{m-k-1}+1} \end{pmatrix} \right) = \max(k,m-e).
\]
Therefore,
\[
\dim (\text{Hull}_e(G_k(\alpha))) = m - \max(k,m-e) = \min(m-k,e).
\]

On the other hand, let \( e \geq k+1 \). So \( q^{k-e} < q^0 \) and hence
\[
 \text{rk} \left( \begin{pmatrix} G_k & \alpha \\ \alpha q & \alpha q^{q^k-1} \\ \vdots & \vdots \\ \alpha q^{q^{m-e-2}} & \alpha q^{q^{m-e-2}} \\ \alpha q^{q^{m-e-1}} & \alpha q^{q^{m-e}} \end{pmatrix} \right) = \max(e,k-m) = \max(e,k-m).
\]
Thus,
\[
\dim (\text{Hull}_e(G_k(\alpha))) = m - \max(e,m-k) = \min(m-e,k).
\]

**Corollary III.1.** Let \( \alpha \) be a self-dual basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \), and \( G_k(\alpha) \) be a Gabidulin code of length \( m \) and dimension \( 1 \leq k \leq m-1 \). Then \( G_k(\alpha) \) is LCD if and only if \( e = 0 \).
Proof. Let \( G_k(\alpha) \) be a Gabidulin code of length \( m \) and dimension \( 1 \leq k \leq m - 1 \). Let \( e = 0 \). Then by Theorem III.1 we get \( \dim \left( \text{Hull}_e(\text{Hull}_c(G_k(\alpha))) \right) = \min(m - k, e) = 0 \). Hence \( G_k(\alpha) \) is LCD.

Conversely, let \( G_k(\alpha) \) be LCD. Then \( \dim \left( \text{Hull}_e(\text{Hull}_c(G_k(\alpha))) \right) = 0 \). Thus, \( k + 1 \leq e \leq m - 1 \) will never be the case. On the other hand, when \( 0 \leq e \leq k \), \( \min(m - k, e) = 0 \) implies \( e = 0 \), since \( m - k > 0 \).

Corollary III.2. Let \( \alpha \) be a self-dual basis of \( \mathbb{F}_q^m \) over \( \mathbb{F}_q \) and \( G_k(\alpha) \) a Gabidulin code of length \( m \) and dimension \( k \leq m - k \). Then \( G_k(\alpha) \) is \( e \)-Galois self-orthogonal if and only if either \( e = k \) or \( k + 1 \leq e \leq m - k \).

Proof. Let \( G_k(\alpha) \) be \( e \)-Galois self-orthogonal. Then \( G_k(\alpha) \subseteq G_k(\alpha)^{\perp} \) and hence \( \dim \left( \text{Hull}_e(\text{Hull}_c(G_k(\alpha))) \right) = k \). We distinguish two cases:

Case (a): When \( 0 \leq e \leq k \), we have by Theorem III.1 that \( \dim \left( \text{Hull}_e(\text{Hull}_c(G_k(\alpha))) \right) = \min(m - k, e) = e = k \), since \( e \leq k \leq m - k \).

Case (b): When \( k + 1 \leq e \leq m - 1 \), we have by Theorem III.1 that \( \dim \left( \text{Hull}_e(\text{Hull}_c(G_k(\alpha))) \right) = \min(m - e, k) = k \) which implies \( m \geq k + e \).

Conversely, for (a), let \( e = k \leq \frac{m}{2} \). Now, Theorem III.1 gives \( \dim \left( \text{Hull}_e(\text{Hull}_c(G_k(\alpha))) \right) = \min(m - k, e) = e = k \). Therefore, \( G_k(\alpha) \) is \( e \)-Galois self-orthogonal.

In case (b), let \( k + 1 \leq e \leq m - k \). Then Theorem III.1 gives \( \dim \left( \text{Hull}_e(\text{Hull}_c(G_k(\alpha))) \right) = \min(m - e, k) = k \). Thus, \( G_k(\alpha) \) is \( e \)-Galois self-orthogonal.

Corollary III.3. Let \( m \) be even. Let \( \alpha \) be a self-dual basis of \( \mathbb{F}_q^m \) over \( \mathbb{F}_q \), and \( G_k(\alpha) \) be a Gabidulin code of length \( m \), dimension \( k = \frac{m}{2} \). Then \( G_k(\alpha) \) is \( e \)-Galois self-orthogonal if and only if \( e = \frac{m}{2} \).

Proof. It follows from Corollary III.2 with \( e = k = \frac{m}{2} \).

Before we give an example we need to recall a known fact.

Lemma III.2. [5], [26] Let \( C \) be a linear code of length \( m \) over \( \mathbb{F}_q \) with the generator matrix \( G \).

1) \( C \) is Euclidean LCD if and only if \( GG^\top \) is non-singular.
2) \( C \) is Hermitian self-dual if and only if \( m \) is even and \( GG^\top \) is the zero matrix, where \( G := G^{m/2} \).

Example III.1. Let \( q = 2 \), \( m = 4 \) and \( \omega \) be a primitive element of \( \mathbb{F}_{2^4} \), where \( \omega^4 = \omega + 1 \). Then \( \{1, \omega, \omega^2, \omega^3\} = \{\beta_1, \beta_2, \beta_3, \beta_4\} \) is a basis of \( \mathbb{F}_{2^4} \) over \( \mathbb{F}_2 \). The matrix \( M = (M_{ij})_{4 \times 4} \) with \( \text{Tr}(\beta_i \beta_j) = M_{ij} \) is given by

\[
M = \begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1
\end{pmatrix}.
\]

Then we have \( EME^\top = I_4 \), where

\[
E = \begin{pmatrix}
1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1
\end{pmatrix}.
\]

Therefore, the self-dual basis \( \alpha = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{1 + \omega^4, \omega + \omega^3, \omega^2 + \omega^3, \omega + \omega^2 + \omega^3\} \) is calculated by \( \sum_{j=1}^{4} E_{ij} \beta_j \). The Gabidulin code \( G_2(\alpha) \) based on the self-dual basis \( \alpha \) is defined by the generator matrix

\[
G = \begin{pmatrix}
1 + \omega^3 & \omega + \omega^3 & \omega^2 + \omega^3 & \omega + \omega^2 + \omega^3 \\
1 + \omega^4 & \omega^2 + \omega^3 & \omega^4 + \omega^3 & \omega^2 + \omega^4 + \omega^6
\end{pmatrix} = \left( \begin{array}{c} \alpha \\ \alpha^2 \end{array} \right).
\]

Now, we verify our results on the \( e \)-Galois hull for \( e = 0, 1, 2, 3 \).

1) Let \( e = 0 \). Then \( GG^\top = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \), a non-singular matrix. Thus, by Lemma III.2 \( G_2(\alpha) \) is an Euclidean LCD code, which verifies Corollary III.1.

2) Let \( e = 1 \). Then \( G^{e+1} = \left( \begin{array}{c} \alpha^2 \\ \alpha^4 \end{array} \right) = \left( \begin{array}{c} \alpha^2 \\ \alpha^4 \end{array} \right) \), and hence

\[
k(\begin{array}{c} G \\ G^{e+1} \end{array}) = k(\begin{array}{c} \alpha \\ \alpha^2 \end{array}) = 3,
\]

i.e., \( \dim \left( \text{Hull}_1(\text{Hull}_c(G_k(\alpha))) \right) = 4 - 3 = 1 = \min(m - k, e) \), which verifies Theorem III.1.

3) Let \( e = 2 \). Then we have

\[
G = G^2 = G^4 = \begin{pmatrix}
1 + \omega^{12} & \omega^4 + \omega^{12} & \omega^8 + \omega^{12} & \omega^4 + \omega^8 + \omega^{12} \\
1 + \omega^{24} & \omega^8 + \omega^{24} & \omega^4 + \omega^8 + \omega^{24}
\end{pmatrix}
\]

and \( GG^\top = O_{2 \times 2} \). Therefore, by Lemma III.2 \( G_2(\alpha) \) is Hermitian self-dual, which verifies Corollary III.3.

4) Let \( e = 3 \). Then \( G^{e+3} = \left( \begin{array}{c} \alpha^3 \\ \alpha^8 \end{array} \right) = \left( \begin{array}{c} \alpha^3 \\ \alpha^8 \end{array} \right) \) and hence

\[
k(\begin{array}{c} G \\ G^{e+3} \end{array}) = k(\begin{array}{c} \alpha \\ \alpha^3 \end{array}) = 3,
\]

i.e., \( \dim \left( \text{Hull}_3(\text{Hull}_c(G_k(\alpha))) \right) = 4 - 3 = 1 = \min(m - k, e) \), which verifies Theorem III.1.

To conclude this section we want to set our results into the context of known results and open problems in the literature. Recently, in [2], [3], [10], the \( e \)-Galois hulls of generalized Reed-Solomon (GRS) codes were determined, whose dimensions are always upper bounded by \( \lfloor \frac{m + e}{2} \rfloor \). As per our knowledge, it is still an open problem to find MDS codes of larger dimensions whose corresponding \( e \)-Galois hull dimensions are known.
Problem III.1. [2], [3], [10] Let $p$ be the characteristic of $\mathbb{F}_q$. Can we construct MDS codes in $\mathbb{F}_q^n$ of dimension $k$, such that $|\frac{p^n+m}{p^n+1}| < k \leq \left|\frac{p^n}{2}\right|$, of which we can determine the dimensions of their $e$-Galois hulls?

With our result we give a solution to Problem III.1, since Theorem III.1 is valid for any $0 \leq k \leq m$. To be precise we need $q$ and $m$ be such that a self-dual basis exists, but on the other hand our codes’ dimensions are not upper bounded.

Solution to Problem III.1. Let $q$ be even or both $q$ and $m$ be odd, and let $\alpha$ be a self-dual basis of $\mathbb{F}_q^m$ over $\mathbb{F}_q$. The Gabidulin code $G_k(\alpha)$ is an MDS code of length $m$ and dimension $k$ of which the dimensions of all $e$-Galois hulls are determined by Theorem III.1.

Example III.2. Let $q^m = 3^{15}$ and $m = 15$. Following the existence result of self-dual bases given by Lemma II.1, let $\alpha$ be a self-dual basis of $\mathbb{F}_3^{15}$ over $\mathbb{F}_3$, and $G_k(\alpha)$ a Gabidulin code of length $15$ and arbitrary dimension $1 \leq k \leq 15$. For $e \geq 3$, we get $|\frac{p^n+1}{p}+m| = 1$. Hence, for $1 < k \leq 15$, $G_k(\alpha)$ is an MDS code of dimension $k > |\frac{p^n+1}{p}+m|$ whose $e$-Galois hull dimensions are completely determined by Theorem III.1. Similarly, for $e = 2$ (respectively $e = 1$) we get previously unknown code parameters for $k > 2$ (respectively $k > 4$).

Even though Gabidulin codes require a large extension field degree (in particular, $m \geq n$), we would like to point out the possible application of Gabidulin codes in constructing entanglement-assisted quantum error-correcting codes (abbreviated as EAEQECs) over $\mathbb{F}_{q^m}$. Brun et al. [1] introduced the concept of entanglement-assisted quantum error-correcting codes by using pre-shared maximally entangled states between sender and receiver. The notation $[[n, k; d; c]]_{q^m}$ EAEQCC refers to a $q^m$-ary quantum code of minimum distance $d$ which encodes $k$ logical qubits into $n$ physical qubits and where $c$ maximally entangled states have been pre-shared. In particular, for $c = 0$ it is a standard quantum code [28], [34]. The Singleton-type bounds for the parameters of a EAEQCC are given in [16] as $k \leq n - d + 1$ and, for $d - 1 \leq \frac{n}{2}$

$$k \leq c + \text{max}(0, n - 2d + 2) = c + n - 2d + 2, \quad (3)$$

whereas for $d - 1 \geq \frac{n}{2}$

$$k \leq \min\left\{c, \frac{(n - d + 1)(c + 2d - 2 - n)}{3d - 3 - n}\right\}.$$ 

Codes attaining (the lower of the applicable) above bounds with equality are called MDS EAEQCCs.

EAEQCCs can be constructed from classical linear codes based on the parity check matrix (see, [17], [23]) and by using the $e$-Galois hull dimensions, see [2], [3], [10].

Lemma III.3. [2, Proposition IV.1] For a linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension $k$ and minimum distance $d$, there exists an EAQECC of parameters $[[n, k - \dim(Hull_k(C)), d; n - k - \dim(Hull_k(C))]]_{q^m}$.

In the light of Lemma III.3 and Theorem III.1 we can construct EAEQCCs of the following parameters.

Theorem III.4. Let $\alpha$ be a self-dual basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and $G_k(\alpha)$ a Gabidulin code of length $m$.

1) For $0 \leq e \leq k$ there exists an $[[m, k - e, m - k - 1; m - k - e + 1]]_{q^m}$ EAQECC, where $e = \min(m - k, e)$.
2) For $k + 1 \leq e \leq m - 1$ there exists an $[[m, k - e, m - k + 1; m - k - e]]_{q^m}$ EAQECC, where $e = \min(m - m - e, k)$.

Note that in Theorem III.4, for $d - 1 \leq \frac{m}{2}$ we get $k \geq \left\lceil\frac{m}{2}\right\rceil$, and the codes satisfy the bound (3) with equality and are hence MDS EAEQCCs. It is worth mentioning that [2], [3], [10] also constructed (MDS) EAEQCCs using the $e$-Galois hull dimension, but their codes have dimension $k$ upper bounded by $|\frac{p^n+1}{p}+m|$ or $|\frac{p^n+1}{p}+m|$, where $q = p^n$ and $2e \not| h$. Since in our case $k$ has no such restriction, the code parameters in Theorem III.4 are more flexible than those of previously known constructions based on the $e$-Galois hull.

IV. CONCLUSION

We investigated the $e$-Galois hulls of Gabidulin codes constructed from self-dual bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The dimensions of their $e$-Galois hull can be determined with a very easy formula, for any $0 \leq e \leq m - 1$. Since self-dual bases exist if and only if $q$ is even, or both $q$ and $m$ are odd (see Lemma II.1), we have hence established a large family of MDS codes for which all $e$-Galois hull dimensions are known. This had previously been posed as an open problem for MDS codes of (relatively) large dimension. Furthermore, we can construct entanglement-assisted quantum error-correcting codes from these Gabidulin codes.

It is interesting to see that the relation of a code to its $e$-Galois dual code depends heavily on the parameter $e$. In particular, we showed that Gabidulin codes generated by a self-dual (finite extension field) basis are always self-dual with respect to the Hermitian inner product, i.e., for $e = \frac{m}{2}$. Note that for the existence of a self-dual basis we need $q$ to be even in this case. In contrast, for the Euclidean inner product, i.e. $e = 0$, it was shown in [27] that self-dual Gabidulin codes (or any other maximum rank distance (MRD) codes) do not exist for even $q$.

In this paper, we focused on Gabidulin codes $G_k(\alpha)$ generated by a self-dual basis vector $\alpha$. In future work we will investigate the hull dimension of $G_k(\alpha)$ for other, non-self-dual, bases $\alpha$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Moreover, we will study other properties of dual codes with respect to the $e$-Galois inner product, as e.g. MacWilliams identities. Furthermore, since we know that for small $e$, the codes studied in this paper have a small $e$-Galois hull dimension, we want to study the performance of the known algorithms for computing automorphism groups or checking the equivalence of codes when using the $e$-Galois product in them, for $e \neq 0$.

ACKNOWLEDGMENTS

The authors thank Markus Grassl for his constructive comments on an earlier version of this work.
REFERENCES

[1] T. A. Brun, I. Devetak, and M.H. Hsieh, “Catalytic quantum error correction”, IEEE Trans. Inf. Theory, vol. 60, no. 6, pp. 3073–3089, Jun. 2014.

[2] M. Cao, “MDS codes with Galois hulls of arbitrary dimensions and the related entanglement-assisted quantum error correction”, IEEE Trans. Inf. Theory, vol. 67, no. 12, pp. 7964-7984, Dec. 2021.

[3] M. Cao, “Galois hulls of MDS codes and their quantum error correction”, arXiv:2002.12892v2 [cs.IT]. Apr. 2020.

[4] C. Carlet, and S. Guilley, “Complementary dual codes for countermeasures to side-channel attacks”, Adv. Math. Commun., vol. 10, no. 1, pp. 131–150, 2016.

[5] C. Carlet, S. Mesnager, C. Tang, and Y. Qi, “Euclidean and Hermitian LCD MDS codes”, Des. Codes Cryptogr., vol. 86, pp. 2605–2618, 2018.

[6] J. de la Cruz, “On dually almost MRD codes”, Finite Fields Appl., vol. 53, pp. 1-20, 2018.

[7] J. de la Cruz, J. R. Evilla, and F. Ozbudak, “Hermitian rank metric codes and duality”, IEEE Access, vol. 9, pp. 38479–38487, 2021.

[8] S. T. Dougherty, S. Mesnager, and P. Sole, “Secret-sharing schemes based on self-dual codes”, IEEE Information Theory Workshop. IEEE, pp. 338–342, 2008.

[9] Y. Fan, and L. Zhang, “Galois self-dual constacyclic codes”, Des. Codes Cryptogr., vol. 84, no. 3, pp. 473–492, 2017.

[10] X. Fang, R. Jin, J. Luo, and W. Ma, “New Galois Hulls of GRS Codes and Application to EAQECCs”, Cryptogr. Commun., vol. 14, pp. 145–159, 2022.

[11] W. Fang, F. Fu, L. Li, and S. Zhu, “Euclidean and Hermitian hulls of MDS codes and their application to quantum codes”, IEEE Trans. Inf. Theory, vol. 66, no. 6, pp. 3527-3537, 2020.

[12] E. M. Gabidulin, “Theory of codes with maximum rank distance”, Probl. Inf. Transm., vol. 1, no. 2, pp. 1–12, 1985.

[13] E. M. Gabidulin, “Rank Codes”, TUM University Press, 2021.

[14] Y. Gao, Q. Yue, X. Huang, and J. Zeng, “Hulls of generalized Reed Solomon codes via Goppa codes and their applications to quantum codes”, IEEE Trans. Inf. Theory, vol. 67, no. 10, pp. 6619-6626, 2021.

[15] E. Gorla, “Rank-metric codes”, Concise Encyclopedia of Coding Theory, Chapman and Hall/CRC, pp. 227-250, 2021.

[16] M. Grassl, F. Huber, and A. Winter, “Entropic proofs of Singleton bounds for quantum error-correcting codes”, IEEE Trans. Inform. Theory, vol. 68, no. 6, pp. 3942-3950, 2022.

[17] K. Guenda, T.A. Gulliver, S. Jitman, and S. Thipworawimon, “Linear ℓ-intersection pairs of codes and their applications”, Des. Codes Cryptogr., vol. 88, pp. 133–152, 2020.

[18] A-L. Horlemann-Trautmann, and K. Marshall, “New criteria for MRD and Gabidulin codes and some rank-metric code constructions”, Adv. Math. Commun., vol. 11, no. 3, pp. 533-548, 2021.

[19] L. Jin, S. Ling, J. Luo, and C. Xing, “Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes”, IEEE Trans. Inform. Theory, vol. 56, no. 9, pp. 4735-4740, 2010.

[20] L. Jin, H. Kan, and J. Wen, “Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes”, Des. Codes Cryptogr., vol. 84, no. 3, pp. 463–471, 2017.

[21] J. Leon, “Computing automorphism groups of error-correcting codes”, IEEE Trans. Inf. Theory, vol. 28, no. 3, pp. 496–511, 1982.

[22] J. Leon, “Permutation group algorithms based on partition, I: theory and algorithms”, J. Symb. Comput., vol. 12, pp. 533–583, 1991.

[23] X. Liu, L. Yu, and P. Hu, “New entanglement-assisted quantum codes from ℓ-Galois dual codes”, Finite Fields Appl., vol. 55, pp. 21–32, 2019.

[24] G. Lunardon, R. Trombetti, and Y. Zhou, “Generalized twisted Gabidulin codes”, J. Comb. Theory, Series A, vol. 159, pp. 79-106, 2022.

[25] G. Luo, X. Cao, and X. Chen, “MDS codes with hulls of arbitrary dimensions and their quantum error correction”, IEEE Trans. Inf. Theory, vol. 65, pp. 2944-2952, 2019.

[26] J. L. Massey, “Linear codes with complementary duals”, Discrete Math. vol. 106(107), pp. 337–342, 1992.

[27] G. Nebe, and W. Willems, “On self-dual MRD codes”, Adv. Math. Commun., vol. 10, no. 3, pp. 633-642, 2016.

[28] E. M. Rains, “Nonbinary quantum codes”, IEEE Trans. Inf. Theory, vol. 45, no. 6, pp. 1827-1832, 1997.

[29] A. Ravagnani, “Rank-metric codes and their duality theory”, Des. Codes Cryptogr. vol. 80, pp. 197-216, 2016.

[30] 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, 1980.

[31] N. Sendrier, “Finding the permutation between equivalent codes: the support splitting algorithm”, IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1193–1203, 2000.

[32] J. Sheekey, “A new family of linear maximum rank distance codes”, Adv. Math. Commun., vol. 10, no. 3, pp. 475–488, 2016.

[33] J. Sheekey, and G. Van de Voorde, “Rank-metric codes, linear sets, and their duality”, Des. Codes Cryptogr., vol. 88, pp. 655–675, 2020.

[34] P. W. Shor, “Scheme for reducing decoherence in quantum memory”, Phys. Rev. A, vol. 52, pp. 2493-2496, 1995.

[35] L. Sok, and G. Qian, “Linear codes with arbitrary dimensional hull and their applications to EAQECCs”, Quantum Inf. Process, vol. 21, no. 72, 2022.

[36] Z.-X. Wan, “Lectures on finite fields and Galois rings”, World Scientific Publishing Company, Aug. 2003.