

Decoding a class of maximum Hermitian rank metric codes

Wrya K. Kadir^{*}, Chunlei Li^{*}, and Ferdinando Zullo^{***}

^{*}Informatics Department, University of Bergen

^{**}Dipartimento di Matematica e Fisica, Università degli Studi della Campania “Luigi Vanvitelli”

Abstract

Maximum Hermitian rank metric codes were introduced by Schmidt in 2018 and in this paper we propose both interpolation-based encoding and decoding algorithms for this family of codes when the length and the minimum distance of the code are both odd.

1 Introduction

Let $\mathbb{F}_q^{n \times n}$ be the set of the square matrices of order n defined over \mathbb{F}_q , which is the finite field of q elements. We can equip $\mathbb{F}_q^{n \times n}$ with the following metric

$$d(A, B) = \text{rk}(A - B),$$

where $\text{rk}(A - B)$ is the rank of the difference matrix $A - B$. If \mathcal{C} is a subset of $\mathbb{F}_q^{n \times n}$ with the property that for each $A, B \in \mathcal{C}$ then $d(A, B) \geq d$ with $1 \leq d \leq n$, then \mathcal{C} is called a *rank metric code with minimum distance d* , or that \mathcal{C} is a *d -code* [9]. Furthermore, we say that \mathcal{C} is *\mathbb{F}_q -linear* if \mathcal{C} is an \mathbb{F}_q -subspace of $(\mathbb{F}_q^{n \times n}, +, \cdot)$, where $+$ is the classical matrix addition and \cdot is the scalar multiplication by an element of \mathbb{F}_q . Examples are rank metric codes whose codewords are alternating matrices [4], symmetric matrices [6, 8, 13] and Hermitian matrices [9, 11]. In this paper we deal with the latter case.

Consider the conjugation map $\bar{\cdot}$ from \mathbb{F}_{q^2} to itself: $x \mapsto \bar{x} = x^q$. Let $A \in \mathbb{F}_{q^2}^{n \times n}$ and denote by A^* its conjugate transpose, that is A^* is obtained by the transposition of the matrix A in which the conjugate map is applied to all of its entries. A matrix $A \in \mathbb{F}_{q^2}^{n \times n}$ is said to be *Hermitian* if $A^* = A$. Denote by $H_n(q^2)$ the set of all Hermitian matrices of order n over \mathbb{F}_{q^2} . In [9, Theorem 1], Schmidt proved that if \mathcal{C} is an \mathbb{F}_q -linear rank metric code with minimum distance d contained in $H_n(q^2)$, then

$$|\mathcal{C}| \leq q^{n(n-d+1)}.$$

When the equality is achieved, we say that \mathcal{C} is a *maximum Hermitian d -code* or a *maximum Hermitian rank metric code*.

Each rank metric code can be described equivalently in terms of q -polynomials. Let $\mathcal{L}_{n,q}$ denote the quotient \mathbb{F}_q -algebra of the algebra of linearized polynomials over \mathbb{F}_{q^n} with respect to $(x - x^{q^n})$, i.e.

$$\mathcal{L}_{n,q} = \left\{ \sum_{i=0}^{n-1} a_i x^{q^i} : a_i \in \mathbb{F}_{q^n} \right\}.$$

It is well known that $\mathcal{L}_{n,q}$ is isomorphic to the \mathbb{F}_q -algebra of square matrices over \mathbb{F}_q . Using this fact and following [6], the set $H_n(q^2)$ of Hermitian matrices of order n over \mathbb{F}_{q^2} can be identified

^{*}The research of the last author was supported by the project “VALERE: VAnviteLli pEr la RicErca” of the University of Campania “Luigi Vanvitelli” and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

as the following set of linearized polynomials

$$\mathcal{H}_n(q^2) = \left\{ \sum_{i=0}^{n-1} c_i x^{q^{2i}} : c_{n-i+1} = c_i^{q^{2n-2i+1}} \text{ for } i \in \{0, \dots, n-1\} \right\} \subseteq \mathcal{L}_{n, q^2},$$

where the indices are taken modulo n . Note that if n is odd then $c_{(n+1)/2}$ belongs to \mathbb{F}_{q^n} .

There are some examples of maximum Hermitian d -codes, see [9, 11]. The first two examples were given in [9, Theorems 4 and 5]. In this abstract, we consider the decoding of the following class of codes.

Theorem 1.1 [9, Theorem 5] *Let n and d be odd integers satisfying $1 \leq d \leq n$. The Hermitian forms $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \rightarrow \mathbb{F}_{q^2}$ given by $H(x, y) = \text{Tr}(y^q L(x))$ with*

$$L(x) = (b_0 x)^{q^{(n+1)}} + \sum_{j=1}^{\frac{n-d}{2}} \left((b_j x)^{q^{(n+2j+1)}} + b_j^q x^{q^{(n-2j+1)}} \right), \quad (1)$$

as b_0 ranges over \mathbb{F}_{q^n} and $b_1, \dots, b_{\frac{n-d}{2}}$ range over $\mathbb{F}_{q^{2n}}$, form an additive d -code in $\mathcal{H}_n(q^2)$, the set of $n \times n$ Hermitian matrices over \mathbb{F}_{q^2} , and for $z \in \mathbb{F}_{q^{2n}}$ we define $\text{Tr}(z) = z + z^q + \dots + z^{q^{n-1}}$ which stands for the trace function $\text{Tr} : \mathbb{F}_{q^{2n}} \rightarrow \mathbb{F}_{q^2}$.

The above statement also holds when one extends the q^2 -polynomials to q^{2s} -polynomials with the integer s satisfying $\text{gcd}(s, 2n) = 1$.

Our work in this abstract is also motivated by the recent work of De La Cruz, Evilla and Özbudak [3], where in Section 6 they suggested studying decoding algorithm for Hermitian rank metric codes. A summary of the existing interpolation-based decoding algorithms of rank metric codes is given in [5, Section V.].

2 Encoding and Decoding of Hermitian MRD codes

2.1 Encoding

Assume that $\{\alpha_1, \dots, \alpha_n\}$ is an \mathbb{F}_{q^2} -basis of $\mathbb{F}_{q^{2n}}$ such that $\text{Tr}(\alpha_i^q \alpha_j)$ is zero if $i \neq j$ and 1 if $i = j$. The property we require on the basis $\{\alpha_1, \dots, \alpha_n\}$ naturally extends the notion of *self-dual basis* in this setting, for this reason we will call it a *Hermitian self-dual basis* and such a basis always exists, see e.g. [1, Theorem 4.1]. Throughout what follows, we denote $x^{[i]} = x^{q^{2i}}$ for the simplicity of presentation.

Let $L(x)$ as in Theorem 1.1. For the Hermitian form in Theorem 1.1, we have

$$H(x, y) = \text{Tr}(y^q L(x)) = \text{Tr}(x^q L(y)).$$

Let $x, y \in \mathbb{F}_{q^{2n}}$, then $x = \sum_{i=1}^n x_i \alpha_i$ and $y = \sum_{i=1}^n y_i \alpha_i$, for some $x_i, y_i \in \mathbb{F}_{q^2}$. It is clear that $\text{Tr}(x^q y) = \langle (x_1^q, \dots, x_n^q), (y_1, \dots, y_n) \rangle = \sum_{i=1}^n x_i^q y_i$. Now, denote by \mathcal{H} the associated matrix of H with respect to the ordered \mathbb{F}_{q^2} -basis $(\alpha_1, \dots, \alpha_n)$ and denote by $\mathcal{H}(i, j)$ its (i, j) -entry, namely, $\mathcal{H}(i, j) = H(\alpha_i, \alpha_j) = \text{Tr}(\alpha_i^q L(\alpha_j))$.

In the following we show how the codewords of the additive d -code in Theorem 1.1 can be expressed in the Hermitian matrix form. Note that

$$\begin{aligned} H(x, y) &= \text{Tr} \left(\left(\sum_i y_i \alpha_i \right)^q \sum_j x_j L(\alpha_j) \right) = \text{Tr} \left(\sum_{i,j} y_i^q x_j \alpha_i^q L(\alpha_j) \right) \\ &= \sum_{i,j} y_i^q x_j \text{Tr}(\alpha_i^q L(\alpha_j)) = \sum_{i,j} y_i^q x_j \mathcal{H}(i, j) = (y_1, \dots, y_n)^q \cdot \mathcal{H} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \end{aligned}$$

In the literature, no encoding method has been given for Hermitian d -codes. In the following we show that the evaluation of the corresponding linearized polynomial at linearly independent elements $\alpha_1, \dots, \alpha_n$ is a proper encoding method.

Let $h = (h_1, \dots, h_n)$ be the Hermitian vector corresponding to the Hermitian matrix \mathcal{H} , that is

$$h_r = \sum_i \alpha_i H(\alpha_i, \alpha_r).$$

Since $H(\alpha_i, \alpha_r) = \text{Tr}(\alpha_i^q f(\alpha_r))$, we can write h_r as

$$h_r = \sum_i \alpha_i \text{Tr}(\alpha_i^q L(\alpha_r)) = \sum_i \alpha_i \text{Tr} \left(\alpha_i^q \sum_j c_j \alpha_j \right) = \sum_i \alpha_i \sum_j c_j \text{Tr}(\alpha_i^q \alpha_j) = \sum_i c_i \alpha_i,$$

where $L(\alpha_r) = \sum_j c_j \alpha_j$, by using the fact that $L(x)$ is linear over \mathbb{F}_{q^2} and the fact that $(\alpha_1, \dots, \alpha_n)$ is a Hermitian self-dual basis. From the above calculations we see that the evaluation encoding is the right way of encoding Hermitian d -codes, since $h_r = L(\alpha_r)$.

Let $m = (n+1)/2$, $\kappa = (n-d)/2$ and H be the Hermitian form given in Theorem 1.1. Then the linearized polynomial in (1) can be written as

$$L(x) = (b_0 x)^{[m]} + \sum_{j=1}^{\kappa} \left((b_j x)^{[m+j]} + b_j^q x^{[m-j]} \right).$$

Let $\{1, \eta\}$ be an \mathbb{F}_{q^n} -basis of $\mathbb{F}_{q^{2n}}$. Let $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ be a Hermitian self-dual basis of $\mathbb{F}_{q^{2n}}$. For the maximum Hermitian d -code in Theorem 1.1 and the evaluation points $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$, the encoding of a message $f = (f_0, \dots, f_{k-1}) \in \mathbb{F}_{q^n}^k$ can be expressed as the evaluation of the following linearized polynomial at points $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$:

$$\begin{aligned} L(x) &= (f_0 x)^{[m]} + \left(\sum_{j=1}^{\kappa} (f_j + \eta f_{\frac{k-1}{2}+j})^q x^{[m-j]} + (f_j + \eta f_{\frac{k-1}{2}+j} x)^{[m+j]} \right) \\ &= \tilde{f}_0 x + \tilde{f}_1 x^{[1]} + \dots + \tilde{f}_{n-1} x^{[n-1]}. \end{aligned} \quad (2)$$

Let $M = \left(\alpha_i^{[j]} \right)_{n \times n}$ be the $n \times n$ Moore matrix generated by α_i 's. So the encoding of the maximum Hermitian rank metric code can be expressed as

$$(f_0, \dots, f_{k-1}) \mapsto (L(\alpha_0), \dots, L(\alpha_{n-1})) = \tilde{f} \cdot M^T, \quad (3)$$

where $\tilde{f} = (\tilde{f}_0, \dots, \tilde{f}_{n-1})$ and M^T is the transpose of the matrix M . As shown in (2), the first $m - \kappa$ and the last $m - \kappa - 2$ elements of \tilde{f} are zero, we only employ k columns of the Moore matrix in the encoding process.

2.2 Interpolation Decoding

For a received word $r = c + e$ with an error e added to the codeword c during transmission, when the error e has rank $t \leq \lfloor \frac{d-1}{2} \rfloor$, the unique decoding task is to recover the unique codeword c such that $d_r(c, r) \leq \lfloor \frac{d-1}{2} \rfloor$.

Suppose $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$ is an error interpolation polynomial such that

$$g(\alpha_i) = e_i = r_i - c_i, \quad i = 0, \dots, n-1. \quad (4)$$

It is clear that the error vector e is uniquely determined by the polynomial $g(x)$, and denote $\tilde{g} = (g_0, \dots, g_{n-1})$. From (3) and (4) it follows that

$$r = c + e = (\tilde{f} + \tilde{g})M^T.$$

This is equivalent to

$$r \cdot (M^T)^{-1} = (0, \dots, 0, \tilde{f}_{m-\kappa}, \dots, \tilde{f}_{m+\kappa}, 0, \dots, 0) \\ + (g_0, \dots, g_{m-\kappa-1}, g_{m-\kappa}, \dots, g_{m+\kappa}, g_{m+\kappa+1}, \dots, g_{n-1}).$$

where $\tilde{f}_m = f_0^{[m]}$ and for $j = 1, 2, \dots, \kappa$, $\tilde{f}_{m-j} = (f_j + \eta f_{\kappa+j})^q$ and $\tilde{f}_{m+j} = \tilde{f}_{m-j}^{q^{n+2j}}$. Letting $\beta = (\beta_0, \dots, \beta_{n-1}) = r \cdot (M^T)^{-1}$, we obtain

$$\begin{cases} (g_0, \dots, g_{m-\kappa-1}) = (\beta_0, \dots, \beta_{m-\kappa-1}) \\ (g_{m+\kappa+1}, \dots, g_{n-1}) = (\beta_{m+\kappa+1}, \dots, \beta_{n-1}) \end{cases} \quad (5)$$

Equivalently, we have

$$g_{m+\kappa+j} = \beta_{m+\kappa+j} \text{ for } j = 1, 2, \dots, d-1, \quad (6)$$

where the subscripts are taken modulo n . In addition, we have

$$g_{m-\kappa+j} = \beta_{m-\kappa+j} - \tilde{f}_{m-\kappa+j} \text{ for } j = 1, \dots, 2\kappa. \quad (7)$$

With the relation $\tilde{f}_{m+j} = \tilde{f}_{m-j}^{q^{n+2j}}$ for $1 \leq j \leq \kappa$, it is sufficient to recover the coefficients $g_{m+\kappa+1}, \dots, g_m$.

Therefore, the task of correcting error e is equivalent to reconstructing $g(x)$ from the available information characterized in the above relations (6) and then apply $g(x)$ to recover \tilde{f} . This reconstruction process heavily depends on the property of the associated Dickson matrix of $g(x)$ and will be discussed in next subsection.

2.3 Polynomial reconstruction

The Dickson matrix associated with $g(x)$ can be given by

$$G = \left(g_{i-j}^{[j]} \pmod{n} \right)_{n \times n} = (G_0 \ G_1 \ \dots \ G_{n-1}), \quad (8)$$

where the indices i, j run through $\{0, 1, \dots, n-1\}$ and G_j is the j -th column of G .

According to the properties of the Dickson matrix, when D has rank t , any $t \times t$ matrix formed by t successive rows and columns in G is nonsingular, see e.g. [12] and [2]. Then G_0 can be expressed as a linear combination of G_1, \dots, G_t , namely, $G_0 = \lambda_1 G_1 + \lambda_2 G_2 + \dots + \lambda_t G_t$, where $\lambda_1, \dots, \lambda_t$ are elements in $\mathbb{F}_{q^{2n}}$. This yields the following recursive equations

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \dots + \lambda_t g_{i-t}^{[t]}, \quad 0 \leq i < n, \quad (9)$$

where the subscripts in g_i 's are taken modulo n . Recall that the elements $g_0, \dots, g_{m-\kappa-1}$ and $g_{m+\kappa+1}, \dots, g_{n-1}$ are known from (5). Hence, we obtain the following linear equations with known coefficients and variables $\lambda_1, \dots, \lambda_t$:

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \dots + \lambda_t g_{i-t}^{[t]}, \quad m + \kappa + t + 1 \leq i < n + m - \kappa \pmod{n}. \quad (10)$$

The above recurrence gives a generalized version of q -linearized shift register as described in [10], where $(\lambda_1, \dots, \lambda_t)$ is the connection vector of the shift register. It is the *key equation* for the decoding algorithm in this paper, by which we shall reconstruct $g(x)$ in two major steps:

Step 1. derive $\lambda_1, \dots, \lambda_t$ from (5) and (10);

Step 2. use $\lambda_1, \dots, \lambda_t$ to compute $g_{m-\kappa}, \dots, g_{m+\kappa}$ from (9).

Step 1 is the critical step in the decoding process, and Step 2 is simply a recursive process that can be done in linear time in $\mathbb{F}_{q^{2n}}$. The following discussion shows how the procedure of Step 1 works.

As discussed in the beginning of this section, for an error vector with $\text{rk}(e) = t \leq \lfloor \frac{d-1}{2} \rfloor$, (10) contains a system of $(n - \kappa) - t = d - 1 - t \geq t$ affine linear equations in the variables $\lambda_1, \dots, \lambda_t$, which has rank t . Hence the variables $\lambda_1, \dots, \lambda_t$ can be uniquely determined. Here we assume the code has high code rate, for which the Berlekamp-Massey algorithm is more efficient. Although the recurrence equation (10) is a generalized version of the ones in [7, 10], the modified Berlekamp-Massey algorithm can be applied here to recover the coefficients $\lambda_1, \dots, \lambda_t$.

3 Conclusion

In this abstract we have proposed both interpolation-based encoding and decoding algorithms for a family of maximum Hermitian rank metric codes when the length and the minimum distance of the code are both odd. In the future we will extend it to other classes of maximum rank distance codes with restrictions.

References

- [1] R. C. Bose and I. Chakravarti. Hermitian varieties in a finite projective space $PG(n, q^2)$. *Canadian Journal of Mathematics*, 18:1161–1182, 1966.
- [2] B. Csajbók. Scalar q -subresultants and Dickson matrices. *Journal of Algebra*, 547:116–128, 2020.
- [3] J. De La Cruz, J. R. Evilla, and F. Özbudak. Hermitian rank metric codes and duality. *IEEE Access*, 9:38479–38487, 2021.
- [4] P. Delsarte and J.-M. Goethals. Alternating bilinear forms over $GF(q)$. *Journal of Combinatorial Theory, Series A*, 19(1):26–50, 1975.
- [5] W. K. Kadir, C. Li, and F. Zullo. On interpolation-based decoding of maximum rank distance codes. *Submitted to International Symposium on Information Theory (ISIT)*, 2021.
- [6] G. Longobardi, G. Lunardon, R. Trombetti, and Y. Zhou. Automorphism groups and new constructions of maximum additive rank metric codes with restrictions. *Discrete Mathematics*, 343(7):111871, 2020.
- [7] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *International Symposium on Information Theory (ISIT)*, pages 398–398, June 2004.
- [8] K.-U. Schmidt. Symmetric bilinear forms over finite fields with applications to coding theory. *Journal of Algebraic Combinatorics*, 42(2):635–670, 2015.
- [9] K.-U. Schmidt. Hermitian rank distance codes. *Designs, Codes and Cryptography*, 86(7):1469–1481, 2018.
- [10] V. Sidorenko, G. Richter, and M. Bossert. Linearized shift-register synthesis. *IEEE Transactions on Information Theory*, 57(9):6025–6032, Sep. 2011.
- [11] R. Trombetti and F. Zullo. On maximum additive Hermitian rank-metric codes. *Journal of Algebraic Combinatorics*, pages 1–21, 2020.
- [12] B. Wu and Z. Liu. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*, 22:79–100, 2013.
- [13] Y. Zhou. On equivalence of maximum additive symmetric rank-distance codes. *Designs, Codes and Cryptography*, 88(5):841–850, 2020.