ON THE DIMENSION OF HERMITIAN SUBFIELD SUBCODES FROM HIGHER DEGREE PLACE

SABIRA EL KHALFAOUI, GÁBOR NAGY, JADE NARDI

Abstract.

1. Introduction

The advent of quantum computers poses significant threats to classical cryptographic schemes, necessitating the development of post-quantum cryptographic primitives that are resilient against quantum attacks. In this context, Algebraic-Geometry (AG) codes have gained considerable attention due to their excellent error-correcting capabilities and potential applications in secure communication and cryptographic protocols. Among various classes of AG codes, subfield subcodes stand out for their inherent resistance to structural attacks, making them prime candidates for deployment in post-quantum cryptography.

Constructingg subfield subcodes, a process also known as restriction, is a simple yet effective technique in cryptography for hiding a code's structure. This is especially useful in the McEliece cryptosystem, where it's important that the code's structure isn't easily recognized. Subfield subcodes help meet this security need, making them a fundamental element in designing secure cryptographic systems.

This paper, we investigate subfield subcodes of Hermitian codes from higher degree place, with a particular emphasis on determining their exact dimensions...
An important application of subfield subcodes of AG codes is in the McEliece cryptosystem, a public-key encryption scheme that has withstood for several years and is renowned for its security against quantum attacks. The security of the McEliece cryptosystem hinges on the hardness of decoding random linear codes. By using subfield subcodes of AG codes as the underlying codes, we can achieve a system that not only inherits the quantum-resistant properties of these codes but also benefits from their efficient decoding algorithms.
In this paper ....

2. Algebraic Geometry (AG) codes

Hermitian curves and their divisors. For more details we refer the readers to [Sti09, Ste12].

The Hermitian curve, denoted as $\mathscr{H}_q$, over the finite field $\mathbb{F}_{q^2}$ in affine coordinates, is given by the equation:

$$\mathscr{H}_q : Y^q + Y = X^{q+1}.$$

This curve has a genus $g = \frac{q(q-1)}{2}$, classifying it as a maximal curve because it achieves the maximum number of $\mathbb{F}_{q^2}$-rational points, which is $\#\mathscr{H}_q(\mathbb{F}_{q^2}) = q^3+1$. Additionally, $\mathscr{H}_q$ possesses a unique singular point at infinity, denoted P_∞.

A divisor on $\mathscr{H}_q$ is a formal sum $D = n_1Q_1 + \cdots + n_kQ_k$ where $n_1, \cdots, n_k$ are integers, and $Q_1, \cdots, Q_k$ are points on $\mathscr{H}_q$. The degree of the divisor D is defined as $\deg(D) = \sum_{i=1}^k n_i$. The valuation of D at a point Q_i is $v_{Q_i}(D) = n_i$, and the support of D is the set $\{Q_i \mid n_i \neq 0\}$.

The Frobenius automorphism, denoted as Fr_{q^2}, is defined over the algebraic closure $\overline{\mathbb{F}}_{q^2}$ and acts on elements by

$$\mathrm{Fr}_{q^2} : \overline{\mathbb{F}}_{q^2} \to \overline{\mathbb{F}}_{q^2}, \quad x \mapsto x^{q^2}.$$

It acts on points of $\mathscr{H}_q$ by applying to their coordinates. A point Q on $\mathscr{H}_q$ is $\mathbb{F}_{q^2}$-rational if and only if it is fixed by $\mathrm{Fr}_{q^2}(Q)$. In $\overline{\mathbb{F}}_{q^2}$, points on $\mathscr{H}_q$ correspond one-to-one with the places of the function field $\overline{\mathbb{F}}_{q^2}(\mathscr{H}_q)$.

For a divisor D, its Frobenius image is given by

$$\mathrm{Fr}_{q^2}(D) = n_1 \mathrm{Fr}_{q^2}(Q_1) + \cdots + n_k \mathrm{Fr}_{q^2}(Q_k).$$

D is $\mathbb{F}_{q^2}$-rational if $D = \mathrm{Fr}_{q^2}(D)$. Notably, if all points $Q_1, \ldots, Q_k$ are in $\mathscr{H}_q(\mathbb{F}_{q^2})$, then D is inherently $\mathbb{F}_{q^2}$-rational.

Riemann-Roch space. For a non-zero function g in the function field $\bar{\mathbb{F}}_{q^2}$ and a place P ,$v_P(g)$ stands for the order of g at P. If $v_P(g) > 0$ then P is a zero of g, while if $v_P(g) < 0$,then P is a pole of g with multiplicity $-v_P(g)$. The principal divisor of a non-zero function g is $(g) = \sum_P v_P(g)P$.

The *Riemann–Roch space* associated with an $\mathbb{F}_{q^2}$-rational divisor G is the $\mathbb{F}_{q^2}$ vector space

$$\mathscr{L}(G) := \left\{ g \in \mathbb{F}_{q^2}(\mathscr{H}_q) \mid (g) + G \geq 0 \right\} \cup 0,$$

with dimension $\ell(G)$.

From [Sti09, Riemann's Theorem 1.4.17], we have

$$\ell(G) \geq \deg(G) + 1 - \mathfrak{g},$$

with equality if $\deg(G) \geq 2\mathfrak{g} - 1$.

In this work, our primary focus is on an $\mathbb{F}_{q^2}$-rational divisor G of the form sP where P is a degree r place in $\mathbb{F}_{q^2}(\mathscr{H}_q)$ and s is a positive integer. In the extended constant field of $\mathbb{F}_{q^2}(\mathscr{H}_q)$ with degree r, let $P_1, P_2, \cdots, P_r$ be the extensions of P. These points are degree-one places in $\mathbb{F}_{q^{2r}}(\mathscr{H}_q)$, and, by appropriately labeling the indices, $P_i = \mathrm{Fr}^i_{q^2}(P_1)$, where indices are considered modulo r.

Hermitian codes. Here, we outline the construction of an AG code from the Hermitian curve

In algebraic coding theory, Hermitian codes stand out as a significant class of algebraic geometry (AG) codes, renowned for their distinctive properties. These codes are constructed from Hermitian curves defined over finite fields. These codes are typically viewed as functional AG codes, denoted by $C_{\mathcal{L}}(D, G)$. In this standard approach, the divisor G is usually a multiple of a single place of degree one. The set $\mathcal{P}$, encompassing all rational points on $\mathscr{H}_q$, is listed as $\{Q_1, \ldots, Q_n\}$. This approach gives rise to a structure referred to as a one-point code. However, it is important to note that recent research in the field suggests that using a more varied selection for the divisor G can result in the creation of better AG codes [MM05, KN13].

Given a divisor $D = Q_1 + Q_2 + \cdots + Q_n$ where all Q_i are distinct rational points, and an $\mathbb{F}_{q^2}$-rational divisor G such that $\mathrm{Supp}(G) \cap \mathcal{P} = \varnothing$. By numbering the points in $\mathcal{P}$, we define an evaluation map $\mathrm{ev}_{\mathcal{P}}$ such that $\mathrm{ev}_{\mathcal{P}}(g) = (g(Q_1), \ldots, g(Q_n))$ for $g \in \mathcal{L}(G)$.

The functional AG code associated with the divisor G is

$$C_{\mathcal{L}}(D, G) := \{(g(Q_1), g(Q_2), \cdots, g(Q_n)) \mid g \in \mathcal{L}(G)\},$$

Theorem 2.1. [Sti09, Theorem 2.2.2] *$C_{\mathcal{L}}(D,G)$ is an $[n,k,d]$ code with parameters*

$$k = \ell(G) - \ell(G-D) \quad \text{and} \quad d \geq n - \deg G.$$

The dual of an AG code can be described as a residue code (see [Sti09] for more details), *i.e.*

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\Omega}(D,G).$$

Moreover, the differential code $C_{\Omega}(D,G)$ is analogous to the functional code $C_{\mathcal{L}}(D, W+D-G)$, where W represents a canonical divisor of $\overline{\mathbb{F}}_{q^2}(\mathscr{H}_q)$. Notably, they share identical dimensions and minimum distances; however, this correspondence does not preserve all crucial properties of the code.

Subfield Subcode and trace code. For the efficient construction of codes over $\mathbb{F}_q$, one approach involves working with codes originally defined over an extension field, $\mathbb{F}_{q^m}$. When considering a code $\mathcal{C}$ within $\mathbb{F}_{q^m}^n$, a subfield subcode of $\mathcal{C}$ is its restriction to the field $\mathbb{F}_q$ This process, often employed in defining codes like BCH codes, Goppa codes, and alternant codes, plays a foundational role.

Let q be a prime power, and m a positive integer. Let C denote a linear code of parameters $[n,k]$ defined over the finite field $\mathbb{F}_{q^m}$. The *subfield subcode* of C over $\mathbb{F}_q$, represented as $C|_{\mathbb{F}_q}$, is the set

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n,$$

which consists of all codewords in C that have their components in $\mathbb{F}_q$.

The subfield subcode $C|_{\mathbb{F}_q}$ is a linear code over $\mathbb{F}_q$ with parameters $[n, k_0, d_0]$, satisfying the inequalities $d \leq d_0 \leq n$ and $n-k \leq n-k_0 \leq m(n-k)$. Moreover, a parity check matrix for C over $\mathbb{F}_q$ provides up to $m(n-k)$ linearly independent parity check equations over $\mathbb{F}_q$ for the subfield subcode $C|_{\mathbb{F}_q}$.

Typically, the minimum distance d_0 of the subfield subcode exceeds that of the original code C.

Let $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ denote the trace function from $\mathbb{F}_{q^m}$ down to $\mathbb{F}_q$, expressed as

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + x^{q^2} + \ldots + x^{q^{m-1}}.$$

For any vector $c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$, we define

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c) = \left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_1), \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_2), \ldots, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_n)\right).$$

Furthermore, for a linear code C of length n and dimension k over $\mathbb{F}_{q^m}$, the code $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(C)$ is a linear code of length n and dimension k_1 over $\mathbb{F}_q$.

A seminal result by Delsarte connects subfield subcodes with trace codes:

Theorem 2.2 ([Del75])**.** *Let C be a $[n,k]$ linear code over $\mathbb{F}_q$. Then the dual of the subfield subcode of C is the trace code of the dual code of C, i.e.,*

$$(C|_{\mathbb{F}_q})^{\perp} = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(C^{\perp}).$$

Finding the exact dimension of a subfield subcode of a linear code is typically a hard problem. However, a basic estimation can be obtained by applying Delsarte's theorem [Del75]:

$$\dim C|_{\mathbb{F}_q} \geq n - m(n-k). \tag{1}$$

In Chapter 9 of Stichtenoth's work [Sti09], various results are presented on subfield subcodes and trace codes of AG codes. We will extend and adapt these results to the context of Hermitian codes in this section, focusing on some specific cases for detailed discussion.

Applying Theorem 9.1.6 in [Sti09] to Hermitian codes:

Theorem 2.3. *Consider the Hermitian codes*

$$\mathcal{C}_{\mathcal{L}} := C_{\mathcal{L}}(D,G) \text{ and } \mathcal{C}_{\Omega} := C_{\Omega}(D,G),$$

where $D = Q_1 + \ldots + Q_n$ (with pairwise distinct places $Q_1, \ldots, Q_n$ of degree one), and $G = sP$ where P is a degree r pace on $\mathscr{H}_q$ with $\operatorname{supp} D \cap \operatorname{supp} G = \emptyset$ and $\deg G < n$. Suppose that G_1 is a divisor of $\mathbb{F}_{q^2}(\mathscr{H}_q)$ satisfying

$$G_1 \leq G \quad \text{and} \quad q \cdot G_1 \leq G. \tag{2}$$

Then

$$\dim \operatorname{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathcal{C}_{\mathcal{L}}) \leq \begin{cases} m\left(\ell(G) - \ell\left(G_1\right)\right) + 1 & \text{if } G_1 \geq 0, \\ m\left(\ell(G) - \ell\left(G_1\right)\right) & \text{if } G_1 \ngeq 0, \end{cases} \tag{3}$$

and

$$\dim C_{\Omega}|_{\mathbb{F}_q} \geq \begin{cases} n - 1 - m\left(\ell(G) - \ell\left(G_1\right)\right) & \text{if } G_1 \geq 0, \\ n - m\left(\ell(G) - \ell\left(G_1\right)\right) & \text{if } G_1 \ngeq 0. \end{cases} \tag{4}$$

The biggest divisor G_1 that satisfies the condition (2) (with respect to the degree) is the following:

$$G_1 = \left\lceil \frac{q(q-1)}{r} \right\rceil P \quad \text{and} \quad G = q.G_1,$$

in (3) and (4) we can replace $\ell(G_1)$ and $\ell(G)$ by $\deg G_1$ and $\deg G$ since $\deg G_1 = q(q-1) = 2\mathfrak{g}$, which follows immediately from the Riemann-Roch Theorem. Moreover, we derive the following corollary from Theorem 9.1.6 [Sti09]

Corollary. *With the notation as above. Let P be a place on $\mathscr{H}_q$ of degree r such that:*

$$G_1 = \left\lceil \frac{q(q-1)}{r} \right\rceil P \quad \text{and} \quad G = q.G_1,$$

then

$$\dim C_{\mathcal{L}}(D, G_1)_{|\mathbb{F}_q} = 1.$$

Proof. Let f be a function in $\mathscr{L}(G_1)$ such that $f(Q_i) \in \mathbb{F}_q$ for $i = 1, \cdots, n$. Then $f^q - f \in \mathscr{L}(G)$ (since $\mathscr{L}(G_1)^q \subseteq \mathscr{L}(G)$), hence $f^q - f \in \mathscr{L}(G-D)$ where

$$\mathscr{L}(G-D) = \operatorname{Ker}\left(\operatorname{ev}_{\mathcal{P}}\right) = \left\{x \in \mathscr{L}(G) \mid v_{P_i}(x) > 0 \text{ for } i = 1, \ldots, n\right\},$$

since we assumed that $\deg(G-D) < n$, it follows that $f^q - f = 0$ which implies that $f \in \mathbb{F}_q$. Consequently $\dim C_{\mathcal{L}}(D, G_1)_{|\mathbb{F}_q} = 1$. □

3. Degree 3 places of the Hermitian curve

In this section we collect useful facts on the degree 3 places of the Hermitian curve, their stabilizer subgroups, and Riemann-Roch spaces. The Hermitian curve $\mathscr{H}_q$ has affine equation

$X^{q+1} = Y + Y^q$. The Hermitian function field $\bar{\mathbb{F}}_{q^2}(\mathscr{H}_q)$ is generated by x, y such that $x^{q+1} = y + y^q$ holds. The Frobenius field automorphism $\mathrm{Fr} : x \mapsto x^{q^2}$ of the algebraic closure $\bar{\mathbb{F}}_{q^2}$ incudes an action on rational functions, places, divisors and curve automorphisms. For this action, we keep using the notation Fr in the exponent: P^{Fr}, f^{Fr}, D^{Fr}, etc.

Let K be a field extension of $\mathbb{F}_{q^2}$. An affine point is a pair $(a, b) \in K^2$. A projective point $(a : b : c)$ is a 1-dimensional subspace $\{(at, bt, ct) \mid t \in K\}$ of K^3. If $c \neq 0$, then the projective point $(a : b : c)$ is identified with the affine point $(a/c, b/c)$. For $u = (u_1, u_2, u_3), v = (v_1, v_2, v_3) \in K^3$, we define the Hermitian form

$$\langle u, v\rangle = u_1 v_1^q - u_2 v_3^q - u_3 v_2^q.$$

Clearly, $\langle u, v\rangle$ is additive in u and v, $\langle \alpha u, \beta v\rangle = \alpha\beta^q \langle u, v\rangle$, and

$$\langle u, v\rangle^q = \langle v^{\mathrm{Fr}}, u\rangle.$$

The point u is self-conjugate, if

$$0 = \langle u, u\rangle = u_1^{q+1} - u_2 u_3^2 - u_2^q u_3.$$

This is the projective equation $X^{q+1} - YZ^q - Y^q Z = 0$ of the Hermitian curve $\mathscr{H}_q$.

Let $a_1, b_1 \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ be scalars such that $a_1^{q+1} = b_1 + b_1^q$. In other words, (a_1, b_1) is an affine point of $\mathscr{H}_q : X^{q+1} = Y + Y^q$, defined over $\mathbb{F}_{q^6}$. Write $p_1 = (a_1, b_1, 1)$, $p_2 = p_1^{\mathrm{Fr}} = (a_1^{q^2}, b_1^{q^2}, 1)$, $p_3 = p_2^{\mathrm{Fr}} = (a_1^{q^4}, b_1^{q^4}, 1)$. Then $\langle p_i, p_i\rangle = 0$, and

$$0 = \langle p_i, p_i\rangle^q = \langle p_i^{\mathrm{Fr}}, p_i\rangle = \langle p_{i+1}, p_i\rangle$$

hold for $i = 1, 2, 3$, the indices taken modulo 3. Since $\langle ., .\rangle$ is nontrivial, $\gamma_i = \langle p_i, p_{i+1}\rangle \neq 0$. Clearly, $\gamma_{i+1} = \gamma_i^{q^2}$.

Let $\beta_1 \in \mathbb{F}_{q^6}$ be an element such that $\beta_1^{q^3+1} = 1$. Define $\beta_2 = \beta_1^{q^2}$, $\beta_3 = \beta_1^{q^4}$. Then

$$\beta_i \beta_{i+1}^q = \beta_i^{q^3+1} = 1.$$

For $p'_i = \beta_i p_i$, this implies

$$\langle p'_i, p'_{i+1}\rangle = \beta_i \beta_{i+1}^q \langle p_i, p_{i+1}\rangle = \langle p_i, p_{i+1}\rangle.$$

Hence, for all $i, j \in \{1, 2, 3\}$,

$$\langle p'_i, p'_j\rangle = \langle p_i, p_j\rangle.$$

This shows that we can extend the map $p_i \mapsto p'_i$ to a unitary linear map $B : u \mapsto u'$ in the following way. Write

$$u = x_1 p_1 + x_2 p_2 + x_3 p_3,$$

with $x_i = \langle u, p_{i+1}\rangle/\gamma_i$, and define

$$u' = x_1 p'_1 + x_2 p'_2 + x_3 p'_3 = x_1 \beta_1 p_1 + x_2 \beta_2 p_2 + x_3 \beta_3 p_3.$$

The extension B is unique. Moreover, B commutes with the Frobenius map Fr:

$$(p'_i)^{\mathrm{Fr}} = (\beta_i p_i)^{\mathrm{Fr}} = \beta_i^{q^2} p_{i+1} = \beta_{i+1} p_{i+1} = p'_{i+1} = (p_i^{\mathrm{Fr}})'.$$

In other words, B is a well-defined element of the general unitary group $GU(3, q)$. The set $\mathcal{B} = \{B \mid \beta_1 \in \mathbb{F}_{q^6},\ \beta_1^{q^3+1} = 1\}$ is a cyclic group of unitary transformations, its order is $|\mathcal{B}| = q^3 + 1$.

In the projective plane, B induces a projective linear transformation $\hat{B}$. $\hat{B}$ is trivial if and only if $\beta_1 = \beta_2 = \beta_1^{q^2}$, that is, if and only if $\beta_i \in \mathbb{F}_{q^2}$. As $\gcd(q^3+1, q^2-1) = q+1$, $\hat{B}$ is trivial if and only if $\beta_1^{q+1} = 1$. The set $\hat{\mathcal{B}} = \{\hat{B} \mid B \in \mathcal{B}\}$ is a cyclic group of unitary projective linear transformations, its order is $|\hat{\mathcal{B}}| = q^2 - q + 1$.

Similarly, let $\delta_1 \in \mathbb{F}_{q^6}$ be such that $\delta_1^{q^3+1} = \gamma_1^{1-q^2}$. Since

$$\gamma_1^{q^3} = \langle p_1, p_2 \rangle^{q^3} = \langle p_2^{\mathrm{Fr}}, p_1 \rangle^{q^2} = \langle p_2^{\mathrm{Fr}^2}, p_1^{\mathrm{Fr}} \rangle = \langle p_1, p_2 \rangle = \gamma_1,$$

we have $\gamma_1 \in \mathbb{F}_{q^3}$, and there are q^3+1 solutions for $\delta_1^{q^3+1} = \gamma_1^{1-q^2}$. Write $\delta_2 = \delta_1^{q^2}$, $\delta_3 = \delta_2^{q^2}$. As before, the map $p_i \mapsto \delta_i p_{i+1}$ preserves the Hermitian form, hence it extends to a unitary linear map Δ, which commutes with Fr and normalizes $\mathcal{B}$. Δ^3 maps p_i to $\delta_1\delta_2\delta_3 p_i$. This implies that Δ induces a projective linear map $\hat{\Delta}$ of order 3.

Notice that a linear transformation

$$A : \begin{cases} X_1' &= a_{11}X_1 + a_{12}X_2 + a_{13}X_3 \\ X_2' &= a_{21}X_1 + a_{22}X_2 + a_{23}X_3 \\ X_3' &= a_{31}X_1 + a_{32}X_2 + a_{33}X_3 \end{cases}$$

determines a partial affine map

$$\alpha : (X, Y) \mapsto \left(\frac{a_{11}X + a_{12}Y + a_{13}}{a_{31}X + a_{32}Y + a_{33}}, \frac{a_{21}X + a_{22}Y + a_{23}}{a_{31}X + a_{32}Y + a_{33}} \right).$$

α acts on rational functions by $f^\alpha(X,Y) = f(\alpha^{-1}(X,Y))$. If A is unitary, then $(x', y') = \alpha(x, y)$ satisfies $(x')^{q+1} = y' + (y')^q$, and α induces a field automorphism of $\bar{\mathbb{F}}_{q^2}(\mathscr{H}_q)$. In this way, the unitary linear maps B and Δ induce automorphisms of the function field, which we denote by B^* and Δ^*.

In the basis $\{p_1, p_2, p_3\}$, the Hermitian form has the shape

$$\begin{aligned} \langle u, v \rangle &= \langle x_1p_1 + x_2p_2 + x_3p_3, y_1p_1 + y_2p_2 + y_3p_3 \rangle \\ &= x_1y_2^q \langle p_1, p_2 \rangle + x_2y_3^q \langle p_2, p_3 \rangle + x_3y_1^q \langle p_3, p_1 \rangle \\ &= \gamma_1 x_1 y_2^q + \gamma_1^{q^2} x_2 y_3^q + \gamma_1^{q^4} x_3 y_1^q. \end{aligned}$$

In this coordinate frame, the Hermitian curve has projective equation

$$\gamma_1 X_1 X_2^q + \gamma_1^{q^2} X_2 X_3^q + \gamma_1^{q^4} X_3 X_1^q = 0.$$

Let x, y be the generators of the function field $\bar{\mathbb{F}}_{q^2}(\mathscr{H}_q)$ such that $x^{q+1} = y + y^q$. Write

$$\ell_i = \langle (x, y, 1), p_i \rangle = a_i^q x - y - b_i^q.$$

Then

$$(x, y, 1) = \frac{\ell_2}{\gamma_1} p_1 + \frac{\ell_3}{\gamma_2} p_2 + \frac{\ell_1}{\gamma_3} p_3$$

and

$$0 = x^{q+1} - y - y^q = \langle (x,y,1), (x,y,1) \rangle = \frac{\ell_1 \ell_2^q}{\gamma_1^q} + \frac{\ell_2 \ell_3^q}{\gamma_2^q} + \frac{\ell_3 \ell_1^q}{\gamma_3^q}.$$

In our study, we make use of a polynomial denoted as $R(X,Y) = X \prod_{\substack{c \in \mathbb{F}_{q^2} \\ c^q + c \neq 0}} (Y - c)$, where c ranges over $\mathbb{F}_{q^2}$ with $c^q + c \neq 0$. This polynomial plays a crucial role in our investigation of differential codes arising from a degree 3 place on the Hermitian curve H defined over $\mathbb{F}_{q^2}$.

We utilize its properties to derive our results, which are discussed further in this work. In the function field, we observe a fundamental relationship which is expressed in the following propos

Proposition 3.1. *In the function field, we have $x^q R(x,y) = y^{q^2} - y$ and $R(x,y) = x^{q^2} - x$.*

Proof. contenu... □

This proposition highlights a key aspect of the relationship between lines and Hermitian curves, specifically regarding their tangential interactions and intersections. For more in-depth insights into this topic, readers are encouraged to consult [KN13, Section 2].

3.1. **Riemann-Roch basis associated with a degree 3 place.** The main result of this paper deals with an $\mathbb{F}_{q^2}$-rational divisor $G = sP$ where P is a degree-3 place in $\mathbb{F}_{q^2}(\mathscr{H}_q)$ and s is a positive integer. As stated above, in the extended constant field of $\mathbb{F}_{q^2}(\mathscr{H}_q)$ with degree 3, let P_1, P_2, P_3 be the extensions of P. These points are degree-one places in $\mathbb{F}_{q^6}(\mathscr{H}_q)$, and, by appropriately labeling the indices, $P_{j+1} = \mathrm{Fr}(P_j)$, where Fr is the q^2-th power Frobenius map and indices are considered modulo 3. Additionally, P can be identified with the $\mathbb{F}_{q^2}$-rational divisor $P_1+P_2+P_3$ in $\mathbb{F}_{q^6}(\mathscr{H}_q)$. The Riemann-Roch space associated with the divisor sP [KN13] is defined as:

$$\mathscr{L}(sP) = \left\{ \frac{f}{(\ell_1\ell_2\ell_3)^u} \mid f \in \mathbb{F}_{q^2}[X,Y], \deg f \leq 3u, v_{P_i}(f) \geq v \right\} \cup \{0\}, \tag{5}$$

where $\ell_i = 0$ represents the equation of the tangent line at P_i on $\mathscr{H}_q$, and $s = u(q+1) - v$ with $0 \leq v \leq q$.

After establishing the Riemann Roch space as outlined in Equation 5 we introduce a set of fundamentals, in Equation 6. In contrast to the basis this new framework provides insights into the characteristics of the space. It comprises components of the type $\left(\frac{\ell_i}{\ell_{i+2}}\right)^u \left(\frac{\ell_{i+1}}{\ell_i}\right)^{v.U}$, where ℓ_i denotes the equation of the line at P_i, on $\mathscr{H}_q$ as previously indicated. The parameters u and v are bound by conditions.

$$\mathscr{L}(sP) = \left\langle \left(\frac{\ell_i}{\ell_{i+2}}\right)^u \left(\frac{\ell_{i+1}}{l_i}\right)^{v-u} \middle| \begin{array}{ll} 0 \leqslant v \leqslant q & \\ v+1 \leqslant 3u & (q+1)u - v \leqslant s \\ i = 1,2,3 & \end{array} \right\rangle \tag{6}$$

$$\mathscr{L}(sP)/\mathcal{L}((s-1)P) = \left\langle \left(\frac{\ell_i}{\ell_{i+2}}\right)^u \left(\frac{\ell_{i+1}}{\ell_i}\right)^{v-u} \middle| \begin{array}{l} i = 1,2,3 \\ s = (q+1)u - v \end{array} \right\rangle \tag{7}$$

Proposition 3.2. *The basis 6 consists of eigenvectors of α.*

4. The dimension of Hermitian subfield subcodes from degree 3 place (main result)

4.1. **Hermitian codes and their subfield subcodes from degree 3 place.** Let $n = q^3$ and the divisor $D = Q_1 + Q_2 + \cdots + Q_n$ be the sum of $\mathbb{F}_{q^2}$-rational affine points of $\mathscr{H}_q$. For a positive integer s, we denote by $C_{\mathcal{L}}(D, sP)$ the degree-3 place functional AG code. This has length $n = q^3$. If $2\mathfrak{g} - 2 < s < n$, then the dimension of $C_{\mathcal{L}}(D, sP)$ is $k = 3s - \mathfrak{g} + 1$ which is equal to the dimension of the Riemann-Roch space $\mathscr{L}(sP)$, and the designed minimum distance of $C_{\mathcal{L}}(D, sP)$ is $d = q^3 - 3s$.

Proposition 4.1. *The generators of $C_{\mathcal{C}}\left(D+P_\infty, sP\right)$ can be expressed in terms of the basis 6 for $s=2\mathfrak{g}$ and $s=2\mathfrak{g}+1$.*

In our study, we carried out experiments to accurately compute the exact dimension of the subfield subcodes $C_q(s)$ for $q \leq 16$ and $0 \leq s \leq n$. Alongside these investigations of the dimension of the Hermitian code $C_{\mathcal{L}}(\mathcal{P}, G)$ and its trace code, we noted an unusual behavior in the dimension when considering $s = q-1$, which leads to the following proposition:

Proposition 4.2. *Let $q \geq 3$, and $C_{\mathcal{L}}(D, G)$ be the Hermitian code associated with the divisor $G=(q-1)P$, where P is a degree 3 place, then*

$$\dim C_{\mathcal{L}}(D, G) = 4.$$

Proof. A voir (rewrite)

Let $\ell_i = 0$ be the line P_iP_{i+1}, it is the tangent to $\mathscr{H}_q$ at P_i. More precisely, the intersection divisor of ℓ_i and $\mathscr{H}_q$ is $qP_i + P_{i+1}$. This implies that the principal divisor of ℓ_1/ℓ_2 satisfies

$$\operatorname{div}(\ell_i/\ell_{i+1}) = qP_i - (q-1)P_{i+1} - P_{i+2}.$$

For $\alpha \in \mathbb{F}_{q^6}$, w define the function

$$\begin{aligned} w_\alpha &= \alpha\ell_1/\ell_2 + (\alpha\ell_1/\ell_2)^{\mathrm{Frob}_{q^2}} + (\alpha\ell_1/\ell_2)^{\mathrm{Frob}^2_{q^2}} \\ &= \alpha\ell_1/\ell_2 + \alpha^{q^2}\ell_2/\ell_3 + \alpha^{q^4}\ell_3/\ell_1. \end{aligned}$$

On the one hand, w_α is defined over $\mathbb{F}_{q^2}$. On the other hand, Korchmáros and Nagy showed in [KN13, Theorem 3.1]

$$v_{P_i}(w_\alpha) = -q+1.$$

Hence, w_α is contained in the Riemann-Roch space $\mathcal{L}((q-1)P)$. In fact, $\dim \mathcal{L}((q-1)P) = 4$ and $1, w_{\alpha_1}, w_{\alpha_2}, w_{\alpha_3}$ is a basis of $\mathcal{L}((q-1)P)$, provided $\alpha_1, \alpha_2, \alpha_3$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^6}$. ☐

Conjecture 4.1. For a prime power $q \geq 3$, let $\mathcal{C}_{\mathcal{L}} = \mathcal{C}_{\mathcal{L}}(D, (q-1)P)$ be the Hermitian code, where P is a degree 3 place. Let $Tr(\mathcal{C}_{\mathcal{L}})$ denotes the trace code $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathcal{C}_{\mathcal{L}})$. We conjecture that:

$$\dim Tr(\mathcal{C}_{\mathcal{L}}) = 7.$$

Experimental results indicate that for $0 \leq s < 2\mathfrak{g}$, the dimension of $C_{\mathcal{L}}(D, sP)_{|\mathbb{F}_q}$ is 1. Additionally, in the corollary 2 presented earlier demonstrates this result for $s = \frac{q(q-1)}{3} = \frac{2}{3}\mathfrak{g}$.

Theorem 4.3. *For a prime power $q \geq 3$, let $C_q(s) = C_{\mathcal{L}}(\mathcal{P}, G)_{|\mathbb{F}_q}$ denote the subfield subcode of the degree-3 place one-point Hermitian code. Then*

$$\dim C_q(s) = \begin{cases} 1 & \text{for } 0 \leq s < 2\mathfrak{g} \\ 7 & \text{for } s = 2\mathfrak{g} \text{ and } q > 2 \\ 10 & \text{for } s = 2\mathfrak{g}+1 \text{ and } q > 3 \end{cases}$$

Proof. **Case 1: $\mathbf{0 \leq s < \frac{2}{3}\mathfrak{g}}$** or from corollary ...

Observe that constant polynomials belong to $\mathscr{L}(sP)$ for all non-negative s, ensuring that $\dim C_q(s) \geq 1$. To establish that $\dim C_q(s) = 1$ for $0 \leq s < \frac{2}{3}\mathfrak{g}$, we fix an arbitrary integer s in this range and consider a generic element $(c_1, \ldots, c_{q^3}) \in C_q(s)$. This corresponds to a function g in $\mathscr{L}(sP)$ such that $c_i = g(Q_i)$ is an element of $\mathbb{F}_q$ for each $i = 1, \ldots, q^3$.

Next, we note that there exists a $\gamma \in \mathbb{F}_q$ such that at least q^2 of the c_i values are equal to γ. In other words, the function $g-\gamma$ is in $\mathscr{L}(sP)$ and has at least q^2 zeros on $\mathscr{H}_q$. However, a non-zero function in $\mathscr{L}(sP)$ cannot have more than $q(q-1)$ zeros, leading us to conclude that $g-\gamma$ must be the zero function. This implies that every c_i is equal to γ, and hence, $C_q(s)$ consists of constant vectors. This completes the proof, demonstrating that $\dim C_q(s) = 1$ for $0 \leq s < \frac{2}{3}\mathfrak{g}$.

Case 1 part 2: $s = 2\mathfrak{g} - 1$?

Case 2: $s = 2\mathfrak{g}$

Let $\ell_i = 0$ be the line P_iP_{i+1}, it is the tangent to $\mathscr{H}_q$ at P_i. More precisely, the intersection divisor of ℓ_i and $\mathscr{H}_q$ is $qP_i + P_{i+1}$. This implies that the principal divisor of ℓ_1/ℓ_2 satisfies

$$\operatorname{div}(\ell_i/\ell_{i+1}) = qP_i - (q-1)P_{i+1} - P_{i+2}.$$

For $\alpha \in \mathbb{F}_{q^6}$, w define the function

$$\begin{aligned} w_\alpha &= \alpha\ell_1/\ell_2 + (\alpha\ell_1/\ell_2)^{\mathrm{Frob}_{q^2}} + (\alpha\ell_1/\ell_2)^{\mathrm{Frob}_{q^2}^2} \\ &= \alpha\ell_1/\ell_2 + \alpha^{q^2}\ell_2/\ell_3 + \alpha^{q^4}\ell_3/\ell_1. \end{aligned}$$

On the one hand, w_α is defined over $\mathbb{F}_{q^2}$. On the other hand, Korchmáros and Nagy showed in [KN2013, Theorem 3.1]

$$v_{P_i}(w_\alpha) = -q + 1.$$

Hence, w_α is contained in the Riemann-Roch space $\mathcal{L}((q-1)P)$. In fact, $\dim \mathcal{L}((q-1)P) = 4$ and $1, w_{\alpha_1}, w_{\alpha_2}, w_{\alpha_3}$ is a basis of $\mathcal{L}((q-1)P)$, provided $\alpha_1, \alpha_2, \alpha_3$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^6}$.

This implies

$$w_\alpha^q \in \mathcal{L}(q(q-1)P),$$

and for all $\beta \in \mathbb{F}_{q^2}$,

$$W_{\alpha,\beta} = \beta w_\alpha + (\beta w_\alpha)^q \in \mathcal{L}(q(q-1)P).$$

The following claims are straightforward to show:

(1) For any $\mathbb{F}_{q^2}$-rational affine place Q_i, $W_{\alpha,\beta}(Q_i) \in \mathbb{F}_q$.
(2) $\mathcal{W} = \{W_{\alpha,\beta} \mid \alpha \in \mathbb{F}_{q^6}, \beta \in \mathbb{F}_{q^2}\}$ is a linear space over $\mathbb{F}_q$.
(3) $\dim_{\mathbb{F}_q} \mathcal{W} = 6$ and $\dim_{\mathbb{F}_q}(\mathbb{F}_q + \mathcal{W}) = 7$.
(4) $\mathrm{eval}_D(\mathbb{F}_q + \mathcal{W})$ is a subspace of $C_{q(q-1)}$ of dimension 7.

This finishes the proof.

□

special case $q = 2$ the dimension is 5

References

[Del75] Philippe Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Transactions on Information Theory*, 21(5):575–576, 1975.

[KN13] Gábor Korchmáros and Gábor P Nagy. Hermitian codes from higher degree places. *Journal of Pure and Applied Algebra*, 217(12):2371–2381, 2013.

[MM05] Gretchen L Matthews and Todd W Michel. One-point codes using places of higher degree. *IEEE transactions on information theory*, 51(4):1590–1593, 2005.

[Ste12] Serguei A Stepanov. *Codes on algebraic curves*. Springer Science & Business Media, 2012.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.