ON THE DIMENSION OF HERMITIAN SUBFIELD SUBCODES FROM HIGHER DEGREE PLACE

GÁBOR P. NAGY AND SABIRA EL KHALFAOUI

ABSTRACT. The focus of our research is the examination of Hermitian curves over finite fields, specifically concentrating on places of degree 3 and their role in constructing Hermitian codes. We begin by studying the structure of the Riemann-Roch space associated with these degree 3 places, aiming to determine essential characteristics such as the basis. The investigation then turns to Hermitian codes, where we analyze both functional and differential codes of degree 3 places, focusing on their parameters and automorphisms. Additionally, we delve into the study of subfield subcodes and trace codes, determining their structure by giving lower bounds for their dimensions. This presents a complex problem in coding theory. Based on numerical experiments, we formulate a conjecture for the dimension of some subfield subcodes of Hermitian codes.

Our comprehensive exploration seeks to deepen the understanding of Hermitian codes and their associated subfield subcodes related to degree 3 places, thereby contributing to the advancement of algebraic coding theory and code-based cryptography.

1. INTRODUCTION

The emergence of quantum computers present 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.

In the realm of linear codes over finite field extensions, the process of constructing subfield subcodes, commonly known as restriction, involves converting a linear code C defined over a larger finite field extension $\mathbb{F}_{q^n}$ into a code confined within a subfield $\mathbb{F}_{q^m}$, where m devides n. This strategic adaptation confines the codewords of C to elements within the smaller field $\mathbb{F}_{q^m}$, thereby concealing the intricate structural details inherent to C. This concept is exemplified by Reed-Solomon codes, which are AG codes constructed over a projective line. They are widely recognized and utilized in practical applications, with their subfield subcodes represented by Goppa codes. Notably, in cryptography, particularly within the McEliece cryptosystem, subfield subcodes are crucial for hiding the code's structure, thus enhancing its resistance against distinguisher attacks [15, 7]. The consistent strength of the McEliece cryptosystem, based on Goppa codes as introduced by McEliece in 1978 [13], emphasizes its effectiveness in resisting such attacks. Despite subsequent proposals leveraging Reed-Solomon codes [4], AG codes, and their subcodes [5], all have been vulnerable to structural attacks. By applying restriction, cryptographic systems can enhance their security by reducing the risk of potential attacks targeting the distinguishability of the chosen subfield subcode. Given the increasing interest in AG codes, particularly Hermitian codes, they are being assessed as feasible alternatives to Reed-Solomon codes in specific applications [11]. Hermitian codes have been extensively investigated in previous studies [17, 10, 19, 9, 14], particularly those

associated with the point at infinity of the Hermitian curve. However, in [8, 12], authors introduced an alternative construction of Hermitian codes associated with higher-degree places on the Hermitian curve.

Our contribution involves conducting further investigation into Hermitian codes associated with degree 3 places to derive additional properties and establish explicit bases for the corresponding Riemann-Roch spaces, aligning with prior findings presented in [8]. These codes exhibit improved minimum distances, as demonstrated by the Matthews-Michel bound [12], which has been subsequently enhanced and improved by Korchmáros and Nagy in [8]. In addition to this, we focus on exploring the properties of their subfield subcodes. Our investigation particularly emphasizes determining their exact dimensions. Subfield subcodes of Hermitian codes associated with degree 3 places hold promise for constructing a variant of the McEliece cryptosystem. This proposal can enhance the key size, thereby ensuring the required security level by NIST [1].

The paper is structred as follows. in Section 2 we introduce fundamental concepts, covering the essential background of AG codes constructed from the Hermitian curve, including Hermitian curves, divisors, and the Riemann-Roch space. In Section 3 we give some geometric properties of Hermitian degree 3 places, their stabilizer subgroups and in Section 4 the corresponding Riemann-Roch spaces. Using this foundation, Section 5 delves into the characteristics of Hermitian codes associated with degree 3 places, considering both functional and differential codes. Finally, Section 6 investigates Hermitian subfield subcodes from degree 3 places, discussing their construction, dimensionality, and potential applications.

2. Algebraic Geometry (AG) codes

2.1. **Hermitian curves and their divisors.** For more details we refer the readers to [18, 16, 3].

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 Q_∞.

A divisor on $\mathscr{H}_q$ is a formal sum $D = n_1 Q_1 + \cdots + n_k Q_k$ 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 as follows:

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

It acts on points of $\mathscr{H}_q$ by applying Fr_{q^2} 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.

2.2. **Riemann-Roch spaces.** For a non-zero function g in the function field $\overline{\mathbb{F}}_{q^2}$ 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 [18, 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, $P_i = \mathrm{Fr}_{q^2}^i(P_1)$, where indices are considered modulo r.

2.3. 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 [12, 8].

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 ev_D such that $\mathrm{ev}_D(g) = (g(Q_1), \ldots, g(Q_n))$ 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. [18, Theorem 2.2.2] $C_{\mathcal{L}}(D, G)$ *is an* $[n, k, d]$ *code with parameters*

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

The dual of an AG code can be described as a residue code (see [18] 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.

2.4. Subfield subcodes and trace codes.

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 C within $\mathbb{F}_{q^m}^n$, a subfield subcode of 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 ([6]). *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 [6]:

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

In [18, Chapter 9], various results are discussed regarding subfield subcodes and trace codes of AG codes. This motivated us to formulate the following propositions on the dimension of the subfield subcodes of AG codes, which are useful for the case $G = sP$ with a place P of higher degree.

Proposition 2.3. *Let G_1 be a positive divisor of the Hermitian curve $\mathscr{H}_q$, and $D = Q_1 + \cdots + Q_n$ the sum of $\mathbb{F}_{q^2}$-rational places such that $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. Assume that $\deg G_1 < n/q$. 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 $f^q - f \in \mathscr{L}(qG_1)$ (since $\mathscr{L}(G_1)^q \subseteq \mathscr{L}(qG_1)$), hence $f^q - f \in \mathscr{L}(qG_1 - D)$ where

$$\mathscr{L}(qG_1 - D) = \ker(\mathrm{ev}_D) = \{ x \in \mathscr{L}(qG_1) \mid v_{P_i}(x) > 0 \text{ for } i = 1, \ldots, n \}.$$

Since $\deg(qG_1 - D) < 0$, it follows that $\mathscr{L}(qG_1 - D) = 0$, and $f^q - f = 0$ which implies that $f \in \mathbb{F}_q$. Consequently $\dim C_{\mathcal{L}}(D, G_1)|_{\mathbb{F}_q} = 1$. $\square$

3. The geometry of Hermitian degree 3 places

In this section we collect useful facts on the degree 3 places of the Hermitian curve, their stabilizer subgroups, and Riemann-Roch spaces.

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

$$\langle u, v \rangle^q = \langle v^{\mathrm{Fr}_{q^2}}, u \rangle.$$

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 $u = (u_1 : u_2 u_3)$ be a projective point. The polar line of u has equation

$$u^{\perp} : \langle (X_1, X_2, X_3), u \rangle = u_1^q X_1 - u_3 X_2 - u_2 X_3 = 0.$$

If u is on $\mathscr{H}_q$, then $u^{\perp}$ is the tangent line at u. More precisely, $u^{\perp}$ intersects $\mathscr{H}_q$ at u and $u^{\mathrm{Fr}_{q^2}}$ with multiplicities q and 1, respectively. If u is $\mathbb{F}_{q^2}$-rational, then $u = u^{\mathrm{Fr}_{q^2}}$, and the intersection multiplicity is $q + 1$.

3.2. Unitary transformations and curve automorphism.

Let A be a 3×3 matrix. The linear map $u \mapsto uA$ will be denoted by A as well. If A is invertible, then it induces a projective linear transformation, denoted by $\hat{A} : (u_1 : u_2 : u_3) \mapsto (u_1' : u_2' : u_3') = (u_1 : u_2 : u_3)^{\hat{A}}$, where

$$u_1' = a_{11} u_1 + a_{21} u_2 + a_{31} u_3,$$
$$u_2' = a_{12} u_1 + a_{22} u_2 + a_{32} u_3,$$
$$u_3' = a_{13} u_1 + a_{23} u_2 + a_{33} u_3.$$

We use the same notation $\hat{A} : (X, Y) \mapsto (X', Y') = (X, Y)^{\hat{A}}$ for the partial affine map

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

The action $f(X, Y) \mapsto f((X, Y)^{\hat{A}^{-1}})$ of $\hat{A}$ on rational functions will be denoted by A^*. The following lemma is straightforward.

Lemma 3.1. *Let $f(X, Y)$ be a polynomial of total degree n. Define the degree n homogeneous polynomial $F(X, Y, Z) = Z^n f(x/Z, Y/Z)$. Then*

$$f^{A^*}(X, Y) = \frac{F((X, Y, 1)A^{-1})}{(a_{13}X + a_{23}Y + a_{33})^n}.$$

We remark that the line $a_{13}X + a_{23}Y + a_{33} = 0$ can be seen as the pre-image of the line at infinity under $\hat{A}$.

The linear transformation A is unitary, if

$$\langle uA, vA \rangle = \langle u, v \rangle$$

holds for all u, v. Since $\langle ., . \rangle$ is non-degenerate, unitary transformations are invertible. Moreover, for all u, v one has

$$\langle (v^{\mathrm{Fr}_{q^2}})A, uA \rangle = \langle v^{\mathrm{Fr}_{q^2}}, u \rangle$$
$$= \langle u, v \rangle^q$$
$$= \langle uA, vA \rangle^q$$
$$= \langle (vA)^{\mathrm{Fr}_{q^2}}, uA \rangle.$$

This implies $(v^{\mathrm{Fr}_{q^2}})A = (vA)^{\mathrm{Fr}_{q^2}}$ for all v, that is, A and Fr_{q^2} commute. This shows that unitary transformations are defined over $\mathbb{F}_{q^2}$. They form a group, which is denoted by $GU(3,q)$. A useful fact is that if b_1, b_2, b_3 is a basis and

$$\langle b_i A, b_j A \rangle = \langle b_i, b_j \rangle$$

for all $i, j \in \{1, 2, 3\}$, then A is unitary.

Let $A \in GU(3,q)$. If (x, y) is a generic point of $\mathscr{H}_q$, then $(x', y') = (x, y)^{\hat{A}}$ satisfies

$$(x')^{q+1} - y' - (y')^q = \langle x', y' \rangle = \langle x, y \rangle = 0.$$

Hence, (x', y') is a generic point of $\mathscr{H}_q$, and A^* induces an automorphism of the function field $\overline{\mathbb{F}}_{q^2}(\mathscr{H}_q)$. If A is defined over Fr_{q^2}, then A^* is an automorphism of $\mathbb{F}_{q^2}(\mathscr{H}_q)$.

3.3. **Places of degree 3 and their lines.** 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 $a_2 = a_1^{q^2}$, $b_2 = b_1^{q^2}$, $a_3 = a_2^{q^2}$, $b_3 = b_2^{q^2}$, and $p_i = (a_i, b_i, 1)$. Then $p_{i+1} = p_i^{\mathrm{Fr}_{q^2}}$, $\langle p_i, p_i \rangle = 0$, and

$$0 = \langle p_i, p_i \rangle^q = \langle p_i^{\mathrm{Fr}_{q^2}}, p_i \rangle = \langle p_{i+1}, p_i \rangle$$

hold for $i = 1, 2, 3$, the indices taken modulo 3. Since $\langle ., . \rangle$ is non-trivial, $\gamma_i = \langle p_i, p_{i+1} \rangle \in \mathbb{F}_{q^6} \setminus \{0\}$. More precisely,

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

which shows $\gamma_i \in \mathbb{F}_{q^3} \setminus \{0\}$. Clearly, $\gamma_{i+1} = \gamma_i^{q^2}$ and $\gamma_{i+2} = \gamma_i^q$. By $\gamma_i \neq 0$, the vectors p_1, p_2, p_3 are linearly independent over $\mathbb{F}_{q^6}$.

Let K be a field containing $\mathbb{F}_{q^6}$. Since p_1, p_2, p_3 is a basis in K^3, any $u \in K^3$ can be written as

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

with $x_i \in K$. Computing

$$\langle u, p_{i+1} \rangle = \langle x_1 p_1 + x_2 p_2 + x_3 p_3, p_{i+1} \rangle = x_i \langle p_i, p_{i+1} \rangle,$$

we obtain $x_i = \langle u, p_{i+1} \rangle / \gamma_i$. In the basis p_1, p_2, p_3, the Hermitian form has the shape

$$\begin{aligned}
\langle u, v \rangle &= \langle x_1 p_1 + x_2 p_2 + x_3 p_3, y_1 p_1 + y_2 p_2 + y_3 p_3 \rangle \\
&= x_1 y_2^q \langle p_1, p_2 \rangle + x_2 y_3^q \langle p_2, p_3 \rangle + x_3 y_1^q \langle p_3, p_1 \rangle \\
&= \gamma_1 x_1 y_2^q + \gamma_1^{q^2} x_2 y_3^q + \gamma_1^{q^4} x_3 y_1^q.
\end{aligned}$$

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 $\overline{\mathbb{F}}_{q^2}(\mathscr{H}_q)$ 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

(2)
$$0 = x^{q+1} - y - y^q = \langle (x, y, 1), (x, y, 1) \rangle = \frac{\ell_1 \ell_2^q}{\gamma_1^q} + \frac{\ell_2 \ell_3^q}{\gamma_2^q} + \frac{\ell_3 \ell_1^q}{\gamma_3^q}.$$

The Hermitian curve $\mathscr{H}_q$ is non-singular, the places of $\overline{\mathbb{F}}_{q^2}(\mathscr{H}_q)$ correspond to the projective points over the algebraic closure $\overline{\mathbb{F}}_{q^2}$. Let P_i denote the place corresponding to $(a_i : b_i : 1)$. P_i is defined over $\mathbb{F}_{q^6}$, $P_{i+1} = P_i^{\mathrm{Fr}_{q^2}}$, and

$$P = P_1 + P_2 + P_3$$

is an $\mathbb{F}_{q^2}$-rational place of degree 3.

The line $a_i^q X - Y - b_i^q = 0$ is tangent to $\mathscr{H}_q$ at p_i, the intersection multiplicities are q and 1 at p_i and p_{i+1}, respectively. This implies that the zero divisor $(\ell_i)_0$ is $qP_i + P_{i+1}$, and the principal divisor of ℓ_i is

$$(3) \qquad\qquad (\ell_i) = qP_i + P_{i+1} - (q+1)Q_\infty.$$

3.4. **The stabilizer of a degree 3 place.** Let $\beta_1 \in \mathbb{F}_{q^6}$ be an element such that $\beta_1^{q^3+1} = 1$. Define $\beta_2 = \beta_1^{q^2}$, $\beta_3 = \beta_2^{q^2}$. 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 $B = B(\beta_1) : u \mapsto u'$ 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

$$(4) \qquad\qquad u' = x_1 p_1' + x_2 p_2' + x_3 p_3' = x_1 \beta_1 p_1 + x_2 \beta_2 p_2 + x_3 \beta_3 p_3.$$

The extension B is a unique unitary transformation. As we have seen in Section 3.2, this implies that $B = B(\beta_1)$ is a well-defined element of the general unitary group $GU(3, q)$. The set

$$\mathcal{B} = \{ B(\beta_1) \mid \beta_1 \in \mathbb{F}_{q^6}, \ \beta_1^{q^3+1} = 1 \}$$

is a cyclic subgroup of $GU(3, q)$, whose 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, whose order is $|\hat{\mathcal{B}}| = q^2 - q + 1$.

In a similar way, we fix the elements

$$\delta_i = \gamma_i^{\frac{q^3-q}{2}}.$$

Since $\gamma_1 \in \mathbb{F}_{q^3}$, $\delta_i \in \mathbb{F}_{q^3}$. Moreover,

$$\delta_i^{q^3+1} = \delta_i^2 = \gamma_i^{q^3-q} = \gamma_i^{1-q}.$$

As before, the map

$$\Delta : p_i \mapsto p_i'' = \delta_i p_{i-1}$$

preserves the Hermitian form:

$$\langle p_i'', p_{i+1}'' \rangle = \langle \delta_i p_{i-1}, \delta_{i+1} p_i \rangle = \delta_i^{q^3+1} \langle p_{i-1}, p_i \rangle = \gamma_i^{1-q} \gamma_{i-1} = \gamma_i.$$

Hence, Δ extends to a unitary linear map, which commutes with Fr_{q^2} and normalizes $\mathcal{B}$. Indeed,

$$p_i^{\Delta^{-1}B\Delta} = (\delta_{i+1}^{-1}p_{i+1})^{B\Delta} = (\delta_{i+1}^{-1}\beta_{i+1}p_{i+1})^{\Delta} = \beta_{i+1}p_i,$$

hence, $\Delta^{-1}B\Delta = B^{q^2}$. Δ^3 maps p_i to $\delta_1\delta_2\delta_3 p_i$, and

$$\delta_1\delta_2\delta_3 = \delta_1^{1+q+q^2} = \left(\gamma_1^{\frac{q^3-q}{2}}\right)^{1+q+q^2} = \left(\gamma_1^{q^3-1}\right)^{\frac{(q+1)q}{2}} = 1.$$

Therefore, Δ has order 3.

As introduced in Section 3.2, the unitary transformation B and Δ induce automorphisms B^* and Δ^* of the function field.

Proposition 3.2. *The group $\mathcal{B}^* = \{B^* \mid B \in \mathcal{B}\}$ of curve automorphisms has order $q^2 - q + 1$, and Δ^* normalizes $\mathcal{B}^*$ by*

$$(\Delta^*)^{-1}B^*\Delta^* = (B^*)^{q^2} = (B^*)^{q-1}.$$

Both $\mathcal{B}^*$ and Δ^* stabilize the degree 3 place P. □

Proposition 3.3. *Let $\beta_1 \in \mathbb{F}_{q^6}$ be an element such that $\beta_1^{q^3+1} = 1$. Define $\beta_2 = \beta_1^{q^2}$, $\beta_3 = \beta_2^{q^2}$, and the unitary map $B = B(\beta_1) \in \mathcal{B}$. Then*

$$\left(\frac{\ell_i}{\ell_{i+1}}\right)^{B^*} = \beta_i^{q+1}\left(\frac{\ell_i}{\ell_{i+1}}\right).$$

Proof. By Lemma 3.1,

$$\begin{aligned}
\ell_i^{B^*} &= \frac{\langle (x,y,1)B^{-1}, p_i\rangle}{w} \\
&= \frac{\langle (x,y,1), p_iB\rangle}{w} \\
&= \frac{\langle (x,y,1), \beta_ip_i\rangle}{w} \\
&= \frac{\beta_i^q\ell_i}{w},
\end{aligned}$$

where the linear $w = w_1x + w_2y + w$ over $\mathbb{F}_{q^2}$ depends only on B. Therefore,

$$\left(\frac{\ell_i}{\ell_{i+1}}\right)^{B^*} = \frac{\beta_i^q}{\beta_{i+1}^q}\left(\frac{\ell_i}{\ell_{i+1}}\right) = \beta_i^{q-q^3}\left(\frac{\ell_i}{\ell_{i+1}}\right) = \beta_i^{q+1}\left(\frac{\ell_i}{\ell_{i+1}}\right). \qquad \square$$

4. Riemann-Roch spaces associated with a degree 3 place

In this section, we keep using the notation of the previous section: P_i is a degree 1 place of $\mathbb{F}_{q^6}(\mathscr{H}_q)$, associated to the projective point $(a_i : b_i : 1)$. $P_i^{\mathrm{Fr}_{q^2}} = P_{i+1}$; the index $i = 1, 2, 3$ is always taken modulo 3. $P = P_1 + P_2 + P_3$ is an $\mathbb{F}_{q^2}$-rational place of degree 3 of $\mathbb{F}_{q^2}(\mathscr{H}_q)$. The generators x, y of $\overline{\mathbb{F}}_{q^2}(\mathscr{H}_q)$ satisfy $x^{q+1} = y + y^q$. The rational function $\ell_i = a_i^qx - y - b_i^q$ is obtained from the tangent line of $\mathscr{H}_q$ at P_i.

4.1. **Basis and decomposition of the Riemann-Roch space.** Let s, u, v be positive integers such that $v \leq q$ and $s = u(q+1)-v$. Clearly, u, v are uniquely defined by s. In [8], the Riemann-Roch space associated with the divisor sP is given as

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

The Weierstrass semigroup [2] $H(P)$ consists of the integers $s \geq 0$ such that the pole divisor $(f)_\infty = sP$ for some $f \in \mathbb{F}_{q^2}(\mathscr{H}_q)$. If $s \notin H(P)$, then it is called a Weierstrass gap; the set of Weierstrass gaps is denoted by $G(P)$. By [8, Theorem 3.1], we have

$$G(P) = \{u(q+1) - v \mid 0 \leq v \leq q,\ 0 < 3u \leq v\}.$$

By the Weierstrass Gap Theorem [18, Theorem 1.6.8], $|G(P)| = \mathfrak{g}$ for a place of degree 1. In our case, P has degree 3 and the situation is slightly more complicated.

Lemma 4.1.

$$3|G(P)| = \begin{cases} \mathfrak{g} & \text{if } q \equiv 0, 1 \pmod{3}, \\ \mathfrak{g} - 1 & \text{if } q \equiv 2 \pmod{3}. \end{cases}$$

Proof. The lemma follows from

$$
\begin{aligned}
|G(P)| &= \sum_{1 \leq u \leq q/3} |\{3u, \ldots, q\}| \\
&= \sum_{i=1}^{\lfloor q/3 \rfloor} q + 1 - 3u \\
&= \frac{\lfloor q/3 \rfloor (2q - 1 - 3\lfloor q/3 \rfloor)}{2}.
\end{aligned}
$$
$\square$

The following proposition gives an explicit basis for the Riemann-Roch space $\mathscr{L}(sP)$ over the extension field $\mathbb{F}_{q^6}$.

Proposition 4.2. *Let t, u, v be positive integers such that $v \leq q$ and $t = u(q+1) - v$. Define the rational functions*

$$U_{t,i} = \ell_i^{2u-v} \ell_{i+1}^{v-u} \ell_{i+2}^{-u} = \left(\frac{\ell_i}{\ell_{i+2}} \right)^u \left(\frac{\ell_{i+1}}{\ell_i} \right)^{v-u}, \qquad i = 1, 2, 3.$$

Define $U_{0,i} = 1$ as the constant function for $i = 1, 2, 3$. Then the following hold:

(i) $(U_{t,i})^{\mathrm{Fr}_{q^2}} = U_{t,i+1}$.

(ii) The principal divisor of $U_{t,i}$ is

$$(U_{t,i}) = -tP + \big((3u - v - 1)q + (q - v)\big)P_i + \big(v(q - 2) + 3u\big)P_{i+1}.$$

In particular, if $3u \geq v + 1$, then $(U_{t,i}) \geq -tP$.

(iii) The elements $U_{t,i}$, $t \geq 0$, $i = 1, 2, 3$ are linearly independent with the following exception: $q \equiv 2 \pmod 3$, $t = (q^2 - q + 1)/3$,

$$(5) \qquad \frac{U_{t,1}}{\gamma_1^q} + \frac{U_{t,2}}{\gamma_2^q} + \frac{U_{t,3}}{\gamma_3^q} = 0.$$

(iv) The set

$$\mathcal{U}(s) = \{U_{t,i} \mid t \in H(P),\ t \leq s,\ i = 1, 2, 3,\ (3t, i) \neq (q^2 - q + 1, 3)\}$$

of rational functions is a basis of $\mathscr{L}(sP)$ over $\mathbb{F}_{q^6}$.

Proof. Notice first that u, v are uniquely defined by t, hence $U_{t,i}$ is well-defined. (i) is trivial, and (ii) is straightforward from (3). To show (iii), let us write a linear combination in the form

$$(6) \qquad \alpha_1 U_{t,1} + \alpha_2 U_{t,2} + \alpha_3 U_{t,3} = \sum_{r < t,i} \lambda_{r,i} U_{r,i}$$

such that $(\alpha_1, \alpha_2, \alpha_3) \neq (0,0,0)$. The right hand side has valuation at least $-t+1$ at P_1, P_2, P_3. If $t \neq (q^2 - q + 1)/3$ and $\alpha_i \neq 0$, then the right hand side has valuation $-t$ at P_{i+2}. Hence, $\alpha_i = 0$ for all $i = 1, 2, 3$, a contradiction. Assume $t = (q^2 - q + 1)/3$. Then

$$U_{t,i} = \frac{\ell_i \ell_{i+1}^q}{(\ell_1 \ell_2 \ell_3)^{\frac{q+1}{3}}},$$

and (5) follows from (2). We can use (5) to eliminate $U_{t,3}$ from (6), that is, we may assume $\alpha_3 = 0$. Then again, the only term which has valuation $-t$ at P_{i+2} is $\alpha_i U_{t,i}$ with $\alpha_i \neq 0$. Since the left and right hand sides of (6) must have the same valuations at P_1, P_3, $\alpha_1 = \alpha_2 = 0$ must hold, a contradiction.

(iv) By (iii), $\mathcal{U}(s)$ consists of linearly independent elements. To show that it is a basis of $\mathscr{L}(sP)$, it suffices to show that $|\mathcal{U}(s)| = \dim(\mathscr{L}(sP)$ for $3s \geq 2\mathfrak{g} - 2$. On the one hand, in this case $\dim(\mathscr{L}(sP) = 3s + 1 - \mathfrak{g}$. On the other hand,

$$|\mathcal{U}(s)| = 1 + 3(s - |G(P)|) - \varepsilon = 3s + 1 - (3|G(P)| + \varepsilon),$$

where $\varepsilon = 0$ if $q \equiv 0, 1 \pmod 3$, and $\varepsilon = 1$ if $q \equiv 2 \pmod 3$. By Lemma 4.1, $3|G(P)| + \varepsilon = \mathfrak{g}$, and the claim follows. $\qquad\square$

It is useful to have a decomposition of $\mathscr{L}(sP)$ over $\mathbb{F}_{q^2}$.

Theorem 4.3. *For $t \geq 0$ integer and $\alpha \in \mathbb{F}_{q^6}$ define the rational function*

$$W_{t,\alpha} = \alpha U_{t,1} + \alpha^{q^2} U_{t,2} + \alpha^{q^4} U_{t,3}$$

and the $\mathbb{F}_{q^2}$-linear space

$$\mathcal{W}_t = \{W_{t,\alpha} \mid \alpha \in \mathbb{F}_{q^6}\}.$$

For $t \in H(P)$, we have

$$\dim(\mathcal{W}_t) = \begin{cases} 1 & \text{if } t = 0, \\ 2 & \text{if } q \equiv 2 \pmod 3 \text{ and } t = (q^2 - q + 1)/3, \\ 3 & \text{otherwise.} \end{cases}$$

The $\mathbb{F}_{q^2}$-rational Riemann-Roch space $\mathscr{L}(sP)$ has the direct sum decomposition

$$\text{(7)} \qquad\qquad \mathscr{L}(sP) = \bigoplus_{t \in H(P), \, t \leq s} \mathcal{W}_t.$$

Proof. For $t \in H(P)$, $\mathcal{W}_t$ is the set of $\mathbb{F}_{q^2}$-rational functions in the space spanned by $U_{t,1}, U_{t,2}, U_{t,3}$. The claims follow from Proposition 4.2. $\qquad\square$

4.2. Invariant subspaces of $\mathscr{L}(sP)$.

Lemma 4.4. *Let $b \in \mathbb{F}_{q^6}$ such that $b^{q^3+1} = 1$. Then $(b^{q+1})^{q^2} = (b^{q+1})^{q-1}$ and $(b^{q+1})^{q^4} = (b^{q+1})^{-q}$.*

Proof. By assumption, b^{q+1} has order $q^2 - q + 1$. The claim follows from the facts that $q^2 - (q - 1)$ and $q^4 - q$ are divisible by $q^2 - q + 1$. $\qquad\square$

The following lemma shows that the basis elements in $\mathcal{U}(s)$ are eigenvectors of $\mathcal{B}^*$.

Lemma 4.5. *Let $\beta_1 \in \mathbb{F}_{q^6}$ be an element such that $\beta_1^{q^3+1} = 1$. Define $\beta_2 = \beta_1^{q^2}$, $\beta_3 = \beta_2^{q^2}$, and the unitary map $B = B(\beta_1) \in \mathcal{B}$. Then*

$$(U_{t,i})^{B^*} = \beta_i^{t(q+1)} U_{t,i}.$$

Proof. Proposition 3.3 implies

$$\left(\frac{\ell_i}{\ell_{i+2}}\right)^{B^*} = \frac{1}{\beta_{i+2}^{q+1}}\left(\frac{\ell_i}{\ell_{i+2}}\right)$$

and

$$\left(\frac{\ell_{i+1}}{\ell_i}\right)^{B^*} = \frac{1}{\beta_i^{q+1}}\left(\frac{\ell_{i+1}}{\ell_i}\right).$$

By Lemma 4.4, $\frac{1}{\beta_{i+2}^{q+1}} = (\beta_i^{q+1})^{-q^4} = (\beta_i^{q+1})^q$. Write $t = u(q+1) - v$ with $0 \leq v \leq q$. Then,

$$B^* : \left(\frac{\ell_i}{\ell_{i+2}}\right)^u \left(\frac{\ell_{i+1}}{\ell_i}\right)^{v-u} \mapsto (\beta_i^{q+1})^{qu}\left(\frac{\ell_i}{\ell_{i+2}}\right)^u (\beta_i^{q+1})^{-v+u}\left(\frac{\ell_{i+1}}{\ell_i}\right)^{v-u}$$

The result follows from the definition of u and v. $\qquad\square$

Proposition 4.6. (i) Let $\beta_1 \in \mathbb{F}_{q^6}$ be an element such that $\beta_1^{q^3+1} = 1$, and $B = B(\beta_1) \in \mathcal{B}$. Then

$$(W_{t,\alpha})^{B^*} = W_{t,\beta_1^{t(q+1)}\alpha}.$$

(ii) The subspaces $\mathcal{W}_t$, $t \in H(P)$ are $\mathcal{B}^*$-invariant.
(iii) The $\mathbb{F}_{q^2}\mathcal{B}^*$-modules $\mathcal{W}_t$ and $\mathcal{W}_s$ are isomorphic if and only if one of the following holds:
a) $s \equiv t \pmod{q^2 - q + 1}$,
b) $s \equiv (q-1)t \pmod{q^2 - q + 1}$, or
c) $s \equiv -qt \pmod{q^2 - q + 1}$.

Proof. (i) and (ii) follow from Lemma 4.5. (iii) The $\Phi : \mathcal{W}_t \to \mathcal{W}_s$ be an $\mathbb{F}_{q^2}\mathcal{B}^*$-module isomorphism can be written as

$$(W_{t,\alpha})^\Phi = W_{t,\alpha\varphi},$$

where $\varphi : \mathbb{F}_{q^6} \to \mathbb{F}_{q^6}$ is an $\mathbb{F}_{q^2}$-linear bijection. Moreover,

$$(W_{t,\alpha})^{B^*\Phi} = (W_{t,\beta_1^{t(q+1)}\alpha})^\Phi = W_{s,(\beta_1^{t(q+1)}\alpha)\varphi},$$
$$(W_{t,\alpha})^{\Phi B^*} = (W_{s,\alpha\varphi})^{B^*} = W_{s,\beta_1^{s(q+1)}(\alpha\varphi)}.$$

Since $b = \beta_1^{q+1}$ satisfies $b^{q^2-q+1} = 1$, this means that for any $\alpha, b \in \mathbb{F}_{q^6}$, b^{q^2-q+1}, we have

$$(b^t\alpha)\varphi = b^s(\alpha\varphi).$$

Let b be an element of order $q^2 - q + 1$ in $\mathbb{F}_{q^6}$. If b^t or b^s is in $\mathbb{F}_{q^2}$, then $b^t = b^s$ and a) holds. Assume that neither b^t nor b^s is in $\mathbb{F}_{q^2}$. Then $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}(b^t) = \mathbb{F}_{q^2}(b^s)$, and over $\mathbb{F}_{q^2}$, the minimal polynomial of b^t has degree 3. Assume $b^{3t} + c_1 b^{2t} + c_2 b^t + c_3 = 0$ with $c_0, c_1, c_2 \in \mathbb{F}_{q^2}$. Then

$$\begin{aligned}
0 &= (b^{3t} + c_1 b^{2t} + c_2 b^t + c_3)\varphi \\
&= (b^{3t}\varphi) + c_1(b^{2t}\varphi) + c_2(b^t\varphi) + c_3(1\varphi) \\
&= (b^{3s} + c_1 b^{2s} + c_2 b^s + c_3)(1\varphi).
\end{aligned}$$

As φ is bijective, $0 = b^{3s} + c_1 b^{2s} + c_2 b^s + c_3$ follows. This means that b^s has the same minimal polynomial, and $b^t \to b^s$ extends to a field automorphism of $\mathbb{F}_{q^6}$ over $\mathbb{F}_{q^2}$. This implies $b^s = b^t$, $b^s = (b^t)^{q^2}$ or $b^s = (b^t)^{q^4}$, and the claim follows. $\qquad\square$

5. Hermitian codes of degree 3 places and their duals

In this section, we explore Hermitian codes of degree 3 places on the Hermitian curve $\mathscr{H}_q$. Let P be a degree 3 place on $\mathscr{H}_q$. Given a divisor $D = Q_1 + Q_2 + \cdots + Q_n$, where $n = q^3$ and Q_i are $\mathbb{F}_{q^2}$-rational affine points on $\mathscr{H}_q$, we set the parameters $G = sP$ and $\widetilde{D} = D + Q_\infty$ for a positive integer s.

5.1. Functional Hermitian codes of degree 3 places.
Given a divisor D and G, we define the degree 3 place functional Hermitian code $C_{\mathcal{L}}(D, sP)$ as:

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

This code forms an $[n, k]$ AG code, where $k \geq 3s - \mathfrak{g} + 1$, achieving equality when $\lfloor \frac{2\mathfrak{g}-2}{3} \rfloor < s < n$. Moreover, the code has a minimum distance $d \geq d^* = q^3 - 3s$, where d^* the designed minimum distance.

Additionally, another degree 3 place functional Hermitian code associated with G, denoted by $C_{\mathcal{L}}(\widetilde{D}, G)$, is constructed by evaluating functions in $\mathscr{L}(G)$ on all rational points $Q_1, Q_2, \cdots, Q_n$, and the point at infinity Q_∞, as follows:

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

Clearly, $C_{\mathcal{L}}(\widetilde{D}, G)$ has length of $n + 1$. Concerning the dimension, we have the following result.

Proposition 5.1. *If $s < q^3/3$, then $\mathscr{L}(sP)$, $C_{\mathcal{L}}(D, G)$ and $C_{\mathcal{L}}(\widetilde{D}, G)$ have the same dimension.*

Proof. If $f \in \ker \mathrm{ev}_D$, then $f \in \mathscr{L}(sP - D)$, which is trivial if $s < q^3/3$. In this case, $\ker \mathrm{ev}_{\widetilde{D}}$ is trivial as well. $\qquad\square$

Remark. Numerical experiments show that $\mathscr{L}(sP)$, $C_{\mathcal{L}}(D, G)$ and $C_{\mathcal{L}}(\widetilde{D}, G)$ have the same dimension if $s < (q^3 + 1)/3 + q - 1$.

In the study of the divisors D and $\widetilde{D}$, we make use of the polynomial

$$R(X, Y) = X \prod_{\substack{c \in \mathbb{F}_{q^2} \\ c^q + c \neq 0}} (Y - c).$$

As shown in [8, Section 2], the principal divisor of $R(x, y) \in \mathbb{F}_{q^2}(\mathscr{H}_q)$ is

$$(8) \qquad\qquad (R(x, y)) = D - q^3 Q_\infty.$$

Further properties of $R(x, y)$ are given in the following proposition.

Proposition 5.2. *In the function field, we have*

$$x^q R(x, y) = y^{q^2} - y \qquad and \qquad R(x, y) = x^{q^2} - x.$$

The differential of $R(x, y)$ is

$$d(R(x, y)) = -dx.$$

Proof. Clearly,

$$\prod_{\substack{c \in \mathbb{F}_{q^2} \\ c^q + c = 0}} (Y - c) = Y^q + Y,$$

and

$$\prod_{\substack{c \in \mathbb{F}_{q^2} \\ c^q + c \neq 0}} (Y - c) = \frac{\displaystyle\prod_{c \in \mathbb{F}_{q^2}} (Y - c)}{\displaystyle\prod_{\substack{c \in \mathbb{F}_{q^2} \\ c^q + c = 0}} (Y - c)} = \frac{Y^{q^2} - Y}{Y^q + Y}.$$

Hence, by $x^{q+1} = y + y^q$,

$$x^q R(x, y) = x^{q+1} \prod_{\substack{c \in \mathbb{F}_{q^2} \\ c^q + c \neq 0}} (y - c) = x^{q+1} \frac{y^{q^2} - y}{y^q + y} = y^{q^2} - y.$$

Using this we obtain

$$x^q(x^{q^2} - x) = (x^{q+1})^q - x^{q+1} = y^q + y^{q^2} - (y + y^q) = y^{q^2} - y = x^q R(x, y).$$

Canceling by x^q, we get $R(x, y) = x^{q^2} - x$, and $d(R(x, y)) = -dx$ follows immediately. $\square$

5.2. **Differential Hermitian codes of degree 3 places.** Differential Hermitian codes of degree 3 places are essential counterparts to functional codes on the Hermitian curve $\mathscr{H}_q$. The dual code $C_\Omega(D, G)$ of $C_\mathcal{L}(D, G)$ is referred to as the differential code. It constitutes an $[n, \ell(G - D) - \ell(G) + \deg D, d^\perp]$ code, where $d^\perp \leq \deg(G) - (2\mathfrak{g} - 2)$, with $\deg(G) - (2\mathfrak{g} - 2)$ being its designed distance.
  [18, Proposition 8.1.2] provides an explicit description of the differential code as functional code

$$C_\Omega(D, G) = C_\mathscr{L}(D - G + (dt) - (t)),$$

where t is an element of $\mathbb{F}_{q^2}(\mathscr{H}_q)$ such that $v_{Q_i}(t) = 1$ for all $i \in \{1, \ldots, q^3, \infty\}$. If $G = sP$ and $D = Q_1 + \cdots + Q_{q^3}$, then $t = R(x, y)$ is a good choice with

$$(dt) = (-dx) = (2\mathfrak{g} - 2)Q_\infty = (q - 2)(q + 1)Q_\infty,$$

see [18, Lemma 6.4.4]. Then, (8) implies the following proposition:

Proposition 5.3.

$$C_\Omega(D, sP) = C_\mathscr{L}(D, (q^3 + q^2 - q - 2)Q_\infty - sP).   \square$$

The computation of $C_\Omega(\widetilde{D}, sP)$ is more complicated. We claim the next results for prime powers $q \equiv 2 \pmod 3$, since the proofs are rather transparent in this case. We are certain that they hold for $q \equiv 1 \pmod 3$, as well. Our opinion is supported by numerical experiments with $q \leq 8$.

Lemma 5.4. *Assume $q \equiv 2 \pmod 3$ and define the $\mathbb{F}_{q^2}$-rational function*

$$T = \frac{1}{3}\left(\frac{\ell_1^{q^2}}{\ell_2} + \frac{\ell_2^{q^2}}{\ell_3} + \frac{\ell_3^{q^2}}{\ell_1}\right).$$

Then

$$d\left(\frac{R}{(\ell_1 \ell_2 \ell_3)^{\frac{q^2 - q + 1}{3}}}\right) = -\left(\frac{T}{(\ell_1 \ell_2 \ell_3)^{\frac{q^2 - q + 1}{3}}}\right) dx.$$

Proof. We have $d\ell_i = (a_i - x)^q dx$, and

$$\begin{aligned}
\ell_i^{q^2} - \ell_{i+1} &= a_i^{q^3} x^{q^2} - y^{q^2} - b_i^{q^3} - (a_{i+1}^q x - y - b_{i+1}^q) \\
&= a_{i+1}^q(x^{q^2} - x) - (y^{q^2} - y) \\
&= a_{i+1}^q R(x, y) - x^q R(x, y) \\
&= (a_{i+1} - x)^q R(x, y).
\end{aligned}$$

Hence,

$$d(\ell_1\ell_2\ell_3) = \ell_1\ell_2\ell_3 \cdot \left(\frac{(a_1-x)^q}{\ell_1} + \frac{(a_2-x)^q}{\ell_2} + \frac{(a_3-x)^q}{\ell_3} \right) dx$$

$$= \ell_1\ell_2\ell_3 \cdot \left(\frac{\ell_1^{q^2}/\ell_2}{R} + \frac{\ell_2^{q^2}/\ell_3}{R} + \frac{\ell_3^{q^2}/\ell_1}{R} \right) dx$$

$$= \frac{\ell_1\ell_2\ell_3}{R}(3T - 3)dx.$$

This implies

$$d\left(R(\ell_1\ell_2\ell_3)^{\frac{-q^2+q-1}{3}} \right) = \left(-(\ell_1\ell_2\ell_3)^{\frac{-q^2+q-1}{3}} \right) dx+$$

$$R\left(-\frac{1}{3}(\ell_1\ell_2\ell_3)^{\frac{-q^2+q-4}{3}} \right) \frac{\ell_1\ell_2\ell_3}{R}(3T-3)dx.$$

By easy cancellation

$$d\left(R(\ell_1\ell_2\ell_3)^{\frac{-q^2+q-1}{3}} \right) = \left(-(\ell_1\ell_2\ell_3)^{\frac{-q^2+q-1}{3}} \right) dx + -\frac{1}{3}(\ell_1\ell_2\ell_3)^{\frac{-q^2+q-1}{3}}(3T-3)dx$$

$$= -\left(\frac{T}{(\ell_1\ell_2\ell_3)^{\frac{q^2-q+1}{3}}} \right) dx. \qquad \square$$

Lemma 5.5. *Assume $q \equiv 2 \pmod 3$ and define the $\mathbb{F}_{q^2}$-rational functions*

$$T = \frac{1}{3}\left(\frac{\ell_1^{q^2}}{\ell_2} + \frac{\ell_2^{q^2}}{\ell_3} + \frac{\ell_3^{q^2}}{\ell_1} \right) \qquad \text{and} \qquad R_1 = \frac{R}{(\ell_1\ell_2\ell_3)^{\frac{q^2-q+1}{3}}}.$$

Let G be a divisor of $\mathbb{F}_{q^2}(\mathscr{H}_q)$ whose support is disjoint from the support of $\widetilde{D}$. Then

$$\mathscr{L}(\widetilde{D} - G + (dR_1) - (R_1)) = \mathscr{L}\left(\frac{(q^2-1)(q+1)}{3}P - G \right) \cdot \frac{(\ell_1\ell_2\ell_3)^{\frac{q^2-1}{3}}}{T}.$$

Proof. We have

$$\widetilde{D} - G + (dR_1) - (R_1) = \widetilde{D} - G + (T) - \frac{q^2-q+1}{3}(\ell_1\ell_2\ell_3) + (dx) - (R) + \frac{q^2-q+1}{3}(\ell_1\ell_2\ell_3)$$

$$= \widetilde{D} - G + (T) + (dx) - (R)$$

$$= Q_\infty + q^3 Q_\infty + (2\mathfrak{g} - 2)Q_\infty - G + (T)$$

$$= (q^2-1)(q+1)Q_\infty - G + (T)$$

$$= \frac{(q^2-1)(q+1)}{3}P - \left((\ell_1\ell_2\ell_3)^{\frac{q^2-1}{3}} \right) - G + (T).$$

For the Riemann-Roch spaces, the results follows. $\qquad \square$

Lemma 5.6. *For any $i, j \in \{1, 2, 3\}$, we have*

$$\left(\frac{\ell_i}{\ell_j} \right)(Q_\infty) = 1.$$

Proof. We use the local expansion $\tau(t) = (t : 1 : t^{q+1} + \cdots)$ of $\mathscr{H}_q$ at Q_∞. The dots stand for terms of higher degree.

$$\left(\frac{\ell_i}{\ell_j} \right)(\tau(t)) = \frac{a_i^q t - 1 - b_i^q(t^{q+1} + \cdots)}{a_j^q t - 1 - b_j^q(t^{q+1} + \cdots)},$$

which implies

$$\left(\frac{\ell_i}{\ell_j}\right)(Q_\infty) = \left(\frac{\ell_i}{\ell_j}\right)(\tau(0)) = 1.$$ $\square$

Lemma 5.7. *Assume $q \not\equiv 0 \pmod 3$ and define the $\mathbb{F}_{q^2}$-rational functions*

$$T = \frac{1}{3}\left(\frac{\ell_1^{q^2}}{\ell_2} + \frac{\ell_2^{q^2}}{\ell_3} + \frac{\ell_3^{q^2}}{\ell_1}\right) \qquad and \qquad T_1 = \frac{(\ell_1\ell_2\ell_3)^{\frac{q^2-1}{3}}}{T}.$$

Then $T_1(Q_\infty) = 1$.

Proof. Since

$$\frac{\ell_i^{q^2}}{\ell_{i+1}(\ell_1\ell_2\ell_3)^{\frac{q^2-1}{3}}}$$

is the product of terms like ℓ_i/ℓ_j, it takes the value 1 at Q_∞. This implies $(1/T_1)(Q_\infty) = 1$. $\square$

To state our main result on differential codes, we need the notion of the monomial equivalence of codes. Let $C \leq \mathbb{F}_q^n$ be linear subspaces and $\boldsymbol{\mu} = (\mu_1, \dots, \mu_n) \in (\mathbb{F}_q^*)^n$ with non-zero entries. We define the Schur product

$$\boldsymbol{\mu} \star C = \{(\mu_1 x_1, \dots, \mu_n x_n) \mid (x_1, \dots, x_n) \in C\}.$$

The vector $\boldsymbol{\mu}$ is also called a multiplier. Clearly, $\boldsymbol{\mu} \star C \leq \mathbb{F}_q^n$. Two linear codes $C_1, C_2 \leq \mathbb{F}_q^n$ are monomially equivalent, if $C_2 = \boldsymbol{\mu} \star C_1$ for some multiplier $\boldsymbol{\mu}$.

Theorem 5.8. *Assume $q \equiv 2 \pmod 3$ and define the $\mathbb{F}_{q^2}$-rational functions*

$$T = \frac{1}{3}\left(\frac{\ell_1^{q^2}}{\ell_2} + \frac{\ell_2^{q^2}}{\ell_3} + \frac{\ell_3^{q^2}}{\ell_1}\right) \qquad and \qquad T_1 = \frac{(\ell_1\ell_2\ell_3)^{\frac{q^2-1}{3}}}{T}.$$

Let G be a divisor of $\mathbb{F}_{q^2}(\mathscr{H}_q)$ whose support is disjoint from the support of $\widetilde{D}$. Define $\mu_i = T_1(Q_i)$ for $i \in \{1, \dots, q^3, \infty\}$, and write $\boldsymbol{\mu} = (\mu_i)$. Then all entries $\mu_i \in \mathbb{F}_{q^2}^*$, and

$$C_\Omega(\widetilde{D}, G) = \boldsymbol{\mu} \star C_{\mathscr{L}}\left(\widetilde{D}, \frac{(q^2-1)(q+1)}{3}P - G\right).$$

Proof. If $i \in \{1, \dots, q^3\}$, then $\ell_i^{q^2}(Q_i) = \ell_{i+1}(Q_i)$. Therefore, $T(Q_i) = 1$ and $T_1(Q_1)$ is a well-defined non-zero element in $\mathbb{F}_q$. Lemma 5.7 implies $T_1(Q_\infty) = 1$. The theorem follows from Lemma 5.5. $\square$

Corollary.

$$C_\Omega(\widetilde{D}, sP) = \boldsymbol{\mu} \star C_{\mathcal{L}}\left(\widetilde{D}, \left(\frac{(q^2-1)(q+1)}{3} - s\right)P\right).$$

6. Hermitian subfield subcodes from degree 3 places

In this section, we study the subfield subcodes of $C_{\mathcal{L}}(D, sP)$. As before, q is a prime power, $s \geq 0$ integer, and P is a place of degree 3 of the Hermitian curve $\mathscr{H}_q$. The divisor $D = Q_1 + \cdots + Q_n$, $n = q^3$, is defined as the sum of the $\mathbb{F}_{q^2}$-rational affine places of $\mathscr{H}_q$. The rational place at infinity is Q_∞ and $\widetilde{D} = D + Q_\infty$.

6.1. **Trace maps of Hermitian functions and Hermitian codes.** We collect properties of the maps $z \mapsto z^q + z$ and $z \mapsto z^q - z$, where z is either a field element, a function, or a vector. We refer to $z^q + z$ as the trace of z, and to the map itself as the trace map $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$. Clearly, Tr is linear over $\mathbb{F}_q$.

Lemma 6.1. *Consider a positive divisor G_1. The trace map satisfies the following properties:*

(i) *For any function $f \in \mathscr{L}(G_1)$, its trace lies within $\mathscr{L}(qG_1)$, implying $\mathrm{Tr}(\mathscr{L}(G_1)) \subseteq \mathscr{L}(qG_1)$.*
(ii) *Similarly, for any codeword $c \in C_{\mathcal{L}}(D, G_1)$, its trace resides in $C_{\mathcal{L}}(D, qG_1)$.*
(iii) *$\mathrm{Tr}(C_{\mathcal{L}}(D, G_1))$ is an $\mathbb{F}_q$-linear subspace of $C_{\mathcal{L}}(D, qG_1) \cap \mathbb{F}_q^n$.*

Proof. Since $G_1 \geq 0$, we have $\mathscr{L}(G_1), \mathscr{L}(G_1)^q \leq \mathscr{L}(qG_1)$, hence (i) holds. (i) implies (ii). (iii) follows trivially. $\square$

Proposition 6.2. *Let G_1 be a positive divisor satisfying $\deg G_1 < n/q$. Then $\mathrm{ev}_D(\mathrm{Tr}(C_{\mathcal{L}}(D, G_1)))$ is an $\mathbb{F}_q$-linear subfield subcode of $C_{\mathcal{L}}(D, qG_1)$. Its dimension is*

$$\dim_{\mathbb{F}_q}(\mathrm{Tr}(C_{\mathcal{L}}(D, G_1))) = 2\dim_{\mathbb{F}_{q^2}}(\mathscr{L}(G_1)) - 1.$$

Proof. The first statement follows from Lemma 6.1. Since $\deg(G_1) < n$, the evaluation map is injective. To compute the dimension, we have to show that the kernel of $\mathrm{Tr} : C_{\mathcal{L}}(D, G_1) \to C_{\mathcal{L}}(D, qG_1)$ has dimension 1 over $\mathbb{F}_q$. Define $\varepsilon \in \mathbb{F}_{q^2}$ such that $\varepsilon = 1$ if q is even, and $\varepsilon = g^{(q+1)/2}$, if q is odd and g is a primitive element in $\mathbb{F}_{q^2}$. Then $\varepsilon^{q-1} = -1$. For the codeword $u \in C_{\mathcal{L}}(D, G_1)$, we have

$$\mathrm{Tr}(u) = u^q + u = 0 \Longrightarrow 0 = \varepsilon^q(u^q + u) = (\varepsilon u)^q - (\varepsilon u),$$

that is, $\varepsilon u \in \mathbb{F}_q^n$. By Proposition 2.3, $C_{\mathcal{L}}(D, G_1)|_{\mathbb{F}_q}$ has dimension 1, hence the same is true for the kernel of $\mathrm{Tr} : C_{\mathcal{L}}(D, G_1) \to C_{\mathcal{L}}(D, qG_1)$. $\square$

6.2. **An explicit subfield subcode.** In this subsection, we study a subfield subcode of $C_{\mathcal{L}}(D, (q^2 - q + 1)P)$. As $q^2 - q + 1 = (q-1)(q+1) - (q-1)$, one has

$$U_{q^2-q+1,i} = \frac{\ell_i^q \ell_{i+2}}{\ell_{i+1}\ell_{i+2}^q}.$$

The vector space $\mathcal{W}_{q^2-q+1} \leq \mathscr{L}((q^2 - q + 1)P)$ consists of the functions

$$W_{q^2-q+1,\alpha} = \alpha \frac{\ell_1^q \ell_3}{\ell_2 \ell_3^q} + \alpha^{q^2} \frac{\ell_2^q \ell_1}{\ell_3 \ell_1^q} + \alpha^{q^4} \frac{\ell_3^q \ell_2}{\ell_1 \ell_2^q}, \qquad \alpha \in \mathbb{F}_{q^6}.$$

For rational functions $f, g \in \mathbb{F}_{q^6}(\mathscr{H}_q)$, we introduce the relation

$$f \approx g \Longleftrightarrow f(Q_i) = g(Q_i) \quad \text{for all } i \in \{1, \ldots, q^3, \infty\}.$$

This is clearly an equivalence relation, which can be also written in terms of the principal divisor

$$f \approx g \Longleftrightarrow (f - g) \geq \widetilde{D},$$

or in terms of the evaluation map

$$f \approx g \Longleftrightarrow \mathrm{ev}_{\widetilde{D}}(f) = \mathrm{ev}_{\widetilde{D}}(g).$$

Lemma 6.3. (i) *$(U_{q^2-q+1,i})^q \approx U_{q^2-q+1,i+2}$.*
(ii) *$(W_{q^2-q+1,\alpha})^q \approx W_{q^2-q+1,\alpha^{q^3}}$.*

Proof. Lemma 5.6 implies $U_{q^2-q+1,i}(Q_\infty) = 1$. In the proof of Lemma 5.4 we have seen that $\ell_i^{q^2} - \ell_{i+1} = (a_{i+1} - x)^q R(x,y)$. Therefore, $(\ell_i^{q^2} - \ell_{i+1})(Q_i) = 0$ for all $i \in \{1, \ldots, q^3\}$. This shows

$$(U_{q^2-q+1,i})^q(Q_i) = \left(\frac{\ell_i^{q^2} \ell_{i+2}^q}{\ell_{i+1}^q \ell_{i+2}^{q^2}} \right)(Q_i)$$

$$= \left(\frac{\ell_{i+1} \ell_{i+2}^q}{\ell_{i+1}^q \ell_{i+}} \right)(Q_i)$$

$$= U_{q^2-q+1,i+2}(Q_i)$$

This proves (i). For (ii):

$$(W_{q^2-q+1,\alpha})^q = (\alpha U_{q^2-q+1,1} + \alpha^{q^2} U_{q^2-q+1,2} + \alpha^{q^4} U_{q^2-q+1,3})^q$$

$$\approx \alpha^q U_{q^2-q+1,3} + \alpha^{q^3} U_{q^2-q+1,1} + \alpha^{q^5} U_{q^2-q+1,2}$$

$$= \alpha^{q^3} U_{q^2-q+1,1} + (\alpha^{q^3})^{q^2} U_{q^2-q+1,2} + (\alpha^{q^3})^{q^4} U_{q^2-q+1,3}$$

$$= W_{q^2-q+1,\alpha^{q^3}}. \qquad \square$$

Proposition 6.4. *The set*

$$\widetilde{\mathcal{W}} = \{\mathrm{ev}_D(W_{q^2-q+1,\alpha}) \mid \alpha \in \mathbb{F}_{q^3}\}$$

is a 3-dimensional $\mathbb{F}_q$-linear subfield subcode of $C_\mathcal{L}(D, (q^2 - q + 1)P)$.

Proof. Lemma 6.3(ii) implies that $\mathrm{ev}_D(W_{q^2-q+1,\alpha})$ has $\mathbb{F}_q$-entries if and only if $\alpha^{q^3} = \alpha$. $\qquad \square$

6.3. **Main result and a conjecture.**

Theorem 6.5. *Let $q \geq 3$ be a prime power, $n = q^3$, $D = Q_1 + \cdots + Q_n$ the sum of rational affine places of $\mathbb{F}_{q^2}(\mathcal{H}_q)$, and P a place of degree 3. For the dimension of the subfield subcode of the one-point Hermitian code yields*

$$\dim C_\mathcal{L}(D, sP)|_{\mathbb{F}_q} \geq \begin{cases} 7 & \text{for } s = 2\mathfrak{g} = q(q-1), \\ 10 & \text{for } s = 2\mathfrak{g} + 1 = q^2 - q + 1. \end{cases}$$

Proof. Set $G_1 = (q-1)P$. By Proposition 6.2,

$$\mathcal{T} = \mathrm{ev}_D(\mathrm{Tr}(\mathscr{L}(G_1)))$$

is an $\mathbb{F}_q$-linear subspace in $C_\mathcal{L}(D, q(q-1)P)|_{\mathbb{F}_q}$. Since $\dim(\mathscr{L}((q-1)P)) = 4$, $\mathcal{T}$ has dimension 7. This proves $\dim C_\mathcal{L}(D, q(q-1)P)|_{\mathbb{F}_q} \geq 7$.

Let $\widetilde{\mathcal{W}}$ the 3-dimensional $\mathbb{F}_q$-linear subfield subcode of $C_\mathcal{L}(D, (q^2 - q + 1)P)$ given in Proposition 6.4. We show that $\mathcal{T} \cap \widetilde{\mathcal{W}} = \{0\}$; the inequality $\dim C_\mathcal{L}(D, (q^2 - q + 1)P)|_{\mathbb{F}_q} \geq 10$ will follow. On the one hand,

$$\widetilde{\mathcal{W}} \leq \mathrm{ev}_D(\mathcal{W}_{q^2-q+1}).$$

On the other hand, using Theorem 4.3, we have

$$\mathcal{T} \leq \mathrm{ev}_D(\mathscr{L}(q(q-1)P)) = \mathrm{ev}_D \left(\bigoplus_{t \in H(P), t \leq q(q-1)} \mathcal{W}_t \right).$$

As ev_D is injective on $\mathscr{L}((q^2 - q + 1)P)$, and

$$\left(\bigoplus_{t \in H(P), t \leq q(q-1)} \mathcal{W}_t \right) \cap \mathcal{W}_{q^2-q+1} = \{0\},$$

we obtain $\mathcal{T} \cap \widetilde{\mathcal{W}} = \{0\}$. This completes the proof. $\qquad \square$

Our proof was constructive, we used the subfield subcodes given explicitly in the previous subsections. Based on computer calculations for small q, we have the following conjecture.

Conjecture 6.1. *If $q \geq 4$, then equalities hold in Theorem 6.5.*

The claim of the conjecture has some equivalent formulations.

Proposition 6.6. *The following are equivalent.*
 (i) $\dim C_{\mathcal{L}}(D, (q^2 - q)P)|_{\mathbb{F}_q} = 7$.
 (ii) $\dim C_{\mathcal{L}}(D, (q^2 - q - 1)P)|_{\mathbb{F}_q} = 1$.
 (iii) $\dim C_{\mathcal{L}}(D, sP)|_{\mathbb{F}_q} = 1$ *for all* $0 \leq s \leq 2\mathfrak{g} - 1 = q^2 - q - 1$.

Proof. We use the notation of the proof of Theorem 6.5. Assume (i). We have $\mathscr{L}((q-1)P) = \mathcal{W}_0 \oplus \mathcal{W}_{q-1}$. Moreover, $\mathcal{T}$ is an $\mathbb{F}_q\mathcal{B}$-module which decomposes into the direct sum of a 1-dimensional and a 6-dimensional submodule. Notice that non-trivial irreducible $\mathbb{F}_q\mathcal{B}$-module have dimension 6. Since $\mathcal{T} \cap C_{\mathcal{L}}(D, (q^2 - q - 1)P)$ is a proper submodule, the only possibility is the it is 1-dimensional over $\mathbb{F}_q$. (ii) follows. Trivially, (ii) implies (iii). Let us now assume (iii).

$$\dim_{\mathbb{F}_q} C_{\mathcal{L}}(D, (q^2 - q)P)/C_{\mathcal{L}}(D, (q^2 - q - 1)P) = 6,$$

therefore,

$$\dim_{\mathbb{F}_q} C_{\mathcal{L}}(D, (q^2 - q)P)|_{\mathbb{F}_q}/C_{\mathcal{L}}(D, (q^2 - q - 1)P)|_{\mathbb{F}_q} \leq 6.$$

This implies $\dim C_{\mathcal{L}}(D, (q^2 - q)P)|_{\mathbb{F}_q} \leq 7$. Together with Theorem 6.5, we have (i). $\square$

We have partial result related to case (iii) of Proposition 6.6.

Proposition 6.7. $\dim C_{\mathcal{L}}(D, sP)|_{\mathbb{F}_q} = 1$ *for all* $0 \leq s \leq \frac{2}{3}\mathfrak{g}$.

Proof. Fix an arbitrary integer s in the range $0 \leq s < \frac{2}{3}\mathfrak{g}$ 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 $i = 1, \ldots, q^3$. 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 $\deg(G) \leq 2\mathfrak{g} = q(q-1)$ 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, $C_{\mathcal{L}}(D, sP)|_{\mathbb{F}_q}$ consists of constant vectors. This completes the proof. $\square$

References

[1] Post-Quantum Cryptography. `http://csrc.nist.gov/projects/post-quantum-cryptography`. Updated: March 25, 2020.

[2] Peter Beelen, Maria Montanucci, and Lara Vicino. Weierstrass semigroups and automorphism group of a maximal curve with the third largest genus. *arXiv preprint arXiv:2303.00376*, 2023.

[3] Antonio Cossidente, Gabor Korchmáros, and Fernando Torres. On curves covered by the hermitian curve. *Journal of Algebra*, 216(1):56–76, 1999.

[4] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based attacks on public-key cryptosystems using reed–solomon codes. *Designs, Codes and Cryptography*, 73:641–666, 2014.

[5] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. Cryptanalysis of mceliece cryptosystem based on algebraic geometry codes and their subcodes. *IEEE Transactions on Information Theory*, 63(8):5404–5418, 2017.

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

[7] Jean-Charles Faugere, Valérie Gauthier-Umana, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high-rate mceliece cryptosystems. *IEEE Transactions on Information Theory*, 59(10):6830–6844, 2013.

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

[9] Gábor Korchmáros, Gábor P Nagy, and Marco Timpanella. Codes and gap sequences of hermitian curves. *IEEE Transactions on Information Theory*, 66(6):3547–3554, 2019.

[10] John Little, Keith Saints, and Chris Heegard. On the structure of hermitian codes. *Journal of pure and applied algebra*, 121(3):293–314, 1997.

[11] Thomas G Macdonald and Michael B Pursley. Hermitian codes for frequency-hop spread-spectrum packet radio networks. *IEEE transactions on wireless communications*, 2(3):529–536, 2003.

[12] 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.

[13] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[14] Jian Ren. On the structure of hermitian codes and decoding for burst errors. *IEEE transactions on information theory*, 50(11):2850–2854, 2004.

[15] Nicolas Sendrier. On the security of the mceliece public-key cryptosystem. In *Information, Coding and Mathematics: Proceedings of Workshop honoring Prof. Bob McEliece on his 60th birthday*, pages 141–163. Springer, 2002.

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

[17] Henning Stichtenoth. A note on hermitian codes over gf (q/sup 2/). *IEEE transactions on Information Theory*, 34(5):1345–1348, 1988.

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

[19] Kyeongcheol Yang and P Vijay Kumar. On the true minimum distance of hermitian codes. In *Coding Theory and Algebraic Geometry: Proceedings of the International Workshop held in Luminy, France, June 17–21, 1991*, pages 99–107. Springer, 1992.

Bolyai Institute, University of Szeged, Aradi Vértanúk tere 1, H-6720 Szeged, Hungary; and Institute of Mathematics, Budapest University of Technology and Economics, Műegyetem rkp. 3, H-1111 Budapest, Hungary.

Email address: `nagyg@math.u-szeged.hu, nagy.gabor.peter@ttk.bme.hu`

Univ Rennes, IRMAR - UMR 6625, F-35000 Rennes, France

Email address: `sabiraelkhalfaoui@gmail.com`