

# 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  $m$  is a divisor of  $n$ . 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 [Sen02, FGUO<sup>+</sup>13]. The consistent strength of the McEliece cryptosystem, based on Goppa codes as introduced by McEliece in 1978 [McE78], emphasizes its effectiveness in resisting such attacks. Despite subsequent proposals leveraging Reed-Solomon codes [CGGU<sup>+</sup>14], AG codes, and their subcodes [CMCP17], all have been vulnerable to structural attacks. By

---

*Date:* March 5, 2024.

*Key words and phrases.* Hermitian curves, Degree 3 places, Riemann-Roch space, Hermitian codes, Subfield subcodes, Automorphisms of Hermitian codes.

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 [MP03]. Hermitian codes have been extensively investigated in previous studies [Sti88, LSH97, YK92, KNT19, Ren04], particularly those associated with the point at infinity of the Hermitian curve. However, in [KN13, MM05], 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 [KN13].

In consideration of the necessity for explicit and simplified bases to substantiate assertions concerning Hermitian codes, and given the advantageous properties demonstrated by their subfield subcodes, which adhere to the security assumptions of the McEliece cryptosystem, our investigation endeavors to delve deeper into this code family. Our objective is to derive additional properties that can be utilized in constructing a secure McEliece cryptosystem.

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 ....

Our contribution,...

TWO IMPORTANT PAPRES: [CKT99, BMV23].

ADD FURTHER REFERENCES!

## 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  $\mathcal{H}_q$ , over the finite field  $\mathbb{F}_{q^2}$  in affine coordinates, is given by the equation:

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

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  $\#\mathcal{H}_q(\mathbb{F}_{q^2}) = q^3 + 1$ . Additionally,  $\mathcal{H}_q$  possesses a unique singular point at infinity, denoted  $Q_\infty$ .

A divisor on  $\mathcal{H}_q$  is a formal sum  $D = n_1 Q_1 + \dots + n_k Q_k$  where  $n_1, \dots, n_k$  are integers, and  $Q_1, \dots, Q_k$  are points on  $\mathcal{H}_q$ . 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  $\text{Fr}_{q^2}$ , is defined over the algebraic closure  $\overline{\mathbb{F}_{q^2}}$  and acts on elements by

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

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

For a divisor  $D$ , its Frobenius image is given by

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

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

**Riemann-Roch space.** For a non-zero function  $g$  in the function field  $\overline{\mathbb{F}}_{q^2}$  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

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

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  $\mathbb{F}_{q^2}(\mathcal{H}_q)$  and  $s$  is a positive integer. In the extended constant field of  $\mathbb{F}_{q^2}(\mathcal{H}_q)$  with degree  $r$ , let  $P_1, P_2, \dots, P_r$  be the extensions of  $P$ . These points are degree-one places in  $\mathbb{F}_{q^{2r}}(\mathcal{H}_q)$ , and, by appropriately labeling the indices,  $P_i = \text{Fr}_{q^2}^i(P_1)$ , 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  $\mathcal{H}_q$ , is listed as  $\{Q_1, \dots, Q_n\}$ . 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  $\text{Supp}(G) \cap \mathcal{P} = \emptyset$ . By numbering the points in  $\mathcal{P}$ , we define an evaluation map  $\text{ev}_{\mathcal{P}}$  such that  $\text{ev}_{\mathcal{P}}(g) = (g(Q_1), \dots, g(Q_n))$  for  $g \in \mathcal{L}(G)$ .

The functional AG code associated with the divisor  $G$  is

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

**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  $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_q)$ . 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  $C$  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  $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$  denote the trace function from  $\mathbb{F}_{q^m}$  down to  $\mathbb{F}_q$ , expressed as

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

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

$$\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c) = (\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_1), \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_2), \dots, \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_n)).$$

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

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

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]:

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

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

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

Then

$$(3) \quad \dim \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathcal{C}_{\mathcal{L}}) \leq \begin{cases} m(\ell(G) - \ell(G_1)) + 1 & \text{if } G_1 \geq 0, \\ m(\ell(G) - \ell(G_1)) & \text{if } G_1 \not\geq 0, \end{cases}$$

and

$$(4) \quad \dim C_{\Omega}|_{\mathbb{F}_q} \geq \begin{cases} n - 1 - m(\ell(G) - \ell(G_1)) & \text{if } G_1 \geq 0, \\ n - m(\ell(G) - \ell(G_1)) & \text{if } G_1 \not\geq 0. \end{cases}$$

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

$$G_1 = \left\lfloor \frac{q(q-1)}{r} \right\rfloor P \quad \text{and} \quad G = q \cdot G_1,$$

in (3) and (4) we can replace  $\ell(G_1)$  and  $\ell(G)$  by  $\deg G_1$  and  $\deg G$  since  $\deg G_1 = q(q-1) = 2g$ , 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  $\mathcal{H}_q$  of degree  $r$  such that:*

$$G_1 = \left\lfloor \frac{q(q-1)}{r} \right\rfloor P \quad \text{and} \quad G = q \cdot G_1,$$

then

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

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

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

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

### 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  $\mathcal{H}_q$  has affine equation  $X^{q+1} = Y + Y^q$ . The Hermitian function field  $\mathbb{F}_{q^2}(\mathcal{H}_q)$  is generated by  $x, y$  such that  $x^{q+1} = y + y^q$  holds. The Frobenius field automorphism  $\text{Fr}_{q^2} : x \mapsto x^{q^2}$  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  $\text{Fr}_{q^2}$  in the exponent:  $P^{\text{Fr}_{q^2}}, f^{\text{Fr}_{q^2}}, D^{\text{Fr}_{q^2}}$ , 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

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

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  $\mathcal{H}_q$ .

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

**3.2. Unitary transformations and curve automorphism.** Let  $A$  be a  $3 \times 3$  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

$$\begin{aligned} u'_1 &= a_{11}u_1 + a_{21}u_2 + a_{31}u_3, \\ u'_2 &= a_{12}u_1 + a_{22}u_2 + a_{32}u_3, \\ u'_3 &= a_{13}u_1 + a_{23}u_2 + a_{33}u_3. \end{aligned}$$

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

$$\begin{aligned} \langle (v^{\text{Fr}_{q^2}})A, uA \rangle &= \langle v^{\text{Fr}_{q^2}}, u \rangle \\ &= \langle u, v \rangle^q \\ &= \langle uA, vA \rangle^q \\ &= \langle (vA)^{\text{Fr}_{q^2}}, uA \rangle. \end{aligned}$$

This implies  $(v^{\text{Fr}_{q^2}})A = (vA)^{\text{Fr}_{q^2}}$  for all  $v$ , that is,  $A$  and  $\text{Fr}_{q^2}$  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  $\mathcal{H}_q$ , 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  $\mathcal{H}_q$ , and  $A^*$  induces an automorphism of the function field  $\bar{\mathbb{F}}_{q^2}(\mathcal{H}_q)$ . If  $A$  is defined over  $\text{Fr}_{q^2}$ , then  $A^*$  is an automorphism of  $\mathbb{F}_{q^2}(\mathcal{H}_q)$ .

**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  $\mathcal{H}_q : X^{q+1} = Y + Y^q$ , 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  $p_{i+1} = p_i^{\text{Fr}_{q^2}}$ ,  $\langle p_i, p_i \rangle = 0$ , and

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

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

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

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  $\bar{\mathbb{F}}_{q^2}(\mathcal{H}_q)$  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

$$(5) \quad 0 = x^{q+1} - y - y^q = \langle (x, y, 1), (x, y, 1) \rangle = \frac{\ell_1 \ell_2^q}{\gamma_1^q} + \frac{\ell_2 \ell_3^q}{\gamma_2^q} + \frac{\ell_3 \ell_1^q}{\gamma_3^q}.$$

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

$$(6) \quad (\ell_i) = qP_i + P_{i+1} - (q+1)Q_\infty.$$

**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

$$(7) \quad u' = x_1 p'_1 + x_2 p'_2 + x_3 p'_3 = x_1 \beta_1 p_1 + x_2 \beta_2 p_2 + x_3 \beta_3 p_3.$$

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,  $\Delta$  extends to a unitary linear map, which commutes with  $\text{Fr}_{q^2}$  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,  $\Delta^{-1}B\Delta = B^{q^2}$ .  $\Delta^3$  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,  $\Delta$  has order 3.

As introduced in Section 3.2, the unitary transformation  $B$  and  $\Delta$  induce automorphisms  $B^*$  and  $\Delta^*$  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  $\Delta^*$  normalizes  $\mathcal{B}^*$  by*

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

Both  $\mathcal{B}^*$  and  $\Delta^*$  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,

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

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

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

#### 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  $\mathbb{F}_{q^6}(\mathcal{H}_q)$ , associated to the projective point  $(a_i : b_i : 1)$ .  $P_i^{\text{Fr}_{q^2}} = P_{i+1}$ ; 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  $\mathbb{F}_{q^2}(\mathcal{H}_q)$ . The generators  $x, y$  of  $\mathbb{F}_{q^2}(\mathcal{H}_q)$  satisfy  $x^{q+1} = y + y^q$ . The rational function  $\ell_i = a_i^q x - y - b_i^q$  is obtained from the tangent line of  $\mathcal{H}_q$  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 [KN13], the Riemann-Roch space associated with the divisor  $sP$  is given as

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

The Weierstrass semigroup  $H(P)$  consists of the integers  $s \geq 0$  such that the pole divisor  $(f)_\infty = sP$  for some  $f \in \mathbb{F}_{q^2}(\mathcal{H}_q)$ . If  $s \notin H(P)$ , then it is called a Weierstrass gap; the set of Weierstrass gaps is denoted by  $G(P)$ . By [KN13, 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 [Sti09, 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

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

The following proposition gives an explicit basis for the Riemann-Roch space  $\mathcal{L}(sP)$  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*

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

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

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

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

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

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:  
 $q \equiv 2 \pmod{3}$ ,  $t = (q^2 - q + 1)/3$ ,

$$(8) \quad \frac{U_{t,1}}{\gamma_1^q} + \frac{U_{t,2}}{\gamma_2^q} + \frac{U_{t,3}}{\gamma_3^q} = 0.$$

(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  $\mathcal{L}(sP)$  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 (6). To show (iii), let us write a linear combination in the form

$$(9) \quad \alpha_1 U_{t,1} + \alpha_2 U_{t,2} + \alpha_3 U_{t,3} = \sum_{r < t, i} \lambda_{r,i} U_{r,i}$$

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 (8) follows from (5). We can use (8) to eliminate  $U_{t,3}$  from (9), 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 (9) 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  $\mathcal{L}(sP)$ , it suffices to show that  $|\mathcal{U}(s)| = \dim(\mathcal{L}(sP))$  for  $3s \geq 2g - 2$ . On the one hand, in this case  $\dim(\mathcal{L}(sP)) = 3s + 1 - g$ . 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,  $3|G(P)| + \varepsilon = g$ , and the claim follows.  $\square$

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

**Proposition 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  $\mathcal{L}(sP)$  has the direct sum decomposition

$$(10) \quad \mathcal{L}(sP) = \bigoplus_{t \in H(P), t \leq s} \mathcal{W}_t.$$

*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.  $\square$

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

**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  $q^2 - q + 1$ .  $\square$

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  $v$ .  $\square$

**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  $\Phi : \mathcal{W}_t \rightarrow \mathcal{W}_s$  be an  $\mathbb{F}_{q^2}\mathcal{B}^*$ -module isomorphism can be written as

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

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

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

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  $b^{3t} + c_1b^{2t} + c_2b^t + c_3 = 0$  with  $c_0, c_1, c_2 \in \mathbb{F}_{q^2}$ . Then

$$\begin{aligned} 0 &= (b^{3t} + c_1b^{2t} + c_2b^t + c_3)\varphi \\ &= (b^{3t}\varphi) + c_1(b^{2t}\varphi) + c_2(b^t\varphi) + c_3(1\varphi) \\ &= (b^{3s} + c_1b^{2s} + c_2b^s + c_3)(1\varphi). \end{aligned}$$

As  $\varphi$  is bijective,  $0 = b^{3s} + c_1b^{2s} + c_2b^s + c_3$  follows. This means that  $b^s$  has the same minimal polynomial, and  $b^t \rightarrow b^s$  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.  $\square$

## 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  $\mathcal{H}_q$ . Let  $P$  be a degree 3 place on  $\mathcal{H}_q$ . 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  $\mathcal{H}_q$ , we set the parameters  $G = sP$  and  $\tilde{D} = D + Q_\infty$  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:

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

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  $C_{\mathcal{L}}(\tilde{D}, G)$ , is constructed by evaluating functions in  $\mathcal{L}(G)$  on all rational points  $Q_1, Q_2, \dots, Q_n$ , and the point at infinity  $Q_\infty$ , as follows:

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

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

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

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

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

**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  $\mathcal{H}_q$ . 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  $d^{\perp} \leq \deg(G) - (2g - 2)$ , with  $\deg(G) - (2g - 2)$  being its designed distance.

In [KN13, Proposition 2.2], the authors provide an explicit description of an equivalence between the codes  $C_{\Omega}(D, G)$  and  $C_{\mathcal{L}}(D, (q^3 + q^2 - q - 2)Q_{\infty} - G)$  constructed on  $\mathcal{H}_q$ . This equivalence is related to the equivalence  $C_{\Omega}(D, G) = C_{\mathcal{L}}(D, W + D - G)$  given in Section 2.

Furthermore, the dual code  $C_{\Omega}(D + Q_{\infty}, G)$  of  $C_{\mathcal{L}}(D + Q_{\infty}, G)$  is denoted as  $C_{\Omega}(D + Q_{\infty}, G)$ , which is equivalent to  $C_{\mathcal{L}}(D + Q_{\infty}, W + D + Q_{\infty} - G)$  and shares the same parameters as  $C_{\Omega}(D + Q_{\infty}, G)$  except for the length, which is  $n + 1$ .

**What content or discussion is required before Proposition 5.1?**

MORE PRECISE INFORMATION ON  $\dim C_{\mathcal{L}}(D, sP)$ ,  $s$  SMALL, USING Prop 4.3 AND THE DECOMPOSITION (10).

**Proposition 5.2.** *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.* Let  $\ell_i = 0$  be the line  $P_i P_{i+1}$ , it is the tangent to  $\mathcal{H}_q$  at  $P_i$ . More precisely, the intersection divisor of  $\ell_i$  and  $\mathcal{H}_q$  is  $qP_i + P_{i+1}$ . This implies that the principal divisor of  $\ell_i/\ell_2$  satisfies

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

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

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

On the one hand,  $w_{\alpha}$  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,  $w_{\alpha}$  is contained in the Riemann-Roch space  $\mathcal{L}((q - 1)P)$ . Then  $1, w_{\alpha_1}, w_{\alpha_2}, w_{\alpha_3}$  is a basis of  $\mathcal{L}((q - 1)P)$ , provided  $\alpha_1, \alpha_2, \alpha_3$  form an  $\mathbb{F}_{q^2}$ -basis of  $\mathbb{F}_{q^6}$ . Thus,  $\dim \mathcal{L}((q - 1)P) = 4$ .  $\square$

**5.3. Dual codes.** 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 5.3.** *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].

## 6. HERMITIAN SUBFIELD SUBCODES FROM DEGREE 3 PLACES

**Proposition 6.1.** *The generators of  $C_{\mathcal{L}}(D + Q_{\infty}, sP)$  can be expressed in terms of the decomposition given in Proposition 4.3 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 7.2**

FEW WORDS ON THE NUMERICAL EXPERIMENTS.

**Conjecture 6.1.** 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  $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathcal{C}_{\mathcal{L}})$ . 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 6.2.** *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:**  $0 \leq s < \frac{2}{3}\mathfrak{g}$  or **from corollary ...**

Observe that constant polynomials belong to  $\mathcal{L}(sP)$  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  $(c_1, \dots, c_{q^3}) \in C_q(s)$ . This corresponds to a function  $g$  in  $\mathcal{L}(sP)$  such that  $c_i = g(Q_i)$  is an element of  $\mathbb{F}_q$  for each  $i = 1, \dots, q^3$ .

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  $\gamma$ . In other words, the function  $g - \gamma$  is in  $\mathcal{L}(sP)$  and has at least  $q^2$  zeros on  $\mathcal{H}_q$ . However, a non-zero function in  $\mathcal{L}(sP)$  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  $\gamma$ , 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:**  $s = 2g$ 

Let  $\ell_i = 0$  be the line  $P_i P_{i+1}$ , it is the tangent to  $\mathcal{H}_q$  at  $P_i$ . More precisely, the intersection divisor of  $\ell_i$  and  $\mathcal{H}_q$  is  $qP_i + P_{i+1}$ . This implies that the principal divisor of  $\ell_1/\ell_2$  satisfies

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

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

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

On the one hand,  $w_\alpha$  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,  $w_\alpha$  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)  $\operatorname{ev}_D(\mathbb{F}_q + \mathcal{W})$  is a subspace of  $C_{q(q-1)}$  of dimension 7.

This finishes the proof. □

**special case  $q = 2$  the dimension is 5**



## REFERENCES

- [BMV23] 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.
- [CGGU<sup>+</sup>14] 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.
- [CKT99] Antonio Cossidente, Gabor Korchmáros, and Fernando Torres. On curves covered by the hermitian curve. *Journal of Algebra*, 216(1):56–76, 1999.
- [CMCP17] 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.
- [Del75] Philippe Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Transactions on Information Theory*, 21(5):575–576, 1975.
- [FGUO<sup>+</sup>13] 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.
- [KN13] Gábor Korchmáros and Gábor P Nagy. Hermitian codes from higher degree places. *Journal of Pure and Applied Algebra*, 217(12):2371–2381, 2013.
- [KNT19] 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.
- [LSH97] John Little, Keith Saints, and Chris Heegard. On the structure of hermitian codes. *Journal of pure and applied algebra*, 121(3):293–314, 1997.
- [McE78] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.
- [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.
- [MP03] 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.
- [Ren04] Jian Ren. On the structure of hermitian codes and decoding for burst errors. *IEEE transactions on information theory*, 50(11):2850–2854, 2004.
- [Sen02] 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.
- [Ste12] Serguei A Stepanov. *Codes on algebraic curves*. Springer Science & Business Media, 2012.
- [Sti88] Henning Stichtenoth. A note on hermitian codes over  $\text{gf}(q^{\sup 2})$ . *IEEE transactions on Information Theory*, 34(5):1345–1348, 1988.
- [Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.
- [YK92] 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:* `nagy@math.u-szeged.hu`, `nagy.gabor.peter@ttk.bme.hu`

UNIV RENNES, IRMAR - UMR 6625, F-35000 RENNES, FRANCE

*Email address:* `sabiraelkhalfauoui@gmail.com`