Codes and gap sequences of Hermitian curves

Gábor Korchmáros, Gábor P. Nagy, Marco Timpanella

***Abstract*—Hermitian functional and differential codes are AG-codes defined on a Hermitian curve. To ensure good performance, the divisors defining such AG-codes have to be carefully chosen, exploiting the rich combinatorial and algebraic properties of the Hermitian curves. In this paper, the case of differential codes $C_\Omega(\mathtt{D}, m\mathtt{T})$ on the Hermitian curve $\mathscr{H}_{q^3}$ defined over $\mathbb{F}_{q^6}$ is worked out where $\mathrm{supp}(\mathtt{T}) := \mathscr{H}_{q^3}(\mathbb{F}_{q^2})$, the set of all $\mathbb{F}_{q^2}$-rational points of $\mathscr{H}_{q^3}$, while $\mathtt{D}$ is taken, as usual, to be the sum of the points in the complementary set $D = \mathscr{H}_{q^3}(\mathbb{F}_{q^6}) \setminus \mathscr{H}_{q^3}(\mathbb{F}_{q^2})$. For certain values of m, such codes $C_\Omega(\mathtt{D}, m\mathtt{T})$ have better minimum distance compared with true values of 1-point Hermitian codes. The automorphism group of $C_L(\mathtt{D}, m\mathtt{T})$, $m \le q^3 - 2$, is isomorphic to $PGU(3, q)$.**

***Index Terms*—AG-code, Weierstrass gap, pure gap, Hermitian curve; 14H55, 11T71, 11G20, 94B27**

I. Introduction

Algebraic-geometry (AG) codes, also called Goppa-codes, are certain linear codes arising from an algebraic curve $\mathcal{X}$ defined over a finite field; see for instance [1], [7], [10], [19]. In this paper, we work on the projective plane $PG(2, \mathbb{F}_{q^6})$ defined over the finite field $\mathbb{F}_{q^6}$ of order q^6 and equipped with homogeneous coordinates (X, Y, Z). The points and lines of $PG(2, \mathbb{F}_{q^6})$ with coordinates in the subfield $\mathbb{F}_{q^2}$ are the points and lines of the projective subplane $PG(2, \mathbb{F}_{q^2})$ of $PG(2, \mathbb{F}_{q^6})$. We take $\mathcal{X}$ to be the (non-singular) Hermitian curve $\mathscr{H}_{q^3}$ of $PG(2, \mathbb{F}_{q^6})$, with genus $\mathfrak{g}(\mathscr{H}_{q^3}) = \frac{1}{2}q^3(q^3-1)$ and defined by its canonical homogeneous equation

$$X^{q^3+1} - Y^{q^3}Z - YZ^{q^3} = 0, \tag{1}$$

and construct a particular family of AG-codes on the set of all points of $\mathscr{H}_{q^3}$ lying in $PG(2, \mathbb{F}_{q^6})$, that is, on the set $\mathscr{H}_{q^3}(\mathbb{F}_{q^6})$ of its $\mathbb{F}_{q^6}$-rational points. For this purpose, we take a divisor $\mathtt{G}$ whose support comprises all the points of $\mathscr{H}_{q^3}$ lying in the subplane $PG(2, \mathbb{F}_{q^2})$, that is, the $\mathbb{F}_{q^2}$-rational points of $\mathscr{H}_{q^3}$. They satisfy the equation $X^{q+1} - Y^qZ - YZ^q = 0$, and are exactly the $\mathbb{F}_{q^2}$-rational points of the Hermitian curve of $PG(2, \mathbb{F}_{q^2})$ given in its canonical homogenous equation

$$X^{q+1} - Y^qZ - YZ^q = 0. \tag{2}$$

More precisely, we define

$$\mathtt{T} := \sum_{Q \in \mathscr{H}_q(\mathbb{F}_{q^2})} Q$$

and, for a positive integer m, we put $\mathtt{G} = m\mathtt{T}$. Also, we define the set D by complement, that is,

$$D := \mathscr{H}_{q^3}(\mathbb{F}_{q^6}) \setminus \mathscr{H}_q(\mathbb{F}_{q^2}).$$

In particular, D has size $n := q^9 - q^3$. Furthermore, let $\mathtt{D} := \sum_{Q \in D} Q$.

An AG-code arises by evaluating at the points of D the $\mathbb{F}_{q^6}$-rational functions whose poles are prescribed by $\mathtt{T}$ (each with multiplicity $\le m$). It is an AG $[n, k, d]_{q^6}$-code with

$$d \ge n - \deg(m\mathtt{T}) = q^9 - q^3 - m(q^3 + 1)$$

and

$$k = \ell(m\mathtt{T}) - \ell(m\mathtt{T} - \mathtt{D}),$$

where $\ell(\mathtt{P})$ stands, as usual, for the dimension of the Riemann-Roch space associated to a divisor $\mathtt{P}$ on $\mathscr{H}_{q^3}$. Here, if $m(q^3 + 1) = \deg(m\mathtt{T}) > 2\mathfrak{g} - 2 = (q^3 + 1)(q^3 - 2)$, that is, if $m > q^3 - 2$, then the Riemann-Roch Theorem yields $k = \deg(m\mathtt{T}) + 1 - \frac{1}{2}q^3(q^3 - 1)$ whence

$$k = (q^3 + 1)(m - \tfrac{1}{2}(q^3 - 2)), \text{ for } m > q^3 - 2.$$

Such an AG-code is the *Hermitian functional code* $C_L(\mathtt{D}, m\mathtt{T})$ whose Goppa's designed minimum distance is

$$\delta := n - \deg(m\mathtt{T}) = (q^3 + 1)(q^3(q^3 - 1) - m).$$

Support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme, within the SETIT Project 2018-1.2.1-NKP-2018-00004. Partially supported by OTKA grants 119687 and 115288.

G. Korchmáros and M. Timpanella are with Dipartimento di Matematica, Informatica ed Economia, Università della Basilicata, Contrada Macchia Romana, 85100 Potenza (Italy) (e-mail: gabor.korchmaros@unibas.it, marco.timpanella@unibas.it).

G.P. Nagy is with Department of Algebra, Budapest University of Technology, Egri József utca 1, H-1111 Budapest (Hungary) and Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged (Hungary) (e-mail: nagyg@math.bme.hu).

The dual code $C_\Omega(\mathtt{D}, m\mathtt{T})$ of $C_L(\mathtt{D}, m\mathtt{T})$ can also be obtained by computing residuals in the space of holomorphic differentials $\Omega(m\mathtt{T} - \mathtt{D})$. Therefore,

$$C_\Omega(\mathtt{D}, m\mathtt{T}) = \{(\mathrm{res}(df)_{Q_1}, \ldots, \mathrm{res}(df)_{Q_n}) | \; df \in \Omega(m\mathtt{T} - \mathtt{D})\}.$$

For this reason, the latter code is called a *differential code*. It is a $[n, k', d']_{q^6}$-code where

$$d' \geq \deg(m\mathtt{T}) - (2\mathfrak{g} - 2) = (q^3+1)(m - (q^3-2)),$$

and $k' \geq n + \mathfrak{g} - 1 - \deg(m\mathtt{T})$ when $\deg(m\mathtt{T}) > 2\mathfrak{g} - 2$. In particular, equality holds if $\deg(m\mathtt{T}) < n$, that is,

$$k' = (q^3+1)(q^3(q^3-1) - m - \tfrac{1}{2}(q^3-2))$$

for

$$q^3 - 2 < m < q^3(q^3-1).$$

Its Goppa's designed minimum distance is

$$\delta^* = \deg(m\mathtt{T}) - (2\mathfrak{g} - 2) = (q^3+1)(m - (q^3-2)).$$

We exhibit values of m for which the differential code $C_\Omega(\mathtt{D}, m\mathtt{T})$ has good parameters. Its minimum distance is larger than the minimum distance of the one-point Hermitian code with the same length and dimension. The improvement is $O(q^4)$, see Theorem IV.3. The essential ingredient of the proof is the gap sequence of $\mathscr{H}_{q^3}$ on $\mathtt{T}$, which we compute explicitly: see Theorem III.2. We also prove that the group of permutation automorphisms of the code $C_L(\mathtt{D}, m\mathtt{T})$, $m < q^3-2$, is isomorphic to $PGU(3,q)$: see Theorem V.4. The computer algebra systems MAGMA [2] and GAP [5] helped us to formulate the results by computing the gap sequences for $q = 2, 3$ and 4. Moreover, we used these programs to verify that for $q = 2$, the true minimum distance of the code of Theorem IV.3 is equal to its designed minimum distance.

II. Preliminaries

We quote now several geometric and combinatorial properties of the Hermitian curves $\mathscr{H}_q$ and $\mathscr{H}_{q^3}$, the references are [8], [12].

A. Plane algebraic curves

Our notation and terminology are standard. For the theory of plane algebraic curves, the reader is referred to [9, Chapters 1-5]. Let $\mathbb{F}$ be a finite field and fix an algebraic closure $\mathbb{K}$ of $\mathbb{F}$, and let $AG(2,\mathbb{K})$ be the affine plane defined over $\mathbb{K}$. If $F \in \mathbb{K}[X,Y]$, then the *affine plane curve* $\mathscr{F}$ is

$$\mathscr{F} = \{P = (x,y) \in AG(2,\mathbb{K}) | F(x,y) = 0\}.$$

The *degree* of $\mathscr{F}$ is the degree of F. A *component* of $\mathscr{F}$ is a curve $\mathscr{G} = v_a(G)$ such that G divides F. A curve $\mathscr{F}$ is *irreducible* if F is irreducible; otherwise, $\mathscr{F}$ is *reducible* and it splits in irreducible curves, the *components* of $\mathscr{F}$. All these definitions are translated from $AG(2,\mathbb{K})$ to its projective closure $PG(2,\mathbb{K})$ when F is replaced by a form $F^* \in \mathbb{K}[X,Y,Z]$. For a form $F^* \in \mathbb{K}[X,Y,Z]$, the *projective plane curve* $\mathscr{F}$ is

$$\mathbf{v}(F^*) = \{P(x_1,x_2,x_3) \in PG(2,\mathbb{K}) \mid F(x_1,x_2,x_3) = 0\}.$$

If $\mathscr{F}$ is non-singular, that is, it has no singular point in $PG(2,\mathbb{K})$, then its genus equals $\mathfrak{g} = \frac{1}{2}(\deg(\mathscr{F})-1)(\deg(\mathscr{F})-2)$. Basic tools in the theory of plane curves are the theorem of Bézout, see [9, Theorem 3.14] which state the main properties of the intersection of two plane curves $\mathscr{F}$ and $\mathscr{G}$ in terms of their *intersection divisor* $\mathscr{F} \cdot \mathscr{G}$ depending on the *intersection number* $I(P, \mathscr{F} \cap \mathscr{G})$ at a point $P \in PG(2,\mathbb{K})$:

$$\deg(\mathscr{F})\deg(\mathscr{G}) = \sum_{P \in \mathscr{F} \cap \mathscr{G}} I(P, \mathscr{F} \cap \mathscr{G}).$$

B. Riemann-Roch spaces

Let $\mathbb{F}(\mathscr{F})$ be the function field of $\mathscr{F}$ with constant field $\mathbb{F}$, regarded as the subfield of the function field $\mathbb{K}(\mathscr{F})$ of $\mathscr{F}$ over $\mathbb{K}$. The divisors are formal sums of places (or branches) of $\mathbb{K}(\mathscr{F})$. If $\mathscr{F}$ is non-singular, then the places of $\mathbb{K}(\mathscr{F})$ can be identified with the points of $\mathscr{F}$ so that each point is the center of a unique place. For every non-zero function h in $\mathbb{F}(\mathscr{F})$, $\mathrm{Div}(h)$ stands for the principal divisor associated to h. For a divisor $\mathtt{D}$ on $\mathscr{F}$, the *Riemann-Roch space* $\mathscr{L}(\mathtt{D})$ is the vector space consisting of all rational functions which are regular outside $\mathtt{D}$. The dimension $\ell(\mathtt{D})$ of $\mathscr{L}(\mathtt{D})$ and $\deg(\mathtt{D})$ are linked by the Riemann-Roch Theorem, see for instance [9, Theorem 6.70]: $\ell(\mathtt{D}) = \deg(\mathtt{D}) - \mathfrak{g} + 1 + \ell(\mathtt{W} - \mathtt{D})$ where $\mathtt{W}$ is a canonical divisor. In particular,

$$\ell(\mathtt{D}) = \deg(\mathtt{D}) - \mathfrak{g} + 1 \text{ for } \deg(\mathtt{D}) > 2\mathfrak{g} - 2.$$

To compute the dimension of the the Riemann-Roch space $\mathscr{L}(\mathtt{D})$ we use a geometric approach based on the corresponding complete linear series $|\mathtt{D}|$; see [7, Chapter 3] and [9, Chapter 6.2]. Since $\mathscr{F}$ is assumed to be non-singular, the divisors of $|\mathtt{D}|$ are cut out on $\mathscr{F}$ by certain curves of a given degree l which are determined as follows. Take any plane curve $\mathscr{G}$ of degree l such that $\mathscr{G}\cdot\mathscr{F}\succeq \mathtt{D}$ and let $\mathtt{B}=\mathscr{G}\cdot\mathscr{F}-\mathtt{D}$. The curves $\mathscr{U}: U(X,Y)=0$ with $\deg(\mathscr{U})=l$ such that $\mathscr{U}\cdot\mathscr{F}\succeq\mathtt{B}$ form a linear system that contains a linear subsystem Λ free from curves having $\mathscr{F}$ as a component. The curves in Λ cut out the divisors of $|\mathtt{D}|$. The (projective) dimension of $|\mathtt{D}|$ is $\dim(\Lambda)$, that is, the maximum number of linearly independent curves in Λ. In terms of the Riemann-Roch space,

$$\mathscr{L}(\mathtt{D})=\left\{\frac{U(x,y)}{G(x,y)} \mid \deg U\le \deg G, \mathscr{U}\cdot\mathscr{F}\succeq \mathtt{B}\right\}. \tag{3}$$

C. Weierstrass semigroups and gap sequences

For simplicity, assume that $\mathscr{F}$ is a non-singular projective plane curve. For any $\mathbb{F}$-rational point $P\in\mathscr{F}$, a non-gap at P is a non-negative integer g such that there exists $h\in\mathbb{F}(\mathscr{F})$ with pole number g at P which is regular on the remaining points of $\mathscr{F}$, that is, $\mathrm{Div}(h)_\infty=gP$. The Weierstrass semigroup at P consists of all non-gaps at P, that is, of all positive integers other than the gaps at P. In the study of differential codes it is useful to consider the generalization of the gap sequence and the Weierstrass semigroup to several points; see [3], [4], [11], [13], [14], [15], [16].

For an ordered r-tuple $(P_1,P_2,\ldots,P_r)$ of $\mathbb{F}$-rational points of $\mathscr{F}$, a non-gap is an ordered r-tuple of non-negative integers $(g_1,g_2,\ldots,g_r)\in\mathbb{N}_0^r$ such that there exists $h\in\mathbb{K}(\mathscr{F})$ with $\mathrm{Div}(h)_\infty= g_1P_1+g_2P_2+\ldots+g_rP_r$ while the Weierstrass semigroup $\mathbf{H}(P_1,P_2\ldots,P_r)$ consists of all r-tuples of positive integers other than the gaps, that is, the Weierstrass semigroup at $(P_1,P_2\ldots,P_r)$ is

$$\mathbf{H}(P_1,P_2,\ldots,P_r)=\mathbb{N}_0^r\setminus\mathbf{G}(P_1,P_2\ldots,P_r),$$

where $\mathbf{G}(P_1,P_2,\ldots,P_r)$ is the set of all gaps at $(P_1,P_2,\ldots,P_r)$. An equivalent definition of these concepts in terms of Riemann-Roch spaces is stated in the following result.

Lemma II.1 ([4, Lemma 2.2 and Corollary 2.3])**.** *Fix $(n_1,\ldots,n_m)\in\mathbb{N}_0^m$ and write $\mathtt{D}=n_1Q_1+\cdots+n_mQ_m$.*

(a) $(n_1,\ldots,n_m)\in\mathbf{G}(Q_1,\ldots,Q_m)\iff\exists\, i$ *such that* $\ell(\mathtt{D})=\ell(\mathtt{D}-Q_i)$.
(b) $(n_1,\ldots,n_m)\in\mathbf{H}(Q_1,\ldots,Q_m)\iff\forall\, i$ *we have* $\ell(\mathtt{D})=\ell(\mathtt{D}-Q_i)+1$.

A little bit more general concepts are the Weierstrass semigroup and the gap sequence at an effective divisor. Let $\mathtt{D}$ be an effective divisor of $\mathbb{F}(\mathscr{F})$. The Weierstrass semigroup at $\mathtt{D}$ is

$$\mathbf{H}(\mathtt{D})=\{n\in\mathbb{N}_0\mid \exists f\in\mathbb{F}(\mathscr{F})\text{ s.t. }\mathrm{Div}(f)_\infty=n\mathtt{D}\}.$$

The Weierstrass gap sequence at $\mathtt{D}$ is

$$\mathbf{G}(\mathtt{D})=\{n\in\mathbb{N}_0\mid \ell(n\mathtt{D})=\ell((n-1)\mathtt{D})\}.$$

Unfortunately, it is not true that $\mathbf{G}(\mathtt{D})=\mathbb{N}_0\setminus\mathbf{H}(\mathtt{D})$. However, the following holds.

Lemma II.2. *Let $\mathtt{D}=P_1+P_2+\ldots+P_r$ with points $P_1,P_2,\ldots,P_r$ of $\mathscr{F}$. The non-negative integer n is in $\mathbf{G}(\mathtt{D})$ if and only if we have $(k_1,\ldots,k_r)\in\mathbf{G}(P_1,P_2,\ldots,P_r)$ for all integers $k_1,\ldots,k_r\in\{n-1,n\}$ such that $k_i=n$ for at least one index $i\in\{1,\ldots,r\}$.*

D. The geometry of the Hermitian curve $\mathscr{H}_q$

We keep up our notation from Introduction. A line l of $PG(2,\mathbb{F}_{q^2})$ is either a tangent to $\mathscr{H}_q$ at an $\mathbb{F}_{q^2}$-rational point of $\mathscr{H}_q$ or it meets $\mathscr{H}_q$ at $q+1$ distinct $\mathbb{F}_{q^2}$-rational points. In terms of intersection divisors, see [9, Section 6.2],

$$\mathscr{H}_q\cdot l=\begin{cases}(q+1)Q, & Q\in\mathscr{H}_q;\\ \sum_{i=1}^{q+1}Q_i, & Q_i\in\mathscr{H}_q,\ Q_i\neq Q_j,\ 1\le i<j\le n.\end{cases}$$

Through every point $V\in PG(2,\mathbb{F}_{q^2})$ not in $\mathscr{H}_q(\mathbb{F}_{q^2})$ there are q^2-q secants and $q+1$ tangents to $\mathscr{H}_q$. The arising $q+1$ tangency points are the common points of $\mathscr{H}_q$ with the polar line of V relative to the unitary polarity associated to $\mathscr{H}_q$. Let $V=(1:0:0)$. Then the line l_∞ of equation $Z=0$ is tangent at $P_\infty=(0:1:0)$ while another line through V with equation $Y-cZ=0$ is either a tangent or a secant according as c^q+c is 0 or not. This gives rise to the polynomial

$$R_q(X,Y)=X\prod_{c\in\mathbb{F}_{q^2},\,c^q+c\neq 0}(Y-c) \tag{4}$$

of degree q^2-q+1. By [9, Theorem 6.42],

$$\mathrm{Div}(R_q(x,y))_\infty=(q^2-q+1)(q+1)P_\infty=(q^3+1)P_\infty.$$

The above results can be stated for $\mathscr{H}_{q^3}$ by replacing q with q^3. In particular.

$$\begin{aligned}\mathrm{Div}(R_{q^3}(x,y))_\infty&=(q^6-q^3+1)(q^3+1)P_\infty\\&=(q^9+1)P_\infty.\end{aligned}$$

E. Intersection of the Hermitian curves $\mathscr{H}_{q^3}$ and $\mathscr{H}_q$

As we pointed out in Introduction, since $x^{q^3}=x^q$ for all $x\in\mathbb{F}_{q^2}$, we have $\mathscr{H}_q(\mathbb{F}_{q^2})=\mathscr{H}_{q^3}(\mathbb{F}_{q^2})$, that is, all $\mathbb{F}_{q^2}$-rational points of $\mathscr{H}_q$ lie on $\mathscr{H}_{q^3}$. Moreover, the curves $\mathscr{H}_q$ and $\mathscr{H}_{q^3}$ have the same tangent line t_Q at any point $Q\in\mathscr{H}_q(\mathbb{F}_{q^2})$. Their intersection multiplicity at Q is therefore

$$I(Q,\mathscr{H}_q\cap\mathscr{H}_{q^3})=I(Q,\mathscr{H}_q\cap t_Q)=q+1.$$

By the theorem of Bézout [9, Theorem 3.14], $\mathscr{H}_q$ and $\mathscr{H}_{q^3}$ have no further common points. As in the Introduction, define the divisors

$$\mathtt{D}=\sum_{Q\in\mathscr{H}_{q^3}\setminus\mathscr{H}_q}Q\qquad\text{and}\qquad\mathtt{T}=\sum_{Q\in\mathscr{H}_q}Q\tag{5}$$

on $\mathscr{H}_{q^3}$. Then $\deg(\mathtt{D})=q^9-q^3$, $\deg(\mathtt{T})=q^3+1$ and the intersection divisor is

$$\mathscr{H}_q\cdot\mathscr{H}_{q^3}=(q+1)\mathtt{T}.$$

Let $H_q(X,Y)=X^{q+1}-Y^q-Y$ be the affine polynomial of $\mathscr{H}_q$. From [9, Theorem 6.42],

$$\mathrm{Div}(H_q)=(q+1)\mathtt{T}-(q^3+1)(q+1)P_\infty\tag{6}$$

in $\mathbb{F}_{q^6}(\mathscr{H}_{q^3})$. In particular,

$$(q+1)\mathtt{T}\equiv(q^3+1)(q+1)P_\infty.\tag{7}$$

F. Equivalence of functional and differential Hermitian codes

Lemma II.3. *For any divisor $\mathtt{G}$ of $\mathscr{H}_{q^3}$,*

$$\Omega(\mathtt{G}-\mathtt{D})=dx\,R_{q^3}^{-1}\,\mathscr{L}(-\mathtt{G}-\mathtt{T}+(q^6-1)(q^3+1)P_\infty).$$

Proof. The proof is similar to that of [13, Lemma 2.1]. Since x is a separable variable of $\mathbb{F}_{q^6}(\mathscr{H}_{q^3})$, we may write the differential ω as $\omega=hdx$. Then

$$\begin{aligned}\omega=&hdx\in\Omega(\mathtt{G}-\mathtt{D})\Leftrightarrow\mathrm{Div}(\omega)\succeq\mathtt{G}-\mathtt{D}\\&\Leftrightarrow\mathrm{Div}(h)\succeq\mathtt{G}-\mathtt{D}-\mathrm{Div}(dx)\\&\Leftrightarrow\mathrm{Div}(R_{q^3}h)\succeq\mathtt{G}-\mathtt{D}-\mathrm{Div}(dx)+\mathrm{Div}(R_{q^3})\\&\Leftrightarrow\mathrm{Div}(R_{q^3}h)\succeq\mathtt{G}+\mathtt{T}-(q^6-1)(q^3+1)P_\infty.\end{aligned}$$

In the last step, we used the following facts: $\mathrm{Div}(dx)=(2\mathfrak{g}-2)P_\infty$, $\mathrm{Div}(R_{q^3})=\mathtt{D}+\mathtt{T}-(q^9+1)P_\infty$, and $q^9-2\mathfrak{g}+1=(q^6-1)(q^3+1)$. Therefore

$$\begin{aligned}&\omega=hdx\in\Omega(\mathtt{G}-\mathtt{D})\Leftrightarrow\\&\qquad h\in R_{q^3}^{-1}\mathscr{L}(-\mathtt{G}-\mathtt{T}+(q^6-1)(q^3+1)P_\infty),\end{aligned}$$

which proves the lemma. □

Proposition II.4. *Let $\mathtt{G}$ be an effective divisor on $\mathscr{H}_{q^3}$, with $\mathrm{supp}(\mathtt{G})\cap\mathrm{supp}(\mathtt{D})=\emptyset$. The differential code $C_\Omega(\mathtt{D},\mathtt{G})$ and the functional code $C_L(\mathtt{D},-\mathtt{G}-\mathtt{T}+(q^6-1)(q^3+1)P_\infty)$ are monomially equivalent.*

Proof. By Lemma II.3, every differential in $\Omega(\mathtt{G}-\mathtt{D})$ can be written as $\omega=R_{q^3}^{-1}fdx$ with $f\in\mathscr{L}(-\mathtt{G}-\mathtt{T}+(q^6-1)(q^3+1)P_\infty)$. As $\mathtt{G}$ and $\mathtt{T}$ are effective, f only has poles at infinity. From the Horizon Theorem [18, Section 4.3] f is a polynomial in x and y. Also, P_∞ is not a pole of ω. Hence $\mathrm{res}_{P_\infty}(\omega)=0$.

Take a point $S(a,b)\in\mathscr{H}_{q^3}\setminus\{P_\infty\}$. Then, $b^{q^3}+b=a^{q^3+1}$, $t=x-a$ is a local parameter at S, and the local expansion of y at S is $y(t)=b+ta^{q^3}+t^{q^3+1}[\dots]$. Therefore $f(a+t,y(t))=f(a,b)+t[\dots]$ while $R_{q^3}(a,b)=0$ and $R_{q^3}(a+t,y(t))=ut+t^2[\dots]$ with nonzero $u=u(S)$ given by

$$u=\begin{cases}\displaystyle\prod_{c\in\mathbb{F}_{q^6},\,c^{q^3}+c\neq0}(b-c), & for\ a=0.\\ \displaystyle a^{q^3+1}\prod_{c\in\mathbb{F}_{q^6},\,c^{q^3}+c\neq0,\,c\neq b}(b-c), & for\ a\neq0.\end{cases}$$

Thus,

$$\begin{aligned}g(a+t,y(t))&=R_{q^3}(a+t,y(t))^{-1}f(a+t,y(t))\\&=u^{-1}f(a,b)t^{-1}+\cdots,\end{aligned}$$

whence

$$\mathrm{res}_S(gdx)=\mathrm{res}_t(u^{-1}f(a,b)t^{-1}+\cdots)=u^{-1}f(S),$$

showing the monomial equivalence between the codes $C_\Omega(\mathtt{D},\mathtt{G})$ and $C_L(\mathtt{D},-\mathtt{G}-\mathtt{T}+(q^6-1)(q^3+1)P_\infty)$. □

Proposition II.5. *Let m be a positive integer. The codes $C_\Omega(\mathtt{D},m\mathtt{T})$ and $C_L(\mathtt{D},(q^6-m-2)\mathtt{T})$ are monomially equivalent.*

Proof. Since $a=(q^6-1)/(q+1)$ is an integer, Equation (7) implies $(q^6-1)(q^3+1)P_\infty=a(q+1)(q^3+1)P_\infty\equiv a(q+1)\mathtt{T}=(q^6-1)\mathtt{T}$. By Proposition II.4, our claim follows.

□

III. The gap sequence of $\mathscr{H}_{q^3}$ at $\mathrm{supp}(\mathtt{T})$

In this section we prove some results on the Riemann-Roch space $\mathscr{L}(m\mathtt{T})$ of $\mathscr{H}_{q^3}$. We keep our notation of the previous section. Moreover $\mathscr{R}_q$ stands for the completely reducible plane curve with affine equation $R_q(X,Y) = 0$. For $Q \in \mathrm{supp}(\mathtt{T})$, we have $I(Q, \mathscr{R}_q \cap \mathscr{H}_{q^3}) = 1$. In particular, for the intersection divisor $\mathscr{R}_q \cdot \mathscr{H}_{q^3} = \mathtt{T} + \mathtt{T}' \succeq \mathtt{T}$.

Lemma III.1. *Let $0 < m \le q^3-2$ be an integer and write $m = m_0(q+1)+m_1$, $0 \le m_1 \le q$. Define the polynomial $G(X,Y) = H_q(X,Y)^{m_0} R_q(X,Y)^{m_1}$. Then*

$$\deg G = m_0(q+1) + m_1(q^2-q+1)$$

and

$$\begin{aligned}\mathbf{v}(G) \cdot \mathscr{H}_{q^3} &= m_0(\mathscr{H}_q \cdot \mathscr{H}_{q^3}) + m_1(\mathscr{R}_q \cdot \mathscr{H}_{q^3}) \\ &= m\mathtt{T} + m_1\mathtt{T}' \\ &\succeq m\mathtt{T}.\end{aligned}$$

Furthermore, for the Riemann-Roch space,

$$\mathscr{L}(m\mathtt{T}) = \left\{ \frac{F(x,y)}{G(x,y)} \mid \deg F \le \deg G \text{ and } \mathbf{v}(F) \cdot \mathscr{H}_{q^3} \succeq m_1 \mathtt{T}' \right\}.$$

Proof. This follows from Equation (3), applied to $\mathscr{F} = \mathscr{H}_{q^3}$ and $\mathtt{D} = m\mathtt{T}$. □

Theorem III.2. *Let $0 < m \le q^3-2$ be an integer and write $m = m_0(q+1)+m_1$, $0 \le m_1 \le q$.*

(a) *If $(m_0+1)(q+1) < (q+1-m_1)(q^2-q+1)$ then*

$$\begin{aligned}\mathscr{L}(m\mathtt{T}) &= \mathscr{L}(m_0(q+1)\mathtt{T}) \\ &= \left\{ \frac{F(x,y)}{H_q(x,y)^{m_0}} \mid \deg F \le m_0(q+1) \right\}\end{aligned}$$

In particular, $\ell(m\mathtt{T}) = \ell(m_0(q+1)\mathtt{T}) = \binom{m_0(q+1)+2}{2}$.

(b) *If $(m_0+1)(q+1) \ge (q+1-m_1)(q^2-q+1)$ then*

$$\frac{R_q^{q+1-m_1}}{H_q^{m_0+1}} \in \mathscr{L}(m\mathtt{T}) \setminus \mathscr{L}((m-1)\mathtt{T}).$$

Proof. (a) We use the notation of Lemma III.1. Let $F(X,Y)$ be a polynomial with $\deg F \le \deg G$ and $\mathbf{v}(F) \cdot \mathscr{H}_{q^3} \succeq m_1\mathtt{T}'$. By assumption,

$$\deg F \le m_0(q+1) + m_1(q^2-q+1) < q^3 - q.$$

We prove that $R_q^{m_1} \mid F$. Otherwise $m_1 \ge 1$ and there is a linear component $\ell : L = 0$ of $\mathscr{R}_q$ such that $F = F_0 L^k$, $L \nmid F_0$ and $k < m_1$. As ℓ is not a tangent of $\mathscr{H}_{q^3}$, for all points Q in $\ell \setminus \mathscr{H}_q$ we have

$$I(Q, \mathbf{v}(F_0) \cap \mathscr{H}_{q^3}) \ge m_1 - k \ge 1.$$

Clearly we have $q^3 - q$ choices for Q, and since $\deg F_0 \le \deg F < q^3 - q$, our assumption $L \nmid F_0$ is inconsistent with the theorem of Bézout. Hence, $F = F_1 R_q^{m_1}$ and $F/G = F_1/H_q^{m_0}$ is the generic element of $\mathscr{L}(m\mathtt{T})$, with $\deg F_1 \le m_0(q+1)$.

(b) Equation (6) together with

$$\mathrm{Div}(R_q) = \mathtt{T} + \mathtt{T}' - (q^3+1)(q^2-q+1)P_\infty$$

yield

$$\begin{aligned}\mathrm{Div}\left(\frac{R_q^{q+1-m_1}}{H_q^{m_0+1}}\right) = &- m\mathtt{T} + (q+1-m_1)\mathtt{T}' \\ &+ (q^3+1)((m_0+1)(q+1) \\ &- (q+1-m_1)(q^2-q+1))P_\infty.\end{aligned}$$

Our assumption $(m_0+1)(q+1) \ge (q+1-m_1)(q^2-q+1)$ implies the claim. □

Since $2\mathfrak{g} - 2 = (q^3+1)(q^3-2)$, if $m > q^3-2$ then $\deg(m\mathtt{T}) > 2\mathfrak{g}-2$ and

$$\ell(m\mathtt{T}) = \deg(m\mathtt{T}) + 1 - \mathfrak{g} = (q^3+1)(m - \frac{q^3-2}{2}).$$

Corollary III.3. *The Weierstrass gap sequence at $\mathtt{T}$ is*

$$\mathbf{G}(\mathtt{T}) = \{m_0(q+1) + m_1 \mid 1 \le m_1 < q+1 - \frac{(m_0+1)(q+1)}{q^2-q+1}\}.$$

Proof. The claim follows from Theorem III.2, except for $m_1 = 0$. In this case, $1/H_q^{m_0} \in \mathscr{L}(m\mathtt{T}) \setminus \mathscr{L}((m-1)\mathtt{T})$, which shows that $m = m_0(q+1) \notin \mathbf{G}(\mathtt{T})$. □

IV. Hermitian codes $C_\Omega(\mathtt{D}, k\mathtt{T})$

In this section we exhibit some values of m which produce good Hermitian codes. We compare our code with the one-point Hermitian code of the same length and dimension. We rely on the following result by Carvalho and Torres [4, Theorem 3.4].

Proposition IV.1. *Suppose that $\alpha, \alpha+1, \ldots, \beta$ is a sequence of consecutive numbers in $\mathbf{G}(\mathtt{T})$. Let*

$k := \alpha + \beta - 1$. *Then, the minimum distance of the differential code* $C_\Omega(\mathtt{D}, k\mathtt{T})$ *satisfies*

$$d \geq k(q^3+1) - (q^3-2)(q^3+1) + (\beta - \alpha + 1)(q^3+1),$$

where the last term is the improvement on the designed minimum distance.

Proof. With notation of [4, Section 3], $n_i = \alpha$, $p_i = \beta$ for $i = 1, \ldots, q^3+1$, $m = q^3+1$ and $\mathtt{T} = Q_1 + \cdots + Q_m$. □

Lemma IV.2. *Let* $q \geq 3$ *be a prime power and define the integer*

$$k' = \begin{cases} \left(q^6 - q^3 - q^2 - \frac{1}{2}q - 1\right)(q^3+1) & \textit{for } q \textit{ even,} \\ \left(q^6 - q^3 - q^2 + \frac{1}{2}(q-1)\right)(q^3+1) & \textit{for } q \textit{ odd.} \end{cases}$$

Then the one-point functional code $C_L(\mathtt{D}, k'P_\infty)$ *has parameters*

$$\left[q^9 - q^3, \left(q^6 - \frac{3}{2}q^3 - q^2 - \frac{q}{2}\right)(q^3+1), \right. \\ \left. \leq \left(q^2 + \frac{q}{2} + 1\right)(q^3+1) + q^3\right]$$

for q *even, and*

$$\left[q^9 - q^3, \left(q^6 - \frac{3}{2}q^3 - q^2 + \frac{q+1}{2}\right)(q^3+1), \right. \\ \left. \leq \left(q^2 - \frac{q-1}{2}\right)(q^3+1) + q^3\right]$$

for q *odd.*

Proof. We give the proof for q even, the odd case is similar. It is straightforward to see that the length is $n = q^9 - q^3$, the dimension is as given, and

$$\delta = n - k' = (q^2 + \frac{q}{2} + 1)(q^3+1)$$

is the designed minimum distance. For

$$a = q^3 - q^2 - \frac{1}{2}q - 3$$
$$b = q^3 - q^2 - \frac{1}{2}q - 1$$

we compute $k' = q^9 - q^6 + aq^3 + b$. Let $\mathtt{D}'$ be the sum of the affine points of $\mathscr{H}_{q^3}$. As $a < b = a+2$, [21, line 4) of Table 1] implies that the true minimum distance of $C_L(\mathtt{D}', k'P_\infty)$ is

$$q^9 - k' = \delta + q^3 = (q^2 + \frac{q}{2} + 1)(q^3+1) + q^3.$$

Since $C_L(\mathtt{D}, k'P_\infty)$ is obtained from $C_L(\mathtt{D}', k'P_\infty)$ by deleting q^3 positions, the minimum distance of $C_L(\mathtt{D}, k'P_\infty)$ is at most $\delta + q^3$. □

Theorem IV.3. *Let* $q \geq 3$ *be a prime power and define the integer*

$$k = \begin{cases} q^3 + q^2 + \frac{q}{2} - 1 & \textit{for } q \textit{ even,} \\ q^3 + q^2 - \frac{q+1}{2} - 1 & \textit{for } q \textit{ odd.} \end{cases}$$

Then the differential code $C_\Omega(\mathtt{D}, k\mathtt{T})$ *has parameters*

$$\left[q^9 - q^3, \left(q^6 - \frac{3}{2}q^3 - q^2 - \frac{q}{2}\right)(q^3+1), \right. \\ \left. \geq \delta + \left(\frac{q}{2} - 1\right)(q^3+1)\right]$$

for q *even, and*

$$\left[q^9 - q^3, \left(q^6 - \frac{3}{2}q^3 - q^2 + \frac{q+1}{2}\right)(q^3+1), \right. \\ \left. \geq \delta + \frac{q-1}{2}(q^3+1)\right]$$

for q *odd, where*

$$\delta = \deg(k\mathtt{D}) - 2\mathfrak{g} + 2 = (q^3+1)(k - q^3 + 2)$$

is the designed minimum distance of $C_\Omega(\mathtt{D}, k\mathtt{T})$.

Proof. Let $q \geq 4$ be even and $m_0 := q^2/2$. Then

$$\frac{(m_0+1)(q+1)}{q^2-q+1} = \frac{q^3+q^2+2q+2}{2(q^2-q+1)} \\ = \frac{q}{2} + 1 + \frac{3q}{2(q^2-q+1)}.$$

This implies

$$\left\lfloor q + 1 - \frac{(m_0+1)(q+1)}{q^2-q+1} \right\rfloor = \left\lfloor \frac{q}{2} - \frac{3q}{2(q^2-q+1)} \right\rfloor \\ = \frac{q}{2} - 1$$

for $q > 2$. By Corollary III.3,

$$\alpha = \frac{q^2(q+1)}{2} + 1, \ldots, \beta = \frac{q^2(q+1)}{2} + \frac{q}{2} - 1$$

is a sequence of consecutive gap numbers. Moreover, $k = \alpha + \beta - 1$. As $\deg(k\mathtt{T}) > 2\mathfrak{g} - 2$, we have

$$\dim(C_\Omega(\mathtt{D}, k\mathtt{T})) = n + \mathfrak{g} - \deg(k\mathtt{T}) - 1 \\ = (q^6 - \frac{3}{2}q^3 - q^2 - \frac{1}{2}q)(q^3+1).$$

Proposition IV.1 improves the designed minimum distance

$$\delta = \deg(k\mathtt{T}) - 2\mathfrak{g} + 2 = (q^2 + \frac{q}{2} + 1)(q^3 + 1).$$

of $C_\Omega(\mathtt{D}, k\mathtt{T})$ by

$$(\beta - \alpha + 1)\deg(\mathtt{T}) = (\frac{q}{2} - 1)(q^3 + 1).$$

This proves the theorem for $q \geq 4$ even. Similar computation applies for $q \geq 3$ odd with $m_0 = (q^2 - 1)/2$. □

Remark IV.4. (a) *Lemma IV.2 and Theorem IV.3 show that the code $C_\Omega(\mathtt{D}, k\mathtt{T})$ performs much better than the one-point Hermitian code of the same length and dimension; the improvement is approximatively $q^4/2$.*

(b) *In [20, Theorem 2.5], the authors show the existence of a divisor $\mathtt{G}$ such that $C_\Omega(\mathtt{D}, k\mathtt{T})$ and $C_\Omega(\mathtt{D}, \mathtt{G})$ have the same length and dimension, and $C_\Omega(\mathtt{D}, \mathtt{G})$ has a minimum distance $\delta + O(q^6)$. While the parameter of $C_\Omega(\mathtt{D}, \mathtt{G})$ is better, no explicit construction for $\mathtt{G}$ is known.*

(c) *We compare the parameters of our code with the bound given by Matthews and Michel; see [17, Theorem 3.5]. The Matthews-Michel bound improves the designed minimum distance of AG-codes when the support of the defining divisor consists of a unique place P of higher degree. The improvement is given in term of the Weierstrass gap sequence at P. In [13], this sequence was computed for degree 3 places of the Hermitian curve, and the arising Matthews-Michel bound was specified. It should be noticed that the case of higher degree places is open and appears to be more difficult. In [13, Theorem 4.1] the improvement is shown to be at most $3q$ for the Hermitian curve over $\mathbb{F}_{q^2}$. In our context, this means an improvement of $3q^3$ for the designed minimum distance, which is asymptotically worse than the improvement $q^4/2$ of the codes in Theorem IV.3.*

(d) *When $q = 2$ then $k = 12$ and $C = C_\Omega(\mathtt{D}, 12\,\mathtt{T})$ is a $[504, 423]_{64}$-code with designed minimum distance $\delta = 54$. Theorem IV.3 gives no improvement for the minimum distance, and indeed, the true minimum distance of C is 54. To see this, consider the equivalent functional code $C' = C_L(\mathtt{D}, 50\,\mathtt{T})$, together with the polynomial $R_8(X, Y)$ of degree 57 introduced in (4). Take any 51 linear factors of $R_8(X, Y)$ including $X, Y - \tau, Y - \tau^2$, where τ is the primitive element of $\mathbb{F}_4$, Then their product $R^*(X, Y)$ defines a (totally reducible) curve of degree 51 that covers the 9 points of $\mathscr{H}_2(\mathbb{F}_4)$, and as many as $9 \cdot (51 - 3) + 3 \cdot (9 - 3) = 450$ further points of $\mathscr{H}_8(\mathbb{F}_{64})$. Moreover, let $g = R^*(x, y)/(x^3 - y - y^2)^{17}$. Then $g \in \mathscr{L}(50\,\mathtt{T})$ and g determines a codeword of C' with weight $504 - 450 = 54$.*

V. The permutation automorphisms of $C_L(\mathtt{D}, m\mathtt{T})$

Definition V.1. *Let $\mathscr{X}$ be a smooth irreducible curve over $\mathbb{F}_q$, $Q_1, \ldots, Q_n \in \mathscr{X}(\mathbb{F}_q)$, $\mathtt{D} = Q_1 + \cdots + Q_n$, and $\mathtt{C}$ be an $\mathbb{F}_q$-rational divisor on $\mathscr{X}$ with $\mathrm{supp}(\mathtt{D}) \cap \mathrm{supp}(\mathtt{C}) = \emptyset$. A monomial automorphism of $C_L(\mathtt{D}, \mathtt{C})$ is a triple (α, β, γ), where α is an automorphism of $\mathscr{L}(\mathtt{C})$, β is a permutation of $\{Q_1, \ldots, Q_n\}$ and γ is a $\{Q_1, \ldots, Q_n\} \to \mathbb{F}_q$ map. Moreover, for all $P \in \{Q_1, \ldots, Q_n\}$ and $f \in \mathscr{L}(\mathtt{C})$ yields*

$$\alpha(f)(P) = \gamma(P) f(\beta(P)). \tag{8}$$

If $\gamma = 1$ is constant then (α, β) is called a permutation automorphism of $C_L(\mathtt{D}, \mathtt{C})$. If α and β are the identity maps then one speaks of a pure monomial automorphism.

With the notation of the previous definition, let τ be an automorphism of the function field $\mathbb{F}_q(\mathscr{X})$ and assume that τ preserves the divisors $\mathtt{D}$ and $\mathtt{C}$. Then, τ induces an automorphism α of $\mathscr{L}(\mathtt{C})$ and a permutation β of $Q_1, \ldots, Q_n$. In fact, α is the restriction of τ to $\mathscr{L}(\mathtt{C})$, and β is defined in such a way that (8) holds. We say that (α, β) is an *inherited permutation automorphism* of $C_L(\mathtt{D}, \mathtt{C})$, induced by τ.

The following proposition generalizes [15, Theorem 4.1] in such a way, that it can be applied to certain codes $C_L(\mathtt{D}, m\mathtt{T})$ of the Hermitian curve $\mathscr{H}_{q^3}$.

Proposition V.2. *Let $\mathscr{X} : F(X, Y) = 0$ be a smooth irreducible plane curve over $\mathbb{F}_q$, $Q_1, \ldots, Q_n \in \mathscr{X}(\mathbb{F}_q)$, $\mathtt{D} = Q_1 + \cdots + Q_n$, and $\mathtt{C}$ be an $\mathbb{F}_q$-rational divisor on $\mathscr{X}$ with $\mathrm{supp}(\mathtt{D}) \cap \mathrm{supp}(\mathtt{C}) = \emptyset$. Let x, y be generators of the function field $\mathbb{F}_q(\mathscr{X})$ satisfying $F(x, y) = 0$. Assume that the following hold:*

(a) *The points* $Q_1, \dots, Q_n$ *are affine.*
(b) *There is a curve* $\mathscr{G} : G(X,Y) = 0$ *and an effective divisor* $\mathtt{B}$*, defined over* $\mathbb{F}_q$*, such that* $\mathscr{X} \cdot \mathscr{G} = \mathtt{C} + \mathtt{B}$*.*
(c) *There is a polynomial* $S(X,Y) \in \mathbb{F}_q[X,Y]$ *such that* $\frac{1}{S(x,y)}, \frac{x}{S(x,y)}, \frac{y}{S(x,y)} \in \mathscr{L}(\mathtt{C})$*.*
(d) $n > (\deg G)(\deg F)^2$*.*

Then all permutation automorphisms of $C_L(\mathtt{D},\mathtt{C})$ *are inherited.*

Proof. Let (α, β) be a permutation automorphism of $C_L(\mathtt{D},\mathtt{C})$. By (a) we can set $Q_i = (a_i, b_i)$ and $\beta(Q_i) = Q_{i'} = (a_{i'}, b_{i'})$ with $a_i, b_i, a_i', b_i' \in \mathbb{F}_q$. Equation (3), (b) and (c) imply the existence of polynomials $u(X,Y)$, $v(X,Y)$, $w(X,Y)$ of degree at most $\deg(G)$ such that

$$\alpha\left(\frac{1}{S(x,y)}\right) = \frac{w(x,y)}{G(x,y)},$$
$$\alpha\left(\frac{x}{S(x,y)}\right) = \frac{u(x,y)}{G(x,y)},$$
$$\alpha\left(\frac{y}{S(x,y)}\right) = \frac{v(x,y)}{G(x,y)}.$$

By $\alpha(f)(P) = f(\beta(P))$ we have

$$\begin{aligned}\frac{u(a_i,b_i)}{G(a_i,b_i)} &= \alpha\left(\frac{x}{S(x,y)}\right)(a_i,b_i)\\ &= \left(\frac{x}{S(x,y)}\right)(a_{i'},b_{i'})\\ &= \frac{a_{i'}}{S(a_{i'},b_{i'})}\end{aligned}$$

for all $i = 1, \dots, n$. Similarly, $\frac{w(a_i,b_i)}{G(a_i,b_i)} = \frac{1}{S(a_{i'},b_{i'})}$ and $\frac{v(a_i,b_i)}{G(a_i,b_i)} = \frac{b_{i'}}{S(a_{i'},b_{i'})}$. This implies

$$a_{i'} = \frac{u(a_i,b_i)}{w(a_i,b_i)}, \qquad b_{i'} = \frac{v(a_i,b_i)}{w(a_i,b_i)}. \tag{9}$$

Define the polynomial

$$F^*(X,Y) = w(X,Y)^{\deg(F)} F\left(\frac{u(X,Y)}{w(X,Y)}, \frac{v(X,Y)}{w(X,Y)}\right).$$

Clearly, $\deg(F^*) \le \deg(F)\deg(G)$, and

$$F^*(a_i,b_i) = w(a_i,b_i)^{\deg(F)} F(a_{i'}, b_{i'}) = 0$$

holds for $i = 1, \dots, n$. In particular $\mathscr{X}^* : F^*(X,Y) = 0$ and $\mathscr{X}$ have at least n points in common. The theorem of Bézout and (d) imply $F \mid F^*$.

Since $w(x,y) \neq 0$, the curve $\mathscr{W} : w(X,Y) = 0$ has a finite number of points in common with $\mathscr{X}$. Take an arbitrary affine point $(a,b) \in \mathscr{X}(\bar{\mathbb{F}}_q)$, not on $\mathscr{W}$. We have

$$0 = F^*(a,b) = w(a,b)^{\deg(F)} F\left(\frac{u(a,b)}{w(a,b)}, \frac{v(a,b)}{w(a,b)}\right),$$

which implies

$$F\left(\frac{u(a,b)}{w(a,b)}, \frac{v(a,b)}{w(a,b)}\right) = 0.$$

This means that the rational map

$$\bar{\tau}(X,Y) = \left(\frac{u(X,Y)}{w(X,Y)}, \frac{v(X,Y)}{w(X,Y)}\right)$$

maps any point of $\mathscr{X}(\bar{\mathbb{F}}_q)$ to $\mathscr{X}$, up to a finite number of exceptions. Since $\bar{\tau}$ is defined over $\mathbb{F}_q$, we obtain that

$$\tau : x \mapsto \frac{u(x,y)}{w(x,y)}, \quad y \mapsto \frac{v(x,y)}{w(x,y)}$$

extends to a homomorphism of the function field $\mathbb{F}_q(\mathscr{X})$ to itself. We show that τ is surjective. Notice that we identified the places of $\mathbb{F}_q(\mathscr{X})$ and the points of $\mathscr{X}$, and, the action of τ on the places and the action of $\bar{\tau}$ on the points are equivalent.

By Equation (9), τ induces β on $Q_1, \dots, Q_n$. For all $f \in \mathscr{L}(\mathtt{C})$ we have $\tau(f)(Q_i) = f(Q_{i'}) = \alpha(f)(Q_i)$. As $n > \deg(\mathtt{C})$, the evaluation map $f \to (f(Q_1), \dots, f(Q_n))$ is injective and $\alpha(f) = \tau(f)$ holds. In particular, $1/S(x,y)$, $x/S(x,y)$ and $y/S(x,y)$ are in the image of τ, hence $x, y \in Im(\tau)$, which shows that τ is indeed an automorphism of $\mathbb{F}_q(\mathscr{X})$. We have also seen that τ induces the permutation automorhism (α, β), which is therefore inherited. □

We can extend this method to monomial automorphisms.

Proposition V.3. *Under the hypothesis of Proposition V.2, if* $\deg(G) < \deg(F)$ *and* (α, β, γ) *is a monomial automorphism of* $C_L(\mathtt{D},\mathtt{C})$*, then* γ *is constant. In particular, the monomial automorphism group of* $C_L(\mathtt{D},\mathtt{C})$ *is the direct product of the permutation automorphism group by the pure monomial automorphism group.*

Proof. With the notation of Proposition V.2, we have

$$\alpha(f)(a_i,b_i)) = \gamma(a_i,b_i) f(a_{i'}, b_{i'}),$$

for all $i = 1, \ldots, n$. Therefore, as in the proof of that proposition, there exist polynomials $u(X,Y), v(X,Y)$ and $w(X,Y)$ of degree at most $\deg(G)$ such that

$$\frac{w(a_i,b_i)}{G(a_i,b_i)} = \gamma(a_i,b_i)\frac{1}{S(a_{i'},b_{i'})},$$
$$\frac{u(a_i,b_i)}{G(a_i,b_i)} = \gamma(a_i,b_i)\frac{a_{i'}}{S(a_{i'},b_{i'})},$$
$$\frac{v(a_i,b_i)}{G(a_i,b_i)} = \gamma(a_i,b_i)\frac{b_{i'}}{S(a_{i'},b_{i'})}.$$

for all $i = 1, \ldots, n$. Then (9) holds and as shown in the proof of Proposition V.2

$$\tau : x \mapsto \frac{u(x,y)}{w(x,y)}, \quad y \mapsto \frac{v(x,y)}{w(x,y)}$$

is an automorphism of $\mathbb{F}_q(\mathscr{X})$. Let (α', β^{-1}) be the inverse of the permutation automorphism (α, β) induced by τ. Then $(\alpha^*, \beta^*, \gamma) = (\alpha, \beta, \gamma) \circ (\alpha', \beta^{-1})$ is a pure monomial automorphism and

$$\alpha^*(f)(a_i,b_i) = \gamma(a_i,b_i) f(a_i,b_i), \tag{10}$$

for all $i = 1, \ldots, n$. Now, Equation (3) applied to the functions $\alpha^*\left(\frac{1}{S(x,y)}\right)$ and $\frac{1}{S(x,y)}$ implies the existence of polynomials $r^*(X,Y)$ and $s^*(X,Y)$ of degree at most $\deg(G)$ such that

$$\frac{1}{S(X,Y)} = \frac{s^*(X,Y)}{G(X,Y)} \quad \text{and} \quad \alpha^*\left(\frac{1}{S(X,Y)}\right) = \frac{r^*(X,Y)}{G(X,Y)}. \tag{11}$$

Then equations (10) and (11), give $\gamma(a_i,b_i) = \frac{r^*(a_i,b_i)}{s^*(a_i,b_i)}$ for all $i = 1, \ldots, n$. Therefore we define $\gamma(X,Y) = \frac{r^*(X,Y)}{s^*(X,Y)}$. The same argument applied to each $f \in \mathscr{L}(\mathtt{C})$ yields

$$f(X,Y) = \frac{s(X,Y)}{G(X,Y)}, \qquad \alpha^*(f)(X,Y) = \frac{r(X,Y)}{G(X,Y)}, \tag{12}$$

where $s(X,Y)$ and $r(X,Y)$ are polynomials of degree at most $\deg(G)$. Then, by equations (10) and (12) we have

$$\frac{r(a_i,b_i)}{G(a_i,b_i)} = \gamma(a_i,b_i)\frac{s(a_i,b_i)}{G(a_i,b_i)},$$

for all $i = 1, \ldots, n$. In particular,

$$r(a_i,b_i)s^*(a_i,b_i) - r^*(a_i,b_i)s(a_i,b_i) = 0$$

for all $i = 1, \ldots, n$. Since $r(X,Y), r^*(X,Y), s(X,Y), s^*(X,Y)$ have degree at most $\deg(G)$, and

$$(\deg(G))^2(\deg(F)) \le (\deg(G))(\deg(F))^2 < n,$$

Bézout's theorem yields $rs^* = r^*s$. In other words, $\alpha(f) = r^*/s^* f$ for all $f \in \mathscr{L}(\mathtt{C})$. We show that this only holds when r^*/s^* is a constant. Since α is an endomorphism of the finite dimensional vector space $\mathscr{L}(\mathtt{C})$ over $\mathbb{F}_q$, α is represented by a matrix A with respect to a fixed basis. By the classical Cayley-Hamilton Theorem, there exists a polynomial $u(T)$ over $\mathbb{F}_q$ such that $u(A)$ is the zero matrix. Since $A^i(f) = \alpha^i(f) = (r^*/s^*)^i f$, this yields $u(A)(f) = u(r^*/s^*)f$ for all $f \in \mathscr{L}(\mathtt{C})$. Therefore, $u(r^*/s^*) = 0$ in $\mathbb{K}(\mathscr{X})$. In particular, for any (a_i,b_i), $u(r^*/s^*)$ valuated in (a_i,b_i) equals zero. On the other hand, since r^*/s^* valuated in (a_i,b_i) gives an element, say k, in $\mathbb{F}_q$, $T-k$ is a factor of $u(T)$. Therefore, $u(T) = (T-k)^i v(T)$. This factorization, interpreted in $\mathbb{K}(\mathscr{X})[T]$, gives $u(r^*/s^*) = (r^*/s^* - k)^i v(r^*/s^*)$. If $r^*/s^* \neq k$, then $v(r^*/s^*) = 0$, and the above argument can be repeated for $v(T)$. Since $\deg v(t) < \deg u(T)$, this ends up with $r^*/s^* = k$, a constant. To conclude the proof observe that every pure monomial automorphism with constant γ commutes with any permutation automorphism. □

Now, we are able to compute the group of monomial automorphisms of the functional code $C_L(\mathtt{D}, m\mathtt{T})$ for several values of m.

Theorem V.4. *Let $q+1 \le m \le q^3-2$ be an integer and write $m = m_0(q+1) + m_1$, $0 \le m_1 \le q$. If $m_1 \le \frac{q^3-2-m}{q(q+1)}$, then the following hold:*

- (a) *The group of permutation automorphisms of $C_L(\mathtt{D}, m\mathtt{T})$ is isomorphic to the projective unitary group $PGU(3,q)$.*
- (b) *The group of monomial automorphisms of $C_L(\mathtt{D}, m\mathtt{T})$ is isomorphic to the direct product of the projective unitary group $PGU(3,q)$ by a cyclic group of order q^6-1.*

Proof. We apply Proposition V.2 for the curve $\mathscr{H}_{q^3}$ over $\mathbb{F}_{q^6}$. Condition (a) is immediate. Conditions (b) and (c) follow from Lemma III.1 with $G(X,Y) =$

$H_q^{m_0} R_q^{m_1}$ and $S(X,Y) = H_q^{m_0}$, $m_0 > 0$. Hence,

$$\begin{aligned}\deg(G) &= m_0(q+1) + m_1(q^2+q+1)\\ &= m + m_1 q(q+1)\\ &\le q^3 - 2\end{aligned}$$

and

$$\deg(G)\deg(H_{q^3})^2 \le (q^3-2)(q^3+1)^2 < q^9 - q^3 = n.$$

This means that Condition (d) of Proposition V.2 holds, and all permutation automorphisms of $C_L(\mathtt{D}, m\mathtt{T})$ are inherited. It is known that $\mathrm{Aut}(\mathbb{F}_{q^6}(\mathscr{H}_{q^3})) \cong PGU(3,q^3)$, and the action of $\mathrm{Aut}(\mathbb{F}_{q^6}(\mathscr{H}_{q^3}))$ on the $\mathbb{F}_{q^6}$-rational places is equivalent to the action of $PGU(3,q^3)$ on the points of $\mathscr{H}_{q^3}$. Clearly, if $\tau \in \mathrm{Aut}(\mathbb{F}_{q^6}(\mathscr{H}_{q^3}))$ induces a permutation automorphism of $C_L(\mathtt{D}, m\mathtt{T})$, then τ preserves $\mathtt{D}$. Thus, it preserves $\mathrm{supp}(\mathtt{T}) = \mathscr{H}_q$ and $\tau' \in PGU(3,q)$. This finishes the proof of (a). Since $\deg(G) < \deg(H_{q^3}) = q^3+1$, Proposition V.3 implies (b). $\square$

REFERENCES

[1] I. Blake, C. Heegard, T. Hoholdt and Victor Wei, Algebraic geometric codes, *IEEE Trans. Inform. Theory* **44** (1998), 2596–2618.

[2] W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system. I. The user language, *J. Symbolic Comput.* **24** 235-265, (1997).

[3] C. Carvalho and T. Kato, On Weierstrass semigroups and sets: review of new results, *Geom. Dedicata* **239** 195–210, (2009).

[4] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, *Des. Codes Cryptogr.* **35**, 211–225 (2005).

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008, (http://www.gap-system.org)

[6] A. Garcia, S.J. Kim and R.F. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes. *J. Pure Appl. Algebra* **84**, 199–207 (1993).

[7] V.D. Goppa, *Geometry and codes.* Translated from the Russian by N. G. Shartse. Mathematics and its Applications (Soviet Series), 24. Kluwer Academic Publishers Group, Dordrecht, 1988. x+157 pp..

[8] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, second ed., Oxford Univ. Press, Oxford, 1998, xiv+555 pp.

[9] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over a finite field.* Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008. xx+696 pp

[10] T. Hoholdt and R. Pellikaan, On the decoding of algebraic-geometric codes, *IEEE Trans. Inform. Theory* **41** (1995), 1589–1614.

[11] M. Homma, The Weierstrass semigroup of a pair of points on a curve, *Arch. Math.* **67**, 337–348 (1996).

[12] D.R. Hughes and F.C. Piper, *Projective Planes*, Graduate Texts in Mathematics **6**, Springer, New York, 1973, x+291 pp.

[13] G. Korchmáros, G.P. Nagy, Hermitian codes from higher degree places. J. Pure Appl. Algebra 217 (2013), no. 12, 2371–2381.

[14] G. Korchmáros, G.P. Nagy, Lower bounds on the minimum distance in Hermitian one-point differential codes. Sci. China Math. 56 (2013), no. 7, 1449–1455.

[15] G. Korchmáros, P. Speziali, Hermitian codes with automorphism group isomorphic to PGL(2,q) with q odd. Finite Fields Appl. 44 (2017), 1–17.

[16] G.L. Matthews, The Weierstrass Semigroup of an m-Tuple of Collinear Points on a Hermitian Curve. Finite Fields and Applications. Lecture Notes in Computer Science, vol. 2948, pp. 12–24. Springer, Berlin (2004)

[17] G.L. Matthews and T.W. Michel. One-Point Codes Using Places of Higher Degree, *IEEE Trans. Inform. Theory* **51** 2005, 1590-1593.

[18] O. Pretzel, Codes and Algebraic Curves, *Oxford Lecture Series in Mathematics and its Applications, 8*. The Clarendon Press, Oxford University Press, New York, 1998. xii+192 pp.

[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009. xiv+355 pp.

[20] C.P. Xing and H. Chen, Improvements on parameters of one-point AG-codes from Hermtian codes, *IEEE Trans. Inform. Theory* **48** 2002, 535-537.

[21] K. Yang and P. V. Kumar, On the True Minimum Distance of Hermitian Codes, in *Coding theory and algebraic geometry*, Lecture Notes in Mathematics, 1992, Volume **1518/1992**, 99-10.