Codes and gap sequences of Hermitian curves

G. Korchmáros\textsuperscript{a,1}, G.P. Nagy\textsuperscript{b,2,3}, M. Timpanella\textsuperscript{a}

\textsuperscript{a}Dipartimento di Matematica e Informatica, Universit\`a della Basilicata, Contrada Macchia Romana, 85100 Potenza (Italy)

\textsuperscript{b}Department of Algebra, Budapest University of Technology, H-1111, Budapest, Egri József uca 1, Hungary

\textsuperscript{c}Bolyai Institute, University of Szeged, H-6720 Szeged, Aradi vétanák tere 1, Hungary

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 \( C_{\Omega}(D, mT) \) on the Hermitian curve \( H_{q^3} \) defined over \( F_{q^6} \) is worked out where \( \text{supp}(T) := H_{q^3}(F_{q^2}) \), the set of all \( F_{q^2} \)-rational points of \( H_{q^3} \), while \( D \) is taken, as usual, to be the sum of the points in the complementary set \( D = H_{q^3}(F_{q^6}) \setminus H_{q^3}(F_{q^2}) \). For certain values of \( m \), such codes \( C_{\Omega}(D, mT) \) have better minimum distance compared with true values of 1-point Hermitian codes. The automorphism group of \( C_L(D, mT) \), \( m \leq q^3 - 2 \), is isomorphic to \( \text{PGU}(3,q) \).

Keywords: AG code, Weierstrass gap, pure gap, Hermitian curve

2000 MSC: 14H55, 11T71, 11G20, 94B27

1. Introduction

Algebraic-geometry (AG) codes, also called Goppa-codes, are certain linear codes arising from an algebraic curve \( X \) defined over a finite field; see for instance \([1, 7, 10, 18]\). In this paper, we work on the projective plane \( PG(2, F_{q^6}) \) defined over the finite field \( F_{q^6} \) of order \( q^6 \) and equipped with homogeneous coordinates \((X, Y, Z)\). The points and lines of \( PG(2, F_{q^6}) \) with coordinates in the subfield \( F_{q^2} \) are the points and lines of the projective subplane \( PG(2, F_{q^2}) \) of \( PG(2, F_{q^6}) \). We take \( X \) to be the (non-singular) Hermitian curve \( \mathcal{H}_{q^3} \) of \( PG(2, F_{q^6}) \), with genus \( g(\mathcal{H}_{q^3}) = \frac{1}{2}q^3(q^3 - 1) \) and defined by its canonical homogeneous equation

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

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

\[ X^{q+1} - Y^q Z - YZ^q = 0. \]
More precisely, we define
\[ T := \sum_{Q \in \mathcal{H}_q\left(\mathbb{F}_{q^2}\right)} Q \]
and, for a positive integer \( m \), we put \( G = mT \). Also, we define the set \( D \) by complement, that is,
\[ D := \mathcal{H}_q\left(\mathbb{F}_{q^2}\right) \setminus \mathcal{H}_q\left(\mathbb{F}_{q^2}\right). \]
In particular, \( D \) has size \( n := q^9 - q^3 \). Furthermore, let \( d := \sum_{Q \in D} Q \).

An AG-code arises by evaluating at the points of \( D \) the \( \mathbb{F}_{q^6} \)-rational functions whose poles are prescribed by \( T \) (each with multiplicity \( \leq m \)). It is an AG \([n, k, d]_{q^6}\)-code with
\[ d \geq n - \text{deg}(mT) = q^9 - q^3 - m(q^3 + 1) \quad \text{and} \quad k = \ell(mT) - \ell(mT - D) \]
where \( \ell(P) \) stands, as usual, for the dimension of the Riemann-Roch space associated to a divisor \( P \) on \( \mathcal{H}_q \). Here, if \( m(q^3 + 1) = \text{deg}(mT) > 2g - 2 = (q^3 + 1)(q^3 - 2) \), that is, if \( m > q^3 - 2 \), then the Riemann-Roch Theorem yields \( k = \text{deg}(mT) + 1 - \frac{1}{2}q^3(q^3 - 1) \) whence
\[ k = (q^3 + 1)(m - \frac{1}{2}(q^3 - 2)), \]
for \( m > q^3 - 2 \).

Such an AG-code is the Hermitian functional code \( C_L(D, mT) \) whose Goppa’s designed minimum distance is
\[ \delta := n - \text{deg}(mT) = (q^3 + 1)(q^3(q^3 - 1) - m). \]

The dual code \( C_{\Omega}(D, mT) \) of \( C_L(D, mT) \) can also be obtained by computing residuals in the space of holomorphic differentials \( \Omega(mT - D) \). Therefore,
\[ C_{\Omega}(D, mT) = \{(\text{res}(df)_{Q_1}, \ldots, \text{res}(df)_{Q_n}) | df \in \Omega(mT - D)\}. \]
For this reason, the latter code is called a differential code. It is a \([n, k', d']_{q^6}\)-code where
\[ d' \geq \text{deg}(mT) - (2g - 2) = (q^3 + 1)(m - (q^3 - 2)), \]
and \( k' \geq n + \ell(mT - D) - \ell(mT) \). In particular, equality holds if \( m \text{deg}(T) < n \), that is,
\[ k' = (q^3 + 1)(q^3 - 1) - m - \frac{1}{2}(q^3 - 2), \]
for \( m < q^3(q^3 - 1) \).

Its Goppa’s designed minimum distance is
\[ \delta^* = \text{deg}(mT) - (2g - 2) = (q^3 + 1)(m - (q^3 - 2)). \]

We exhibit values of \( m \) for which the differential code \( C_{\Omega}(D, mT) \) has good parameters. Its minimum distance is larger that the minimum distance of the one-point Hermitian code with the same length and dimension. The improvement is \( O(q^4) \), see Theorem 4.3. The essential ingredient of the proof is the gap sequence of \( \mathcal{H}_{q^3} \) on \( T \), which we compute explicitly: see Theorem 3.2. We also prove that the group of permutation automorphisms of the code \( C_L(D, mT) \), \( m < q^3 - 2 \), is isomorphic to \( \text{PGU}(3, q) \): see Theorem 5.4.

2. Preliminaries

We quote now several geometric and combinatorial properties of the Hermitian curves \( \mathcal{H}_q \) and \( \mathcal{H}_{q^3} \), the references are \([8, 12]\). Motivating examples and computations are implemented in the computer algebra systems MAGMA \([2]\) and GAP \([5]\).
2.1. 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 $F$ be a finite field and fix an algebraic closure $K$ of $F$, and let $AG(2, K)$ be the affine plane defined over $K$. If $F \in K[X, Y]$, then the affine plane curve $F$ is

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

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

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

If $\mathcal{F}$ is non-singular, that is, it has no singular point in $PG(2, K)$, then its genus equals $g = \frac{1}{2}(\deg(\mathcal{F}) - 1)(\deg(\mathcal{F}) - 2)$. 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 $\mathcal{F}$ and $\mathcal{G}$ in terms of their intersection divisor $\mathcal{F} \cdot \mathcal{G}$ depending on the intersection number $I(P, \mathcal{F} \cap \mathcal{G})$ at a point $P \in PG(2, K)$:

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

2.2. Riemann-Roch spaces

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

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

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

$$L(D) = \left\{ \frac{U(x, y)}{G(x, y)} \mid \deg U \leq \deg G, \mathcal{U} \cdot \mathcal{F} \geq B \right\}.$$  

2.3. Weierstrass semigroups and gap sequences

For simplicity, assume that $\mathcal{F}$ is a non-singular projective plane curve. For any $F$-rational point $P \in \mathcal{F}$, a non-gap at $P$ is a non-negative integer $g$ such that there exists $h \in F(\mathcal{F})$ with pole number $g$ at $P$ which is regular on the remaining points of $\mathcal{F}$, that is, $\operatorname{Div}(h)_{\infty} = gP$. 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 the generalization of the gap sequence and the Weierstrass semigroup to several points; see [3, 4, 11, 13, 14, 15].

3
For an ordered $r$-tuple $(P_1, P_2, \ldots, P_r)$ of $\mathbb{F}$-rational points of $\mathcal{F}$, a non-gap is an ordered $r$-tuple of non-negative integers $(g_1, g_2, \ldots, g_r) \in \mathbb{N}^r_0$ such that there exists $h \in \mathbb{K}((\mathcal{F}))$ with $\text{Div}(h)_\infty = g_1 P_1 + g_2 P_2 + \ldots + g_r P_r$ 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

$$\mathbf{H}(P_1, P_2, \ldots, P_r) = \mathbb{N}^r_0 \setminus \mathbf{G}(P_1, P_2, \ldots, P_r),$$

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 2.1** ([4, Lemma 2.2 and Corollary 2.3]). Fix $(n_1, \ldots, n_m) \in \mathbb{N}_0^m$ and write $D = n_1 Q_1 + \cdots + n_m Q_m$.

(i) $(n_1, \ldots, n_m) \in \mathbf{G}(Q_1, \ldots, Q_m) \iff \exists i$ such that $\ell(D) = \ell(D - Q_i)$.

(ii) $(n_1, \ldots, n_m) \in \mathbf{H}(Q_1, \ldots, Q_m) \iff \forall i$ we have $\ell(D) = \ell(D - Q_i) + 1$.

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

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

The Weierstrass gap sequence at $D$ is

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

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

**Lemma 2.2.** Let $D = P_1 + P_2 + \ldots + P_r$ with points $P_1, P_2, \ldots, P_r$ of $\mathcal{F}$. The non-negative integer $n$ is in $\mathbf{G}(D)$ if and only if for all integers $k_1, \ldots, k_m$ with

$$(n - 1, \ldots, n - 1) < (k_1, \ldots, k_m) \leq (n, \ldots, n)$$

we have $(k_1, \ldots, k_m) \in \mathbf{G}(P_1, P_2, \ldots, P_r)$.

2.4. The geometry of the Hermitian curve $\mathcal{H}_q$

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

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

Through every point $V \in PG(2, \mathbb{F}_{q^2})$ not in $\mathcal{H}_q(\mathbb{F}_{q^2})$ there are $q^2 - q$ secants and $q + 1$ tangents to $\mathcal{H}_q$. The arising $q + 1$ tangency points are the common points of $\mathcal{H}_q$ with the polar line of $V$ relative to the unitary polarity associated to $\mathcal{H}_q$. Let $V = (1 : 0 : 0)$. Then the line $l_\infty$ 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 $c^2 + c$ is 0 or not. This gives rise to the polynomial

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

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

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

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

$$\text{Div}(R_{q^3}(x, y))_\infty = (q^6 - q^3 + 1)(q^3 + 1)P_\infty = (q^9 + 1)P_\infty.$$
2.5. Intersection of the Hermitian curves $\mathcal{H}_q^3$ and $\mathcal{H}_q$

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

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

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

$$D = \sum_{Q \in \mathcal{H}_q^3 \backslash \mathcal{H}_q} Q \quad \text{and} \quad T = \sum_{Q \in \mathcal{H}_q} Q$$

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

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

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

$$\text{Div}(H_q) = (q+1)T - (q^3 + 1)(q+1)P_\infty$$

in $\mathbb{F}_q^*(\mathcal{H}_q^3)$. In particular,

$$(q+1)T \equiv (q^3 + 1)(q+1)P_\infty. \quad (7)$$

2.6. Equivalence of functional and differential Hermitian codes

**Lemma 2.3.** For any divisor $G$ of $\mathcal{H}_q^3$,

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

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

$$\omega = hdx \in \Omega(G - D) \iff \text{Div}(\omega) \geq G - D \iff \text{Div}(h) \geq G - D - \text{Div}(dx) \iff \text{Div}(R_q h) \geq G - D - \text{Div}(dx) + \text{Div}(R_q) \iff \text{Div}(R_q h) \geq G + T - (q^6 - 1)(q^3 + 1)P_\infty.$$

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

$$\omega = hdx \in \Omega(G - D) \iff h \in R_q^{-1} L(-G - T + (q^6 - 1)(q^3 + 1)P_\infty),$$

which proves the lemma. \hfill \square

**Proposition 2.4.** Let $G$ be an effective divisor on $\mathcal{H}_q^3$, with $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. The differential code $C_\Omega(D, G)$ and the functional code $C_L(D, -G - T + (q^6 - 1)(q^3 + 1)P_\infty)$ are monomially equivalent.

**Proof.** By Lemma 2.3, every differential in $\Omega(G - D)$ can be written as $\omega = R_q^{-1} f dx$ with $f \in L(-G - T + (q^6 - 1)(q^3 + 1)P_\infty)$. As $G$ and $T$ are effective, $f$ only has poles at infinity. From the Horizon Theorem [17, Section 4.3] $f$ is a polynomial in $x$ and $y$. Also, $P_\infty$ is not a pole of $\omega$. Hence $\text{res}_{P_\infty}(\omega) = 0$. 

5
Take a point \( S(a,b) \in \mathcal{H}_{q^3} \setminus \{ P_\infty \} \). Then, \( b^2 + b = a^3 + 1 \), \( t = x - a \) is a local parameter at \( S \), and the local expansion of \( y \) at \( S \) is \( y(t) = b + ta^3 + ta^3 + 1 \ldots \). Therefore \( f(a + t, y(t)) = f(a, b) + t[\ldots] \) with nonzero \( u = u(S) \) given by

\[
u = \begin{cases} \prod_{c \in \mathbb{F}_q, c^3 + c \neq 0} (b - c), & \text{for } a = 0. \\ \prod_{c \in \mathbb{F}_q, c^3 + c \neq 0, c \neq b} (b - c), & \text{for } a \neq 0. \end{cases}
\]

Thus,

\[
g(a + t, y(t)) = R_{q^3}(a + t, y(t))^{-1}f(a + t, y(t)) = u^{-1}f(a, b)t^{-1} + \cdots,
\]

whence

\[
\text{res}_S(gdx) = \text{res}_S(u^{-1}f(a, b)t^{-1} + \cdots) = u^{-1}f(S),
\]

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

**Proposition 2.5.** Let \( m \) be a positive integer. The codes \( C_\Omega(\mathcal{D}, mT) \) and \( C_L(\mathcal{D}, (q^6 - m - 2)T) \) are monomially equivalent.

**Proof.** This follows from Proposition 2.4 and Equation (7). \( \square \)

3. **The gap sequence of** \( \mathcal{H}_{q^3} \) **at** \( \text{supp}(T) \)

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

**Lemma 3.1.** Let \( 0 < m \leq q^3 - 2 \) be an integer and write \( m = m_0(q + 1) + m_1, 0 \leq m_1 \leq q \). 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

\[
\nu(G) \cdot \mathcal{H}_{q^3} = m_0(\mathcal{A}_q \cdot \mathcal{H}_{q^3}) + m_1(\mathcal{A}_q \cdot \mathcal{H}_{q^3}) = mT + mT' \geq mT.
\]

Furthermore, for the Riemann-Roch space,

\[
\mathcal{L}(mT) = \left\{ \frac{F(x, y)}{G(x, y)} \mid \deg F \leq \deg G \text{ and } \nu(F) \cdot \mathcal{H}_{q^3} \geq m_1T' \right\}.
\]

**Proof.** This follows from Equation (3), applied to \( \mathcal{F} = \mathcal{H}_{q^3} \) and \( G = mT \). \( \square \)

**Theorem 3.2.** Let \( 0 < m \leq q^3 - 2 \) be an integer and write \( m = m_0(q + 1) + m_1, 0 \leq m_1 \leq q \).

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

\[
\mathcal{L}(mT) = \mathcal{L}(m_0(q + 1)T)
\]

\[
= \left\{ \frac{F(x, y)}{H_q(x, y)^{m_0}} \mid \deg F \leq m_0(q + 1) \right\}.
\]

In particular, \( \ell(mT) = \ell(m_0(q + 1)T) = \left( \frac{m_0(q + 1) + 2}{2} \right) \).
b) If \((m_0 + 1)(q + 1) \geq (q + 1 - m_1)(q^2 - q + 1)\) then
\[
\frac{R_q^{m_1} - 1}{H_q^{m_0+1}} \in \mathcal{L}(mT) \setminus \mathcal{L}((m-1)T).
\]

**Proof.**
a) We use the notation of Lemma 3.1. Let \(F(X, Y)\) be a polynomial with \(\deg F \leq \deg G\) and \(v(F) = \mathcal{H}_q^3 \geq m_1 T'\). By assumption,
\[
\deg F \leq m_0(q + 1) + m_1(q^2 - q + 1) < q^3 - q.
\]
We prove that \(R_q^{m_1} | F\). Otherwise \(m_1 \geq 1\) and there is a linear component \(\ell : L = 0\) of \(\mathcal{H}_q\) such that \(F = F_0 L^k, L \notdivides F_0\) and \(k < m_1\). As \(L\) is not a tangent of \(\mathcal{H}_q^3\), for all points \(Q\) in \(\ell \setminus \mathcal{H}_q\) we have
\[
I(Q, v(F_0) \cap \mathcal{H}_q^3) \geq m_1 - k \geq 1.
\]
Clearly we have \(q^3 - q\) choices for \(Q\), and since \(\deg F_0 \leq \deg F < q^3 - q\), our assumption \(L \notdivides F_0\) 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 \(\mathcal{L}(mT)\), with \(\deg F_1 \leq m_0(q + 1)\).

b) Equation (6) together with
\[
\text{Div}(R_q) = T + T' - (q^3 + 1)(q^2 - q + 1)P_\infty
\]
yield
\[
\text{Div} \left( \frac{R_q^{m_1} - 1}{H_q^{m_0+1}} \right) = -mT + (q + 1 - m_1)T'
+ (q^3 + 1)((m_0 + 1)(q + 1) - (q + 1 - m_1)(q^2 - q + 1))P_\infty.
\]
Our assumption \((m_0 + 1)(q + 1) \geq (q + 1 - m_1)(q^2 - q + 1)\) implies the claim.

Since \(2q - 2 = (q^3 + 1)(q^3 - 2)\), if \(m > q^3 - 2\) then \(\deg(mT) > 2q - 2\) and
\[
\ell(mT) = \deg(mT) + 1 - g = (q^3 + 1)(m - \frac{q^3 - 2}{2}).
\]

**Corollary 3.3.** The Weierstrass gap sequence at \(T\) is
\[
G(T) = \{ m_0(q + 1) + m_1 \mid 1 \leq m_1 < q + 1 - \frac{(m_0 + 1)(q + 1)}{q^2 - q + 1} \}.
\]

**Proof.** The claim follows from Theorem 3.2, except for \(m_1 = 0\). In this case, \(1/H_q^{m_0} \in \mathcal{L}(mT) \setminus \mathcal{L}((m-1)T)\), which shows that \(m = m_0(q + 1) \notin G(T)\).

4. Hermitian codes \(C_\Omega(D, kT)\)

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 4.1.** Suppose that \(\alpha, \alpha + 1, \ldots, \beta\) is a sequence of consecutive numbers in \(G(T)\). Let \(k := \alpha + \beta - 1\). Then, the minimum distance of the differential code \(C_\Omega(D, kT)\) 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 \( T = Q_1 + \cdots + Q_m \).

**Lemma 4.2.** Let \( q > 3 \) be a prime power and define the integer

\[
k' = \begin{cases} 
(q^6 - q^3 - q^2 - \frac{1}{2}q - 1)(q^3 + 1) & \text{for } q \text{ even}, \\
(q^6 - q^3 - q^2 + \frac{1}{2}(q - 1))(q^3 + 1) & \text{for } q \text{ odd}.
\end{cases}
\]

Then the one-point functional code \( C_{L}(D, k'P_{\infty}) \) has parameters

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

\[
\leq \left( q^2 + \frac{q}{2} + 1 \right)(q^3 + 1) + q^3
\]

for \( q \) even, and

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

\[
\leq \left( q^2 - \frac{q - 1}{2} \right)(q^3 + 1) + q^3
\]

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 \( D' \) be the sum of the affine points of \( \mathcal{X}_{q^3} \). As \( a < b = a + 2 \), [20, line 4) of Table 1] implies that the true minimum distance of \( C_{L}(D', k'P_{\infty}) \) is

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

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

**Theorem 4.3.** Let \( q > 3 \) be a prime power and define the integer

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

Then the differential code \( C_{12}(D, kT) \) has parameters

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

\[
\geq \delta + \left( \frac{q}{2} - 1 \right)(q^3 + 1)
\]
for \( q \) even, and
\[
q^9 - q^3, \left( q^6 - \frac{3}{2} q^3 - q^2 + \frac{q + 1}{2} \right) (q^3 + 1),
\]
\[
\geq \delta + \frac{q - 1}{2}(q^3 + 1)
\]
for \( q \) odd, where
\[
\delta = \deg(k\mathcal{D}) - 2g + 2 = (q^3 + 1)(k - q^3 + 2)
\]
is the designed minimum distance of \( C_\Omega(D, kT) \).

Proof. Let \( q \geq 4 \) be even and \( m_0 := \frac{q^3}{2} \). 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
\[
\left| q + 1 - \frac{(m_0 + 1)(q + 1)}{q^2 - q + 1} \right| = \left| \frac{q}{2} - \frac{3q}{2(q^2 - q + 1)} \right| = \frac{q}{2} - 1
\]
for \( q > 2 \). By Corollary 3.3,
\[
\alpha = \frac{q^2(q + 1)}{2} + 1, \ldots, \beta = \frac{q^2(q + 1)}{2} + \frac{q - 1}{2}
\]
is a sequence of consecutive gap numbers. Moreover, \( k = \alpha + \beta - 1 \). As \( \deg(kT) > 2g - 2 \), we have
\[
\dim(C_\Omega(D, kT)) = n + g - \deg(kT) - 1
\]
\[
= (q^6 - \frac{3}{2} q^3 - q^2 - \frac{1}{2} q)(q^3 + 1).
\]
Proposition 4.1 improves the designed minimum distance
\[
\delta = \deg(kT) - 2g + 2 = (q^2 + \frac{q}{2} + 1)(q^3 + 1).
\]
of \( C_\Omega(D, kT) \) by
\[
(\beta - \alpha + 1) \deg(T) = \frac{q}{2} - 1)(q^3 + 1).
\]
This proves the theorem for \( q \geq 4 \) even. Similar computation applies for \( q \geq 5 \) odd with \( m_0 = (q^2 - 1)/2 \). \( \Box \)

**Remark 4.4.**
(i) Lemma 4.2 and Theorem 4.3 show that the code \( C_\Omega(D, kT) \) performs much better than the one-point Hermitian code of the same length and dimension; the improvement is approximatively \( q^4/2 \).

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

5. The permutation automorphisms of \( C_L(D, mT) \)

**Definition 5.1.** Let \( \mathcal{X} \) be a smooth irreducible curve over \( \mathbb{F}_q \), \( Q_1, \ldots, Q_n \in \mathcal{X}(\mathbb{F}_q) \), \( D = Q_1 + \cdots + Q_n \), and \( \mathcal{C} \) be an \( \mathbb{F}_q \)-rational divisor on \( \mathcal{X} \) with \( \text{supp}(D) \cap \text{supp}(\mathcal{C}) = \emptyset \). A monomial automorphism of \( C_L(D, \mathcal{C}) \) is a triple \((\alpha, \beta, \gamma)\), where \( \alpha \) is an automorphism of \( \mathcal{X}(\mathcal{C}) \), \( \beta \) is a permutation of \( \{Q_1, \ldots, Q_n\} \) and \( \gamma \) is a \( \{Q_1, \ldots, Q_n\} \to \mathbb{F}_q \) map. Moreover, for all \( P \in \{Q_1, \ldots, Q_n\} \) and \( f \in \mathcal{L}(\mathcal{C}) \) yields
\[
\alpha(f)(P) = \gamma(P)f(\beta(P)).
\]
If \( \gamma = 1 \) is constant then \((\alpha, \beta)\) is called a permutation automorphism of \( C_L(D, \mathcal{C}) \). If \( \beta \) is the identity permutation and \( \gamma \) is constant then one speaks of a pure monomial automorphism.
With the notation of the previous definition, let τ be an automorphism of the function field \( \mathbb{F}_q(\mathcal{C}) \) and assume that τ preserves the divisors D and C. Then, τ induces an automorphism α of \( \mathcal{C}(\mathbb{C}) \) and a permutation β of \( Q_1, \ldots, Q_n \). In fact, α is the restriction of τ to \( \mathcal{C}(\mathbb{C}) \), and β is defined in such a way that (8) holds. We say that \((α, β)\) is an inherited permutation automorphism of \( C_L(D, \mathbb{C}) \), induced by τ.

The following proposition generalizes [15, Theorem 4.1] in such a way, that it can be applied to certain codes \( C_L(D, \mathbb{C}) \) of the Hermitian curve \( \mathcal{H}_q^3 \).

Proposition 5.2. Let \( \mathcal{C} : F(X, Y) = 0 \) be a smooth irreducible plane curve over \( \mathbb{F}_q \), \( Q_1, \ldots, Q_n \in \mathcal{C}(\mathbb{F}_q) \), \( D = Q_1 + \cdots + Q_n \), and \( C \) be an \( \mathbb{F}_q \)-rational divisor on \( \mathcal{C} \) with \( \text{supp}(D) \cap \text{supp}(C) = \emptyset \). Let \( x, y \) be generators of the function field \( \mathbb{F}_q(\mathcal{C}) \) satisfying \( F(x, y) = 0 \). Assume that the following hold:

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

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

Proof. Let \((α, β)\) be a permutation automorphism of \( C_L(D, \mathbb{C}) \). By (a) we can set \( Q_i = (a_i, b_i) \) and \( β(Q_i) = Q_i' = (a_i', b_i') \) with \( a_i, b_i, a_i', b_i' \in \mathbb{F}_q \). Equation (3) and (b) 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 \( α(f)(P) = f(β(P)) \) we have

\[
u(a_i, b_i) \frac{G(a_i, b_i)}{G(a_i, b_i)} = \alpha \left( \frac{x}{S(x, y)} \right) (a_i, b_i)
= \frac{x}{S(x, y)} (a_i', b_i')
= \frac{S(a_i', b_i')}{S(a_i, b_i)}
\]

for all \( i = 1, \ldots, n \). This implies

\[
a_i' = \frac{u(a_i, b_i)}{w(a_i, b_i)}, \quad b_i' = \frac{v(a_i, b_i)}{w(a_i, b_i)}, \quad (9)
\]

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, \( \deg(F^*) \leq \deg(F) \deg(G) \), and

\[
F^*(a_i, b_i) = w(a_i, b_i)^{\deg(F)} F(a_i', b_i') = 0
\]

holds for \( i = 1, \ldots, n \). In particular \( \mathcal{C}^* : F^*(X, Y) = 0 \) and \( \mathcal{C}^* \) have at least \( n \) points in common. The theorem of Bézout and (d) imply \( F | F^* \).
Since \( w(x, y) \neq 0 \), the curve \( \mathcal{W} : w(X, Y) = 0 \) has a finite number of points in common with \( \mathcal{X} \).

Take an arbitrary affine point \((a, b) \in \mathcal{X}(\overline{F}_q)\), not on \( \mathcal{W} \). We have

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

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 \( \mathcal{X}(\overline{F}_q) \) to \( \mathcal{X} \), up to a finite number of exceptions. Since \( \bar{\tau} \) is defined over \( F_q \), 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 an homomorphism of the function field \( F_q(\mathcal{X}) \) to itself. We show that \( \tau \) is surjective. Notice that we identified the places of \( F_q(\mathcal{X}) \) and the points of \( \mathcal{X} \), and, the action of \( \tau \) on the places and the action of \( \bar{\tau} \) on the points are equivalent.

By Equation (9), \( \tau \) induces \( \beta \) on \( Q_1, \ldots, Q_n \). For all \( f \in \mathcal{X}(\mathbb{C}) \) we have \( \tau(f)(Q_i) = f(Q_i) = \alpha(f)(Q_i) \). As \( n > \text{deg}(\mathcal{C}) \), the evaluation map \( f \mapsto (f(Q_1), \ldots, f(Q_n)) \) 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 \( \tau \), hence \( x, y \in \text{Im}(\tau) \), which shows that \( \tau \) is indeed automorphism of \( F_q(\mathcal{X}) \). We have also seen that \( \tau \) induces the permutation automorphism \((\alpha, \beta)\), which is therefore inherited.

We can extend this method to monomial automorphisms.

**Proposition 5.3.** Under the hypothesis of Proposition 5.2, if \( \text{deg}(G) < \text{deg}(F) \) and \((\alpha, \beta, \gamma)\) is a monomial automorphism of \( C_L(\mathbb{D}, \mathbb{C}) \), then \( \gamma \) is constant. In particular, the monomial automorphism group of \( C_L(\mathbb{D}, \mathbb{C}) \) is the direct product of the permutation automorphism group by the pure monomial automorphism group.

**Proof.** With the notation of Proposition 5.2, 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 \( \text{deg}(G) \) 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 showed in the proof of Proposition 5.2

\[
\tau : x \mapsto \frac{u(x, y)}{w(x, y)}, \quad y \mapsto \frac{v(x, y)}{w(x, y)}
\]
is an automorphism of $\mathbb{F}_q(\mathbb{K})$. Let $(\alpha', \beta^{-1})$ be the inverse of the permutation automorphism $(\alpha, \beta)$ induced by $\tau$. Then $(\alpha^*, \beta^*, \gamma) = (\alpha, \beta, \gamma) \circ (\alpha', \beta^{-1})$ is a pure monomial automorphism and

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

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

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

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 $r(X, Y) = \frac{r^*(X, Y)}{s^*(X, Y)}$. The same argument applied to each $f \in \mathcal{L}(\mathbb{K})$ yields

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

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 $(\deg(G))^2(\deg(F)) \leq (\deg(G))(\deg(F))^2 < n$, Bézout’s theorem yields $rs^* = r^*s$. In other words, $r(f) = r^*/s^*f$ for all $f \in \mathcal{L}(\mathbb{K})$. We show that this only holds when $r^*/s^*$ is a constant. Since $\alpha$ is an endomorphism of the finite dimensional vector space $\mathcal{L}(\mathbb{K})$ over $\mathbb{F}_q$, $\alpha$ 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 $A^i(f) = \alpha^i(f) = (r^*/s^*)^if$, this yields $u(A) = u(r^*/s^*)f$ for all $f \in \mathcal{L}(\mathbb{K})$. Therefore, $u(r^*/s^*) = 0$ in $\mathbb{K}(\mathbb{K})$. In particular, for any $(a_i, b_i)$, $u(r^*/s^*)$ valued in $(a_i, b_i)$ equals zero. On the other hand, since $r^*/s^*$ valued in $(a_i, b_i)$ gives an element, say $k$, in $\mathbb{F}_q$, $T - k$ is a factor of $u(T)$. Therefore, $u(T) = (T - k)^\mu v(T)$. This factorization, interpreted in $\mathbb{K}(\mathbb{K})[T]$, gives $u(r^*/s^*) = (r^*/s^* - k)^\mu v(r^*/s^*)$. 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 $\gamma$ commutes with any permutation automorphism.

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

**Theorem 5.4.** Let $0 < m \leq q^3 - 2$ be an integer and write $m = m_0(q + 1) + m_1$, $0 \leq m_1 \leq q$. If $m_1 \leq \frac{q^3 - 2 - m}{q(q + 1)}$, then the following hold:

(i) The group of permutation automorphisms of $C_L(\mathbb{D}, m\mathcal{T})$ is isomorphic to the projective unitary group $\text{PGU}(3, q)$.

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

**Proof.** We apply Proposition 5.2 for the curve $\mathbb{F}_q^6$ over $\mathbb{F}_q$. Condition (a) is immediate. Conditions (b) and (c) follow from Lemma 3.1 with $G(X, Y) = H^m_q R^{m_1}_q$ and $S(X, Y) = H^{m_0}_q$. Hence,

$$\deg(G) = m_0(q + 1) + m_1(q^2 + q + 1) = m + m_1q(q + 1) \leq q^3 - 2$$
and
\[ \deg(G) \deg(H_{q^3})^2 \leq (q^3 - 2)(q^3 + 1)^2 < q^9 - q^3 = n. \]

This means that Condition (d) of Proposition 5.2 holds, and all permutation automorphisms of \( C_L(D, mT) \) are inherited. It is known that \( \text{Aut}(\mathbb{F}_{q^6}(\mathcal{H}_{q^3})) \cong PGU(3, q^3) \), and the action of \( \text{Aut}(\mathbb{F}_{q^6}(\mathcal{H}_{q^3})) \) on the \( \mathbb{F}_{q^6} \)-rational places is equivalent to the action of \( PGU(3, q^3) \) on the points of \( \mathcal{H}_{q^3} \). Clearly, if \( \tau \in \text{Aut}(\mathbb{F}_{q^6}(\mathcal{H}_{q^3})) \) induces a permutation automorphism of \( C_L(D, mT) \), then \( \tau \) preserves \( D \). Thus, it preserves \( \text{supp}(T) = \mathcal{H}_{q^3} \) and \( \tau' \in PGU(3, q) \). This finishes the proof of (i). Since \( \deg(G) < \deg(H_{q^3}) = q^3 + 1 \), Proposition 5.3 implies (ii).

\[ \square \]

+ MAKE REMARK on the importance of these \( m \)'s ??

References


