Hermitian codes from higher degree places

G. Korchmáros* and G.P. Nagy

Abstract

Matthews and Michel [28] investigated the minimum distances in certain algebraic-geometry codes arising from a higher degree place \( P \). In terms of the Weierstrass gap sequence at \( P \), they proved a bound that gives an improvement on the designed minimum distance. In this paper, we consider those of such codes which are constructed from the Hermitian function field \( \mathbb{F}_{q^2}(\mathcal{H}) \). We determine the Weierstrass gap sequence \( G(P) \) where \( P \) is a degree 3 place of \( \mathbb{F}_{q^2}(\mathcal{H}) \), and compute the Matthews and Michel bound with the corresponding improvement. We show more improvements using a different approach based on geometry. We also compare our results with the true values of the minimum distances of Hermitian 1-point codes, as well as with estimates due Xing and Chen [32].

Keywords: AG code, Weierstrass gap, Hermitian curve.
Mathematics Subject Classification (2000) 14H55, 11T71, 11G20, 94B27

1 Introduction

Algebraic-geometry (AG) codes are linear codes constructed from algebraic curves defined over a finite field \( \mathbb{F}_q \). The best known such general construction was originally introduced by Goppa, see [17]. It provides linear codes from certain rational functions whose poles are prescribed by a given \( \mathbb{F}_q \)-rational divisor \( G \), by evaluating them at some set of \( \mathbb{F}_q \)-rational places disjoint from \( \text{supp}(G) \). The dual to such a code can be obtained by computing residues of differential forms. The former are the functional codes, and the latter

*This research was performed while the first author was a visiting professor at the Bolyai Institute of University of Szeged during the second semester of the academic year 2011-12. The visit was financially supported by the TAMOP-4.2.1/B-09/1/KONV-2010-0005 project.
are the differential codes. If the $\mathbb{F}_q$-rational places are $Q_1, \ldots, Q_n$ and $D = Q_1 + \ldots + Q_n$, then $C_L(D, G)$ and $C_\Omega(D, G)$ stand for the corresponding functional and differential codes, respectively. For $n > \deg G > 2q - 2$ where $q$ is the genus of the curve, a lower bound on the minimum distance for $C_L(D, G)$ is $n - \deg G$, and for $C_\Omega(D, G)$ is $\deg G - (2q - 2)$. These values are the designed minimum distance.

Typically the divisor $G$ is taken to be a multiply $mP$ of a single place $P$ of degree one. Such codes are the one-point codes, and have been extensively investigated; see [3, 16] and the bibliography therein. It has been shown however that AG-codes with better parameters than the comparable one-point Hermitian code may be obtained by allowing the divisor $G$ to be more general; see the recent papers [1, 2, 10, 11, 12, 18] and the references therein.

In [28] this possibility is discussed for one-point differential codes arising from places of higher degree, that is, for $C_\Omega(D,G)$ with $G = mP$, where $P$ is a place of degree $r > 1$. From [28, Theorem 3.4], there exist special values of $m$ for which such a code $C_\Omega(D,G)$ has bigger minimum distance than the designed one by at least $r$. The Matthews-Michel bound, see [28, Theorem 3.5], shows that even better improvements may occur whenever the gap sequence at $P$ has certain specific properties. This is verified in [28] by the examples computed by MAGMA [4] for $q = 7^2, 8^2$ and $r = 3$ where the curve is, as usual, the Hermitian curve over $\mathbb{F}_{q^2}$. Nevertheless, the applicability of the above results to any $q$ requires detailed knowledge of the gap sequence at $P$ rising the problem of determining such a sequence, in particular at a degree 3 point $P$ of the Hermitian curve over $\mathbb{F}_{q^2}$. Our Theorem 3.1 solves this problem and together with [28, Theorem 3.5] provides an improvement on the designed minimum distance for an infinite family of differential codes, see Proposition 4.1. This confirms the importance of knowledge of gap sequences at $r$-tuples of places in the study of functional and differential codes, as clearly emerged from previous and current work by several authors, see [5, 6, 7, 8, 15, 22, 23, 24, 26, 27, 29].

In Section 5 we give more improvements using a different approach based on geometry rather than function field theory, the essential ingredient being the Noether “AF+BG” theorem. Our main result is stated in Theorem 5.10.

In Section 6 examples are given to illustrate and compare the above improvements. For the Hermitian curve over $\mathbb{F}_{2^2}$ with a point $P$ of degree $r = 3$, the Matthews-Michel bound as well as Theorem 5.10 show that $C_\Omega(D, 18P)$ is a $[343, 309, d]$-code with $d \geq 20$. This improves the previous Xing-Chen bound by 2, see [32], and the designed minimum distance by 6. Indeed, using MAGMA, we were able to prove that such a code has minimal distance 20.
2 Background and Preliminary Results

Our notation and terminology are standard. The reader is referred to [20, 31] and the survey paper [21].

Let \( \mathcal{X} \) be a (projective, non-singular, geometrically irreducible algebraic curve) of genus \( g \), defined over a finite field \( \mathbb{F}_q \) of order \( q = p^r \) and viewed as curve over the algebraic closure of \( \mathbb{F}_q \). Let \( \mathbb{F}_q(\mathcal{X}) \) be the function field of \( \mathcal{X} \) with constant field \( \mathbb{F}_q \). For every non-zero function \( f \in \mathbb{F}_q(\mathcal{X}) \), \( \text{Div}(f) \) stands for the principal divisor associated with \( f \) while \( \text{Div}(f)_0 \) and \( \text{Div}(f)_\infty \) for its zero and pole divisor. Furthermore, for every separable function \( f \in \mathbb{F}_q(\mathcal{X}) \), \( df \) is the exact differential arising from \( f \), and \( \Omega \) denotes the set of all these differentials. Also, \( \text{res}_D(df) \) is the residue of \( df \) at a place of \( D \) of \( \mathbb{F}_q(\mathcal{X}) \). For any divisor \( A \) of \( \mathbb{F}_q(\mathcal{X}) \), let

\[
\mathcal{L}(A) = \{ f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} \mid \text{Div}(f) \geq -A \} \cup \{0\}
\]

and \( \ell(A) = \dim(\mathcal{L}(A)) \). Furthermore, let

\[
\Omega(A) = \{ df \in \Omega \mid \text{Div}(df) \geq A \} \cup \{0\}.
\]

Let \( D = Q_1 + \ldots + Q_n \) be a divisor where \( Q_1, \ldots, Q_n \) are \( n \) distinct degree one places of \( \mathbb{F}_q(\mathcal{X}) \). Let \( G \) be another divisor of \( \mathbb{F}_q(\mathcal{X}) \) whose support \( \text{supp}(G) \) contains none of the places \( P_i \) with \( 1 \leq i \leq n \). For any function \( f \in \mathcal{L}(G) \), the evaluation of \( f \) at \( D \) is given by \( \text{ev}_D(f) = (f(Q_1), \ldots, f(Q_n)) \). This defines the evaluation map \( \text{ev}_D : \mathcal{L}(G) \to \mathbb{F}_q^n \) which is \( \mathbb{F}_q \)-linear and also injective when \( n > \deg(G) \). Therefore, its image is a subspace of the vector space \( \mathbb{F}_q^n \), or equivalently, an AG \( [n, k, d] \)-code where \( d \geq n - \deg(G) \) and if \( \deg(G) > 2g - 2 \) then \( k = \deg(G) + 1 - g \). Such a code is the functional code \( C_L(D, G) \) with designed minimum distance \( n - \deg(G) \). The dual code \( C_{\Omega}(D, G) \) of \( C_L(D, G) \) is named differential code, since

\[
C_{\Omega}(D, G) = \{ (\text{res}(df)_{Q_1}, \ldots, \text{res}(df)_{Q_n}) \mid df \in \Omega(G - D) \}.
\]

The differential code \( C_{\Omega}(D, G) \) is a \( [n, \ell(G - D) - \ell(G) + \deg D, d] \)-code with \( d \geq \deg(G) - (2g - 2) \), and its designed minimum distance is \( \deg(G) - (2g - 2) \).

In this paper we are interested in differential codes \( C_{\Omega}(D, G) \) with \( G = mP \) where \( P \) is a degree \( r \) place of \( \mathbb{F}_q(\mathcal{X}) \). Let \( P_1, \ldots, P_r \) be the extensions of \( P \) in the constant field extension of \( \mathbb{F}_q(\mathcal{X}) \) of degree \( r \). Then \( P_1, \ldots, P_r \) are degree one places of \( \mathbb{F}_q^r(\mathcal{X}) \) and, up to labeling the indices, \( P_{j+1} = \text{Fr}(P_j) \) where \( \text{Fr} \) is the \( q \)-th Frobenius map and the indices are taken modulo \( n \). Also, \( P \) may be identified with the \( \mathbb{F}_q^r \)-divisor \( P_1 + \ldots + P_r \) of \( \mathbb{F}_q^r(\mathcal{X}) \). The relationship between the Weierstrass semigroups \( H(P) \) of \( \mathbb{F}_q(\mathcal{X}) \) and
Our results concern differential codes arising from a degree 3 place on the Hermitian curve $\mathcal{H}$ defined over $\mathbb{F}_q$. The proofs use several geometric and combinatorial properties of $\mathcal{H}$ that we quote now, the references are [19] and [23]. In the projective plane $PG(2, \mathbb{F}_q^2)$ equipped with homogeneous coordinates $(X, Y, Z)$, a canonical form of $\mathcal{H}$ is $X^{q+1} - Y^qZ - YZ^q = 0$ so that $\mathcal{H} = \mathcal{V}(X^{q+1} - Y^qZ - YZ^q)$. Every degree one place of the function field $\mathbb{F}_q^2(\mathcal{H})$ of $\mathcal{H}$ corresponds to a point of $\mathcal{H}$ in $PG(2, \mathbb{F}_q^2)$, and this holds true for the degree one places of the constant field extension $\mathbb{F}_q(\mathcal{H})$ which correspond to the points of $\mathcal{H}$ in $PG(2, \mathbb{F}_q^2)$. Moreover, a place $P$ of degree $r > 1$ of $\mathbb{F}_q^2(\mathcal{H})$ is represented by a divisor $P_1 + P_2 + \ldots + P_r$ of the constant field extension $\mathbb{F}_q^2(\mathcal{H})$ where $P_1$ are degree one places of $\mathbb{F}_q^2(\mathcal{H})$ with $P_i = \text{Fr}^i(P_1)$ for $i = 0, 1, \ldots, r - 1$. Furthermore,

$$|\mathcal{H}(\mathbb{F}_q^2)| = |\mathcal{H}(\mathbb{F}_q)| = q^3 + 1, |\mathcal{H}(\mathbb{F}_q^6)| = q^{12} + 1 + q^4(q - 1).$$

A line $l$ of $PG(2, \mathbb{F}_q^2)$ is either a tangent to $\mathcal{H}$ at an $\mathbb{F}_q^2$-rational point of $\mathcal{H}$ or it meets $\mathcal{H}$ at $q + 1$ distinct $\mathbb{F}_q^2$-rational points. In terms of intersection divisors, see [20] Section 6.2,

$$I(\mathcal{H}, l) = \begin{cases} (q + 1)Q, & Q \in \mathcal{H}(\mathbb{F}_q^2); \\ \sum_{i=1}^{q+1} Q_i, & Q_i \in \mathcal{H}(\mathbb{F}_q^2), Q_i \neq Q_j, 1 \leq i < j \leq n. \end{cases}$$

Through every point $V \in PG(2, \mathbb{F}_q^2)$ not in $\mathcal{H}(\mathbb{F}_q^2)$ there are $q^2 - q + 1$ secants and $q + 1$ tangents to $\mathcal{H}$. The corresponding $q + 1$ tangency points are the common points of $\mathcal{H}$ with the polar line of $V$ relative to the unitary polarity associated to $\mathcal{H}$. 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

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

\hspace{1cm} (2)
of degree $q^2 - q + 1$. By [20, Theorem 6.42],
\[
\text{Div}(R(x, y)) = (q^2 - q + 1)(q + 1)P_\infty = (q^3 - 1)P_\infty.
\]

Assume from now on that
\[
D = \sum_{Q \in \mathcal{H}(\mathcal{F}_{q^2})\setminus\{P_\infty\}} Q.
\]

Proposition 2.2 below gives an explicit description of a (monomial) equivalence between the codes $C_\Omega(D, G)$ and $C_L(D, (q^3 + q^2 - q - 2)P_\infty - G)$ constructed on $\mathcal{H}$. It may be noted that this is related to the equivalence $C_\Omega(D, G) = C_\Omega(D, K + D - G)$ for a canonical divisor $K$, mentioned in [21, Section III].

The proof of Proposition 2.2 relies on the following lemma where $\mathbb{F}_{q^2}(\mathcal{H}) = \mathbb{F}_{q^2}(x, y)$ with $x^{q+1} - y^q - y = 0$, and $x$ is separable function.

**Lemma 2.1.** For any divisor $E$ of $\mathbb{F}_{q^2}(\mathcal{H})$,

(i) $\Omega(E) = dx \mathcal{L}(-E + \text{Div}(dx))$,

(ii) $\mathcal{L}(D + \text{Div}(dx) + E) = R(x, y)^{-1}\mathcal{L}((q^3 + q^2 - q - 2)P_\infty + E)$.

**Proof.** Obviously, $\text{Div}(f dx) = \text{Div}(f) + \text{Div}(dx) \succeq E$ if and only if $\text{Div}(f) \succeq E - \text{Div}(dx)$, which proves (i). To show (ii), notice that the zeros of $R(x, y)$ are the points in $\mathcal{H}(\mathcal{F}_{q^2})$ each with multiplicity one. From [20, Theorem 6.42],
\[
\text{Div}(R(x, y)) = D + P_\infty - \deg R(q + 1)P_\infty = D - q^3P_\infty.
\]

Since $\text{Div}(dx) = (2g - 2)P_\infty = (q^2 - q - 2)P_\infty$, this gives
\[
\mathcal{L}((q^3 + q^2 - q - 2)P_\infty + E) = \mathcal{L}(D - \text{Div}(R(x, y)) + \text{Div}(dx) + E).
\]

Thus, $f \in \mathcal{L}((q^3+q^2-q-2)P_\infty+E)$ and $f \in R(x, y)^{-1}\mathcal{L}(D - \text{Div}(dx) + E)$ are equivalent conditions. \qed

**Proposition 2.2.** The codes $C_\Omega(D, G)$ and $C_L(D, (q^3 + q^2 - q - 2)P_\infty - G)$ are monomially equivalent.

**Proof.** By Lemma 2.1, every differential in $C_\Omega(D, G)$ can be written as $h dx$ with $h \in \mathcal{L}(D - G + \text{Div}(dx)) = R(x, y)^{-1}\mathcal{L}((q^3 + q^2 - q - 2)P_\infty - G)$. Let $f = g R(x, y) \in \mathcal{L}((q^3 + q^2 - q - 2)P_\infty - G)$. Then $f \in \mathbb{F}_{q^2}[x, y]$ with $x^{q+1} - y^q - y = 0$. Also, $P_\infty$ is not a pole of $g dx$. Hence $\text{res}_{P_\infty}(g dx) = 0$. Take a point $S \in \mathcal{H}(\mathcal{F}_{q^2})$ other than $P_\infty$. Then $S = (a, b, 1)$ with $b^q + b = c^{q+1}$. Also, $t = x - a$ is a local parameter at $S$, and the local expansion of $y$ at $S$...
is \( y(t) = b + ta^q + t^{q+1} \ldots \). Therefore \( f(a + t, y(t)) = f(a, b) + t[\ldots] \) while \( R(a, b) = 0 \) and \( R(a + t, y(t)) = ut + t^2[\ldots] \) with nonzero \( u \) given by

\[
\begin{align*}
    u &= \left\{ \begin{array}{l}
        \prod_{c \in \mathbb{F}_{q^2}, c^i+c \neq 0} (b - c), \quad \text{for } a = 0, \\
        a^{q+1} \prod_{c \in \mathbb{F}_{q^2}, c^i+c \neq 0, c \neq b} (b - c), \quad \text{for } a \neq 0.
    \end{array} \right.
\end{align*}
\]

Thus,

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

whence

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

which shows the monomial equivalence between the codes \( C_G(D, G) \) and \( C_L(D, (q^3 + q^2 - q - 2)P_\infty - G) \).

The group \( \text{Aut}(\mathcal{H}) \) of all automorphisms of \( \mathcal{H} \) is defined over \( \mathbb{F}_{q^2} \) and it is a projective group of \( PG(2, \mathbb{F}_{q^2}) \) isomorphic to the projective unitary group \( PGU(3, q) \). Furthermore, \( \text{Aut}(\mathcal{H}) \) acts doubly transitively on \( \mathcal{H}(\mathbb{F}_{q^2}) \), transitively on the points of \( PG(2, \mathbb{F}_{q^2}) \) not in \( \mathcal{H}(\mathbb{F}_{q^2}) \), as well as on the points in \( \mathcal{H}(\mathbb{F}_{q^2}) \setminus \mathcal{H}(\mathbb{F}_{q^2}) \), and also on the set of all triangles in \( \mathcal{H}(\mathbb{F}_{q^2}) \setminus \mathcal{H}(\mathbb{F}_{q^2}) \) which are invariant under the action of the Frobenius map. The latter property shows that the geometry of degree 3 places of \( \mathbb{F}_{q^2}(\mathcal{H}) \) is independent on the choice of \( P \). Write \( P = P_1 + P_2 + P_3 \) with \( P_i \in \mathcal{H}(\mathbb{F}_{q^2}) \setminus \mathcal{H}(\mathbb{F}_{q^2}) \) and fix a projective frame \((X_1, X_2, X_0)\) whose vertices are the points \( P_i \). For a suitable choice of the unity point \( U_0 \in \mathcal{H}(\mathbb{F}_{q^2}) \), the equation of \( \mathcal{H} \) becomes

\[
X_1 X_0^q + X_2 X_0^q + X_0^q X_1 = 0,
\]

see [11, Proposition 4.6] where the non-singular matrix \( M \) realizing the change of coordinates \((X, Y, Z) \rightarrow (X_1, X_2, X_0)\) is given explicitly. In doing so, every \( f \in \mathcal{H}(\mathbb{F}_{q^2}) \) will have an equation in \((X_1, X_2, X_0)\). In other words, the linear map \( \mu \) of \( \mathcal{H}(\mathbb{F}_{q^2}) \) associated to \( M \) takes \( \mathcal{H}(\mathbb{F}_{q^2}) \) to a subfield \( \mathcal{H}(\mathbb{F}_{q^2}) \) which is isomorphic to (but distinct from) \( \mathcal{H}(\mathbb{F}_{q^2}) \).

For \( i = 0, 1, 2 \mod 3 \), the tangent to \( \mathcal{H} \) at \( P_i \) is the line \( l_i = P_i P_{i+1} \) of equation \( X_{i+1} = 0 \). Therefore

\[
I(\mathcal{H} \cap l_i) = qP_i + P_{i+1}, \quad i = 0, 1, 2 \mod 3.
\]  

(4)
Let $l_i = v(\ell_i)$. Then

\[
\text{Div}(\ell_1) = qP_1 + P_2 - (q + 1)P_\infty, \\
\text{Div}(\ell_2) = qP_2 + P_3 - (q + 1)P_\infty, \\
\text{Div}(\ell_0) = qP_3 + P_1 - (q + 1)P_\infty, \\
\text{Div}(\ell_1\ell_2\ell_0) = (q + 1)P - 3(q + 1)P_\infty.
\]

Observe that $v(\ell_1\ell_2\ell_0)$ is defined over $\mathbb{F}_{q^2}$ while $l_i$ is defined over $\mathbb{F}_{q^d}$.

**Lemma 2.3.** Let $C$ be any (possible singular or reducible) plane curve not containing the tangent $l_i$ to $\mathcal{H}$ at $P_i$ as a component where $0 \leq i \leq 2$. If $I(P_i, \mathcal{H} \cap C) \leq q$, then

\[ I(P_i, \mathcal{H} \cap C) = I(P_i, l_i \cap C). \]

**Proof.** We prove the assertion for $i = 1$. We use affine coordinates $(X, Y)$ with $X = X_1/X_0$, $Y = X_2/X_0$ so that $\mathcal{H}$ has equation $Y + X^q + XY^q = 0$ and $P_1 = (0, 0)$. Then $X$ is a local parameter at $P_1$ and the expansion of $Y$ is $Y(X) = X^q(-1 + X[\ldots])$. Furthermore, $\ell_1$ has equation $Y = 0$. Let $F(X, Y) = 0$ be an affine equation of $C$. Then $I(P_1, \ell_1 \cap C) = m$ if and only if $F(X, 0) = c_1X^m(c_2 + X[\ldots])$ with nonzero $c_1, c_2 \in \overline{\mathbb{F}}_{q^2}$. Since $Y$ does not divide $F(X, Y)$ and $I(P_1, \mathcal{H} \cap C) \leq q$, we also have $F(X, Y(X)) = d_1X^m(d_2 + X[\ldots])$ with nonzero $d_1, d_2 \in \overline{\mathbb{F}}_{q^2}$. Therefore $I(P_1, \mathcal{H} \cap C) = m$. \hfill \Box

From the above discussion we have the following result

**Proposition 2.4.** Let $m = m_1(q + 1) + m_0$ with $m_1$ and $m_0$ non-negative integers such that $m_0 \leq q$. In $\mathbb{F}_{q^2}(\mathcal{H})$, take a degree 3 place $P$ together with a degree one place $P_{\infty}$ $\mathbb{F}_{q^2}$-rational. Let

\[
A_1 = (q^3 + q^2 - q - 2)P_{\infty} - mP, \\
A_2 = (q^2 - 3m_1 - 1)(q + 1)P_{\infty} - (P_{\infty} + m_0P).
\]

Then the codes $C_L(D, A_1)$ and $C_L(D, A_2)$ are monomially equivalent.

**Proof.** The monomial equivalence of the two codes follows from $A_2 = A_1 + m_1(\ell_1\ell_2\ell_3)$ after observing that the $\mathbb{F}_{q^2}$-rational polynomial $\ell_1\ell_2\ell_0$ has neither zeros nor poles in $\text{supp} \ D$. \hfill \Box

**Remark 2.5.** By Propositions 2.2 and 2.4, the differential code $C_{\Omega}(D, mP)$ and the functional code $C_L(D, (q^2 - 3m_1 - 1)(q + 1)P_{\infty} - (P_{\infty} + m_0P))$ are
monomially equivalent. They have length \( q^3 \), dimension \( q^3 + \frac{1}{2}(q^2 - q - 2) - 3m \) and designed minimum distance
\[
\delta = 3m - q^2 + q + 2. \tag{5}
\]
In particular, \( 3m \geq q^2 - q - 2 \geq 0 \) holds.

**Remark 2.6.** Propositions \( 2.2 \) shows that if \( m_0 = 0 \) then \( C_L(D, A_2) \) is \( C_L(D, tP_\infty) \) with \( t = (q^2 - 3m_1 - 1)(q + 1) \). For such particular codes, the minimum distance problem has been solved in [30, 33]. Therefore we may limit ourselves to the case where \( m = m_1(q + 1) + m_0 \) with \( m_0 > 0 \).

## 3 The Weierstrass gap sequence of places of higher degree

As we have pointed out in the Introduction, in the study of differential codes \( C_{\Omega}(D, G) \) where \( \text{supp}(G) \) consists of just one place \( P \), possibly of degree \( r > 1 \), a key issue is to determine the gap sequence at \( P \). In the case where \( P \) has degree one, this essentially requires to determine the Weierstrass semigroup at \( P \) and the relative computations can generally be carried out using methods from classical algebraic geometry. For instance, for the Hermitian function field \( \mathbb{F}_{q^2}(\mathcal{H}) \), the Weierstrass semigroup is as simple as possible being generated by \( q \) and \( q + 1 \). The analog question for places of degree \( r > 1 \) is still open even for \( \mathbb{F}_{q^2}(\mathcal{H}) \), apart from some smallest values of \( q \) namely \( q \leq 9 \) where the computations were carried out by using the MAGMA; see [28].

In this section we determine the gap sequence of \( \mathbb{F}_{q^2}(\mathcal{H}) \) at any place \( P \) of degree 3, see Theorem 3.1. It turns out that the smallest non-gap is \( q - 2 \), and we first explain why this occur.

There exists \( \alpha \in \text{Aut}(\mathcal{H}) \) of order 3 which has no fixed point off \( \mathcal{H}(\mathbb{F}_{q^2}) \) and acts on \( \{P_1, P_2, P_3\} \) as a 3-cycle. The quotient curve \( C = \mathcal{H}/\langle \alpha \rangle \) is a \( \mathbb{F}_{q^2} \)-maximal curve. Furthermore, the place of \( P \) of \( \mathbb{F}_{q^2}(C) \) lying under \( P \) is unramified and the smallest non-gap at \( P \) is \( q - 2 \). Take \( f \in \mathbb{F}_{q^2}(C) \) such that \( \text{Div}(f)_\infty = (q - 2)\tilde{P} \). Then \( f \) can also be viewed as an element of \( \mathbb{F}_{q^2}(\mathcal{H}) \) and \( \text{Div}(f)_\infty = (q - 2)\tilde{P} \) remains true in \( \mathbb{F}_{q^2}(\mathcal{H}) \). Viceversa, if \( i < q - 2 \) is a non-gap at \( P \), let \( f \in \mathbb{F}_{q^2}(\mathcal{H}) \) with \( \text{Div}(f)_\infty = iP \) and \( f^\alpha = f \). The latter property implies that \( f \in \mathbb{F}_{q^2}(C) \) with \( \text{Div}(f)_\infty = i\tilde{P} \). But this is impossible since \( q - 2 \) is the smallest non gap at \( \tilde{P} \).

**Theorem 3.1.** For any degree 3 place \( P \) of \( \mathbb{F}_{q^2}(\mathcal{H}) \), the Weierstrass gap sequence at \( P \) is
\[
G(P) = \{u(q + 1) - v \mid 0 \leq v \leq q, 0 < 3u \leq v\}. \tag{6}
\]
Proof. For two integers $u, v$ with $0 \leq v \leq q$, $0 < 3u \leq v$, let $m = u(g+1) - v$. First we construct the complete linear series $|m(P_1 + P_2 + P_3)|$ using [20, Theorem 6.52]. From (4), we have $\sum_{i=0}^{1} I(P_i, \mathcal{H} \cap l_i) = (q+1)(P_1 + P_2 + P_3)$. This shows that the curve $v((\ell_1 \ell_2 \ell_3)^u)$ of degree $3u$ is an adjoint of the divisor $m(P_1 + P_2 + P_3)$. Therefore, up to the fixed divisor $v(P_1 + P_2 + P_3)$, the complete linear series $|m(P_1 + P_2 + P_3)|$ consists of the divisors cut out by the adjoint curves $\Phi$ of degree 3 for which $I(P_i, \mathcal{H} \cap \Phi) \geq v$ for $i = 0, 1, 2$. Reformulating this in terms of Riemann-Roch spaces; see [20, Section 6.4], gives

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

Since $v \leq q$ and the tangent line at $P_i$ is $v(\ell_i)$, this together with Lemma 2.3 yield $I(\ell_i \cap v(f), P_i) \geq v$. Moreover, $P_{i+1} \in v(f) \cap v(\ell_i)$. Therefore, counted with multiplicity, $v(\ell_i)$ and $v(f)$ have at least $v+1$ common points. If $\deg v(f) = 3u \leq v$ then Bézout’s theorem, see [20, Theorem 3.14], yields $\ell_i \mid f$. This holds for $i = 0, 1, 2$. Thus, $\ell_1 \ell_2 \ell_3 \mid f$. Hence $f/(\ell_1 \ell_2 \ell_3)^{u-1} = g/(\ell_1 \ell_2 \ell_3)^{u-1}$ with $\deg g \leq 3(u-1)$. This yields that $L(mP) \subseteq L((m+1)P)$. Therefore, the right hand side in (4) is indeed in $G(P)$.

Viceversa, assume that $0 \leq v \leq q$ and $3u > v$. Let $w = \ell_1^{2u-v} \ell_2^{-u} \ell_3^{-u}$. Then $\text{Div}(w) = m_1P_1 + m_2P_2 + m_3P_3$, where

- $m_1 = (2u - v)q - u,$
- $m_2 = (v - u)q + 2u - v,$
- $m_3 = -uq - u + v.$

Obviously, $m_3 = -m$. Also, $m_2 \leq m_3$ is equivalent to $vq \leq 2v - 3u < 2v$. Since $q \geq 2$, this yields $v = 0$ and $0 \leq -3u$, a contradiction. Now, assume $m_1 \leq m_3$. Then $(3u - v)q \leq v \leq q$, which implies $3u - v \leq 1$. As $3u > v$, this yields $3u = v + 1$ and $v = q$ whence $m = \frac{1}{3}(q^2 - q + 1)$ follows. Thus, $\deg(mP) = 3m > 2g - 1$, where $g = \frac{1}{2}q(q - 1)$ is the genus of $\mathcal{H}$. From [28, Proposition 2.1], $m$ is not in $G(P)$.

We are left with the case where $m_1, m_2 > m_3 = -m$. For $w \in \mathbb{F}_q(\mathcal{H})$, let $\text{Tr}(w) = w + \text{Fr}(w) + \text{Fr}^2(w)$. Obviously $\text{Tr}(w) \in \mathbb{F}_q(\mathcal{H})$. Furthermore,

$$v_{P_i}(\text{Tr}(w)) \leq \min\{v_{P_1}(w), v_{P_2}(\text{Fr}(w)), v_{P_3}(\text{Fr}^2(w)))\}$$

$$= \min\{v_{P_1}(w), v_{P_2}(w), v_{P_3}(w)\}$$

$$= \min\{m_1, m_2, m_3\} = -m$$

for $i = 0, 1, 2$. As the minimum is unique by assumption, the equality holds. Therefore $m$ is not in $G(P)$. \qed
As a corollary we have the following result.

**Corollary 3.2.** The maximal consecutive gap sequences in $G(P)$ are $(u - 1)q + u, \ldots, u(q - 2)$, where $u$ is an integer satisfying $0 < 3u \leq q$.

4 On the Matthews-Michel bound for AG-codes from Hermitian curves

Corollary 3.2 allows us to compute explicitly the Matthews-Michel bound (1) on the minimum distance for any one-point differential code $C_{\Omega}(D, mP)$ constructed on $\mathcal{H}$ where $P$ is a degree 3 place and $D$ is defined by (3). Indeed, from Corollary 3.2 we can read out the consecutive gap sequences in $G(mP)$, the longest are $\alpha = (u - 1)q + u, \ldots, u(q - 2)$ when

$m = 2\alpha + t - 1 = m_1(q + 1) + m_0, \quad m_1 = 2u - 2, \quad m_0 = q + 1 - 3u.$

For such a sequence, the Matthews-Michel bound is $(q - 2)(6u - q - 1)$ and it gives an improvement on the designed minimum distance by $3(t + 1) = 3(q + 1 - 3u) = 3m_0$. It should be noted that the improvement is nontrivial when $m_1 = 2u - 2$ satisfies the condition $q - 4 \leq 3m_1 \leq 2(q - 3)$. From the above discussion we have the following result.

**Theorem 4.1.** Let $\mathcal{H}$ be the Hermitian curve over $\mathbb{F}_{q^2}$. Define $P$ to be a degree 3 place in $\mathcal{H}(\mathbb{F}_{q^2})$ and $D$ to be the divisor defined by (3). Let $u$ be an integer with $q + 1 \leq 6u \leq 2(q + 1)$. Let $m = (2u - 1)q - u - 1 = m_1(q + 1) + m_0$ with $0 \leq m_0 \leq q$. Then the minimum distance of the differential code $C_{\Omega}(D, mP)$ is at least

$\delta + 3(q + 1 - 3u) = \delta + 3m_0,$

where $\delta$ is the designed minimum distance of the code given in (3).

5 Improvements on the Matthews-Michel bound

Remark 2.5 tells us that the parameters of the differential code $C_{\Omega}(D, mP)$ may be investigated using the functional code

$$C_L(D, (q^2 - 3m_1 - 1)(q + 1)P_{\infty} - (P_{\infty} + m_0(P_1 + P_2 + P_3))).$$

(7)

The advantage is that more geometry can be exploited, and we will do it with an approach based on the Noether “AF+BG” theorem, see [20, Theorem 4.66]. For our particular need, we state this theorem in the following form.
Lemma 5.1. Let $F = \psi(F)$ and $C = \psi(C)$ be any two (possible singular or reducible) curves defined over $\mathbb{F}_{q^2}$ such that $I(F \cap H) \geq I(C \cap H)$. Then there exist $A, B \in \mathbb{F}_{q^2}[X,Y]$ with $F = AC + BH$. If both $F$ and $C$ are defined over $\mathbb{F}_{q^2}$, then $A, B$ can be chosen in $\mathbb{F}_{q^2}[X,Y]$.

Here, we take $C(X,Y)$ to be the polynomial whose evaluation in $D$ gives a codeword with minimum distance in (7). The curve $C = \psi(C)$ has degree $q^2 - 3m_1 - 1$ and $I(\mathcal{H} \cap C) \geq P_\infty + m_0(P_1 + P_2 + P_3)$. In fact, the complete linear series $|(q^2 - 3m_1 - 1)(q + 1)P_\infty - (P_\infty + m_0(P_1 + P_2 + P_3))|$ is cut out, up to fixed divisor $P_\infty + m_0(P_1 + P_2 + P_3)$, by the (adjoint) curves $A$ of degree $q^2 - 3m_1 - 1$ satisfying the condition $I(\mathcal{H} \cap A) \geq P_\infty + m_0(P_1 + P_2 + P_3)$. In terms of $C$, the minimum distance $d$ of (7) is equal to $q^3 - N$ where $N$ is the number of points of $\mathcal{H}(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ which are also points of $C$.

Let $r_0$ be the non-negative integer satisfying $I(P_i, \psi(C) \cap H) = m_0 + r_0$. From Bézout’s theorem, see [20, Theorem 3.14],

$$(q^2 - 3m - 1)(q + 1) = \deg C \deg \mathcal{H} \geq (q^3 - d) + 3(m_0 + r_0)$$

whence $d \geq \delta + 3r_0$ with $\delta$ being the designed minimum distance, see [5] in Remark 2.5.

Lemma 5.2. If $m_0 + r_0 \geq q + 1$ then $m_0 + r_0 = q + 1$ and the minimum distance is $d = \delta + 3(q + 1 - m_0)$ where $\delta$ is the designed minimum distance given in (5).

Proof. Let $C^*(X,Y) = \ell_i \ell_2 \ell_3 X(Y - c_1) \cdots (Y - c_k)$ for $k + 4 = q^2 - 3m_1 - 1$ with $c_i^3 + c_i \neq 0$. Obviously, $C^*(x,y) \in \mathcal{L}(A_2)$. Also, $I(\psi(C^*) \cap \mathcal{H}) = P_\infty + (q + 1)(P_1 + P_2 + P_3) + B$ where $B$ is the sum of $q + (q + 1)(q^2 - 3m_1 - 5)$ points in $\mathcal{H}(\mathbb{F}_{q^2})$. The weight of the corresponding codeword $c^*$ is

$$d^* = q^3 - \deg B = 3m_1(q + 1) - q^2 + 4q + 5 = \delta + 3(q + 1 - m_0). \quad (8)$$

Now, $d^* \geq d \geq \delta + 3r_0$ together with $m_0 + r_0 \geq q + 1$ yield $r_0 = q + 1 - m_0$ whence $d = d^*$.

Remark 5.3. From (8), a lower bound for the minimum distance of (7) is $\delta + 3(q + 1 - m_0)$ with $\delta$ designed minimum distance given in (5).

As we have pointed out, there are precisely $d \mathbb{F}_{q^2}$-rational points in $\mathcal{H}$ not on $\psi(C)$. Let $E_0$ be the sum of the $\mathbb{F}_{q^2}$-rational points in $\text{supp} \ I(\psi(C) \cap \mathcal{H})$. Then

$$I(\psi(C) \cap \mathcal{H}) = E_0 + E + (m_0 + r_0)P,$$
where \( r_0 \geq 0 \) and \( E \) is an effective divisor defined over \( \mathbb{F}_{q^2} \). The minimum distance \( d \) satisfies
\[
d = \delta + \deg E + 3r_0, \tag{9}
\]
with designed minimum distance given in (5).

For a given integer \( 1 \leq \alpha \leq q \), let \( |U| \) be the complete linear series cut out on \( \mathcal{H} \) by all plane curves of degree \( \alpha \). Then \( ||U| - |E|| \) is a complete linear series consisting of all intersection divisors \( I(F \cap \mathcal{H}) \) with \( F \) ranging over all plane curves of degree \( \alpha \); see [20, Theorem 6.40]. If \( \dim(||U| - |E||) \geq 0 \) then \( ||U| - |E|| \) contains a divisor cut out by a curve defined over \( \mathbb{F}_{q^2} \), as \( E \) itself is defined over \( \mathbb{F}_{q^2} \). Furthermore, since \( \dim(U) = \frac{1}{2} \alpha(\alpha + 3) \), [20, Corollary 6.27] gives \( \dim(||U| - |E||) \geq \frac{1}{2} \alpha(\alpha + 3) - \deg E \). If we take the minimum value of \( \alpha \) for which
\[
\deg E \leq \frac{1}{2} \alpha(\alpha + 3), \tag{10}
\]
then \( ||U| - |E|| \neq \emptyset \). In terms of Riemann-Roch spaces, the \( \mathbb{F}_q \)-linear space
\[
T_\alpha = \{T \in \mathbb{F}_q[X,Y] \mid \deg T \leq \alpha, I(v(T) \cap \mathcal{H}) \geq E\},
\]
has
\[
\dim T_\alpha \geq \frac{1}{2} (\alpha + 1)(\alpha + 2) - \deg E.
\]
and if \( \alpha \) is chosen according to (10) then \( T_\alpha \) is nontrivial. Noether “AF+BG” theorem gives the following result.

**Lemma 5.4.** Assume \( m_0 + r_0 \leq q \). Then for any nonzero \( T \in T_\alpha \) there are polynomials \( A, B \in \mathbb{F}_q[X,Y] \) such that
\[
T \ell_1 \ell_2 \ell_3 R = AC + BH. \tag{11}
\]
If \( T \) is defined over \( \mathbb{F}_{q^2} \) then so are \( A, B \), as well.

**Proof.** From the definition of \( T \),
\[
I(Q, v(T \ell_1 \ell_2 \ell_3 R) \cap \mathcal{H}) \geq I(Q, v(C) \cap \mathcal{H})
\]
for all points \( Q \in PG(2, \mathbb{F}_{q^2}) \) of \( \mathcal{H} \). Therefore, Lemma 5.1 applies.

From now on, whenever a fixed nonzero \( T \in T_\alpha \) is given, then \( A, B \) will denote a polynomials satisfying (11). Comparing the degrees in (11) gives
\[
\deg A = 3m_1 - q + 5 + \alpha. \tag{12}
\]

**Lemma 5.5.** Assume \( m_0 + r_0 \leq q \) and let \( 0 \neq T \in T_\alpha \). Then \( P_1, P_2, P_3 \in v(A) \cap v(B) \).
Lemma 5.8. Assume Lemma 5.7. Assume Lemma 5.6. Proof. As \( I(P_i, v(\ell_1 \ell_2 \ell_3) \cap \mathcal{H}) = q + 1 \) and \( I(P_i, v(R) \cap \mathcal{H}) = 0 \), we have
\[
I(P_i, v(A) \cap \mathcal{H}) + I(P_i, v(C) \cap \mathcal{H}) = I(P_i, v(T) \cap \mathcal{H}) + q + 1 + 0.
\]
This implies \( I(P_i, v(A) \cap \mathcal{H}) \geq q + 1 - m_0 - r_0 \), and \( P_i \in v(A) \). To prove \( P_i \in v(B) \), observe first that if \( \ell_{i-1} \mid A \) then \( \ell_{i-1} \mid B \) and \( P_i \in v(B) \). Assume \( \ell_{i-1} \nmid A \). From \( P_i = \ell_{i-1} \cap \ell_i \),
\[
I(P_i, v(\ell_{i-1}) \cap v(A)) + I(P_i, v(\ell_{i-1}) \cap v(C)) \geq 2.
\]
Therefore \( I(P_i, v(\ell_{i-1}) \cap v(B)) \geq 1 \) follows from \( I(P_i, v(\ell_{i-1}) \cap \mathcal{H}) = 1 \). \( \square \)

**Lemma 5.6.** Assume \( m_0 + r_0 \leq q \), and suppose that there is a nonzero \( T \in T_\alpha \) such that \( \ell_i \nmid A \). Then, \( \alpha + r_0 \geq 2q - 3m_1 - m_0 - 3 \).

**Proof.** Since \( m_0 + r_0 \leq q \) and \( v(\ell_i) \) is the tangent line to \( \mathcal{H} \) at \( P_i \),
\[
I(P_i, v(C) \cap v(\ell_i)) = I(P_i, v(C) \cap \mathcal{H}) = m_0 + r_0.
\]
Moreover,
\[
\deg A - 1 + m_0 + r_0 \geq I(P_i, v(A) \cap v(\ell_i)) + I(P_i, v(C) \cap v(\ell_i)),
\]
and
\[
I(P_i, v(B) \cap v(\ell_i)) + I(P_i, \mathcal{H} \cap v(\ell_i)) \geq 1 + q.
\]
This implies \( \deg A - 1 + m_0 + r_0 \geq 1 + q \). The result follows from [12]. \( \square \)

**Lemma 5.7.** Assume \( m_0 + r_0 \leq q \), \( T_\alpha \neq 0 \), and \( \ell_1 \ell_2 \ell_3 \mid A \) for all \( 0 \neq T \in T_\alpha \). Then \( \alpha \geq m_0 + r_0 + 1 \).

**Proof.** If \( \ell_1 \ell_2 \ell_3 \mid A \) then \( \ell_1 \ell_2 \ell_3 \mid B \) and \( TR = A'C + B'H \) with polynomials \( A', B' \). Take \( \alpha \) to be the least integer with \( T_\alpha \neq 0 \), see [10]. Since supp\((E) \cap supp I(\mathcal{H} \cap v(\ell_1 \ell_2 \ell_3)) = \emptyset \), we have \( \ell_i \nmid T \). The equation
\[
\overbrace{I(P_i, v(T) \cap \mathcal{H})}^{=0} + \overbrace{I(P_i, v(R) \cap \mathcal{H})}^{=m_0 + r_0} = I(P_i, v(A') \cap \mathcal{H}) + I(P_i, v(C) \cap \mathcal{H})
\]
implies \( m_0 + r_0 \leq I(P_i, v(T) \cap \mathcal{H}) = I(P_i, v(T) \cap v(\ell_i)) \). Hence, counted with multiplicity, the line \( \ell_i = 0 \) has at least \( m_0 + r_0 + 1 \) points in common with \( T = 0 \). This implies \( \alpha \geq \deg T \geq m_0 + r_0 + 1 \). \( \square \)

**Lemma 5.8.** Assume \( 2 \leq m_0 + r_0 \leq q \) and let \( T \in T_\alpha \) be a nonzero polynomial such that \( P_i \in v(T) \) and \( \ell_i \nmid A \) for some \( i \in \{1, 2, 3\} \). Then,
\[
I(P_i, v(\ell_i) \cap v(B)) \geq 2.
\]
Proof. We prove the assertion for $i = 1$. Take $P_1P_2P_3$ to be the fundamental triangle of a homogeneous coordinate system $(X, Y, Z)$, and use inhomogeneous coordinates where $Z = 0$ the infinite line, and $P_1$ is the origin. Then

(a) $T(0, 0) = 0$, $R(0, 0) \neq 0$, $\ell_1\ell_2\ell_3 = XY$;

(b) $A(X, Y) = Y(a_1 + \ldots + X^{q+1-(m_0+r_0)}(a_2 + \ldots))$;

(c) $C(X, Y) = c_1Y + c_2X^{m_0+r_0} + \ldots$;

(d) $B(X, Y) = b_0 + b_1X + b_2Y + \ldots$, $H(X, Y) = Y + X^q + XY^{q+1}$.

By Lemma 5.5, $b_0 = 0$. Observe that the polynomials $T \ell_1\ell_2\ell_3R$ and $AC$ contain no term $XY$. From $BH = T \ell_1\ell_2\ell_3R - AC$, the coefficient of $XY$ in the polynomial $BH$ must vanish. This yields $b_1 = 0$. Therefore,

$$2 \leq I(P_1, v(B) \cap v(Y)) = I(P_1, v(B) \cap v(\ell_1)) = I(P_1, v(T) \cap H),$$

whence the assertion follows.

Lemma 5.9. Assume $m_0 + r_0 \leq q$ and let $T \in T_\alpha$ be a nonzero polynomial such that $\ell_i \mid A$ for some $i \in \{1, 2, 3\}$. Then, either $\ell_i \mid T$, or $I(P_1, v(\ell_i) \cap v(T)) \geq m_0 + r_0 - 1$.

Proof. We prove the assertion for $i = 1$. If $\ell_1 \mid A$ then $\ell_1 \mid B$ and $T \ell_2\ell_3R = A'C + B'H$ for some polynomials $A', B'$. On the one hand,

$$I(P_1, v(T \ell_2\ell_3R) \cap H) = I(P_1, v(T) \cap H) + 0 + 1 + 0.$$

On the other hand, $I(P_1, v(A'C) \cap H) = I(P_1, v(A') \cap H) + m_0 + r_0$. Thus,

$$I(P_1, v(T) \cap H) \geq m_0 + r_0 - 1,$$

whence the assertion follows.

We are in a position to prove our main result.

Theorem 5.10. Let $m$ be an integer such that $q^2 - q - 2 \leq 3m \leq 2q^2 - q - 2$ and $q + 1 \nmid m$. Let $d$ and $\delta$ be the minimum distance and the designed minimum distance of the differential code $C_\Omega(D, mP)$, respectively. Write $m = m_1(q + 1) + m_0$ with $0 < m_0 \leq q$. Assume that

$$K = 2q - 3m_1 - m_0 - 4 \geq 0. \quad (13)$$

Then one of the following holds:
(i) \( d = \delta + 3(q + 1 - m_0) \).

(ii) \( d \geq \delta + \frac{1}{2}(m_0 + 1)(m_0 + 2) \).

(iii) \( d \geq \delta + 3K \) and if \( d = \delta + 3K \) then \( m_0 \leq 2 \).

Proof. We continue to work on the equivalent functional code \((7)\) and use the above notation. If \( m_0 + r_0 \geq q + 1 \) then (i) holds by Lemma 5.2. Assume \( m_0 + r_0 \leq q \). According to the discussion made before Lemma 5.4, we may choose \( \alpha \) such that

\[
\frac{\alpha(\alpha + 3)}{2} \geq \deg E \geq \frac{\alpha(\alpha + 1)}{2}.
\]

\( T_\alpha \neq 0 \). If for all nonzero \( T \in T_\alpha \), \( \ell_1 \ell_2 \ell_3 \mid A \) then \( \alpha \geq m_0 + 1 \) by Lemma 5.7, and case (ii) occurs by (10).

Therefore, we may suppose the existence of \( T \in T_\alpha \setminus \{0\} \) such that \( \ell_1 \nmid T \).

By Lemma 5.6 \( \alpha + r_0 \geq K + 1 \) and

\[
\deg E + 3r_0 \geq \frac{\alpha(\alpha + 1)}{2} + 3r_0
\]

\[
\geq \frac{(K + 1 - r_0)(K + 2 - r_0)}{2} + 3r_0
\]

\[
= \frac{(K - r_0 + \frac{3}{2})^2 - \frac{1}{4}}{2} + 3K
\]

\[
\geq 3K.
\]

This proves \( d \geq \delta + 3K \), and also shows that \( d = \delta + 3K \) if and only if equality occurs everywhere in the last computation. Therefore

\[
K - r_0 \in \{1, 2\}, \quad \alpha = K + 1 - r_0 \in \{2, 3\}, \quad \deg E = \frac{1}{2} \alpha(\alpha + 1) \in \{3, 6\}.
\]

It remains to show \( m_0 \leq 2 \).

Assume \( m_0 \geq 3 \), and define the subspace

\[
\tilde{T}_\alpha = \{ T \in T_\alpha \mid P_1 \in v(T) \}
\]

of \( T_\alpha \). Suppose that there is a nonzero polynomial \( T \in \tilde{T}_\alpha \) such that \( \ell_1 \nmid A \). Then Lemma 5.8 improves the inequality in Lemma 5.6 by 1.

Assume \( \ell_1 \mid A \) for all nonzero polynomials \( T \in \tilde{T}_\alpha \), and investigate several cases separately.

Case 1: \( \deg E = 3 \) and \( I(\mathcal{H} \cap r) \geq E \) for some line \( r \).
Remark 5.11. By hypothesis (13) and Remarks 2.5, 2.6, Theorem 5.10 applies to $m$ in the range

$$\frac{1}{3} (q - 1)(q + 1) \leq m \leq \frac{2}{3} q(q + 1), \quad (q + 1) \nmid m. \quad (14)$$
6 Examples

First we compare our bound with the Matthews-Michel bound as stated in Theorem 4.1. It turns out that Theorem 5.10 implies the Matthews-Michel bound for all possible values of $u$. Actually, an effective improvement occurs apart from exceptional cases, namely:

(i) if $m_0 + r_0 \geq q + 1$ then we have an exact value for the minimum distance of $C_\Omega(D, mP)$;

(ii) if $m_0 = 1$ or 2.

In case (ii), several extra information can be obtained on the geometry of the minimum distance codeword. Using this knowledge, we were able to find with a computer aided search by MAGMA and GAP4 \cite{13} that for $q = 7$, the differential code $C_\Omega(D, 18P)$ has a codeword of weight $d = 20$, see the program code in Appendix A. Therefore, the minimum distance is at most 20, showing the sharpness of the Matthews-Michel bound for this specific case.

Next, we present a comparison of our bound with the true values of the minimum distances of Hermitian 1-point codes; see \cite{30, 33} and \cite{32, Table 1}. The parameters of the code $C_\Omega(D, mP)$ can be compared with the parameters of the 1-point differential code $C_\Omega(D, 3mP_\infty)$, or, with the equivalent 1-point functional code $C_L(D, (q^3 + q^2 - q - 2 - 3m)P_\infty)$. Assume that $m$ satisfies

$$q^2 - q - 2 \leq 3m \leq 2q^2 - q - 2$$

and define the integers $a, b$ by $0 \leq a, b \leq q - 1$ by $3m = 2q^2 - (a + 1)q - b - 2$. Then the designed minimum distance is $\delta = 3m - q^2 + q + 2$ and the true minimum distance of $C_\Omega(D, 3mP_\infty)$ is

$$d_{\text{true}} = \begin{cases} 
\delta & \text{if } a < b, \\
\delta + b & \text{if } a \geq b.
\end{cases}$$

The following table contains some values $q$ and $m$ for which our bound is better that the true minimum distance of the compared 1-point code.

| $q$ | cond. on $m$ | values of $m$ improving the 1-point min. distances |
|-----|--------------|--------------------------------------------------|
| 5   | 6 \leq m \leq 14 | 7, 8 |
| 7   | 14 \leq m \leq 29 | 18 |
| 8   | 18 \leq m \leq 39 | 20, 21, 22, 23, 24, 28, 29, 30 |
| 9   | 24 \leq m \leq 50 | 24, 25, 26, 32, 33, 41 |
| 11  | 36 \leq m \leq 76 | 38, 39, 40, 41, 42, 43, 44, 50, 51, 52, 61, 62, 63 |
| 13  | 52 \leq m \leq 107 | 59, 60, 61, 62, 63, 64, 65, 72, 73, 74, 86, 87, 88 |
| 16  | 80 \leq m \leq 164 | 88, 89, 90, 91, 92, 93, 94, 95, 96, 105, 106, 107, 108, 109, 110, 111, 112, 121, 122, 123, 124, 138, 139, 140 |
Finally, we compare our result with the Xing-Chen bound [32, Corollary 2.6]. Xing and Chen [32] used probabilistic method to show the existence of certain divisors $G$ for which the differential code $C_\Omega(D, G)$ with $D$ being as in [3] has good parameters. We confront their results with Theorem 5.10 for small values of $q$. Notice that the results by Xing and Chen are not constructive; they show the existence of an $\mathbb{F}_{q^2}$-rational divisor $G$ such that $\text{supp} \, D \cap \text{supp} \, G = \emptyset$, $t = \deg G$, and the code $C_\Omega(D, G)$ has parameters

$$\left[ q^3, t + 1 - \frac{q^2 - q}{2}, \geq \frac{2q^3 + q^2 - q - 1 - 2t}{4 + \log_q e} \right].$$

a) If $(q, m) = (5, 7), (5, 8)$ or $(7, 19)$ then Xing and Chen improve the designed minimum distance $\delta$ by 2, 2, or 1, respectively. In these cases, Theorem 5.10 improves $\delta$ by 3, 3, and 4, respectively.

b) If $q = 7$ and $m = 18$ then the improvement by Xing and Chen is 4, while Theorem 5.10 gives the true value $d = \delta + 6$.

c) If $q = 8$ and $m = 21$ then the improvement of Theorem 5.10 equals to the improvement by Xing and Chen. However, our method is constructive, giving them the divisor $G$ explicitly.

A Program code

```plaintext
q:=7;
BaseRing:=PolynomialRing(GF(q^2),["x","y"]);
x:=BaseRing.1; y:=BaseRing.2;

LoadPackage("singular");
SetInfoLevel( InfoSingular, 2 );
GBASIS:= SINGULARGBASIS;
SingularSetBaseRing( BaseRing );
SetTermOrdering( BaseRing, "dp" );

H:=x^(q+1)-y-y^q;
R:=x*Product(Filtered(GF(q^2),c->not IsZero(c^q+c)),c->y-c);
a:=Z(q^2);; b:=Z(q^6);;
P:=[b^11896,b^108645];
# Check: P is on the Hermitian curve
IsZero(Value(H,[x,y],P));
```

18
T:=a^26*x^3+a^39*x^2*y+a^32*x*y^2+a^45*x^2+a^40*x*y+
a^18*y^2+a^41*x+a^45*y-a^0;
A:=a^25*x^4+a^7*x^3*y+x^2*y^2+a^10*x*y^3+a^44*y^4+
a^4*x^3+a^19*x^2*y+a^4*x*y^2+a^9*y^3+a^37*x^2+
a^2*x*y+a^3*y^2+a^37*x+a^41*y+a^10;
I:=Ideal(BaseRing,[A,H]);;
liftcoeffs:=SingularInterface("lift", [I,R*T], "matrix");;
C:=liftcoeffs[1][1];;

# Check: I(P,C \cap H)=2
# The tangent of H(X,Y) at P is Y=P[1]^q*X-P[2]^q.
# Substitue this in C(X,Y) and show that X=P[1] is
# a double root.
IsPolynomial(Value(C,[y],[P[1]^q*x-P[2]^q])/(x-P[1])^2);
# Check: C vanishes at te infinite point (0,1,0).
# Show that \text{deg}(C)=42 and Y^{-42} is not a monomial of C.
DegreeIndeterminate(C,y);
# Check: The Hermitian curve has 20 affine rational
# points not lying on C(X,Y)=0.
Hermite:=Filtered(Cartesian(GF(q^2),GF(q^2)),
p->IsZero(Value(H,[x,y],p)));
Size(Hermite);
Number(Hermite,p->not IsZero(Value(C,[x,y],p)));

References

[1] E. Ballico and A. Ravagnani, On Goppa codes on the Hermitian curve,
http://arxiv.org/abs/1202.0894.

[2] E. Ballico and A. Ravagnani, On the geometry of the Hermitian two-
point codes, http://arxiv.org/abs/1202.2453.

[3] E. Ballico and A. Ravagnani, On the geometry of the Hermitian one-
point codes, http://arxiv.org/abs/1203.3162.

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

[5] C. Carvalho and T. Kato, On Weierstrass semigroups and sets: review
of new results, Geom. Dedicata 239 195–210, (2009).
[6] C. Carvalho and T. Kato, Codes from curves with total inflection points, *Des. Codes Cryptogr.* **45**, 359–364 (2007).

[7] C. Carvalho, On V-Weierstrass sets and gaps, *J. Algebra* **312**, 956–962 (2007).

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

[9] A. Cossidente, G. Korchmáros and F. Torres, On curves covered by the Hermitian curve. *J. Algebra* **216** (1999), 56–76.

[10] A. Couvreur, The dual minimum distance of arbitrary-dimensional algebraic-geometric codes, *J. Algebra* **350** (2012), 84–107.

[11] I. Duursma, R. Kirov and S. Park, Distance bounds for algebraic geometric codes, *J. Pure Appl. Algebra*, **215** (2011), 1863–1878.

[12] I. Duursma and S. Park, Coset bounds for algebraic geometric codes. *Finite Fields Appl.* **16** (2010), 36–55.

[13] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.4.12; 2008, (\protect\url{http://www.gap-system.org}).

[14] A. Garcia and R.F. Lax, Goppa codes and Weierstrass gaps. In: Coding Theory and Algebraic Geometry. Proc. Int. Workshop, Luminy/Fr. 1991, Lecture Notes in Mathematics, **1518**, 33–42 (1992).

[15] 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).

[16] O. Geil, C. Munuera, D. Ruano and F. Torres, On the order bounds for one-point AG codes, *Advances in Mathematics of Communication*, **5**, 489-504 (2011).

[17] 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.

[18] C. Güneri, H. Stichtenoth and I. Taskin, Ihsan, Further improvements on the designed minimum distance of algebraic geometry codes, *J. Pure Appl. Algebra* **213** (2009), 87–97.
[19] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, second ed., Oxford Univ. Press, Oxford, 1998, xiv+555 pp.

[20] 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

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

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

[23] M. Homma and S.J. Kim, Goppa codes with Weierstrass pairs, *J. Pure Appl. Algebra* **162**, 273–290 (2001).

[24] M. Homma, S.J. Kim and J. Komeda, A semigroup at a pair of Weierstrass points on a cyclic 4-gonal curve and a bielliptic curve, *J. Algebra* **305**, 1–17 (2006).

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

[26] G.L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, *Des. Codes Cryptogr.* **22**, 107–121 (2001).

[27] 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)

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

[29] G.L. Matthews, Weierstrass semigroups and codes from a quotient of the Hermitian curve, *Des. Codes Cryptogr.* **37**, 473–492 (2005).

[30] H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, *IEEE Trans. Inform. Theory*, vol. **34**, 1345-1348 (1988).

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

[32] 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.
[33] 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.