GENERALIZED HERMITIAN CODES

C. MUNUERA, A. SEPÚLVEDA, AND F. TORRES

Abstract. We investigate one-point algebraic geometry codes defined from curves related to the Hermitian curve. We obtain codes attaining new records on the parameters.

1. Introduction

Goppa constructed error-correcting linear codes, the so-called algebraic geometry (or AG) codes, using tools from algebraic geometry: a (non-singular, projective, geometrically irreducible, algebraic) curve $X$ defined over a finite field and two rational divisors $D$ and $G$ on $X$. These divisors are chosen in a way that $D = P_1 + \ldots + P_n$ is the sum of $n$ distinct rational points and $P_i \notin \text{supp}(G)$, $i = 1, \ldots, n$. The AG code $C(X, D, G)$ is defined as

$$C(X, D, G) := \{ ev(f) = (f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G) \},$$

where $\mathcal{L}(G)$ denotes the Riemann-Roch space associated to $G$, see [7, 15] as general references for all facts concerning AG codes.

Let $q$ be a prime power and let $\mathbb{F}_{q^r}$ be the finite field of order $q^r$, $r \geq 2$. In this paper we are interested in algebraic geometry codes obtained from the non-singular model $X$ over $\mathbb{F}_{q^r}$ of the plane curve

$$(1.1) \quad \sum_{i=0}^{r-1} y^{q^i} = p(x) := x^{1+q} + \ldots + x^{1+q^{r-1}} + x^{q+q^2} + \ldots + x^{q+q^{r-1}} + \ldots + x^{q^2+q^r}$$

or equivalently $s_{r,1}(y, y^q, \ldots, y^{q^{r-1}}) = s_{r,2}(x, x^q, \ldots, x^{q^{r-1}})$, where $s_{r,1}$ and $s_{r,2}$ are respectively the first and second symmetric polynomials in $r$ variables. For $r = 2$ this is the Hermitian curve over $\mathbb{F}_{q^2}$. Codes on that curve (Hermitian codes) have been extensively studied and much is known about them. In particular their parameters and generalized Hamming weights can be found in [1, 9, 11]. For $r > 2$ we obtain the generalized Hermitian curves [5], and generalized Hermitian codes. A basic property of generalized Hermitian curves is the existence of one unique point $Q \in X$ at infinity which is the unique pole of the rational functions $x$ and $y$ (loc. cit.). Hermitian codes and generalized Hermitian codes are the AG codes $C_m = C(X, D, G)$ coming from $X$ and the divisors

$$(1.2) \quad G := mQ \quad \text{and} \quad D := \sum_{P \in X(\mathbb{F}_{q^r}) \setminus \{Q\}} P.$$
Bulygin [3] studied in detail these codes when \( q = 2 \) and \( r \geq 3 \). In this paper we extend these results for \( q \geq 3 \).

2. Arithmetic properties of Generalized Hermitian curves

Throughout, let \( \mathcal{X} \) be the generalized Hermitian curve over \( \mathbb{F}_{q^r} \) and let \( D, G \) be the divisors defined by equation 1.2. Before studying the code \( C(\mathcal{X}, D, mQ) \), we recall some basic properties of \( \mathcal{X} \).

**Lemma 2.1.** (1) \( \mathcal{X} \) has genus \( g = q^{r-1}(q^{r-1} - 1)/2 \) and \( q^{2r-1} + 1 \) rational points.  
(2) \( \text{div}_\infty(x) = q^{r-1}Q \) and \( \text{div}_\infty(y) = (q^{r-1} + q^{-2})Q \).  
(3) Let \( z := x^{q+1} - y^q + x^{q-1}y \). Then \( \text{div}_\infty(z) = (q^r + 1)Q \).  
(4) For each \( \alpha \in \mathbb{F}_{q^r} \) there exists an effective divisor \( D_\alpha \leq D \) of degree \( q^{r-1} \) such that \( \text{div}_0(x - \alpha) = D_\alpha \).  
(5) \( D \sim q^{2r-1}Q \).

**Proof.** (1) and (2) are shown in [5]. (3) was first proved by Bulygin in the binary case [3]. For general \( q \), from equation (1.1) we have
\[
z^{q-1} = h(x) - x^{q^r-q^{-1}} \sum_{i=0}^{r-2} y^{q^i} - y,
\]
where \( h(x) := p(x) - p(x)^q + x^{q^r+q^{r-1}} + \cdots + x^{q^r+q^1} \). After some computation
\[
h(x) = \sum_{i=1}^{r-1} x^{q^i} - \sum_{i=1}^{r-2} x^{q^r+q^i} + \cdots - \sum_{i=0}^{r-2} (x^{q^r+q^i} + \cdots + x^{q^i+q^1}).
\]
This polynomial has degree \( q^r + 1 \) hence \( v(h(x)) = (q^r + 1)v(x) \). Thus
\[
v(x^{q^r-q^{-1}}) + v(\sum_{i=0}^{r-2} y^{q^i}) = (q^r - q^{-1})v(x) + (q^{r-2} + q^{r-3})v(x)
\]
and \( v(z) = q^r + 1 \). To prove (4) note that for each \( \alpha \in \mathbb{F}_{q^r} \) the line \( x = \alpha \) intersects the affine curve given by equation 1.1 at \( q^{r-1} \) distinct points. As a consequence we have \( \text{div}(x^{q^r} - x) = D - q^{2r-1}Q \) and (5) holds. \( \square \)

Given a divisor \( E \), we denote by \( \ell(E) \) the dimension of \( \mathcal{L}(E) \). Let us remember that the Weierstrass semigroup at \( Q \) is defined as
\[
H(Q) = \{ t \in \mathbb{Z} : \ell(tQ) \neq \ell((t-1)Q) \}.
\]

**Proposition 2.2.** The Weierstrass semigroup at \( Q \) is
\[
H(Q) = \langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle.
\]

In particular it is symmetric.
Proof. The sequence \( q^{r-1} < q^{r-1} + q^{r-2} < q^r + 1 \) is telescopic [8, Def. 6.1] hence so is \( \langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle \). By [8, Lemma 6.5], this semigroup is symmetric of genus \( g = q^{r-1}(q^{r-1} - 1)/2 \). From Lemma 2.1 we have \( \langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle \subseteq H(Q) \) and both semigroups have the same genus, so they are equal. \( \square \)

By using this Proposition we can describe basis of \( \mathcal{L}(mQ) \).

**Corollary 2.3.** Let \( z \) be the function defined in Lemma 2.1 and \( m \in \mathbb{Z} \). The set
\[
\{ x^s y^t z^u : 0 \leq s, 0 \leq t < q, 0 \leq u < q^{-2}, sq^{r-1} + t(q^{r-1} + q^{r-2}) + u(q^r + 1) \leq m \}
\]
is a basis of \( \mathcal{L}(mQ) \). \( \square \)

Let us write \( H(Q) = \{ m_1 = 0 < m_2 < \cdots \} \). The curve \( \mathcal{X} \) over \( \mathbb{F}_q \) is said to be **Castle** if \( H(Q) \) is symmetric and \( \# \mathcal{X}(\mathbb{F}_q) = q^m m_2 + 1, [12] \). From Lemma 2.1 and Proposition 2.2 we have

**Corollary 2.4.** \( \mathcal{X} \) is a Castle curve. \( \square \)

3. **Generalized Hermitian codes**

Let \( C_m = C(\mathcal{X}, D, mQ) \). A generator matrix of \( C_m \) is obtained from Corollary 2.3. Its length is \( n = q^{2r-1} \) and its dimension can be computed by using the fact that it is a Castle code, [12]. Define \( \iota(m) := \max\{ j : m_j \leq m \} \) and \( m_0 = -\infty \).

**Proposition 3.1.** Let \( m \) be an integer, \( 1 \leq m \leq n + 2g - 2 \).

(1) \( C_m \) has dimension \( k_m = \iota(m) - \iota(m - n) \).

(2) The dual of \( C_m \) is isometric to \( C_{n+2g-2-m} \).

Then the dimension of \( C_m \) depends only on the semigroup \( H = H(Q) \). Let \( H^* = H \setminus (n + H) \). Then \( \# H^* = n \) [7] and we can restrict to consider GH codes \( C_m \) with \( m \in H^* \). If \( m_1, \ldots, m_n \), is an enumeration of the elements of \( H^* \), then \( \dim(C_{m_1}) = i \). Next we shall give some results on the minimum distance \( d_m \) of \( C_m \). Recall that by the Goppa bound we have \( d_m \geq n - m \). Let us first study the case \( 0 \leq m < n \).

**Proposition 3.2.** Let \( d_m \) be the minimum distance of the GH code \( C_m \). Then

(1) If \( m = aq^{r-1} \) with \( 0 \leq a < q^r \), then \( d_m = n - m \).

(2) If \( m = aq^{r-1} + b(q^{r-1} + q^{r-2}) \) with \( 0 \leq a \leq q^r - q^{r-1} - q^{r-2} \) and \( 0 \leq b < q^{r-1} \), then \( d_m = n - m \).

(3) If \( m = q^{2r-1} - q^{r-1} + b \) with \( 0 \leq b \leq q^{r-1} \), then \( d_m = q^{r-1} \).

**Proof.** (1) Let \( \alpha_1, \ldots, \alpha_n \) be a distinct elements in \( \mathbb{F}_q \). Then \( f = (x - \alpha_1) \cdots (x - \alpha_n) \in \mathcal{L}(mQ) \) and , according to Lemma 2.1 (4), \( ev(f) \) has weight \( n - m \). (2) Consider the set
Proof. If \( a \in \mathbb{F}_{q^r} : p(\alpha) \neq \gamma \), with \( \gamma \in \mathbb{F}_q^\times \). Then \#A \geq q^r - q^{-1} - q^{-2} \geq a. Choose \( a \) distinct elements \( \alpha_1, \ldots, \alpha_a \in A \) and define

\[
f_1 := \prod_{\mu=1}^a (x - \alpha_\mu).
\]

\( f_1 \) has \( aq^{-1} \) distinct zeros in the support of \( D \). On the other hand there exist \( q^{-1} \) distinct elements \( \beta \in \mathbb{F}_{q^r} \) such that \( \beta q^{-1} + \beta q^{-2} + \cdots + \beta = \gamma \in \mathbb{F}_q \). Choose \( b \) of them and define

\[
f_2 := \prod_{\nu=1}^b (y - \beta_\nu).
\]

Therefore \( f_2 \) has \( b(q^{-1} + q^{-2}) \) distinct zeros in the support of \( D \), all of them being distinct from the zeros of \( f_1 \). Then \( f_1 f_2 \in \mathcal{L}(m\mathcal{Q}) \), has \( m \) distinct zeros in the support of \( D \), and the corresponding codeword \( ev(f_1 f_2) \) has weight \( n - m \). (3) From (1) we have \( d_{n-q^{-1}} = q^{-1} \). Therefore \( d_m = q^{-1} \) by [12, Proposition 4 (5)]. \( \square \)

Let us study now the case \( n \leq m \leq n + 2g - 2 \). In this case we can compute the exact minimum distance of all codes \( C_m \).

Lemma 3.3. A non negative integer \( s \) has a unique representation of the form

\[
s = aq^{-1} + bq^{-2} + c,
\]

with \( 0 \leq a, 0 \leq b < q \) and \( 0 \leq c < q^{-2} \). Furthermore \( s \in H(Q) \), if only if \( a \geq b + cq \).

Proof. The first statement is clear. To see the second one, let \( s = aq^{-1} + bq^{-2} + c \) as above. If \( a \geq b + cq \), then \( h = x^{a-b-c}y^{b}z^{c} \in \mathcal{L}(s\mathcal{Q}) \) and \(-v_{\mathcal{Q}}(h) = ((a - b - cq)q^{-1} - b(q^{-2} - q^{-1} - c(q^{-1} + 1))) = s \in H(Q) \). In order to prove the converse, assume \( a < b + cq \) and \( s \in H(Q) \). We may write \( s = iq^{-1} + j(q^{-2} + q^{-1}) + k(q^{-1} + 1) \) with \( 0 \leq i, 0 \leq j < q \) and \( 0 \leq k < q^{-2} \). Then \( j = b, k = c \) and \( a = i + b + cq \), a contradiction. \( \square \)

For \( 0 \leq m \leq n + 2g - 2 \) we define \( m^\perp = n + 2g - 2 - m \). By Proposition (3.1) \( C_{m^\perp} \) is isometric to the dual of \( C_m \). Note that when \( n \leq m \leq n + 2g - 2 \) we have \( m \in H \) and \( 0 \leq m^\perp \leq 2g - 2 \). If \( m^\perp \) is a gap, let \( t^\perp \) be the largest nongap before \( m^\perp \). Then \( C_{m^\perp} = C_{t^\perp} \), and consequently, by dimension reasons, \( C_m = C_t \). Thus we can restrict to consider those \( m \) for which \( m^\perp \) is a nongap. Thus, according to the previous Lemma, we can write \( m^\perp = aq^{-1} + bq^{-2} + c \) with \( 0 \leq b + cq \leq a \leq q^{-1} - 2 \) (since \( m^\perp \leq 2g - 2 \)) and \( b + cq \leq a \) (since \( m^\perp \) is a nongap).

Proposition 3.4. For \( n \leq m \leq n + 2g - 2 \), let \( t^\perp \leq m^\perp = n + 2g - 2 - m \) be the largest integer such that \( t^\perp = aq^{-1} + bq^{-2} + c \), as in Lemma 3.3, with \( a \geq b + cq \). Then the minimum distance \( d_m \) of \( C_m \) verifies

(1) if \( a = b + cq \), then \( d_m = a + 2 \);
(2) if \( a > b + cq \) with \( a = b' + c'q \) and \( b' < b \), then \( d_m = a + 2 \);
(3) if \( a > b + cq \) with \( a = b' + c'q \) and \( b' \geq b \), then \( d_m = a + 1 \).
Proof. As noted above we have $\mathcal{L}(L^Q) = \mathcal{L}(L^T)$. By using a basis of this space we can obtain a parity check matrix $H$ of $C_m$. (1) If $a = b + cq$ then a basis of $\mathcal{L}(L^Q)$ is \{1, $x$, $y$, \ldots, $x^{q-1}$, $x^{q-2}y$, \ldots, $y^{q-1}$, $z$, $x^{q-1}y$, \ldots, $x^a$, \ldots, $y^bz^c$\}. Consider the set \{\(P_i = (0, \beta_i) : i = 1, \ldots, q^r\)\} \subseteq \text{supp}(D) with $\beta_i \neq \beta_j$ for $i \neq j$. Note that $z(P_i) = -(\beta_i)^q$.

By evaluating the functions of the above basis at these points we find a submatrix of $H$ corresponding to the columns of $A$ obtained by choosing any $a+2$ points listed in (3.1) in the given order; and iii) each entry of $H$ is computed as follows:

\[
\left[
\begin{array}{ccccccc}
1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\
\beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{a+2} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\beta_1^{q-1} & \beta_2^{q-1} & \beta_3^{q-1} & \cdots & \beta_{a+2}^{q-1} \\
-\beta_1^q & -\beta_2^q & -\beta_3^q & \cdots & -\beta_{a+2}^q \\
-\beta_1^{q+1} & -\beta_2^{q+1} & -\beta_3^{q+1} & \cdots & -\beta_{a+2}^{q+1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0
\end{array}
\right]
\]

This matrix is singular so its columns are linearly dependent, hence $d(C_m) \leq a+2$. To see the converse, let $A$ be a submatrix of $H$ obtained by choosing any $a+1$ different columns of $H$. Since each column of $H$ corresponds to a point $P_{\alpha, \beta} = (\alpha, \beta)$, we can order the points corresponding to the columns of $A$ as

\[
P_{\alpha_1, \beta_1, 1}, P_{\alpha_1, \beta_1, 2}, \ldots, P_{\alpha_1, \beta_1, b_1}, P_{\alpha_2, \beta_2, 1}, \ldots, P_{\alpha_2, \beta_2, b_2}, \ldots, P_{\alpha_l, \beta_l, 1}, \ldots, P_{\alpha_l, \beta_l, b_l},
\]

where the $\alpha_i$’s are pairwise distinct and $b_1 \geq b_2 \geq \cdots \geq b_l \geq 1$, $b_1 + \cdots + b_l = a + 1$. It is easy to check that $x^{i-1}y^kz^t \in \mathcal{L}(L^Q)$ for $0 \leq k_i + t_iq \leq b_i - 1$, $0 \leq k_i < q$, $1 \leq i \leq l$. Order these functions as

\[
1, y, \ldots, y^{q-1}, z, yz, \ldots, y^{r_1}z^s, x, xy, \ldots, xy^{q-1}, xz, xyz, \ldots, xxy^{r_2}z^{s_2}, \ldots, x^{l-1}, \ldots, x^{l-1}y^{r_l}z^{s_l},
\]

where $r_i + s_iq = b_i - 1$. We construct an $(a+1) \times (a+1)$ submatrix $B$ of $A$ as follows: i) rows correspond to the above functions in the given order; ii) columns correspond to the points listed in (3.1) in the given order; and iii) each entry of $B$ is obtained by evaluation as follows: $B = [B_{ij}]$, $i, j = 1, \ldots, l$, where $B_{ij}$ is the $(b_i \times b_j)$ matrix whose $(u, v)$ entry is $\alpha_j^{i-1}b_{ij}^{u_1}z^{u_2}(P_{\alpha_j, \beta_j, u}), u_1 + u_2q = u - 1$. So $B_{ij} = \alpha_j^{i-1}D_{ij}$, where
After some computation and using induction we obtain

\[ D_{ij} := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_{j,1} & \beta_{j,2} & \cdots & \beta_{j,b_j} \\ \beta_{j,1}^2 & \beta_{j,2}^2 & \cdots & \beta_{j,b_j}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{j,1}^{q-1} & \beta_{j,2}^{q-1} & \cdots & \beta_{j,b_j}^{q-1} \\ z(P_{\alpha_j,\beta_j,1}) & z(P_{\alpha_j,\beta_j,2}) & \cdots & z(P_{\alpha_j,\beta_j,b_j}) \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{j,1}^{r}z_{s_j}(P_{\alpha_j,\beta_j,1}) & \beta_{j,2}^{r}z_{s_j}(P_{\alpha_j,\beta_j,2}) & \cdots & \beta_{j,b_j}^{r}z_{s_j}(P_{\alpha_j,\beta_j,b_j}) \end{pmatrix}, \]

with \( r_i + s_iq = b_i - 1 \). This matrix is equivalent, in the sense that one matrix is obtained from the other by a sequence of elementary row operations, to

\[ \tilde{D}_{ij} := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_{j,1} & \beta_{j,2} & \cdots & \beta_{j,b_j} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{j,1}^{q-1} & \beta_{j,2}^{q-1} & \cdots & \beta_{j,b_j}^{q-1} \\ -\beta_{j,1}^{q} & -\beta_{j,2}^{q} & \cdots & -\beta_{j,b_j}^{q} \\ \vdots & \vdots & \ddots & \vdots \\ (-1)^{s_j}\beta_{j,1}^{b_j-1} & (-1)^{s_j}\beta_{j,2}^{b_j-1} & \cdots & (-1)^{s_j}\beta_{j,b_j}^{b_j-1} \end{pmatrix}. \]

After some computation and using induction we obtain

\[ \det(B) = \left( \prod_{i=1}^{l} \det(D_{i,i}) \right) \left( \prod_{j=2}^{l} \tau_{j}^{b_j} \right) = \left( \prod_{i=1}^{l} \det(\tilde{D}_{i,i}) \right) \left( \prod_{j=2}^{l} \tau_{j}^{b_j} \right), \]

where \( \tau_{j} = \prod_{i=1}^{j-1}(\alpha_j - \alpha_i), j = 2, 3, \ldots, l \). Next, we note that any \( a + 1 \) columns of \( A \) are linearly independent. In fact, since the \( \alpha_i \)'s are pairwise distinct we have \( \tau_{j} \neq 0 \) for \( j = 2, \ldots, l \). Since the \( \beta_{i,j} \)'s are pairwise distinct for a given \( i \), we have \( \det(\tilde{D}_{i,i}) \neq 0 \) hence \( \det(B) \neq 0 \) and \( a + 1 = \text{rank}(B) \leq \text{rank}(A) \leq a + 1 \). Thus \( d_m = a + 2 \). Proofs of (2) and (3) are similar.

Thus we have computed the true minimum distance of all codes \( C_m \) when \( n \leq m \leq n + 2g - 2 \). For \( 0 \leq m < n \) we remark that besides the Goppa bound there are several bounds available to estimate the minimum distance of a code. One of the most interesting is the order bound. For one-point codes we can follow the version of [6], which is briefly explained below. Let \( H^* = H(Q) \setminus (n + H(Q)) = \{ m_1^* = 0 < \cdots < m_n^* \} \) be as above. For \( i = 1, \ldots, n \), let

\[ \Lambda_i^* = \{ m \in H^* : m - m_i^* \in H^* \}. \]

Then the minimum distance of \( C(\mathcal{X}, D, m_i^*Q) \) verifies

\[ d(C(\mathcal{X}, D, m_i^*Q)) \geq d^*(i) = \min\{ \#\Lambda_1^*, \ldots, \#\Lambda_i^* \}. \]
In the following examples we consider some small values of $q$ and $r$. We find several codes with the best known parameters.

**Example 3.5.** Let $q = 3$ and $r = 3$. Then $g = 36$, $n = 243$ and $H(Q) = \langle 9, 12, 28 \rangle$. A simple computation gives $H^* = \{0, 9, 12, 18, 21, 24, 27, 28, 30, 33, 36, 37, 39, 40, 42, 45, 46, 48, 49, 51, 52, 54, 55, 56, 57, 58, 60, 61, 63, 64, 65, 66, 67, 68, 69, 70, 72, 73, \ldots, 244, 245, 246, 247, 248, 249, 250, 251, 253, 254, 256, 257, 258, 259, 260, 262, 263, 265, 266, 268, 269, 272, 274, 275, 277, 278, 281, 284, 286, 287, 290, 293, 296, 302, 305, 314 \}$. Computing the order bound, we find the following codes over $\mathbb{F}_{27}$ with the best known parameters (according to the tables [10]): $[243, 137, \geq 72], [243, 146, \geq 63], [243, 149, \geq 60], [243, 155, \geq 54], [243, 158, \geq 51], [243, 161, \geq 48]$ and $[243, 165, \geq 45]$. Some of these codes are not necessarily the best possible. For example, according to the Gilbert-Varshamov bound, there exist (unknown so far) codes with parameters $[243, 161, \geq 49], [243, 165, \geq 46]$.

**Example 3.6.** Let $q = 2$ and $r = 4$. Then $g = 28$, $n = 128$ and $H(P_\infty) = \langle 2, 12, 17 \rangle$. Computing the order bound, we find a $[128, 5, \geq 111]$ and a $[128, 8, \geq 103]$ codes over $\mathbb{F}_{16}$. Both codes have the best known parameters according to [10].

**Remark 3.7.** In the above example, via the MAGMA computer package [2], we can compute the exact minimum distance of the codes. As a matter of fact, we obtain a $[128, 5, 112]$ code and a $[128, 8, 104]$ code respectively.

The order bound we are using allows us to easily obtain improved codes. For $i = 1, \ldots, n$, consider a function $f_i \in L((n + 2g - 2)Q)$ with $\nu_Q(f) = m_i^\ast$. Given an integer $\delta$, $1 \leq \delta \leq n$, the improved code $C(X, D, Q, \delta)$ is defined as

$$C(X, D, Q, \delta) = \{\{ev(f_i) : \#\Lambda_i^\ast \geq \delta\}.$$ Then $C(X, D, Q, \delta)$ is a code of dimension $\#\{ev(f_i) : \#\Lambda_i^\ast \geq \delta\}$ and minimum distance $\geq \delta$, see [6]. Remark that the functions $f_i$’s can be obtained from the basis stated in Corollary 2.3, so that the code $C(X, D, Q, \delta)$ may be explicitly computed.

**Example 3.8.** Let $q = 3$ and $r = 3$ as in Example 3.5. We find the improved codes with the following best known parameters: $[243, 159, \geq 50], [243, 162, \geq 48], [243, 163, \geq 47], [243, 167, \geq 44], [243, 169, \geq 42]$ and $[243, 171, \geq 40]$. As in previous examples, the Gilbert-Varshamov bound implies the existence of codes $[243, 167, \geq 45], [243, 169, \geq 43], [243, 171, \geq 42]$.

4. **Subcovers of the Generalized Hermitian Curve**

Let $b \in \mathbb{F}_q^\ast$ be such that $T_{F_q^r} (b) = 0$, where $T$ is the trace function. Then for $j = 1$ and $j = r - 2$, we can consider the curve $X_j^\ast$ defined over $\mathbb{F}_{q^r}$ by the affine equation

$$s_{r, 2}(x, x^q, \ldots, x^{q^{r-1}}) = y_j^{q^r-1} + \ldots + b^{q^r-1-q} + 1) y_j^{q^{r-1}} + \ldots + \left(b^{q^r-1-q} + \ldots + b^{q^2-q} + 1 \right) y_j$$
where \( s_{r,2} \) is the second symmetric polynomial in \( r \) variables. This curve was introduced by Deolalikar [4] for \( r = 3 \), and generalized for all \( r \) in [12]. \( \mathcal{X}_r^j \) is covered by the Generalized Hermitian curve and a covering map is given by 
\[
c(x, y) = (x, y^{q^{r-j-1}} + (b_1 y^{q^{r-1}} + \cdots + b_{r-j-1} y^{q^{r-2}} + \cdots b_2 y^{q^2} + 1) + y^{q^{r-1}} + \cdots + b_2 y^{q^2} + 1) y).
\]
The following Proposition states some of the main properties of \( \mathcal{X}_r^j \). See [12] for the proofs.

**Proposition 4.1.** The curve \( \mathcal{X}_r^j \), \( j = 1 \) and \( j = r-2 \), verifies the following properties.

1. The only pole of \( x, Q_j^r \), is totally ramified.
2. The genus of \( \mathcal{X}_r^j \) is \( g = (q^j - 1)q^{r-1}/2 \).
3. The number of rational points of \( \mathcal{X}_r^j \) is \( q^{r+j} + 1 \).
4. The Weierstrass semigroup at \( Q_j^r \) is \( H(Q_j^r) = \langle q^j, q^{r-1} + 1 \rangle \).
5. Let \( z = x^{1+a} + x^{1+q^2} + \cdots + x^{q^{r-3}+q^2} - y^{q^j} \). Then \( \{x^{a}z^b : 0 \leq a, 0 \leq b < q^j \text{ and } aq^j + b(q^{r-1} + 1) = m \} \) is a basis of \( \mathcal{L}(mQ_j^r) \).

For \( m = 0, 1, \ldots \), we can consider the codes \( C_{r,m}^j = C(\mathcal{X}_r^j, D, mQ_j^r) \), where \( D \) is the sum of all rational points of \( \mathcal{X}_r^j \) except \( Q_j^r \). The properties of these codes can be studied in a similar way as done previously for Generalized Hermitian curves. Here we just show an example that this curve provides good codes.

**Example 4.2.** For \( q = 3 \) and \( r = 3 \), the curve \( \mathcal{X}_3^1 \) have genus 9 and 82 rational points over \( \mathbb{F}_{27} \). For \( m = 10 \) we get a \([81, 5, \geq 71]\) code, which is a new record.

**References**


Dept. of Applied Mathematics, University of Valladolid, Avda Salamanca SN, 47012 Valladolid, Castilla, Spain

Faculdade de Matemática, Universidade Federal de Uberlândia, Av. J. N. de Ávila 2160, Uberlândia, 38408-100, MG-Brazil

Institute of Mathematics, Statistics and Computer Science, P.O. Box 6065, University of Campinas, 13083-970, Campinas, SP, Brazil

E-mail address: cmunuera@arq.uva.es
E-mail address: alonso@famat.ufu.br
E-mail address: ftorres@ime.unicamp.br