Higher Hamming weights for locally recoverable codes on algebraic curves

Edoardo Ballico¹, Chiara Marcolla*  

Department of Mathematics, University of Trento, Italy

Abstract

We study locally recoverable codes on algebraic curves. In the first part of the manuscript, we provide a bound on the generalized Hamming weight of these codes. In the second part, we propose a new family of algebraic geometric LRC codes, which are LRC codes from the Norm-Trace curve. Finally, using some properties of Hermitian codes, we improve the bounds on the distance proposed in Barg et al. (2015) [1] of some Hermitian LRC codes.

© 2016 Elsevier Inc. All rights reserved.

1. Introduction

The $v$-th generalized Hamming weight $d_v(C)$ of a linear code $C$ is the minimum support size of $v$-dimensional subcodes of $C$. The sequence $d_1(C),\ldots,d_k(C)$ of generalized Hamming weights was introduced by Wei [37] to characterize the performance of a linear code on the wire-tap channel of type II. Later, the GHWs of linear codes have been used

---

* Corresponding author.
E-mail addresses: ballico@science.unitn.it (E. Ballico), chiara.marcolla@unito.it (C. Marcolla).
¹ The first author is partially supported by MIUR and GNSAGA of INdAM (Italy).

http://dx.doi.org/10.1016/j.ffa.2016.03.004
1071-5797 © 2016 Elsevier Inc. All rights reserved.
in many other applications regarding the communications, as for bounding the covering radius of linear codes [15], in network coding [26], in the context of list decoding [7,9], and finally for secure secret sharing [18]. Moreover, in [2] the authors show in which way an arbitrary linear code gives rise to a secret sharing scheme, in [16,17] the connection between the trellis or state complexity of a code and its GHWs is found and in [4] the author proves the equivalence to the dimension/length profile of a code and its generalized Hamming weight. For these reasons, the GHWs (and their extended version, the relative generalized Hamming weights [21,19]) play a central role in coding theory. In particular, generalized and relative generalized Hamming weights are studied for Reed–Muller codes [10,23] and for codes constructed by using an algebraic curve [6] as Goppa codes [24,38], Hermitian codes [12,25] and Castle codes [27].

In this paper, we provide a bound on the generalized Hamming weight of locally recoverable codes on the algebraic curves proposed in [1]. Moreover, we introduce a new family of algebraic geometric LRC codes and improve the bounds on the distance for some Hermitian LRC codes.

Locally recoverable codes were introduced in [8] and they have been significantly studied because of their applications in distributed and cloud storage systems [3,13,32,34,35]. We recall that a code $C \in (\mathbb{F}_q)^n$ has locality $r$ if every symbol of a codeword $c$ can be recovered from a subset of $r$ other symbols of $c$.

In other words, we consider a finite field $K = \mathbb{F}_q$, where $q$ is a power of a prime, and an $[n,k]$ code $C$ over the field $K$, where $k = \log_q(|C|)$. For each $i \in \{1, \ldots, n\}$ and each $a \in K$ set $C(i,a) = \{c \in C \mid c_i = a\}$. For each $I \subseteq \{1, \ldots, n\}$ and each $S \subseteq C$ let $S_I$ be the restriction of $S$ to the coordinates in $I$.

**Definition 1.** Let $C$ be an $[n,k]$ code over the field $K$, where $k = \log_q(|C|)$. Then $C$ is said to have **all-symbol locality $r$** if for each $a \in \mathbb{F}_q$ and each $i \in \{1, \ldots, n\}$ there is $I_i \subset \{1, \ldots, n\} \setminus \{i\}$ with $|I_i| \leq r$, such that for $C_{I_i}(i,a) \cap C_{I_i}(i,a') = \emptyset$ for all $a \neq a'$.

We use the notation $(n,k,r)$ to refer to the parameters of this code.

Note that if we receive a codeword $c$ correct except for an erasure at $i$, we can recover the codeword by looking at its coordinates in $I_i$. For this reason, $I_i$ is called a **recovering set** for the symbol $c_i$.

Let $C$ be an $(n,k,r)$ code, then the distance of this code has to verify the bound proved in [28,8] that is $d \leq n - k - \lceil k/r \rceil + 2$. The codes that achieve this bound with equality are called **optimal** LRC codes [32,34,35]. Note that when $r = k$, we obtain the Singleton bound, therefore optimal LRC codes with $r = k$ are MDS codes.

**Layout of the paper** This paper is divided as follows. In Section 2 we recall the notions of algebraic geometric codes and the definition of algebraic geometric locally recoverable codes introduced in [1]. In Section 3 we provide a bound on the generalized Hamming weights of the latter codes. In Section 4 we propose a new family of algebraic geometric LRC codes, which are LRC codes from the Norm-Trace curve. Finally, in Section 5 we
improve the bounds on the distance proposed in [1] for some Hermitian LRC codes, using
some properties of the Hermitian codes.

2. Preliminary notions

2.1. Algebraic geometric codes

Let $K = \mathbb{F}_q$ be a finite field, where $q$ is a power of a prime. Let $\mathcal{X}$ be a smooth
projective absolutely irreducible nonsingular curve over $K$. We denote by $K(\mathcal{X})$ the
rational functions field on $\mathcal{X}$. Let $D$ be a divisor on the curve $\mathcal{X}$. We recall that the
Riemann–Roch space associated to $D$ is a vector space $\mathcal{L}(D)$ over $K$ defined as

$$\mathcal{L}(D) = \{f \in K(\mathcal{X}) \mid (f) + D \geq 0\} \cup \{0\},$$

where we denote by $(f)$ the divisor of $f$.

Assume that $P_1, \ldots, P_n$ are rational points on $\mathcal{X}$ and $D$ is a divisor such that $D = P_1 + \ldots + P_n$. Let $G$ be some other divisor such that $\text{supp}(D) \cap \text{supp}(G) = \emptyset$. Then we
can define the algebraic geometric code as follows:

**Definition 2.** The algebraic geometric code (or AG code) $C(D, G)$ associated with the
divisors $D$ and $G$ is defined as

$$C(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subset K^n.$$

The dual $C^\perp(D, G)$ of $C(D, G)$ is an algebraic geometric code.

In other words an algebraic geometric code is the image of the evaluation map
$\text{Im}(\text{ev}_D) = C(D, G)$, where the evaluation map $\text{ev}_D : \mathcal{L}(G) \rightarrow K^n$ is given by

$$\text{ev}_D(f) = (f(P_1), \ldots, f(P_n)) \in K^n.$$

Note that if $D = P_1 + \ldots + P_n$ and we denote by $\mathcal{P} = \{P_1, \ldots, P_n\}$ we can also indicate
$\text{ev}_D$ as $\text{ev}_{\mathcal{P}}$.

2.2. Algebraic geometric locally recoverable codes

In this section we consider the construction of algebraic geometric locally recoverable
codes of [1].

Let $\mathcal{X}$ and $\mathcal{Y}$ be smooth projective absolutely irreducible curves over $K$. Let $g : \mathcal{X} \rightarrow \mathcal{Y}$
be a rational separable map of curves of degree $r + 1$. Since $g$ is separable, then there
exists a function $x \in K(\mathcal{X})$ such that $K(\mathcal{X}) = K(\mathcal{Y})(x)$ and that $x$ satisfies the equation
$x^{r+1} + b_r x^r + \ldots + b_0 = 0$, where $b_i \in K(\mathcal{Y})$. The function $x$ can be considered as a map
$x : \mathcal{X} \rightarrow \mathbb{P}_K$. Let $h = \text{deg}(x)$ be the degree of $x$. 
We consider a subset \( S = \{ P_1, \ldots, P_s \} \subset \mathcal{Y}(K) \) of \( \mathbb{F}_q \)-rational points of \( \mathcal{Y} \), a divisor \( Q_\infty \) such that \( \text{supp}(Q_\infty) \cap \text{supp}(S) = \emptyset \) and a positive divisor \( D = tQ_\infty \). We denote by
\[
\mathcal{A} = g^{-1}(S) = \{ P_{ij}, \text{ where } i = 0, \ldots, r, \ j = 1, \ldots, s \} \subset \mathcal{X}(K),
\]
where \( g(P_{ij}) = P_i \) for all \( i, j \) and assume that \( b_i \) are functions in \( \mathcal{L}(n_i Q_\infty) \) for some natural numbers \( n_i \) with \( i = 1, \ldots, r \).

Let \{\( f_1, \ldots, f_m \)\} be a basis of the Riemann–Roch space \( \mathcal{L}(D) \). By the Riemann–Roch Theorem we have that \( m \geq \deg(D) + 1 - g_\mathcal{Y} \), where \( g_\mathcal{Y} \) is the genus of \( \mathcal{Y} \).

From now on, we assume that \( m = \deg(D) + 1 - g_\mathcal{Y} \), where \( \deg(D) = t\ell \), and we consider the \( K \)-subspace \( V \) of \( K(\mathcal{X}) \) of dimension \( rm \) generated by
\[
\mathcal{B} = \{ f_j x_i^s, \ i = 0, \ldots, r - 1, \ j = 1, \ldots, m \}.
\]

We consider the evaluation map \( ev_{\mathcal{A}} : V \to K^{(r+1)s} \). Then we have the following theorem.

**Theorem 1.** The linear space \( C(D, g) = \text{Span}_{K(r+1)} \langle ev_{\mathcal{A}}(\mathcal{B}) \rangle \) is an \( (n, k, r) \) algebraic geometric LRC code with parameters
\[
\begin{align*}
  n &= (r + 1)s \\
  k &= rm \geq r(t\ell + 1 - g_\mathcal{Y}) \\
  d &\geq n - t\ell(r + 1) - (r - 1)h.
\end{align*}
\]

**Proof.** See Theorem 3.1 of [1]. \( \square \)

The AG LRC codes have an additional property. They are LRC codes \((n, k, r)\) with \( (r + 1) | n \) and \( r | k \). The set \( \{1, \ldots, n\} \) can be divided into \( n/(r + 1) \) disjoint subsets \( U_j \) for \( 1 \leq j \leq s \) with the same cardinality \( r + 1 \). For each \( i \) the set \( I_i \subset \{1, \ldots, n\} \setminus \{i\} \) is the complement of \( i \) in the element of the partition \( U_j \) containing \( j \), i.e. for all \( i, j \in \{1, \ldots, n\} \) either \( I_i = I_j \) or \( I_i \cap I_j = \emptyset \).

Moreover, they have also the following nice property. Fix \( w \in (K)^n \) and denote by \( w_{U_j} = \{ w_i \}, \text{ for any } i \in U_j \}. \) Suppose we receive all the symbols in \( U_j \). There is a simple linear parity test on the \( r + 1 \) symbols of \( U_j \) such that if this parity check fails we know that at least one of the symbols in \( U_j \) is wrong. If we are guaranteed (or we assume) that at most one of the symbols in \( U_j \) is wrong and the parity check is OK, then all the symbols in \( U_j \) are correct. Moreover we can recover an erased symbol \( w_i \), with \( i \in U_j \) using a polynomial interpolation through the points of the recovering set \( w_{U_j} \).

3. **Generalized Hamming weights of AG LRC codes**

Let \( K \) be a field and let \( \mathcal{X} \) be a smooth and geometrically connected curve of genus \( g \geq 2 \) defined over the field \( K \). We also assume \( \mathcal{X}(K) \neq \emptyset \). We recall the following definitions:
**Definition 3.** (See [29,30].) The **K-gonality** $\gamma_K(\mathcal{X})$ of $\mathcal{X}$ over a field $K$ is the smallest possible degree of a dominant rational map $\mathcal{X} \to \mathbb{P}^1_K$. For any field extension $L$ of $K$, we define also the **L-gonality** $\gamma_L(\mathcal{X})$ of $\mathcal{X}$ as the gonality of the base extension $\mathcal{X}_L = \mathcal{X} \times_K L$. It is an invariant of the function field $L(\mathcal{X})$ of $\mathcal{X}_L$.

Moreover, for each integer $i > 0$, the **i-th gonality** $\gamma_{i,L}(\mathcal{X})$ of $\mathcal{X}$ is the minimal degree $z$ such that there is $R \in \text{Pic}^z(\mathcal{X})(L)$ with $h^0(R) \geq i + 1$. The sequence $\gamma_{i,K}(\mathcal{X})$ is the usual gonality sequence [20]. Moreover, the integer $\gamma_{1,K}(\mathcal{X}) = \gamma_K(\mathcal{X})$ is the $K$-gonality of $\mathcal{X}$.

Let $K = \mathbb{F}_q$ a finite field with $q$ elements. Let $C \subset K^n$ be a linear $[n, k]$ code over $K$. We recall that the **support** of $C$ is defined as follows

$$\text{supp}(C) = \{i \mid c_i \neq 0 \text{ for some } c \in C\}.$$ 

So $\sharp \text{supp}(C)$ is the number of nonzero columns in a generator matrix for $C$. Moreover, for any $1 \leq v \leq k$, the **v-th generalized Hamming weight** of $C$ [14, §7.10], [36, §1.1] is defined by

$$d_v(C) = \min\{\sharp \text{supp}(D) \mid D \text{ is a linear subcode of } C \text{ with } \dim(D) = v\}.$$ 

In other words, for any integer $1 \leq v \leq k$, $d_v(C)$ is the $v$-th minimum support weights, i.e. the minimal integer $t$ such that there are an $[n,v]$ subcode $D$ of $C$ and a subset $S \subset \{1,\ldots,n\}$ such that $\sharp(S) = t$ and each codeword of $D$ has zero coordinates outside $S$. The sequence $d_1(C),\ldots,d_k(C)$ of generalized Hamming weights (also called **weight hierarchy** of $C$) is strictly increasing (see Theorem 7.10.1 of [14]). Note that $d_1(C)$ is the minimum distance of the code $C$.

Let us consider $\mathcal{X}$ and $\mathcal{Y}$ smooth projective absolutely irreducible curves over $K$ and let $g : \mathcal{X} \to \mathcal{Y}$ be a rational separable map of curves of degree $r+1$. Moreover we take $r$, $t$, $Q_\infty$, $f_1,\ldots,f_m$ and $A = g^{-1}(S)$ defined as Section 2.2. So we can construct an $(n,k,r)$ algebraic geometric LRC code $C$ as in Theorem 1. For this code we have the following:

**Theorem 2.** Let $C$ be an $(n,k,r)$ algebraic geometric LRC code as in Theorem 1. For every integer $v \geq 2$ we have that

$$d_v(C) \geq n - tr(r+1) - (r-1)h + \gamma_{v-1,K}(\mathcal{X}).$$

**Proof.** Take a $v$-dimensional linear subspace $D$ of $C$ and call

$$E \subseteq \{P_{ij} \mid i = 0,\ldots,r, j = 1,\ldots,s\},$$

the set of common zeros of all elements of $D$. Since $n - d_v(C) = \sharp(E)$, we have to prove that $tr(r+1) + (r-1)h - \sharp(E) \geq \gamma_{v-1,K}(X)$. Fix $u \in D \setminus \{0\}$ and let $F_u$ denote the
zeros of $u$. Note that $F_u$ is contained in the set $\{P_{ij} \mid i = 0, \ldots, r, j = 1, \ldots, s\}$ by the definition of the code $C$. We have $F_u \supseteq E$. By the definition of the integers $t$, $\ell$ and $h := \deg(x)$, we have $\sharp(F_u) \leq t\ell(r + 1) + (r - 1)h$. The divisors $F_u - E$, $u \in D \setminus \{0\}$ form a family of linearly equivalent non-negative divisors, each of them defined over $K$. Since $\dim(D) = v$, the definition of $\gamma_{v-1,K}(\mathcal{X})$ gives $\sharp(F_u) = \sharp(E) \geq \gamma_{v-1,K}(\mathcal{X})$. This inequality for a single $u \in D \setminus \{0\}$ proves the theorem. $\Box$

See Remark 1 for an application of Theorem 2.

4. LRC codes from Norm-Trace curve

In this section we propose a new family of Algebraic Geometric LRC codes, that is, a LRC codes from the Norm-Trace curve. Moreover, we compute the $F_{q^n}$-gonality of the Norm-Trace curve.

Let $K = \mathbb{F}_{q^n}$ be a finite field, where $q$ is a power of a prime. We consider the norm $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ and the trace $\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$, two functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ defined as

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x^1 + x^{q} + \cdots + x^{q^{n-1}} \quad \text{and} \quad \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{n-1}}.$$

The Norm-Trace curve $\chi$ is the curve defined over $K$ by the following affine equation

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y),$$

that is,

$$x^{(q^n-1)/(q-1)} = y^{q^{n-1}} + y^{q^{n-2}} + \cdots + y$$

where $x, y \in K$. (1)

The Norm-Trace curve $\chi$ has exactly $n = q^{2u-1}$ $K$-rational affine points (see Appendix A of [5]), that we denote by $\mathcal{P}_\chi = \{P_1, \ldots, P_n\}$. The genus of $\chi$ is $g = \frac{1}{2}(q^{u-1} - 1)(\frac{q^u-1}{q-1} - 1)$. Note that if we consider $u = 2$, we obtain the Hermitian curve.

Starting from the Norm-Trace curve, we have two different ways to construct Norm-Trace LRC codes.

Projection on $x$ We have to construct a $q^u$-ary $(n, k, r)$ LRC codes. We consider the natural projection $g(x, y) = x$. Then the degree of $g$ is $q^{u-1} = r + 1$ and the degree of $y$ is $h = 1 + q + \cdots + q^{u-1}$.

To construct the codes we consider $S = \mathbb{F}_{q^n}$ and $D = tQ_\infty$ for some $t \geq 1$. Then, using a construction of Theorem 1 we find the parameters for these Norm-Trace LRC codes.

**Proposition 1.** A family of Norm-Trace LRC codes has the following parameters:

$$n = q^{2u-1}, \quad k = mr = (t + 1)(q^{u-1} - 1)$$
and
\[ d \geq n - tq^{u-1} - (q^{u-1} - 1)(1 + q + \cdots + q^{u-1}). \]

**Projection on y** We have to construct a \( q^u \)-ary \((n, k, r)\) LRC codes. We consider the other natural projection \( g'(x, y) = y \). Then \( \deg(g') = 1 + q + \cdots + q^{u-1} = r + 1 \). In this case we take \( S = \mathbb{F}_q^u \setminus M \), where
\[ M = \{ a \in \mathbb{F}_q^u \mid a = q^{u-1} + a^{q^{u-2}} + \cdots + a = 0 \}, \]
so \( r = q + \cdots + q^{u-1} \) and \( h = \deg(x) = q^{u-1} \). Then, using Theorem 1 we have the following

**Proposition 2.** A family of Norm-Trace LRC codes has the following parameters:
\[ n = q^{2u-1} - q^{u-1}, \quad k = mr = (t + 1)(q + \cdots + q^{u-1}) \]
and
\[ d \geq n - tq^{u-1} - (q + \cdots + q^{u-1}) - q^{u-1}(q^{u-1} + \cdots + q - 1). \]

For the Norm-Trace curve \( \chi \) we are able to find the \( K \)-gonality of \( \chi \).

**Lemma 1.** Let \( \chi \) be a Norm-Trace curve defined over \( \mathbb{F}_{q^u} \), where \( u \geq 2 \). We have \( \gamma_{1, \mathbb{F}_{q^u}}(\chi) = q^{u-1} \).

**Proof.** The linear projection onto the \( x \) axis has degree \( q^{u-1} \) and it is defined over \( \mathbb{F}_q \) and hence over \( \mathbb{F}_{q^u} \). Thus \( \gamma_{1, \mathbb{F}_{q^u}}(\chi) \leq q^{u-1} \). Denote by \( z = \gamma_{1, \mathbb{F}_{q^u}}(\chi) \) and assume that \( z \leq q^{u-1} - 1 \). By the definition of \( K \)-gonality, there is a non-constant morphism \( w : \chi \to \mathbb{P}^1 \) with \( \deg(w) = z \) and defined over \( \mathbb{F}_{q^u} \). Since \( w(\chi(\mathbb{F}_{q^u})) \subseteq \mathbb{P}^1(\mathbb{F}_{q^u}) \), we get \( \sharp(\chi(\mathbb{F}_{q^u})) \leq z(q^{u} + 1) \leq (q^{u-1} - 1)(q^{u} + 1) \), that is a contradiction. \( \square \)

**Remark 1.** By Lemma 1, we can apply Theorem 2 to the Norm-Trace curve. In fact, we can consider the gonality sequence over \( K \) of \( \chi \) to get a lower bound on the second generalized Hamming weight of the two families of Norm-Trace LRC codes:

- Let \( t \geq 1 \) and let \( C \) be a \( (q^{2u-1}, (t + 1)(q^{u-1} - 1), q^{u-1} - 1) \) Norm-Trace LRC code. Then we have
\[ d_2(C) \geq q^{2u-1} + q^{u-1} - tq^{u-1} - (q^{u-1} - 1)(1 + q + \cdots + q^{u-1}). \]

- Let \( t \geq 1 \) and let \( C \) be a Norm-Trace LRC code with parameters \( (q^{2u-1} - q^{u-1}, (t + 1)(q + \cdots + q^{u-1}), q + \cdots + q^{u-1}) \). Then we have
\[ d_2(C) \geq q^{2u-1} - (t - 1)q^{u-1} - (1 + q^{u-1})(q + \cdots + q^{u-1}). \]
5. Hermitian LRC codes

In this section we improve the bound on the distance of Hermitian LRC codes proposed in [1] using some properties of Hermitian codes which are a special case of algebraic geometric codes.

5.1. Hermitian codes

Let us consider $K = \mathbb{F}_{q^2}$ a finite field with $q^2$ elements. The Hermitian curve $\mathcal{H}$ is defined over $K$ by the affine equation

$$x^{q+1} = y^q + y \quad \text{where } x, y \in K.$$  \hfill (2)

This curve has genus $g = \frac{q(q-1)}{2}$ and has $q^3 + 1$ points of degree one, namely a pole $Q_\infty$ and $n = q^3$ rational affine points, denoted by $\mathcal{P}_\mathcal{H} = \{P_1, \ldots, P_n\}$ [31].

**Definition 4.** Let $m \in \mathbb{N}$ such that $0 \leq m \leq q^3 + q^2 - q - 2$. Then the Hermitian code $C(m, q)$ is the code $C(D, mQ_\infty)$ where

$$D = \sum_{\alpha^{q+1} = \beta^q + \beta} P_{\alpha, \beta}$$

is the sum of all places of degree one (except $Q_\infty$, that is a point at infinity) of the Hermitian function field $K(\mathcal{H})$.

By Lemma 6.4.4. of [33] we have that

$$\mathcal{B}_{m,q} = \{x^i y^j \mid qi + (q+1)j \leq m, \ 0 \leq i \leq q^2 - 1, \ 0 \leq j \leq q - 1\},$$

forms a basis of $\mathcal{L}(mQ_\infty)$. For this reason, the Hermitian code $C(m, q)$ could be seen as $\text{Span}_{\mathbb{F}_{q^2}}(ev_{\mathcal{P}_\mathcal{H}}(\mathcal{B}_{m,q}))$. Moreover, the dual of $C(m, q)$ denoted by $C(m_\perp, q) = C^\perp(m, q)$ is again an Hermitian code and it is well known (Proposition 8.3.2 of [33]) that the degree $m$ of the divisor has the following relation with respect to $m_\perp$:

$$m_\perp = n + 2g - 2 - m.$$  \hfill (3)

The Hermitian codes can be divided in four phases [11], any of them having specific explicit formulas linking their dimension and their distance [22]. In particular we are interested in the first and the last phase of Hermitian codes, which are:

1 Phase: $0 \leq m_\perp \leq q^2 - 2$. Then we have $m_\perp = aq + b$ where $0 \leq b \leq a \leq q - 1$ and $b \neq q - 1$. In this case, the distance is
\[ \begin{cases} d = a + 1 & \text{if } a > b \\ d = a + 2 & \text{if } a = b. \end{cases} \] (4)

IV Phase: \( n - 1 \leq m_\perp \leq n + 2g - 2 \). In this case \( m_\perp = n + 2g - 2 - aq - b \) where \( a, b \) are integers such that \( 0 \leq b \leq a \leq q - 2 \) and the distance is
\[ d = n - aq - b. \] (5)

5.2. Bound on distance of Hermitian LRC codes

Let \( K = \mathbb{F}_{q^2} \) be a finite field, where \( q \) is a power of a prime. Let \( X = \mathcal{H} \) be the Hermitian curve with affine equation as in (2). We recall that this curve has \( q^3 \mathbb{F}_{q^2} \)-rational affine points plus one at infinity, that we denoted by \( Q_\infty \).

We consider two of the three constructions of Hermitian LRC codes proposed in [1] and we improve the bound on distance of Hermitian LRC codes using properties of Hermitian codes. In particular, if we find an Hermitian code \( C(m, q) = C_{\text{Her}} \) such that \( C_{\text{LRC}} \subset C_{\text{Her}} \), then we have \( d_{\text{LRC}} \geq d_{\text{Her}} \).

**Projection on \( x \)** By Proposition 4 of [1], we have a family of \((n, k, r)\) Hermitian LRC codes with \( r = q - 1 \), length \( n = q^3 \), dimension \( k = (t - 1)(q - 1) \) and distance \( d \geq n - tq - (q - 2)(q + 1) \). Moreover, for these codes, \( S = K, D = tQ_\infty \) for some \( 1 \leq t \leq q^2 - 1 \) and the basis for the vector space \( V \) is
\[ B = \{ x^iy^j \mid j = 0, \ldots, t, \ i = 0, \ldots, q - 2 \}. \] (6)

Using the Hermitian codes, we improve the bound on the distance for any integer \( t \), such that \( q^2 - q + 1 \leq t \leq q^2 - 1 \).

To find an Hermitian code \( C(m, q) = C_{\text{Her}} \) such that \( C_{\text{LRC}} \subset C_{\text{Her}} \), we have to compute the set \( B_{m,q} \), that is, we have to find \( m \). After that, to compute the distance of \( C(m, q) \) we use (4) and (5). We consider the first Hermitian phase: \( 0 \leq m_\perp \leq q^2 - 2 \), that is, \( q^2 - q + 1 \leq t \leq q^2 - 1 \).

For this phase \( m_\perp = aq + b \), where \( 0 \leq b \leq a \leq q - 1 \) and the distance of the Hermitian code is either \( d = a + 1 \) if \( a > b \) or \( d = a + 2 \) if \( a = b \). By (6), \( m \) must be equal to \( m = qt + (q + 1)(q - 2) \) and by (3) we have that \( m_\perp = n + 2g - 2 - m = q(q^2 - t) \). So \( b = 0 \) and \( a = q^2 - t \) and the distance of the Hermitian code is \( d_{\text{Her}} = a + 1 = q^2 - t + 1 \), since \( a > b \). This implies that
\[ d_{\text{LRC}} \geq q^2 - t + 1, \text{ for any } t \geq q^2 - q + 1. \] (7)

Note that (7) improves the bound on the distance proposed in Proposition 4 of [1] since
\[ q^2 - t + 1 > q^3 - tq - (q - 2)(q + 1) \iff t(q - 1) > q(q - 1)^2 + 1 \iff t > q^2 - q. \]

We just proved the following:
Proposition 3. Let $q^2 - q + 1 \leq t \leq q^2 - 1$. It is possible to construct a family of $(n, k, r)$ Hermitian LRC codes $\{C_t\}_{q^2 - q + 1 \leq t \leq q^2 - 1}$ with the following parameters:

$$n = q^3, \quad k = (t - 1)(q - 1), \quad r = q - 1 \quad \text{and} \quad d \geq q^2 - t + 1.$$  

Two recovering sets In [1] the authors propose an Hermitian code with two recovering sets of size $r_1 = q - 1$ and $r_2 = q$, denoted by LRC(2). They consider

$$L = \text{Span}\{x^i y^j, \ i = 0, \ldots, q - 2, \ j = 0, \ldots, q - 1\}$$

and a linear code $C$ obtained by evaluating the functions in $L$ at the points of $B = g^{-1}(\mathbb{F}_{q^2} \setminus M)$, where $g(x, y) = x$ and $M = \{a \in \mathbb{F}_q \mid a^q + a = 0\}$. So $|B| = q^3 - q$. By Proposition 4.3 of [1], the LRC(2) code has length $n = (q^2 - 1)q$, dimension $k = (q - 1)q$ and distance

$$d \geq (q + 1)(q^2 - 3q + 3) = q^3 - 2q^2 + 3. \tag{8}$$

As before, we improve the bound on the distance using Hermitian codes that contains the LRC(2) code. To do this we have to find $m_\perp$. By $L$, we have that $m = q(q - 1) + (q + 1)(q - 2)$ so we are in the fourth phase of Hermitian codes because $m_\perp = n + 2g - 2 - m = q^3 - q^2 + q$. In this case $d_{H} = m_\perp - 2g + 2 = q^3 + 2q + 2$. Since $|B| = q^3 - q$, we have that

$$d_{\text{LRC}} \geq d_{H} - q = q^3 + q + 2. \tag{9}$$

Note that this bound improves bound (8). We just proved the following proposition:

Proposition 4. Let $C$ be a linear code obtained by evaluating the functions in $L$ at the points of $B$. Then $C$ has the following parameters:

$$n = (q^2 - 1)q, \quad k = (q - 1)q, \quad r_1 = q - 1, \quad r_2 = q \quad \text{and} \quad d \geq q^3 + q + 2.$$  

Acknowledgment

The authors would like to thank the anonymous referees for their comments.

References


