THE DUAL GEOMETRY OF HERMITIAN TWO-POINT CODES

EDOARDO BALLICO

Department of Mathematics, University of Trento
Via Sommarive 14, 38123 Povo (TN), Italy

ALBERTO RAVAGNANI

Institut de Mathématiques, Université de Neuchâtel
Emile-Aigrand 11, CH-2000 Neuchâtel, Switzerland

ABSTRACT. In this paper we study the algebraic geometry of any two-point code on the Hermitian curve and reveal the purely geometric nature of their dual minimum distance. We describe the minimum-weight codewords of many of their dual codes through an explicit geometric characterization of their supports. In particular, we show that they appear as sets of collinear points in many cases.

1. INTRODUCTION

Goppa codes were introduced by the Russian Mathematician V. D. Goppa in 1970 (see [9]), who had the idea of employing algebraic curves to construct error correcting codes.

Definition 1. Let $q$ be a prime power, and let $\mathbb{P}^k$ be the projective space of dimension $k$ over the field $\mathbb{F}_q$. Consider a smooth curve $X \subseteq \mathbb{P}^k$ defined over $\mathbb{F}_q$ and an $\mathbb{F}_q$-rational divisor $D$ on $X$. Take points $P_1, \ldots, P_n \in X(\mathbb{F}_q)$ not lying in the support of $D$, and set $\overline{D} := \sum_{i=1}^n P_i$. The Goppa code $C(\overline{D}, D)$ is defined to be the code obtained evaluating the Riemann-Roch space space $L(D)$ at the points $P_1, \ldots, P_n$.

From the definition we see that curves carrying many rational points may produce long codes. On the other hand, the number of $\mathbb{F}_q$-rational points of a smooth curve $X$ defined over $\mathbb{F}_q$ is bounded by the well known Hasse-Weil bound:

$$|X(\mathbb{F}_q)| - q - 1 \leq 2g(X)\sqrt{q},$$

where $g(X)$ is the geometric genus of $X$. As a consequence, curves attaining the bound (which are called maximal) are particularly interesting in coding theory. The Hermitian curve (see Section 2 for definition and properties) is a plane smooth maximal curve defined over finite fields of the form $\mathbb{F}_q^2$. One-point codes from the Hermitian curve (i.e., codes obtained by evaluating vector spaces
of the form $L(mP)$, with $m \in \mathbb{Z}$ and $P$ a rational point of the curve) are probably the most studied algebraic geometric codes (see, among the others, [22], Section 8.3, and [15]). **Two-point** codes from the Hermitian curve are obtained evaluating Riemann-Roch spaces of the form $L(mP + nQ)$, with $a, b \in \mathbb{Z}$ and $P, Q$ distinct rational points of the curve. The minimum distance of any two-point code from the Hermitian curve has been completely determined by Homma and Kim in [14], [12], and [13]. Using different techniques, Park provides in [19] explicit formulas for their dual minimum distances. The results by Park will be stated later in this paper (see Section 2).

Recently, A. Couvreur found a way to characterize the dual minimum distance of some geometric Goppa codes in terms of their projective geometries (see [6]). We extended his approach in [1] in order to find out the dual minimum distances of some $m$-points codes on the Hermitian curve for $m \geq 3$. Here we combine the results by Park, the method of [6], and the projective geometry of the Hermitian curve in order to obtain a geometric description of the minimum-weight codewords of many duals of Hermitian two-point codes. To be precise, we will show that the points in their supports obey some particular geometric laws (such as collinearity).

**Remark 2.** The capability to determine minimum-weight or, more generally, small-weight code-words of Goppa codes is relevant for cryptographic issues. Indeed, in [5] and [4] it is shown that minimum-weight and small-weight codewords of Goppa codes can be used to attack the well known McEliece cryptosystem (see [17] and the references within it).

The remainder of the paper is organized as follows. In Section 2 we state Park’s results and interpret two-point Hermitian codes in terms of evaluations of cohomology groups. The geometric properties of the Hermitian curve are summarized in Section 3, where we also characterize the dual minimum distance of codes from curves in terms of non-vanishing conditions on cohomology groups. We apply the results of Section 3 in Section 4, describing the supports of the minimum-weight codewords of the duals of two-point codes from the Hermitian curve. Computational examples can be found in Section 5.

2. Preliminaries

Let $q$ be a prime power, and let $\mathbb{P}^2$ denote the projective plane over the field $\mathbb{F}_q^2$ with coordinates $(x : y : z)$. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve (see [22], Example VI.3.6) of affine equation

$$y^q + y = x^{q+1}.$$ 

It is well known that $X$ is a maximal curve with $q^3 + 1 \mathbb{F}_q^2$-rational points (see [20] among the others). Choose $m, n \in \mathbb{Z}$ and two distinct points $P, Q \in X(\mathbb{F}_q^2)$. The code obtained evaluating the vector space $L(mP + nQ)$ on $X(\mathbb{F}_q^2) \setminus \{P, Q\}$ is said to be a (classical) two-point code on $X$ ([14], Section 1). Clearly, we may consider only the pairs $(m, n)$ such that $n + m > 0$. Otherwise the resulting code has dimension at most one, and it is not of interest for applications. Since the group of automorphisms of $X$, say $\text{Aut}(X)$, is 2-transitive ([11], pages 572-573) we can assume, without loss of generality, $P = P_\infty$ and $Q = P_0$, where $P_\infty$ is the only point at infinity of $X(\mathbb{F}_q^2)$, of projective coordinates $(0 : 1 : 0)$, and $P_0$ is the point with coordinates $(0 : 0 : 1) \in X(\mathbb{F}_q^2)$. Set $B := X(\mathbb{F}_q^2) \setminus \{P_\infty, P_0\}$ and denote by $C_{m,n}$ the two-point code obtained evaluating the vector space $L(mP_\infty + nP_0)$ on $B$.

**Remark 3.** An explicit basis of $L(mP_\infty + nP_0)$ is well known for any $m, n \in \mathbb{Z}$ (see [7] and [16] for applications in coding theory).
We will widely use the following two results.\(^\text{1}\)

**Theorem 4** ([19], Theorem 3.3). Let \( G = K + mP_\infty + nP_0 \), where \( K \) is a canonical divisor on \( X \). Let \( C^\perp \) be the dual of the code obtained evaluating the vector space \( L(G) \) on the points of \( B \) and denote by \( \delta \) its minimum distance. Write
\[
m = m_0(q + 1) - m_1, \quad 0 \leq m_1 \leq q, \\
n = n_0(q + 1) - n_1, \quad 0 \leq n_1 \leq q.
\]
Set \( d^* := m + n \) and suppose that \( G \) satisfies either
\[
(a) \ \deg(G) > \deg(K) + q, \quad \text{or} \\
(b) \ \deg(K) \leq \deg(G) \leq \deg(K) + q \quad \text{and} \quad G \not\sim sP_\infty \quad \text{and} \quad G \not\sim tP_0, \quad \text{for all} \ s, t \in \mathbb{Z}.
\]
The following formulas hold.
\[
(1) \quad \text{If} \ 0 \leq m_1, n_1 \leq m_0 + n_0, \text{then} \ \delta = d^*.
\]
\[
(2) \quad \text{If} \ 0 \leq m_1 \leq m_0 + n_0 < m_1, \text{then} \ \delta = d^* + m_1 - (m_0 + n_0).
\]
\[
(3) \quad \text{If} \ 0 \leq m_1 \leq m_0 + n_0 < n_1, \text{then} \ \delta = d^* + n_1 - (m_0 + n_0).
\]
\[
(4) \quad \text{If} \ m_0 + n_0 < m_1 \leq n_1 < q, \text{then} \ \delta = d^* + m_1 + n_1 - 2(m_0 + n_0).
\]
\[
(5) \quad \text{If} \ m_0 + n_0 < n_1 \leq m_1 < q, \text{then} \ \delta = d^* + m_1 + n_1 - 2(m_0 + n_0).
\]
\[
(6) \quad \text{If} \ m_0 + n_0 < m_1, n_1 \text{and} \ m_1 = n_1 = q, \text{then} \ \delta = d^* + q - (m_0 + n_0).
\]

**Theorem 5** ([19], Theorem 3.5). Let \( G = mP_\infty + nP_0 \) and let \( C^\perp \) be the dual of the code obtained evaluating the vector space \( L(G) \) on the points of \( B \). Denote by \( \delta \) its minimum distance and write
\[
m = m_0(q + 1) + m_1, \quad 0 \leq m_1 \leq q, \\
n = n_0(q + 1) + n_1, \quad 0 \leq n_1 \leq q.
\]
Suppose that \( G \) satisfies either
\[
(a) \ \deg(G) < \deg(K), \quad \text{or} \\
(b) \ \deg(K) \leq \deg(G) \leq \deg(K) + q \quad \text{and} \quad G \sim sP_\infty \quad \text{or} \quad G \sim tP_0, \quad \text{for some} \ s, t \in \mathbb{Z}.
\]
Then \( \delta = m_0 + n_0 + 2. \)

**Remark 6.** Codes \( C, D \subseteq \mathbb{F}_q^n \) are said to be strongly isometric if \( C = vD \), where \( v \in \mathbb{F}_q^n \) is a vector of non-zero components and
\[
vD := \{(v_1d_1, v_2d_2, \ldots, v_nd_n) : (d_1, d_2, \ldots, d_n) \in D\}.
\]
A strong isometry is an equivalence relation of codes. Strongly isometric codes have the same minimum distance and the same weight distribution. Two codes are strongly isometric if and only if their dual codes are strongly isometric. A strong isometry preserves the supports of the codewords.

The Hermitian curve \( X \subseteq \mathbb{P}^2 \) has a very particular projective geometry (see for example [11]). Let us briefly recall some basic properties (other important facts will be stated in Section 3). For any \( P, Q \in X(\mathbb{F}_q^2) \) we have a linear equivalence \( (q + 1)P \sim (q + 1)Q \). Moreover, for any \( P \in X(\mathbb{F}_q^2) \) we have an isomorphism of sheaves \( \mathcal{O}_X(1) \cong \mathcal{L}((q + 1)P) \), the latter one being the invertible sheaf associated to the divisor \((q + 1)P\) on \( X \). Using these geometric facts we easily deduce that for any pair of integers \((m, n)\) such that \( m + n > 0 \) there exists a tern of integers \((d, a, b)\) such that \( d > 0, 0 \leq a, b \leq q \) and \( L(mP_\infty + nP_0) \cong H^0(X, \mathcal{O}_X(d)(-E)) \), where \( E := aP_\infty + bP_0 \) (as a zero-dimensional subscheme of \( \mathbb{P}^2 \)).

\(^{1}\)If \( X \) is the Hermitian curve and \( P \in X(\mathbb{F}_q^2) \) then any canonical \( \mathbb{F}_q^2 \)-rational divisor \( K \) on \( X \) satisfies the linear equivalence \( K \sim (q - 2)(q + 1)P \).
Remark 7. Notice that isometries of codes induced by linear equivalences of divisors are strong isometries (see for example [18], Remark 2.16). As a consequence, $C_{m,n}$ turns out to be strongly isometric to the two-point code obtained evaluating the vector space $H^0(X, O_X(d)(-E))$ on $B$, here denoted by $C(d,a,b)$.

Remark 8. By the 2-transitivity of Aut($X$), we may also assume $a \leq b$ by permuting (if necessary) $P_0$ and $P_\infty$. Moreover, notice that if $b = 0$ then $C(d,a,b)$ is not a code of interest. Indeed, $C(d,a,0)$ is a one-point code whose parameters can be easily improved by evaluating $H^0(X, O_X(d)(-E))$ on $X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ instead of $B$, obtaining a longer code. Hence, from now on, we will implicitly assume $a \leq b$ and $b \neq 0$ when writing $C(d,a,b)$.

Remark 9. For $m \in \mathbb{Z}_{\geq 0}$, consider the Hermitian one-point code $C_m$ obtained evaluating the vector space $L(mP_\infty)$ on $X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$. Hermitian one-point codes can be easily studied employing the geometric method here presented. In fact, the simple structure of the one-point space $L(mP_\infty)$ can be used to characterize the small-weight codewords of Hermitian one-point codes and also study possible improvements of such codes (see [2]).

3. Coding on the Hermitian curve

In this section we state some technical lemmas on the geometry of the Hermitian curve and certain zero-dimensional subschemes of $\mathbb{P}^2$ (see also [3] and [8]). Then we apply these results to the duals of Hermitian two-point codes, characterizing their minimum-weight codewords in terms of vanishing conditions of cohomology groups.

Lemma 10. Let $X$ be the Hermitian curve. Every line $L$ of $\mathbb{P}^2$ either intersects $X$ in $q + 1$ distinct ($\mathbb{F}_{q^2}$)-rational points, or $L$ is tangent to $X$ at a point $P$ (with contact order $q + 1$). In the latter case $L$ does not intersect $X$ in any other $\mathbb{F}_{q^2}$-rational point different from $P$.

Proof. See [10], part (i) of Lemma 7.3.2, at page 247.

Lemma 11. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve. Fix an integer $e \in \{2, \ldots, q + 1\}$ and $P \in X(\mathbb{F}_{q^2})$. Let $E \subseteq X$ be the divisor $eP$, seen as a closed degree $e$ subscheme of $\mathbb{P}^2$. Let $L_{X,P} \subseteq \mathbb{P}^2$ be the tangent line to $X$ at $P$. Let $T \subseteq \mathbb{P}^2$ be any effective divisor (i.e., a plane curve, possibly with multiple components) of degree $\leq e - 1$ and containing $E$. Then $L_{X,P} \subseteq T$, i.e. $L_{X,P}$ is one of the components of $T$.

Proof. Since $L_{X,P}$ has order of contact $q + 1 \geq e$ with $X$ at $P$, we have $E \subseteq L_{X,P}$. Since we have $\deg(E) > \deg(T)$ and $E \subseteq T \cap L_{X,P}$, Bezout theorem implies $L_{X,P} \subseteq T$.

Lemma 12. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve and let $P \in X(\mathbb{F}_{q^2})$. Denote by $L_{X,P}$ the tangent line to $X$ at $P$. Let $C \subseteq \mathbb{P}^2$ be any irreducible smooth curve defined over $\mathbb{F}_{q^2}$ such that $P \in C(\mathbb{F}_{q^2})$. Let $L_{C,P}$ be the tangent line to $C$ at $P$. Then $2P \subseteq C$ if and only if $L_{X,P} = L_{C,P}$.

Proof. Use both the definition of tangent line and Lemma [11] with $T := L_{C,P}$ and $E := 2P$.

Lemma 13. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve. Choose an integer $d > 0$ and a zero-dimensional scheme $Z \subseteq X(\mathbb{F}_{q^2})$ of degree $z > 0$. The following facts hold.

(a) If $z \leq d + 1$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) = 0$.

(b) If $d + 2 \leq z \leq 2d + 1$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if there exists a line $T_1$ such that $\deg(T_1 \cap Z) \geq d + 2$. 

Lemma 15. Fix any smooth plane curve 

Proof. The previous lemma implies the following useful result.

Lemma 14. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve. Fix an integer $m > 0$ and a zero-dimensional scheme $Z \subseteq X(\mathbb{F}_q^2)$ such that $2 \leq \deg(Z) \leq \max\{2m + 2, 3m, 4m - 5\}$. If $h^1(\mathbb{P}^2, \mathcal{I}_Z(m)) > 0$, then there exists a subscheme $W \subseteq Z$ such that one of the following cases occurs.

(a) $\deg(W) = m + 2$ and $W$ is contained in a line;
(b) $\deg(W) = 2m + 2$ and $W$ is contained in a conic;
(c) $\deg(W) = 3m$ and $W$ is the complete intersection of a curve of degree 3 and a curve of degree $m$;
(d) $\deg(W) = 3m + 1$ and $W$ is contained in a cubic curve.

Proof. Apply Lemma 13.

Lemma 15. Fix any smooth plane curve $X \subseteq \mathbb{P}^2$, an integer $d > 0$, a zero-dimensional scheme $E \subseteq X$ and a finite subset $B \subseteq X$ such that $B \cap E_{\text{red}} = \emptyset$. Let $C$ be the code on $X$ obtained evaluating the vector space $H^0(X, \mathcal{O}_X(d)(-E))$ at the points of $B$. Set $c := \deg(X)$. Assume $\sharp(B) > dc$. We set $n := \sharp(B)$ and $k := h^0(X, \mathcal{O}_X(d) - \deg(E))$, where $h^0(X, \mathcal{O}_X(d)) = \binom{d+2}{2}$ if $d < c$ and $h^0(X, \mathcal{O}_X(d)) = \binom{d+2}{2} - \binom{d-c+2}{2}$ if $d \geq c$. Then $C$ is a code of length $n$ and dimension $k$. Moreover, the minimum distance of $C$ is the minimal cardinality, say $s$, of a subset $S \subseteq B$ of $B$ such that $h^1(\mathbb{P}^2, \mathcal{I}_{S\cup E}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_E(d))$. A given codeword of $C$ has weight $s$ if and only if it is supported by a subset $S \subseteq B$ such that $\sharp(S) = s$ and $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_E(d)).$

Proof. The computation of $h^0(X, \mathcal{O}_X(d))$ is well known. We impose that $B$ does not intersect the support of $E$. The case $E = \emptyset$ is a particular case of [60], Proposition 3.1. In the general case notice that $C$ is obtained evaluating a family of homogeneous degree $d$ polynomials (the ones vanishing on the scheme $E$) at the points of $B$. Since $X$ is projectively normal, the restriction map $\rho_d : H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d)) \to H^0(X, \mathcal{O}_X(d))$ is surjective. As a consequence, the restriction map $\rho_{d,E} : H^0(\mathbb{P}^2, \mathcal{I}_E(d)) \to H^0(X, \mathcal{O}_X(d)(-E))$ is surjective. Hence a finite subset $S \subseteq X \setminus E_{\text{red}}$ imposes independent condition to the space $H^0(X, \mathcal{O}_X(d)(-E))$ if and only if $S$ imposes independent conditions to $H^0(\mathbb{P}^2, \mathcal{I}_E(d))$. On the
other hand, S imposes independent conditions to $H^0(\mathbb{P}^2, \mathcal{I}_E(d))$ if and only if $h^1(\mathbb{P}^2, \mathcal{I}_{EUS}(d)) = h^1(\mathbb{P}^2, \mathcal{I}_E(d))$. Notice that here we use again that $S \cap E = \emptyset$. □

**Remark 16.** In the notation of Lemma 15, a given minimum-weight codeword of $C^\perp$, whose support is $S \subseteq B$, trivially satisfies the condition $h^1(\mathbb{P}^2, \mathcal{I}_{EUS}(d)) > 0$, which is geometrically described by Lemma 14.

**Proposition 17.** Fix integers $d > 2$, $a_i \in \{0, \ldots, q\}$ for $i = 1, 2$ with $a_1 \leq a_2$. Let $r$ be (if it exists) the maximum integer $i \leq 2$ such that $a_i \leq d - 2 + i$. Otherwise, simply set $r := 0$. Define $d' := d - 2 + r > 0$. If $r > 0$ set $a_i' := a_i$ for $i \leq r$ and $a_i' := 0$ otherwise. If $r = 0$ set $a_i' := 0$ for any $i \in \{1, 2\}$. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve and let $P_1 := P_\infty, P_2 := P_0$. Define $E := \sum_{i=1}^2 a_i P_i$. If $r > 0$ define $E' := \sum_{i=r}^2 a'_i P_i$. Otherwise set $E' := 0$. Then the codes obtained evaluating the two vector spaces $H^0(X, \mathcal{O}_X(d)(-E))$ and $H^0(X, \mathcal{O}_X(d')(d' - E'))$ on $B = X(\mathbb{P}^2_q) \setminus \{P_0, P_\infty\}$ are strongly isometric (Remark 6).

**Proof.** If $r = 2$ then $E = E'$, $d = d'$ and so we have nothing to prove. If $r = 1$ then $d' = d - 1$, $a_1' = a_1, a_2' = 0$ and $E' := a_1 P_1$. Consider $E$ and $E'$ as closed subschemes of $\mathbb{P}^2$ of degree $a_1 + a_2$ and $a_1$, respectively. Since the restriction map $H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d)) \to H^0(X, \mathcal{O}_X(d))$ is surjective, then the restriction maps

$$\rho_E : H^0(\mathbb{P}^2, \mathcal{I}_E(d)) \to H^0(X, \mathcal{O}_X(d)(-E)), \quad \rho_{E'} : H^0(\mathbb{P}^2, \mathcal{I}_{E'}(d)) \to H^0(X, \mathcal{O}_X(d)(-E'))$$

are surjective themselves. Every tangent line $T_P X$ to $X$ at a point $P \in X(\mathbb{P}^2_q)$ has order of contact $q + 1$ with $X$ at $P$ (Lemma 10) and hence, by Bezout’s theorem, it intersects $X$ only at $P$. As a consequence $T_P X \cap E$ has degree $a_2$. Since $a_2 > d$ we get that every degree $d$ homogeneous form vanishing on $E$ vanishes also on the line $T_P X$, i.e., it is divided by the equation of $T_P X$. Since $\rho_E$ and $\rho_{E'}$ are surjective and $B \cap T_P X = \emptyset$, we deduce that the codes obtained evaluating $H^0(X, \mathcal{O}_X(d)(-E))$ and $H^0(X, \mathcal{O}_X(d')(d' - E'))$, respectively, are in fact strongly isometric. In the case $r = 0$, repeat the same procedure of case $r = 1$ with $a_2$ and $d$, and then with $a_1$ and $d - 1$. □

Combining Lemma 14, Remark 16 and Proposition 17 we get the following result.

**Proposition 18.** Fix integers $d > 2$, $a_i \in \{0, \ldots, q\}$ for $i = 1, 2$. Let $r, d', E$ and $E'$ be as in Proposition 17. Denote by $C := C(d, a_1, a_2)$ the code obtained evaluating the space $H^0(X, \mathcal{O}_X(d)(-E))$ on $B = X(\mathbb{P}^2_q) \setminus \{P_0, P_\infty\}$ and let $C^\perp$ be its dual code. Let $S \subseteq B$ be the support of a minimum-weight codeword of $C^\perp$ and assume $\deg(E') + \sharp(S) \leq \max\{2d' + 2, 3d', 4d' - 5\}$. There exists a zero-dimensional scheme $W \subseteq E' \cup S$ which satisfies one of the following properties.

(a) $\deg(W) = d' + 2$ and $W$ is contained in a line;
(b) $\deg(W) = 2d' + 2$ and $W$ is contained in a conic;
(c) $\deg(W) = 3d'$ and $W$ is the complete intersection of a curve of degree 3 and a curve of degree $d'$;
(d) $\deg(W) = 3d' + 1$ and $W$ is contained in a cubic curve.

In the following section we apply the previous results to explicitly characterize the supports of the minimum-weight codewords of the duals of Hermitian two-point codes.

4. GEOMETRY OF MINIMUM-WEIGHT CODEWORDS

Following Park’s Theorems 4 and 5 we consider the following three groups, (G1), (G2) and (G3), of two-point Hermitian codes $C(d, a, b)$ (we always assume $0 \leq a \leq b \leq q$ and $b \neq 0$ as in Remark 8). We will denote by $K$ any canonical ($\mathbb{P}^2_q$-rational) divisor on $X$. 


(G1) The codes $C(d,a,b)$ such that $0 < d(q-1) - a - b < \deg(K)$.

(G2) The codes $C(d,a,b)$ such that $\deg(K) \leq d(q-1) - a - b \leq \deg(K) + q$ and $d(q+1)P_\infty - aP_\infty - bP_0$ is not linearly equivalent to a multiple of $P_\infty$ nor to a multiple of $P_0$.

(G3) The codes $C(d,a,b)$ such that $\deg(K) \leq d(q-1) - a - b \leq \deg(K) + q$ and $d(q+1)P_\infty - aP_\infty - bP_0$ is linearly equivalent to a multiple of $P_\infty$ or to a multiple of $P_0$.

**Theorem 19.** Let $C := C(d,a,b)$ be a code of group (G1), with $d > 2$, $0 \leq a \leq b \leq q$, and $b \neq 0$.

Set $a_1 := a$, $a_2 := b$ and define $r$, $d'$, $E$, $E'$ as in Proposition[17] If $a \neq 0$, then the minimum distance of $C^\perp$ is $d$. Let $\{P_1, \ldots, P_d\}$ be the support of a minimum-weight codeword.

(a) If $r = 0$, then $P_1, \ldots, P_d$ are collinear.

(b) If $r = 1$, then $P_\infty, P_1, \ldots, P_d$ are collinear.

(c) If $r = 2$ and $d > 3$, then $P_1, \ldots, P_d$ are collinear.

(d) If $r = 2$ and $d = 3$, then

(d.1) either $P_1, \ldots, P_d$ are collinear,

(d.2) or they lie on the union of the line through $P_0$ and $P_\infty$ and a smooth conic which is tangent to $X$ at both $P_0$ and $P_\infty$,

(d.3) or they lie on an irreducible cubic which is tangent to $X$ at both $P_0$ and $P_\infty$.

If $a = 0$, then the minimum distance of $C^\perp$ is $d + 1$ and $r \neq 0$. Let $\{P_1, \ldots, P_{d+1}\}$ be the support of a minimum-weight codeword of $C^\perp$.

(a) If $r = 1$, then $P_1, \ldots, P_d$ are collinear.

(b) If $r = 2$, then $P_0, P_1, \ldots, P_d$ are collinear.

**Proof.** Denote by $L_{X,P_0}, L_{X,P_\infty}$ the tangent lines to $X$ at $P_0$ and $P_\infty$ (respectively). Denote by $L_{0,\infty}$ the line through $P_0$ and $P_\infty$. Let us consider first the case $a \neq 0$. Keep in mind the linear equivalence

$$d(q+1)P_\infty - aP_\infty - bP_0 \sim ((d-2)(q+1) + (q+1-a))P_\infty + (q+1-b)P_0$$

and apply Theorem[5] with $m_0 := d - 2$, $m_1 := q + 1 - a$, $n_0 := 0$ and $n_1 := q + 1 - b$, obtaining that the minimum distance of $C^\perp$ is $m_0 + m_1 + 2 = d$ (here we use $b \neq 0$). Let $S := \{P_1, \ldots, P_d\} \subseteq B$ be the support of a minimum-weight codeword of $C^\perp$. If $r = 0$, then $d' = d - 2$. Since $\deg(E') + \#(S) = d' + 2$. Proposition[18] applies: there exists a subscheme $W \subseteq \{P_1, \ldots, P_d\}$ of degree $d' + 2 = d - 2 + 2 = d$ contained in a line, and we are done. If $r = 1$, then $a \leq d - 1 < b$ and $d' := d - 2 + 1 = d - 1$. Since $\deg(E') + \#(S) \leq (d - 1) + d = d' + 1 = 2(d' + 1) - 1 = 2d' + 1$, Proposition[18] applies and there exists a subscheme $W \subseteq aP_\infty \cup \{P_1, \ldots, P_d\}$ of degree $d + 1$ and contained in a line $L$. It is immediately seen that $P_\infty \in W$ and $L \neq L_{X,P_\infty}$ (since $a \leq d - 1$ and Lemma[10] applies). Hence the points $P_\infty, P_1, \ldots, P_d$ are collinear. If $r = 2$ then $d' = d$ and $a \leq b \leq d$. In this case $E' = E = aP_\infty + bP_0$. We have $\deg(E) + \#(S) \leq 3d$ and then Proposition[18] applies: either there exists a subscheme $W \subseteq aP_\infty + bP_0 \cup \{P_1, \ldots, P_d\}$ of degree $d + 2$ and contained in a line $L$, or there exists a subscheme $W \subseteq aP_\infty + bP_0 \cup \{P_1, \ldots, P_d\}$ of degree $2d + 2$ and contained in a conic $T$, or there exists a subscheme $W \subseteq aP_\infty + bP_0 \cup \{P_1, \ldots, P_d\}$ of degree $3d$ which is the complete intersection of a curve of degree $3$ and one of degree $d$. In the former case, since $\deg(W) = d + 2$, we see that both $P_\infty$ and $P_0$ must lie on $L$, unless $L = L_{X,P_\infty}$ or $L = L_{X,P_0}$. Since these cases are ruled out by Lemma[10] all the points $P_1, \ldots, P_d$ lie on the line $L_{0,\infty}$. Now assume $\deg(W) = 2d + 2$ and $W$ contained in a conic $T$. The sum of the multiplicities of $P_\infty$ and $P_0$ in $W$, say $e_W(P_\infty)$ and $e_W(P_0)$, must satisfy $e_W(P_\infty) + e_W(P_0) \geq (2d + 2) - d = d + 2 > 4$. Since $e_W(P_\infty) \leq d$ and $e_W(P_0) \leq d$, we deduce (Lemma[11]) $T = L_{X,P_0} \cup L_{X,P_0}$, which contradicts Lemma[10]. Finally, assume $\deg(W) = 3d$. Then $a = b = d > 2$ and $dP_\infty + dP_0 + P_1, \ldots, P_d$ is the complete intersection of a cubic curve $C$ and a curve of degree $d$. If $d > 3$, then Lemma[11] implies $L_{X,P_\infty} \subseteq C$ and $L_{X,P_0} \subseteq C$. By Lemma[10] the
points $P_1, \ldots, P_d$ are collinear (they lie on the line $C - L_{X, P_\infty} - L_{X, P_0}$). If $d = 3$, then it occurs exactly one of the following cases.

- The cubic $C$ is reducible and a degree one component of $C$, say $L$, is tangent to $X$.
  - If $L \neq L_{X, P_\infty}$ and $L \neq L_{X, P_0}$, then Lemma[10] and Lemma[17] imply (keeping in mind our assumption $d > 2$) $L_{X, P_0}, L_{X, P_\infty} \subseteq C - L$. This is forbidden by Lemma[10].
  - If $L = L_{X, P_0}$ (or $L = L_{X, P_\infty}$) then $(d > 2)$ Lemma[11] and Lemma[10] imply also $L_{X, P_0} \subseteq C - L_{X, P_\infty}$ (or $L_{X, P_\infty} \subseteq C - L_{X, P_0}$). Hence $P_1, \ldots, P_d$ lie on the line $C - L_{X, P_\infty} - L_{X, P_0}$.

- The cubic $C$ is reducible and no degree one component of it is tangent to $X$. Let $L \subseteq C$ be a line. By hypothesis, $L$ is not tangent to $X$.
  - If $L$ is not the line through $P_0$ and $P_\infty$, then $3P_\infty \subseteq C - L$ or $3P_0 \subseteq C - L$ (or both). In any case, since $2P_\infty + 2P_0 \subseteq C - L$, we have $L_{X, P_\infty} \subseteq C$ and $L_{X, P_0} \subseteq C$ (here we used Lemma[10] again). As a consequence, $P_1, \ldots, P_d$ lie on $L$ (Lemma[10]).
  - If $L$ is the line through $P_0$ and $P_\infty$, then either $C = L \cup L_{X, P_0} \cup L_{X, P_\infty}$ and $P_1, \ldots, P_d$ lie on $L$ (by Lemma[10]), or $C = L \cup T$, and $T$ is a smooth conic tangent to $X$ at both $P_0$ and $P_\infty$ (remember that $2P_\infty + 2P_0 \subseteq C - L$ and Lemma[12] holds).

- The cubic $C$ is an irreducible curve and tangent (by Lemma[12]) to $X$ at both $P_0$ and $P_\infty$.

Now consider the simpler case $a = 0$. Theorem[5] proves that the minimum distance is $d + 1$. If $r = 0$, then $b > d$ and $0 = a > d - 1$, but we assumed $d > 2$. If $r = 1$, then $\deg(E') + \#(S) = \#(S) = d + 1 = d' + 2$ and Proposition[18] applies: there exists subscheme $W \subseteq \{P_1, \ldots, P_{d+1}\}$ of degree $d' + 2 = d + 1$ and contained in a line. In particular, the points $P_1, \ldots, P_{d+1}$ turn out to be collinear. If $r = 2$, then $b \leq d$, $E' = E$ and $d' = d$. We see that $\deg(E) + \#(S) \leq d + (d + 1) = 2d + 1$ and Proposition[18] applies: there exists a subscheme $W \subseteq bP_0 \cup \{P_1, \ldots, P_d\}$ of degree $d + 2$ and contained in a line $L$. By Lemma[10], $L$ cannot be the tangent line to $X$ at $P_0$. As a consequence, $P_0$ appears is $L$ with multiplicity exactly one and so $P_0, P_1, \ldots, P_{d+1}$ are collinear. 

To complete our analysis we need the following geometric result.

**Lemma 20.** Let $X$ be the Hermitian curve. Let $P, Q \in X(F_{q^2})$ with $P \neq Q$. Assume $nP \sim nQ$ for a certain $0 \leq n < q$. Then $n = 0$.

**Proof.** Assume $n \neq 0$. Let $h := \gcd(n, q + 1) \leq n \leq q$. Write $h = \alpha n + \beta (q + 1)$. We deduce the linear equivalences $hP \sim \alpha n P + \beta (q + 1) P$ and $hQ \sim \alpha n Q + \beta (q + 1) Q$. Since $nP \sim nQ$ then $\alpha n P \sim \alpha n Q$. Hence $hP - \beta (q + 1) P \sim hQ - \beta (q + 1) Q$. Since $\beta (q + 1) P \sim \beta (q + 1) Q$ (as described in Section[2]) we have $hP \sim hQ$ for a certain $1 \leq h \leq q$ which divides $q + 1$ (in particular, we have $h < q$). Notice that $hQ$ is an effective divisor linear equivalent to $hP$. It follows that the linear system $|hP|$ contains $hQ$. Hence $\dim_{F_{q^2}} L(hP) \geq 2$. Since $0 \leq h < q$, from the explicit computation of the Weierstrass semigroup at $P$ (see [21], Proposition 1) we deduce $\dim_{F_{q^2}} L(hP) = 1$, a contradiction.

**Remark 21.** If $C(d, a, b)$ is in group (G3), then we have either $d(q + 1) - aP_\infty - bP_0 \sim sP_\infty$ for a certain $s \in \mathbb{Z}$, or $d(q + 1) - aP_\infty - bP_0 \sim tP_0$ for a certain $t \in \mathbb{Z}$. In the former case $s = d(q + 1) - a - b$, and hence $bP_0 \sim bP_\infty$. Since $b \leq q$, we deduce (see Lemma[20]) $b = 0$, which contradicts our assumptions (Remark[8]). In the latter case we have $d(q + 1)P_\infty - aP_\infty - bP_0 \sim d(q + 1)P_0 - aP_\infty - bP_0$. Since $(q + 1)P_\infty \sim (q + 1)P_0$ (see Section[2]), we deduce $aP_\infty \sim aP_0$ and then (Lemma[20] again) $a = 0$. 


Since we assumed \( b \neq 0 \) (Remark 8) and a canonical divisor \( K \) on \( X \) has degree \( q^2 - q - 2 \), we immediately see that if \( d < q - 1 \) then \( C(d,a,b) \) is of group (G1), for any choice of \( 0 \leq a \leq b \leq q \). If \( d = q - 1 \) and \( a \neq 0 \) then \( C(d,a,b) \) could be either in group (G1), or in group (G2). Indeed, \((q - 1)(q + 1) - a - b \leq q^2 - 2\) for any \( 1 \leq a \leq b \leq q \) and group (G3) is excluded by Remark 21. On the other hand, \( C(q - 1,0,b) \) is always in group (G3), because \( q^2 - q - 2 \leq (q - 1)(q + 1) - b \leq q^2 - 2 \) for any \( 1 \leq b \leq q \). This proves that in order to complete our study of case \( d = q - 1 \) we can analyse separately the codes \( C(q-1,a,b) \) of group (G2), which satisfy \( 1 \leq a \leq b \leq q \), and the codes of the form \( C(q - 1,0,b) \) (obviously \( b \leq q \)), which are in group (G3). Note that in case \( d = q - 1 \) our usual assumption \( d > 2 \) is equivalent to \( q > 3 \).

4.1. Codes \( C(q - 1,a,b) \) of group (G2). In the following Remark 22 we give a characterization of the codes \( C(q - 1,a,b) \) of group (G2).

**Remark 22.** A code \( C(q - 1,a,b) \) of group (G2) satisfies (combining Remark 8 and Remark 21) \( 1 \leq a \leq b \leq q \). The condition of being in group (G2) is

\[
q^2 - q - 2 \leq (q - 1)(q + 1) - a - b \leq q^2 - 2,
\]

which is equivalent to \( a + b \leq q + 1 \) (the right-hand side condition always holds).

Now consider the linear equivalence

\[
(q - 1)(q + 1)P_\infty - aP_\infty - bP_0 \sim (q - 2)(q + 1)P_\infty + (q + 1 - a)P_\infty - bP_0
\]

\[
\sim K + (q + 1 - a)P_\infty - bP_0
\]

and apply Theorem 4 with \( m = q + 1 - a \), \( n = -b \), \( m_0 = 1 \), \( m_1 = a \), \( n_0 = 0 \) and \( n_1 = b \). Since we assumed \( a \leq b \) and Remark 22 holds, only Park’s cases (1), (3) and (4) of Theorem 4 are of our interest. The dual minimum distance, say \( \delta(q - 1,a,b) \), of a code \( C(q - 1,a,b) \) of group (G2) can be read in Table I.

| Park’s case \( \rightarrow \) | (1) | (3) | (4) |
|-----------------------------|-----|-----|-----|
| \( \delta(q - 1,a,b) \)    | \( q + 1 - a - b \) | \( q - a \) | \( q - 1 \) |

**Table 1.** Dual minimum distance of a code \( C(q - 1,a,b) \) of group (G2).

**Theorem 23.** Let \( C(q - 1,a,b) \) be a code of group (G2) (conditions \( d = q - 1 > 2 \), \( 1 \leq a \leq b \leq q \) and \( a + b \leq q + 2 \) will be implicitly assumed). Let \( \delta := \delta(q - 1,a,b) \) be the dual minimum distance of \( C(q - 1,a,b) \), and let \( S := \{ P_1, \ldots, P_\delta \} \) be the support of a minimum-weight codeword. Then one of the following cases occurs.

(a) \( P_1,\ldots, P_\delta \) lie on the line through \( P_0 \) and \( P_\infty \).

(b) \( P_\infty, P_1,\ldots, P_\delta \) are collinear.

(c) \( P_0, P_1,\ldots, P_\delta \) are collinear.

**Proof.** Let us examine separately cases (1), (3) and (4) of Theorem 5. In the notation of Proposition 17 set \( a_1 := a, a_2 := b, d := q - 1, E := aP_\infty + bP_0 \), and define \( E' \) and \( d' \) as in the statement.

---

2Any smooth plane curve of degree \( c \) has genus \( g(X) = (c - 1)(c - 2)/2 \). The degree of a canonical divisor \( K \) on \( X \) is always \( 2g(X) - 2 \). Remember that the Hermitian curve has degree \( q + 1 \).
(1) If $C(q - 1, a, b)$ is described by case (1) of Theorem\textsuperscript{5} then $a, b \leq 1$. Hence $a = b = 1$ and the dual minimum distance is $\delta = q - 1$ (see Table\textsuperscript{1}). Since $d > 2$, we have $E' = E$ and $d' = d$. Notice that $\deg(E') + \sharp(S) = q - 1 + 2 = q + 1 = d + 2$ and Proposition\textsuperscript{18} applies: there exists a subscheme $W \subseteq P_\infty + P_0 \cup \{P_1, \ldots, P_{q-1}\}$ of degree $q + 1$ and contained in a line. This means that $P_1, \ldots, P_{q-1}$ lie on the line through $P_\infty$ and $P_0$.

(2) If $C(q - 1, a, b)$ is described by case (3) of Theorem\textsuperscript{5} then $0 \leq a \leq 1 < b$. Hence $a = 1$.

(2.i) If $b < q$, then $d' = d$, $E' = E$ and the dual minimum distance is $\delta = q - a = q - 1$. Notice that $\deg(E') + \sharp(S) = (q - 1) + (1 + b) = q + b = d + 1 + b$, and Proposition\textsuperscript{18} applies: there exists a subscheme $W \subseteq P_\infty + bP_0 \cup \{P_1, \ldots, P_{q-1}\}$ of degree $q + 1$ and contained in a line. By Lemma\textsuperscript{10}, $P_0$ must appear in $W$ with multiplicity exactly one and $P_1, \ldots, P_{q-1}$ lie on the line through $P_\infty$ and $P_0$.

(2.ii) If $b = q = d + 1$, then $d' = d - 1$, $E' = P_\infty$ and the dual minimum distance is $\delta = q - a = q - 1$. Since $\deg(E') + \sharp(S) = q - 1 + 1 = q - d' = 2d + 2$, Proposition\textsuperscript{18} applies and there exists a subscheme $W \subseteq P_\infty \cup \{P_1, \ldots, P_{q-1}\}$ of degree $d' + 2 = q$ and contained in a line. In other words, the points $P_\infty, P_1, \ldots, P_d$ turn out to be collinear.

(3) If $C(q - 1, a, b)$ is described by case (4) of Theorem\textsuperscript{5} then $1 < a \leq b < q$. In particular, $b \leq d, d' = d$ and $E' = E$. The dual minimum distance is $\delta = q - 1$ and $\deg(E) + \sharp(S) = q - 1 + a + b = d + a + b \leq d + (q + 1) = 2d + 2$. Hence Proposition\textsuperscript{18} applies: either there exists a subscheme $W \subseteq aP_\infty + bP_0 \cup \{P_1, \ldots, P_{q-1}\}$ of degree $q + 1$ and contained in a line $L$, or there exists a subscheme $W \subseteq aP_\infty + bP_0 \cup \{P_1, \ldots, P_{q-1}\}$ of degree $2q$ and contained in a conic $T$. In the former case, Lemma\textsuperscript{10} implies that $P_\infty$ and $P_0$ appear in $W$ with multiplicity exactly one, and so $P_1, \ldots, P_{q-1}$ lie on the line through $P_\infty$ and $P_0$. In the latter case it is immediately seen that $W = aP_\infty + bP_0 + \sum_{i=1}^{q-1} P_i$. Since $\deg(W) = 2q$, we have $a + b = q + 1$. Since our general assumption $d = q - 1 > 2$ holds, it follows $\min\{a, b\} > 2$ and so either $L_{X, P_\infty} \subseteq T$, or $L_{X, P_0} \subseteq T$ (Lemma\textsuperscript{11}). In any case, by Lemma\textsuperscript{10}, either $P_0, P_1, \ldots, P_{q-1}$ are collinear, or $P_\infty, P_1, \ldots, P_{q-1}$ are collinear.

This concludes our proof. \hfill \square

4.2. Codes $C(q - 1, 0, b)$ of group (G3). If $C(q - 1, 0, b)$ is a code of group (G3) (i.e., $d = q - 1 > 2$, $a = 0$, $1 \leq b \leq q$), then its minimum distance, $\delta(q - 1, 0, b)$, is given by Theorem\textsuperscript{5}. Indeed, choose $m = (q - 1)(q + 1), m_0 = q - 1, m_1 = 0, n = -b, n_0 = -1, n_1 = q + 1 - b$, and compute $\delta(q - 1, 0, b) = q$. Let $S := \{P_1, \ldots, P_q\}$ be the support of a minimum-weight codeword. In the notation of Proposition\textsuperscript{17}, set $a_1 := 0, a_2 := b, E := bP_0$ and define $d'$ and $E'$ as in the statement of cited proposition. If $b \leq d = q - 1$, then $E' = E$ and $\deg(E) + \sharp(S) \leq q - 1 + q = 2q - 1 = 2d + 1$. Hence Proposition\textsuperscript{18} applies and gives a zero-dimensional scheme $W \subseteq bP_0 \cup \{P_1, \ldots, P_q\}$ of degree $q + 1$ and contained in a line. By Lemma\textsuperscript{10}, the multiplicity of $P_0$ in $W$ must be exactly one, and then $P_0, P_1, \ldots, P_q$ lie on $L$. If $d = q$, then $E' = 0$ and $d' = d - 1 = q - 2$. Since $\deg(E') + \sharp(S) = q = d + 1$, Proposition\textsuperscript{18} applies: there exists a $W \subseteq \{P_1, \ldots, P_q\}$ of degree $d' + 2 = (d - 1) + 2 = q$ and contained in a line. It follows that the points $P_1, \ldots, P_q$ are collinear.

Let us summarize the previous analysis in the following concise result.

**Theorem 24.** Consider a code $C(q - 1, 0, b)$ of group (G3). Its dual minimum distance is $q$. Let $\{P_1, \ldots, P_q\}$ be the support of a minimum-weight codeword. Then $P_1, \ldots, P_q$ are collinear. Moreover, if $b \leq q - 1$, then $P_0, P_1, \ldots, P_q$ are collinear.

\footnote{The case $\deg(W) \geq 2d + 2 = 2q$ implies $b \geq q$, which contradicts our hypothesis on $b$.}
5. Computational Examples

When \( q \) is small, our results can be checked by writing simple MAGMA programs (see the homepage [http://magma.maths.usyd.edu.au](http://magma.maths.usyd.edu.au)).

**Example 25.** Let \( q = 4 \) (\( q^2 = 16 \)) and let \( X \) be the Hermitian curve defined over \( \mathbb{F}_{16} \) by the affine equation \( y^4 + y = x^5 \). Consider the Hermitian two-point code \( C \) obtained evaluating the vector space \( L(10P_\infty + 3P_0) \) on \( X(\mathbb{F}_{16}) \backslash \{ P_\infty, P_0 \} \) (here \( P_\infty \) and \( P_0 \) are those defined in Section 2). Write \( 10P_\infty + 3P_0 \sim d(q + 1)P_\infty - aP_\infty - bP_0 \) with \((a, b) = (3, 0, 2)\). Note that \( 0 \leq a \leq b \leq q \) and \( d = q - 1 \). Hence our code \( C \) is in fact the code \( C(3, 0, 1) \), with \( q = 4 \), described by Theorem 24. If \( \mathbb{F}_{16} = \langle \alpha \rangle \) and \( \alpha^4 + \alpha + 1 = 0 \) then a (random) minimum-weight codeword of \( C^\perp \) is
\[
\begin{align*}
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, \\
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
\end{align*}
\]
with support made of the points of affine coordinates
\[
P_1 := (\alpha^7, \alpha^7), \quad P_2 := (\alpha^{11}, \alpha^{11}), \quad P_3 := (\alpha^{13}, \alpha^{13}), \quad P_4 := (\alpha^{14}, \alpha^{14}).
\]
Notice that the points are in fact four (Table 1 says that the dual minimum distance of \( C \) has to be 4) and they lie, together with \( P_0 \), on the line defined over \( \mathbb{F}_{16} \) by the homogeneous equation \( x - y = 0 \), as described in Theorem 24.

**Example 26.** In the same notations of Example 25, choose \( q = 5 \) and \((d, a, b) = (4, 1, 1)\). Notice that \( d = q - 1 \) and \( b = 1 \). Hence \( C(4, 1, 1) \) (with \( q = 5 \)) is described by Theorem 23. From the proof we get that the dual minimum distance must be \( q - 1 = 4 \) and points \( P_1, P_2, P_3, P_4 \) of the support of a minimum-weight codeword must lie on the line through \( P_0 \) and \( P_\infty \) (whose equation is \( x = 0 \)). If \( \mathbb{F}_{125} = \langle \beta \rangle \) (with \( \beta^2 + 4\beta + 2 = 0 \)) and we compute the support of a (random) minimum-weight codeword of \( C(4, 1, 1) \perp \), we find out the points of affine coordinates
\[
P_1 := (0, \beta^3), \quad P_2 := (0, \beta^9), \quad P_3 := (0, \beta^{15}), \quad P_4 := (0, \beta^{21}).
\]
As one can easily see, they all lie on the line of equation \( x = 0 \).

6. Conclusions

In this paper we geometrically describe the supports of the minimum-weight codewords of the duals of two-point codes from the Hermitian curve. We use a geometric approach, characterizing the dual minimum distance in terms of non-vanishing conditions on cohomology groups and zero-dimensional schemes in the plane.

Acknowledgement

The authors would like to thank the referees for suggestions that improved the presentation of this work.

**References**

[1] E. Ballico, A. Ravagnani, *A zero-dimensional cohomological approach to Hermitian codes*. [http://arxiv.org/abs/1202.0894](http://arxiv.org/abs/1202.0894)

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

[3] A. Bernardi, A. Gimigliano, M. Ida, *Computing symmetric rank for symmetric tensors*. Journal of Symbolic Computation 46(1), 34–53 (2011).

[4] D. Bernstein, T. Lange, C. Peters, *Attacking and defending the McEliece cryptosystem*. Proceedings of the 2nd International Workshop on Post-Quantum Cryptography. Lecture Notes in Computer Science 5299: 31 – 46.
[5] A. Canteaut, N. Sendrier, Cryptanalysis of the Original McEliece Cryptosystem. Advances in Cryptology – ASIACRYPT98, Kazuo Ohta and Dingyi Pei (eds).
[6] A. Couvreur, The dual minimum distance of arbitrary dimensional algebraic-geometric codes. Journal of Algebra 350(1), 84–107 (2012).
[7] I. M. Duursma, R. Kirov, Improved Two-Point Codes on Hermitian Curves. IEEE Transactions on Information Theory, 57(7), 4469–4476 (2011).
[8] P. Ellia, C. Peskine, Groupes de points de $\mathbf{P}^2$: caractère et position uniforme. Algebraic geometry (L’Aquila, 1988), 111 – 116, Lecture Notes in Mathematics, 1417, Springer Berlin, 1990.
[9] V. D. Goppa, A new class of linear error correcting codes. Problemy Peredachi Informatsii, Vol. 6, 24 – 30 (1970).
[10] J. W. P. Hirschfeld, Projective Geometries over Finite Fields. Clarendon Press, Oxford, 1979.
[11] J. W. P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field. Princeton University Press, 2008.
[12] M. Homma, S. J. Kim, The Two-point Codes on a Hermitian Curve with the Designed Minimum Distance. Designs, Codes and Cryptography, 38, 55–81 (2006).
[13] M. Homma, S. J. Kim, The two-point codes with the designed distance on a Hermitian curve in even characteristic. Designs, Codes and Cryptography, 39, 375–386 (2006).
[14] M. Homma, S. J. Kim, Toward the Determination of the Minimum Distance of Two-Point Codes on a Hermitian Curve. Designs, Codes and Cryptography, 37, 111–132 (2005).
[15] C. Marcolla, M. Pellegrini, M. Sala On the weights of affine-variety codes and some Hermitian codes. WCC 2011 - Workshop on coding and cryptography, 273 – 282 (2011).
[16] H. Maharaj, G. L. Matthews, G. Pirsic, Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences. Journal of Pure and Applied Algebra, 195(3), 261–268 (2005).
[17] R. J. McEliece, A Public-Key Cryptosystem Based On Algebraic Coding Theory. Jet Propulsion Laboratory, DSN Progress Report (1978) 114-116.
[18] C. Munuera, R. Pellikaan, Equality of geometric Goppa codes and equivalence of divisors. Journal of Pure and Applied Algebra, 90, 229–252 (1993).
[19] S. Park, Minimum distance of Hermitian two-point codes. Designs, Codes and Cryptography, 57, 195–213 (2010).
[20] S. A. Stepanov, Codes on Algebraic Curves. Springer, 1999.
[21] H. Stichtenoth, A Note on Hermitian Codes over $GF(2)$. IEEE Transactions on Information Theory, 34, 1345 – 1348 (1988).
[22] H. Stichtenoth, Algebraic function fields and codes. Second Edition. Springer-Verlag, 2009.