The Geometry of Hermitian two-point codes

E. Ballico, A. Ravagnani, M. Sala

Workshop BunnyTn3

The Hermitian curve

The Hermitian curve

The Hermitian curve

$$X \subseteq \mathbb{P}^2$$

is the projective smooth curve defined over $\mathbb{F}_{q^2}$ by the affine equation

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

The Hermitian curve

The Hermitian curve

$$X \subseteq \mathbb{P}^2$$

is the projective smooth curve defined over $\mathbb{F}_{q^2}$ by the affine equation

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

This curve has a very particular geometry.

The Hermitian curve

1. X is maximal (Hasse-Weil) with

$$|X(\mathbb{F}_{q^2})| = q^3 + 1$$

and only one point at infinity,

$$P_\infty = (0 : 1 : 0).$$

2. For any $P \in X(\mathbb{F}_{q^2})$ we get an isomorphism of shaves

$$\mathcal{O}_X(1) \cong \mathcal{L}((q+1)P).$$

The Hermitian curve

3. Every line $L \subseteq \mathbb{P}^2$

The Hermitian curve

3. Every line $L \subseteq \mathbb{P}^2$
   - either is tangent to X at a point $P \in X(\mathbb{F}_{q^2})$, with contact order $q+1$, and does not intersect X in any other $\mathbb{F}_{q^2}$-rational point,
   - or it intersects X in $q+1$ distinct $\mathbb{F}_{q^2}$-rational points.

The Hermitian curve

3. Every line $L \subseteq \mathbb{P}^2$
   - either is tangent to X at a point $P \in X(\mathbb{F}_{q^2})$, with contact order $q+1$, and does not intersect X in any other $\mathbb{F}_{q^2}$-rational point,
   - or it intersects X in $q+1$ distinct $\mathbb{F}_{q^2}$-rational points.
4. The group of automorphisms of X is 2-transitive.

Two-point codes

Two-point codes

Choose

Two-point codes

Choose

- two distinct points $P, Q \in X(\mathbb{F}_{q^2})$,

Two-point codes

Choose

- two distinct points $P, Q \in X(\mathbb{F}_{q^2})$,
- a pair of integers (m, n) such that $m + n > 0$

Two-point codes

Choose

- two distinct points $P, Q \in X(\mathbb{F}_{q^2})$,
- a pair of integers (m, n) such that $m + n > 0$

and consider the code

$$C(m, P, n, Q)$$

obtained **evaluating** the vector space

$L(mP + nQ)$ on the set $X(\mathbb{F}_{q^2}) \setminus \{P, Q\}$.

A standard assumption

A standard assumption

Remark

By the 2-transitivity of $\mathrm{Aut}(X)$ we may assume in $C(m, P, n, Q)$

$$P = P_\infty = (0 : 1 : 0), \qquad Q = P_0 = (0 : 0 : 1).$$

Known results

Known results

- 2006-07: Homma and Kim find the minimum distance of any $C(m, P_\infty, n, P_0)$.
- 2010: Park gives explicit formula for the minimum distance of any $C(m, P_\infty, n, P_0)^\perp$.

Our interpretation of two-point codes

Our interpretation of two-point codes

Lemma

Given a two-point code $C(m, P_\infty, n, P_0)$ on X, there exists a tern of integers (d, a, b) with

$$d > 0, \qquad 0 \leq a, b \leq d, \qquad E := aP_\infty + bP_0$$

such that $C(m, P_\infty, n, P_0)$ is the code obtained evaluating

$$H^0(X, \mathcal{O}_X(d)(-E)) \quad \text{on} \quad X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}.$$

Our interpretation of two-point codes

Lemma

Given a two-point code $C(m, P_\infty, n, P_0)$ on X, there exists a tern of integers (d, a, b) with

$$d > 0, \qquad 0 \leq a, b \leq d, \qquad E := aP_\infty + bP_0$$

such that $C(m, P_\infty, n, P_0)$ is the code obtained evaluating

$$H^0(X, \mathcal{O}_X(d)(-E)) \quad \text{on} \quad X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}.$$

We denote this code by $C(d, a, b)$ and assume $b \neq 0$
(if $b = 0$ then the code is a one-point code).

The proof of the Lemma is based on

1. the isomorphisms of sheaves

$$\mathcal{O}_X(1) \cong \mathcal{L}((q+1)P_\infty) \cong \mathcal{L}((q+1)P_0),$$

2. the geometry of the **tangent lines** to X.

Evaluation codes on arbitrary curves

How to study codes like $C(d, a, b)$?

Evaluation codes on arbitrary curves

How to study codes like $C(d, a, b)$?

The key-result is a characterization of the

support

of any codeword of certain Goppa codes on arbitrary curves.

Theorem

Let K be a finite field and let $X \subset \mathbb{P}^2_K$ be a smooth plane curve of degree c. Fix an integer $d > 0$, a zero-dimensional scheme $E \subset X$ and a finite subset $B \subset X(K)$ such that $B \cap E_{\mathrm{red}} = \emptyset$. Let C be the code obtained evaluating $H^0(X, \mathcal{O}_X(d)(-E))$ on B. Assume $\sharp(B) > dc$.

The minimum distance of $C^\perp$ is the minimal cardinality, say s, of a subset $S \subseteq B$ such that $h^1(\mathbb{P}^2, \mathcal{I}_{S \cup E}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_E(d))$. A codeword of $C^\perp$ has weight w if and only if it is supported by an $S \subseteq B$ such that

1. $\sharp(S) = w$,
2. $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_E(d))$,
3. $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S'}(d))$ for any $S' \subsetneq S$.

The case of Hermitian two-point codes

The case of Hermitian two-point codes

Combining the Theorem and other geometric properties of the Hermitian curve we get the following result.

Corollary

Let X be the Hermitian curve and choose integers

$$0 < d \leq q, \quad 0 \leq a, b \leq d.$$

Set $E := aP_\infty + bP_0$. Denote by $C(d, a, b)$ the code obtained evaluating $H^0(X, \mathcal{O}_X(d)(-E))$ on $B := X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}$ and let δ be the minimum distance of $C(d, a, b)^\perp$. A subset $S \subseteq B$ of cardinality δ is the support of a minimum-weight codeword of $C(d, a, b)^\perp$ if and only if

$$h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0.$$

The key-condition

$$\boxed{h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) > 0}$$

can be described in a purely geometric way, **extending** the recent results by Couvreur on the minimum distance of certain Goppa codes.

The main result

The main result

Corollary

Let X be the Hermitian curve and choose integers

$$0 < d \leq q, \qquad 0 \leq a, b \leq d.$$

Set $E := aP_\infty + bP_0$. Denote by $C(d, a, b)$ the code obtained evaluating $H^0(X, \mathcal{O}_X(d)(-E))$ on $B := X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}$. Let δ be the minimum distance of $C(d, a, b)^\perp$. Assume

$$a + b + \delta \leq 4d - 5.$$

Let $S \subseteq B$ be a set of cardinality δ. Then S is the support of a minimum-weight codeword of $C(d, a, b)^\perp$ if and only if there exists a subscheme $W \subseteq E \cup S$ with one of the following properties.

List of possible cases

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

Our main result

Our main result

Combining this last result with the geometry of the Hermitian curve we **characterized** all the possible supports of a minimum-weight codeword of any $C(d,a,b)^{\perp}$ such that

$$5 < d \leq q,$$

for **any** choice of q.

Here you are some explicit examples.

Example 1

Consider a code $C(d, a, b)$ such that

Example 1

Consider a code $C(d,a,b)$ such that

1. $d > 2$,
2. $1 \leq a, b \leq d$,
3. $d(q+1) - a - b < q^2 - q - 2 \quad$ (in particular, $d \leq q-1$),
4. $a + b < 2d$.

The minimum distance of $C(d, a, b)^\perp$ is d.

The minimum distance of $C(d,a,b)^\perp$ is d.

Let $L_{0,\infty}$ denote the line through P_0 and P_∞. A subset

$$S \subseteq X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}$$

is the support of a minimum-weight codeword of $C(d,a,b)^\perp$

if and only if

The minimum distance of $C(d,a,b)^{\perp}$ is d.

Let $L_{0,\infty}$ denote the line through P_0 and P_∞. A subset

$$S \subseteq X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}$$

is the support of a minimum-weight codeword of $C(d,a,b)^{\perp}$

if and only if

1. $\sharp(S) = d$,
2. $S \subseteq L_{0,\infty}$.

Corollary

Let $C(d, a, b)$ be a code such that

1. $d > 2$,
2. $1 \leq a, b \leq d$,
3. $d(q+1) - a - b < q^2 - q - 2$,
4. $a + b < 2d$.

Then the minimum distance of $C(d, a, b)^{\perp}$ is d and the number of the minimum-weight codewords of $C(d, a, b)^{\perp}$ is

$$(q^2 - 1)\binom{q-1}{d}.$$

Example 2 (small-weight codewords)

Example 2 (small-weight codewords)

Corollary

Consider a code $C(d, a, b)$ such that

$$0 < d \leq q - 2.$$

Example 2 (small-weight codewords)

Corollary

Consider a code $C(d, a, b)$ such that

$$0 < d \leq q - 2.$$

Let w be an integer such that

$$d \leq w \leq \min\{3d - a - b, 2d - 3\}.$$

Example 2 (small-weight codewords)

Corollary

Consider a code $C(d, a, b)$ such that

$$0 < d \leq q - 2.$$

Let w be an integer such that

$$d \leq w \leq \min\{3d - a - b, 2d - 3\}.$$

The supports of a codeword of $C(d, a, b)^\perp$ of weight w are exactly the sets in the following list.

List of possible cases

1. Any subset of w elements of $L_{0,\infty} \cap X(\mathbb{F}_{q^2}) \setminus \{P_0, P_\infty\}$, where $L_{0,\infty}$ is the line through P_0 and P_∞.
2. Any subset of w elements of $L \cap X(\mathbb{F}_{q^2}) \setminus \{P_0, P_\infty\}$, where L is any line through P_0 which is not tangent to X (only if $w \geq d + 1$).
3. Any subset of w elements of $L \cap X(\mathbb{F}_{q^2}) \setminus \{P_0, P_\infty\}$, where L is any line through P_∞ which is not tangent to X (only if $w \geq d + 1$).
4. Any subset of w elements of $L \cap X(\mathbb{F}_{q^2}) \setminus \{P_0, P_\infty\}$, where L is any line which is not tangent to X and such that $P_0, P_\infty \notin L$ (only if $w \geq d + 2$).

Example 3 (smooth conics)

Consider a code $C(d,a,b)$ such that

Example 3 (smooth conics)

Consider a code $C(d, a, b)$ such that

1. $d = q > 3$,
2. $2 < a \leq b < d = q$,
3. $a + b < d + 2$.

The minimum distance of $C(d, a, b)^{\perp}$ is $2d - 2 = 2q - 2$.

The minimum distance of $C(d,a,b)^{\perp}$ is $2d-2=2q-2$.

The points in the support of any minimum-weight codeword of $C(d,a,b)^{\perp}$ lie on a smooth conic which is tangent to the Hermitian curve X at both P_0 and P_{∞}.