Linear codes from Hermitian curves

Korchmáros Gábor

Università degli Studi della Basilicata, Olaszország

közös munka Pietro Speziali doktorandusszal

Kerékjártó Béla szeminárium

2015 szeptember 9
Bolyai Intézet Szeged

1-point Hermitian code from Hermitian Curve

- $\mathcal{X}$:= Hermitian curve of genus $g = \frac{1}{2}(q^2 - q)$ and with (affine) equation $H(X, Y) = Y^q + Y - X^{q+1} = 0$, defined over $\mathbb{F}_{q^2}$.
- $\mathcal{X}(\mathbb{F}_{q^2})$:= set of all points of $\mathcal{X}$ on $PG(2, q^2)$.
- $|\mathcal{X}(\mathbb{F}_{q^2})| = q^3 + 1$, $\mathcal{X}$ has exactly one point at infinity, P_∞;
- $\mathtt{D} := \mathcal{X}(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$; $\mathtt{D} = \{Q_1, Q_2, \ldots, Q_n\}$ with $n = q^3$.
- Fix an integer m such that $1 \le m \le q$;
- $\Phi_m := \{f | f \in \mathbb{F}_{q^2}[X, Y], \deg f \le m\}$; Φ_m is an $\mathbb{F}_{q^2}$-vector space of dimension $m + 1$.
- The evaluation map

$$\mathrm{ev} = \begin{cases} \Phi_m \mapsto V(n, q^2), \\ f \in \Phi_m \mapsto (f(Q_1), \ldots, f(Q_n)) \in V(n, q^2), \end{cases}$$

- is injective. $\mathrm{ev}(\Phi_\mathrm{m})$ is an $m + 1$-dimensional subspace $C_{\mathcal{L}}(\mathtt{D}, mP_\infty)$ of $V(n, q^2)$.
- In coding theory terms: $C_{\mathcal{L}}(\mathtt{D}, P_\infty)$ is a **functional** (or **evaluation**) code, and its **codewords** are the vectors in $C_{\mathcal{L}}(\mathtt{D}, P_\infty)$;

1-point Hermitian code

- *weight* of a codeword $\omega(\mathrm{ev}(f)) :=$ number of the non-zero coordinates of $(\mathrm{ev}(\mathrm{f}))$;
- $\omega(\mathrm{ev}(f)) \geq n - m(q+1)$ and "$=$" is attained;
- In coding theory terms: minimum distance of $C_{\mathcal{L}}(D, mP_\infty) = n - m(q+1) = q^3 - m(q+1)$;
- $C_{\mathcal{L}}(\mathtt{D}, mP_\infty)$ is the *1-point Hermitian code*;
- *How to generalize this construction?*
- Replace the (unique) point P_∞ of $\mathcal{X}$ at infinity by a subset Ω of points in $\mathcal{X}(\mathbb{F}_{q^2})$, and
- Consider not only polynomials but also rational functions defined on $\mathtt{D} = \mathcal{X}(\mathbb{F}_{q^2}) \setminus \Omega$.

Functional Goppa codes from Hermitian curve

- $\mathbb{F}_{q^2}(\mathcal{X})$:= function field of $\mathcal{X}$ over $\mathbb{F}_{q^2}$;
- Divisor:= a finite (formal) sum of places of $\mathbb{F}_{q^2}(\mathcal{X})$;
- Principal divisor:= $\mathrm{Div}(f) = \sum n_P P$ where
- $n_P > 0$ if f has a zero of multiplicity n_p at P, $n_p < 0$ if f has a pole of multiplicity $-n_P$,
- $\mathtt{G}$:= divisor of $\mathbb{F}_{q^2}(\mathcal{X})$; $\Omega := \mathrm{supp}(\mathtt{G})$;
- $\mathtt{D}$:=$\mathbb{F}_{q^2}(\mathcal{X}) \setminus \Omega$, $n := |\mathtt{D}|$;
- $\mathcal{L}(\mathtt{G}) := \{f \mid \mathrm{Div}(f) \succeq -\mathtt{G},\ f \in \mathbb{F}_{q^2}(\mathcal{X})\} \cup \{0\}$, RR space;
- **Functional code**:
  $C_{\mathcal{L}}(\mathtt{D},\mathtt{G}) := \{(f(Q_1),\ldots,f(Q_n)) | f \in \mathcal{L}(\mathtt{G})\}$,
- **length**$(C_{\mathcal{L}}(\mathtt{D},\mathtt{G})) = n$,
- **dim** $C_{\mathcal{L}}(\mathtt{D},\mathtt{G}) \geq \deg(\mathtt{G}) - g + 1 = \deg(\mathtt{G}) - \frac{1}{2}(q^2 - q + 2)$.
- **minimum distance of** $C_{\mathcal{L}}(\mathtt{D},\mathtt{G}) \geq \delta$ with $\delta := n - \deg(\mathtt{G})$,
- ($\delta :=$ **Goppa designed minimum distance**)

The geometry of the Riemann-Roch space

- Divisor: formal sum of points on $\mathcal{X}$: $U = \sum n_Q Q \ n_Q \in \mathbb{Z}$.
- $U \succeq V$ if $n_Q(U) \geq n_Q(V)$ for every $Q \in \mathcal{X}$.
- Intersection multiplicity of $\mathcal{X}$ and a curve C at a point Q: $I(\mathcal{X} \cap C, Q)$.
- Intersection divisor: If $\mathcal{X}$ is not a component of C then $\mathcal{X} \cap C = \{R_1, \ldots, R_m\}$ and

$$\mathcal{X} \cdot C = \sum_{i=1}^{m} I(\mathcal{X} \cap C, Q_i) Q_i.$$

- Bézout's theorem: If $\mathcal{X}$ is not a component of C then

$$(q+1) \deg C = \sum_{i=1}^{m} I(\mathcal{X} \cap C, Q_i).$$

- Nöther AB+FD theorem: $\mathcal{G} := G(X,Y) = 0, \mathcal{T} := T(X,Y) = 0$. If $\mathcal{X} \cdot \mathcal{T} \succeq \mathcal{X} \cdot \mathcal{G}$ then

$$T(X,Y) = A(X,Y)H(X,Y) + B(X,Y)G(X,Y).$$

Goppe codes from Baer subconic, q odd

- C_2: parabola with equation $y = \frac{1}{2}x^2$,
- $C_2 \cap \mathcal{X} = \{P_1, \ldots, P_{q+1}\}$ where $P_1, \ldots, P_{q+1}$ are the points of $\mathcal{X}$ (and C_2) over $\mathbb{F}_q$,
- $\Omega = C_2 \cap \mathcal{H}$ is a Baer subconic,
- $\mathtt{G} := m\mathtt{P}$ with $\mathtt{P} = P_1 + \ldots + P_{q+1}$ and $m \geq 1$,
- $\mathtt{D} := \mathcal{X}(\mathbb{F}_{q^2}) \setminus \Omega$, $Length(C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})) = q^3 - q$,
- $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})/\mathbb{F}_{q^2} \cong PG(r-1, q^2)$ with $r = \dim C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$,
- Choose a curve $\mathcal{F}$ such that $\mathcal{F} \cdot \mathcal{X} \succeq mP$. Let $t = \deg \mathcal{F}$.
- $\mathbf{S}_t$:= linear system of all degree t plane algebraic curves (possible singular, or reducible) defined over $\mathbb{F}_{q^2}$ which do not have $\mathcal{X}$ as a component.
- $\mathbf{\Sigma}_t$:= subset of $\mathbf{S}_t$ consisting of all curves $\mathcal{H}$ such that $\mathcal{H} \cdot \mathcal{X} \succeq \mathcal{F} \cdot \mathcal{X} - mP$.

The minimum distance problem for $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$ is equivalent to the problem of determining the maximum number N of common points of $\mathtt{D}$ and $\mathcal{H}$ with $\mathcal{H}$ ranging over $\mathbf{\Sigma}_t$.

Parameters of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$

$C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$ has length $n = q^3 - q$ and, for $m \le q^2 - q$, has dimension $k =$

$$\begin{cases} \frac{1}{2}\, m(m+3)+1; \text{if } m \text{ even, } m \le q-2; \\ \frac{1}{2}(m-1)(m-2)+1; \text{ if } m \text{ odd, } 0 < m \le \frac{1}{2}(q-1); \\ \frac{1}{2}(m-1)(m-2)+1+2(m+1)-q; m \text{ odd, } \frac{1}{2}(q-1) < m \le q-2; \\ m(q+1)+\frac{1}{2}q(q-1)+1; \text{if } q-2 < m < q^2-q. \end{cases}$$

If $q^2 - q < m \le q^2 - 3$, a bound for k is

$$q^3 - q + \frac{1}{2}q(q-1) + 1 \le k \le m(q+1) - \frac{1}{2}(q^2-q) - \frac{1}{2}r(r+3),$$

where $t = m$ or $t = m+1$ according as m is even or odd, and $r = t - (q^2 - q + 1)$.

Minimum distance of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$

$C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$ has, for $m \le q-2$, minimum distance d equal to

$$\begin{cases} (q+1)(q^2-q-m) = \delta, \text{if } m \text{ even and, } m \le q-2; \\ (q+1)(q^2-q-m) = \delta, \text{if } m \text{ odd, } m \le \frac{1}{2}(q-1); \\ (q+1)(q^2-q-m+1) = \delta+q+1; \text{if } m \text{ odd, } \frac{1}{2}(q-1) < m \le q-2 \end{cases}$$

If $q-2 < m \le q^2-q$, a lower bound for d is

$$d \ge (q+1)(q^2-q-m)$$

and equality holds if either m is odd, or m is even and $m \le q^2 - \frac{1}{2}(3q+1)$. If $q^2-q < m \le q^2-3$, a lower bound for d is

$$d \ge q-1.$$

Automorphisms of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$

Permutation automorphism is (α, β) where α is an injective map on $\mathcal{L}(m\mathtt{P})$ and β is a permutation on $\mathtt{D}$, s.t.

$$\alpha(f)(Q) = f(\beta(Q)) \text{ for all } f \in \mathcal{L}(m\mathtt{P}) \text{ , } Q \in \mathtt{D}.$$

Theorem

Every automorphism of $\mathcal{X}$ fixing Ω defines a permutation automorphism of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$;

Remark

This holds true for every Goppa-code.

Theorem

The permutation automorphism group of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$ is isomorphic to the projective linear group $PGL(2, q)$.

Automorphisms of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$, cont.

Monomial automorphism is (α, β, γ) where α is an injective map on $\mathcal{L}(m\mathtt{P})$, β is permutations on $\mathtt{D}$ and γ is a map from $\mathtt{D}$ into $\mathbb{F}_{q^2}$ such that

$$\alpha(f)(P) = \gamma(P)f(\beta(P)) \text{ for all } f \in \mathcal{L}(m\mathtt{P}),\ P \in \mathtt{D}. \qquad (1)$$

Theorem

The group generated by the permutation, monomial and semilinear automorphisms of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$ is isomorphic to the semidirect product of $P\Gamma L(2, q)$ by a cyclic group of order $q^2 - 1$.

Automorphisms of $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$ cont.

In the literature, the concept of an automorphism of Goppa codes (and any linear codes) is confined to the above three types.

(most general) automorphism of a linear code $[n, k, d]_q$ is a Hamming-distance preserving permutation of vectors which takes codeword to codeword.

If an automorphism is linear then it is monomial.

Open problem Does $C_{\mathcal{L}}(\mathtt{D}, m\mathtt{P})$ have any automorphism other than the linear and semilinear ones ?