Hermitian Line Polar Graßmann Codes

Luca Giuzzi

Università degli Studi di Brescia

2017 Gaeta Fq13

Joint work with Ilaria Cardinali

Projective Codes
Definition

Definition

A linear $[N, K, d_{\min}]_q$-code $\mathcal{C}$ is **projective** if the columns of its generator matrix G are pairwise non–proportional.

Remarks

- *The columns of the generator matrix G of $\mathcal{C}$ determine a set Ω of N distinct points of $\mathrm{PG}(K-1, \mathbb{F}_q)$ (projective system);*
- *Any $\Omega \subseteq \mathrm{PG}(K-1, \mathbb{F}_q)$ with $|\Omega| = N$ uniquely determines a $[N, K]$-projective code $\mathcal{C}(\Omega)$, up to monomial equivalence;*
- *Any semilinear collineation of $\mathrm{P\Gamma L}(K, \mathbb{F}_q)$ stabilizing Ω corresponds to some monomial automorphisms of $\mathcal{C}(\Omega)$;*
- *Codewords of $\mathcal{C}$ correspond to linear functionals on $V_K(\mathbb{F}_q)$.*

Projective Codes
Minimum Weight

- The weights of a projective code are determined by the hyperplane sections of the related projective system Ω
- For any projective code $\mathcal{C}(\Omega)$,

$$d_{\min} = |\Omega| - \max_{\substack{\Pi \leq \mathrm{PG}(K-1,\mathbb{F}_q) \\ \operatorname{codim}\Pi = 1}} |\Pi \cap \Omega|$$

- The study of the weights of $\mathcal{C}(\Omega)$ is equivalent to the study of the hyperplane sections of Ω

Projective Codes
Minimum Weight

- The weights of a projective code are determined by the hyperplane sections of the related projective system Ω
- For any projective code $\mathcal{C}(\Omega)$,

$$d_{\min} = |\Omega| - \max_{\substack{\Pi \leq \mathrm{PG}(K-1,\mathbb{F}_q) \\ \mathrm{codim}\,\Pi = 1}} |\Pi \cap \Omega|$$

- The study of the weights of $\mathcal{C}(\Omega)$ is equivalent to the study of the hyperplane sections of Ω
- Construction of codes associated to projective varieties.

Hermitian polar spaces

Hermitian Polarity

- $\mathbb{F}_{q^2}$: finite field of order q^2;
- $V := V_m(\mathbb{F}_{q^2})$;
- $\eta : V \times V \to \mathbb{F}_{q^2}$: sesquilinear form;
  - m even:
  $$\eta(x, y) := x_1 y_2^q + x_2 y_1^q + \cdots + x_{m-1} y_m^q + x_m y_{m-1}^q;$$
  - m odd:
  $$\eta(x, y) := x_1 y_1^q + x_2 y_3^q + x_3 y_2^q + \cdots + x_{m-1} y_m^q + x_m y_{m-1}^q.$$
- $[p]^{\perp_\eta} := \{[x] \in \mathrm{PG}(V) : \eta(p, x) = 0\}$

Remarks

⚠ *the index m always denotes vector dimension.*

UNIVERSITY OF BRESCIA

Hermitian polar spaces

- Point-line geometry $(\mathcal{H}_m, \mathcal{L}_m)$ such that:
  - Points: $\mathcal{H}_m := \{[p] \in \mathrm{PG}(V_m) \colon \eta(p,p) = 0\}$,
  - Lines: $\mathcal{L}_m := \{[p,q] : \eta(p,p) = \eta(p,q) = \eta(q,q) = 0\}$.

$$\mu_m := |\mathcal{H}_m| = \frac{(q^m + (-1)^{m-1})(q^{m-1} - (-1)^{m-1})}{q^2 - 1};$$

$$N_m := |\mathcal{L}_m| = \frac{\mu_{m-1}\mu_m}{q^2+1}.$$

- Polar-line Grassmannian $\Delta_{2,m} := (\mathcal{L}_m, \Lambda_m)$:
  - Points: $\mathcal{L}_m$,
  - Lines: Λ_m where
    - if $m = 4, 5$: $\Lambda_m = \{\ell_p : [p] \in \mathcal{H}_m\}$ with

$$\ell_p := \{X \in \mathcal{L}_m : [p] \in X \subseteq [p]^{\perp_\eta}\}.$$

    - if $m > 5$: $\Lambda_m = \{\ell_{p,\Pi} : [p] \in \mathcal{H}_m, \Pi \subseteq \mathcal{H}_m\}$ where

$$\ell_{p,\Pi} := \{X \in \mathcal{L}_m : [p] \in X \subseteq [\Pi]\},$$

and Π is a totally η–isotropic 3-space.

Hermitian polar spaces/2

Witt's index n of η

$$n := \begin{cases} m/2 & \text{if } m \text{ even} \\ (m-1)/2 & \text{if } m \text{ odd} \end{cases}$$

Hermitian polar spaces/2

Witt's index n of η

$$n := \begin{cases} m/2 & \text{if } m \text{ even} \\ (m-1)/2 & \text{if } m \text{ odd} \end{cases}$$

- if $m = 4$, then $n = 2$ and $\Delta_{2,4} \cong Q^-(5, q)$
- if $m = 5$, then $n = 2$ and $\Delta_{2,5} = DH(4, q^2)$

Graßmann embedding

- Restriction of the Plücker embedding to $\mathcal{L}_m$:

$$\varepsilon_2 : \begin{cases} \mathcal{L}_m \to \mathrm{PG}(V \wedge V) \\ [a, b] \to [a \wedge b] \end{cases}$$

Graßmann embedding

- Restriction of the Plücker embedding to $\mathcal{L}_m$:

$$\varepsilon_2 : \begin{cases} \mathcal{L}_m \to \mathrm{PG}(V \wedge V) \\ [a, b] \to [a \wedge b] \end{cases}$$

Remarks

- $m = 4$: *the images of lines of* $\Delta_{2,4}$ *are* Baer sublines;
- $m = 5$: *the images of lines of* $\Delta_{2,5}$ *are* Hermitian curves;
- $m > 5$: *the images of lines of* $\Delta_{2,m}$ *are* projective lines *(Projective embedding)*.

Graßmann embedding

Consider the set (projective system $\Omega_m \subseteq \mathrm{PG}(V \wedge V)$

$$\Omega_m := \{\varepsilon_2(\ell) \in \mathrm{PG}(V \wedge V) : \ell \in \mathcal{L}_m\}$$

Theorem

- I. Cardinali, A. Pasini, *Embeddings of line-Grassmannians of polar spaces in Grassmann varieties* In Groups of exceptional type, Coxeter groups and related geometries, volume 82 of Springer Proc. Math. Stat., pages 75–109. Springer, New Delhi (2014).
- R.J. Block, B.N. Cooperstein, *The generating rank of the unitary and symplectic Grassmannians*, J. Combin. Theory Ser. A, **119**, 1, 1–13 (2012).

$$\langle \Omega_m \rangle = V \wedge V.$$

Corollary

The parameters of the Hermitian Line Graßmann code $\mathcal{C}(\Omega_m)$ induced by the projective system Ω_m are $[N_m, K_m]$ where $K_m = \binom{m}{2}$.

Minimum distance

- What about the minimum distance?

Minimum distance

- What about the minimum distance?
- We need to determine

$$\max_{\substack{\Pi \leq PG(K_m-1,\mathbb{F}_{q^2})\\ \operatorname{codim}\Pi=1}} |\Pi \cap \Omega_m|.$$

Minimum distance

- What about the minimum distance?
- We need to determine

$$\max_{\substack{\Pi \leq \mathrm{PG}(K_m - 1, \mathbb{F}_{q^2}) \\ \mathrm{codim}\,\Pi = 1}} |\Pi \cap \Omega_m|.$$

- Hyperplanes Π of $\mathrm{PG}(V \wedge V)$ correspond to alternating bilinear forms φ on V

Remarks

To determine the minimum distance we need to determine the maximum number of lines which are both totally η–isotropic and totally φ–isotropic in $\mathrm{PG}(V)$, where φ varies among all possible alternating bilinear forms on V.

Minimum distance/2

$$m \geq 4$$

Minimum distance/2

$$m \geq 4$$

Theorem (I. Cardinali, LG)

The minimum distance $d_{\min}$ of $\mathcal{C}(\Omega_m)$ is:

$$d_{\min} = \begin{cases} q^{4m-12} - q^{2m-6} & \text{if } m = 4, 6 \\ q^{4m-12} & \text{if } m \geq 8 \text{ is even} \\ q^{4m-12} - q^{3m-9} & \text{if } m \geq 5 \text{ is odd} \end{cases}$$

Minimum weight codewords

Theorem

The minimum weight codewords correspond to bilinear alternating forms φ such that

- *For $m = 5$ or $m \geq 7$,*
  - $\dim \mathrm{Rad}\,\varphi = m - 2$
  - $$[\mathrm{Rad}\,\varphi] \cap \mathcal{H}_m = \begin{cases} [\Pi_2]\mathcal{H}_{m-4} & \text{if } m \text{ is even} \\ [p]\mathcal{H}_{m-3} & \text{if } m \text{ is odd} \end{cases}$$
- *For $m = 4, 6$*
  - $\dim \mathrm{Rad}\,\varphi = 0$
  - $[p]^{\perp_\varphi \perp_\eta} = [p]^{\perp_\eta \perp_\varphi}$ *for all* $[p] \in \mathrm{PG}(V)$

Graßmann embedding

Remarks

- $m = 4$: $\Omega_4 \cong Q^-(5, q) \subseteq \Sigma \cong \mathrm{PG}(5, q) \leq \mathrm{PG}(5, q^2)$
- $m = 4$: *the code* $\mathcal{C}(\Omega_4)$ *is defined over* $\mathbb{F}_q$.

Graßmann embedding

Remarks

- $m = 4$: $\Omega_4 \cong Q^-(5, q) \subseteq \Sigma \cong \mathrm{PG}(5, q) \leq \mathrm{PG}(5, q^2)$
- $m = 4$: *the code* $\mathcal{C}(\Omega_4)$ *is defined over* $\mathbb{F}_q$.
- $m > 4$: Ω_m *is not contained in a proper subgeometry.*
- $m > 4$: *the code* $\mathcal{C}(\Omega_4)$ *is defined over* $\mathbb{F}_{q^2}$.

Graßmann embedding

Remarks

- $m=4$: $\Omega_4 \cong Q^-(5,q) \subseteq \Sigma \cong \mathrm{PG}(5,q) \leq \mathrm{PG}(5,q^2)$
- $m=4$: *the code* $\mathcal{C}(\Omega_4)$ *is defined over* $\mathbb{F}_q$.
- $m>4$: Ω_m *is not contained in a proper subgeometry.*
- $m>4$: *the code* $\mathcal{C}(\Omega_4)$ *is defined over* $\mathbb{F}_{q^2}$.

$$\mathrm{Aut}(\Omega_m) = \begin{cases} \mathrm{PGO}^-(6,q) & \text{if } m=4 \\ \mathrm{P\Gamma U}(K_m,q) & \text{if } m>5 \end{cases}$$

Previous results

- Orthogonal polar spaces:
  - I. Cardinali, LG, "*Codes and Caps from Orthogonal Grassmannians*", Finite Fields Appl. **24** (2013), 148-169.
  - I. Cardinali, LG, K.V. Kaipa, A. Pasini, "*Line Polar Grassmann Codes of Orthogonal Type*", J. Pure Appl. Algebra **220** (2016), 1924-1934.
  - I. Cardinali, LG, "*Minimum distance of Line Orthogonal Grassmann codes in even dimension*", preprint (arXiv:1605:09333).
- Symplectic polar spaces:
  - I Cardinali, LG, "*Minimum distance of symplectic Grassmann codes*", Linear Algebra Appl. **488** (2016), 124-134.
- Encoding/Decoding/Error correction:
  - I. Cardinali, LG, "*Enumerative Coding for Line Polar Grassmannians*", Finite Fields Appl. **46** (2017), 107-138.

Polar spaces

Orthogonal

- $\phi\colon V \to \mathbb{F}_q$: non–singular quadratic form
- Point-line geometry $(\mathcal{P}_o, \mathcal{L}_o)$:
  - $\mathcal{P}_o := \{[p] \in \mathrm{PG}(2n, \mathbb{F}_q)\colon \phi(p) = 0\}$
  - $\mathcal{L}_o := \{[r, s] \subseteq \mathrm{PG}(2n, \mathbb{F}_q) : \phi(r+s) - \phi(r) - \phi(s) = 0\}$

Symplectic

- $\psi\colon V \times V \to \mathbb{F}_q$: non–singular alternating form
- Point-line geometry $(\mathcal{P}_w, \mathcal{L}_w)$:
  - $\mathcal{P}_w := \{[p] \in \mathrm{PG}(2n-1, \mathbb{F}_q)\}$
  - $\mathcal{L}_w := \{[r, s] \subseteq \mathrm{PG}(2n-1, \mathbb{F}_q)\colon \psi(r, s) = 0\}$

Orthogonal Graßmann Codes

Parameters

Theorem I. Cardinali, LG, K.V. Kaipa, A. Pasini, 2013–16–1?

The known parameters of the Orthogonal Graßmann codes $\mathcal{P}_k$ *are*

(n,k)	N	K	d
$1 \leq k < n$	$\prod_{i=0}^{k-1} \frac{q^{2(n-i)}-1}{q^{i+1}-1}$	$\binom{2n+1}{k}$	$d \geq \tilde{d}(q,n,k)$
$(3,3)$	$(q^3+1)(q^2+1)(q+1)$	35	$q^2(q-1)(q^3-1)$
$(n,2)$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$(2n+1)n$	$q^{4n-5}-q^{3n-4}$

q odd

(n,k)	N	K	d
$1 \leq k < n$	$\prod_{i=0}^{k-1} \frac{q^{2(n-i)}-1}{q^{i+1}-1}$	$\binom{2n+1}{k} - \binom{2n+1}{k-2}$	$d \geq \tilde{d}(q,n,k)$
$(3,3)$	$(q^3+1)(q^2+1)(q+1)$	28	$q^5(q-1)$
$(n,2)$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$(2n+1)n-1$	$q^{4n-5}-q^{3n-4}$

q even

$$\tilde{d}(q,n,k) := (q+1)(q^{k(n-k)}-1)+1$$

Symplectic/Lagrangian Graßmann Codes

Parameters

Theorem I. Cardinali, LG, 2016

The known parameters of the symplectic Graßmann codes $\overline{\mathcal{P}}_k$ *are*

(n,k)	N	K	d
$1 \leq k \leq n$	$\prod_{i=0}^{k-1} \frac{q^{2(n-i)}-1}{q^{i+1}-1}$	$\binom{2n}{k} - \binom{2n}{k-2}$	$d \geq \overline{d}(q,n,k)$
$(3,3)$	$(q^3+1)(q^2+1)(q+1)$	14	$q^6 - q^4$
$(n,2)$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$(2n-1)n-1$	$q^{4n-5} - q^{2n-3}$

$$\overline{d}(q,n,k) = \prod_{i=0}^{k-1} \frac{q^{2(n-i)}-1}{q^{i+1}-1} - \begin{bmatrix} 2n \\ k \end{bmatrix}_q + d_s,$$

$$s = \binom{2n}{k-2} + 1$$

- q even: $\overline{\mathcal{P}}_k \leq \mathcal{P}_k$

Hermitian Graßmann Codes/comparison

- n: Witt's index of η
- $s = |\mathbb{F}_{q^2}| = q^2$
- $m = 2n$ or $m = 2n + 1$

$$N = \frac{(q^m + (-1)^{m-1})(q^{m-1} - (-1)^{m-1})(q^{m-2} + (-1)^{m-3})(q^{m-3} - (-1)^{m-3})}{(q^2 - 1)^2(q^2 + 1)}$$

$$K = \binom{m}{2}$$

$$d_{\min} = \begin{cases} s^{4n-6} - s^{2n-3} & \text{if } m = 4, 6 \\ s^{4n-6} & \text{if } m \geq 8 \text{ is even} \\ s^{4n-4} - s^{3n-3} & \text{if } m \geq 5 \text{ is odd} \end{cases}$$

Point enumerators/Hermitian Graßmannians

Theorem (I. Cardinali, LG)

There is a a point enumerator for a Hermitian line Grassmannian $\Delta_{2,m}$ with complexity $O(q^4 m^3)$.

Enumerative coding

- We need a *point enumerator* for $\mathcal{L}_m$, i.e. a function

$$\iota : \{0 \dots N_m - 1\} \to \mathcal{L}_m$$

easy to compute and to invert.

Point enumerators

Enumerators

- For projective Grassmannians
  - N. Silberstein and T. Etzion, *Enumerative coding for Grassmannian space*, IEEE Trans. Inform. Theory, **57** (2011), 365–374.
  - Y. Medvedeva, *Fast enumeration for Grassmannian space*, in "Problems of Redundancy in Information and Control Systems (RED), 2012 XIII International Symposium on". IEEE (2012), 48–52.
- For orthogonal and symplectic polar line Grassmannians
  - I. Cardinali, LG, "*Enumerative Coding for Line Polar Grassmannians*", Finite Fields Appl. **46** (2017), 107-138.

Basic approach

Theorem

- T.M. Cover, *Enumerative source encoding*, IEEE Trans. Information Theory, vol. **IT-19** (1973), 73–77

1. *Introduce an order* $\prec$ *on* $\mathbb{F}_{q^2}^2$;
2. *Choose a canonical representation for the elements of* $\mathcal{L}_m$ *(RREF) as* $(2 \times m)$*-matrices*
$$G = \begin{pmatrix} G_1 & G_2 & \dots & G_m \end{pmatrix};$$
3. *Call* prefix *any* $(2 \times t)$*-matrix* S *with* $t \leq m$;
4. *Construct a prefix enumerator* ψ *such that*
$$\psi(S) := |\{\ell \in \mathcal{L}_m : \text{the representation of } \ell \text{ begins with } S\}|;$$
5. *Define*
$$\iota(G) := \sum_{j=1}^{m} \sum_{X \prec G_j} \psi(G_1, \dots, G_{j-1}, X).$$

Encoding

Given a message $\mathbf{w}$:

1. Represent $\mathbf{w}$ as an antisymmetric $m \times m$ matrix W;
2. Consider the bilinear alternating form φ_W induced by W;
3. For each $i = 0, \ldots, N_m - 1$ evaluate

$$c_i := \varphi(\iota^{-1}(i));$$

4. Transmit the vector $\mathbf{c} = (c_i)_{i=0}^{N_m-1}$.