Calculating the minimum distance of Polar Hermitian Grassmann Codes with elementary methods

Sarah Gregory [1], Fernando Piñero[2], Doel Rivera[3], Lani Southern[4]

[1]University of Richmond

[2]University of Puerto Rico, Ponce

[3]Pontifical Catholic University of Puerto Rico, Ponce

[4]Willamette University

August 28, 2022
Sixth Irsee Conference on Finite Geometries
Irsee, Germany

The Grassmannian

Definition

The Grassmannian, $\mathcal{G}_{\ell,m}(V)$ is the collection of all subspaces of dimension ℓ of a vector space V of length m.
In particular, we take $V = \mathbb{F}_q^m$.

Hermitian Matrix

Definition

A matrix H is Hermitian if $H = \overline{H^T}$.
This gives the property that the entries on the main diagonal are over $\mathbb{F}_q$ and the others are over $\mathbb{F}_{q^2}$, with the entries opposite each other across the main diagonal being conjugates of each other.

For example, over $\mathbb{F}_{q^2}$, H is a 3×3 Hermitian matrix where $a, b, c \in \mathbb{F}_q$ and $x, y, z \in \mathbb{F}_{q^2}$.

$$H = \begin{bmatrix} a & x & y \\ x^q & b & z \\ y^q & z^q & c \end{bmatrix}$$

Over $\mathbb{F}_{q^2}$, the conjugate is equal to taking $\bar{x} = x^q$.

Hermitian Form

Definition

Let V be a vector space over $\mathbb{F}$. Let $B : V \times V \to \mathbb{F}$ satisfying:

- $B(x + x', y) = B(x, y) + B(x', y)$
- $B(x, y + y') = B(x, y) + B(x, y')$
- $B(\alpha x, y) = \alpha B(x, y)$
- $B(x, \alpha y) = \bar{\alpha} B(x, y)$

We say that B is a *sesquilinear* or *Hermitian form*.

Any Hermitian form B is represented B by a map

$$B(x, y) = xH\bar{y}^T$$

where $x, y \in V$ and H is a Hermitian matrix.

Polar Hermitian Grassmannian

Definition

Let V be a vector space of dimension m over the field $\mathbb{F}$. Let B be a Hermitian form. Let W be a subspace of V. We say W is *totally isotropic* with respect to the Hermitian form B if W is a maximal subspace of V satisfying

$$B(v, w) = 0, \forall v, w \in W.$$

Definition

Let V be a vector space of dimension m over the field $\mathbb{F}$. Let B be a Hermitian form. Let $\ell \leq \frac{m}{2}$. The *Polar Hermitian Grassmannian* $\mathbb{H}_{\ell,m}$ is defined as the set of isotropic spaces of $\mathcal{G}_{\ell,m}$. That is

$$\mathbb{H}_{\ell,m} := \{W \in \mathcal{G}_{\ell,m} \mid B(v, w) = 0 \forall v, w \in W\}.$$

Minors

To construct our code, we will use minors. For example, consider the following generic 3×6 matrix X and its corresponding minors of the form $det_I(X)$ where we take I to be a subset of size 3 of the columns of X.

$$X = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & x_{16} \\ x_{21} & x_{22} & x_{23} & x_{24} & x_{25} & x_{26} \\ x_{31} & x_{32} & x_{33} & x_{34} & x_{35} & x_{36} \end{bmatrix}$$

The set $\{1, 2, 3\} \subseteq \{1, 2, 3, 4, 5, 6\}$ is denoted by 123 and its corresponding minor would be

$$det_{123}(X) = \begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}$$

What is a Code?

Linear Code

A *linear code* is a subspace $C \leq \mathbb{F}_q^n$.

- n is the length of the code
- $k = \dim_{\mathbb{F}_q}(C)$ is the dimension of the code
- d is the minimum distance of the code

We say C is an $[n, k, d]_q$ code.

Minimum Distance

The minimum distance of a code is the smallest distance (Hamming distance) between any two codewords. The Hamming distance counts the number of characters which differ between the corresponding positions of two codewords. So if we had (0,1,**0**,0,**1**) and (0,1,**1**,0,**0**), the distance is 2.

Code Construction

We build the Polar Hermitian Grassmann Code by making use of a projective embedding called the Plücker embedding, which is performed as follows:

- For each ℓ–space, $W \in \mathbb{H}_{\ell,m}$, take a $\ell \times m$ matrix, M_W, whose rowspace is W.
- A codeword is given by evaluating an $\mathbb{F}_{q^2}$–linear combinations of ℓ-minors on each representative M_W.

Known Information About Polar Hermitian Grassmann Codes

Cardinali and Giuzzi[4] proved results about the Line Polar Hermitian Grassmann Codes, which are the $\ell = 2$ case. For example,

$C(\mathbb{H}_{2,4})$ is a $[q^4 + q^3 + q + 1, 6, q^4 - q^2]$ code.

In fact, [4] calculates the minimum distance for $C(\mathbb{H}_{2,m})$

Known Results

I have very recently made aware of [2]. De Bryun and Pralle [2] classified all hyperplanes of $DH(5, q)$. The geometric hyperplanes of $DH(5, q)$ are in correspondence to the codewords of $C(\mathbb{H}_{3,6})$. The weight spectrum of $C(\mathbb{H}_{3,6})$ is known.
Our contrubution is:

- We offer an elementary approach using polynomial evaluations.
- Our approach may be generalizable to higher dimensions.
- We may also apply it to other polar Grassmannians.

Auxiliary lemmas

Lemma

Let $P(T) = T^{q+1} + aT^q + bT + c$ *be a polynomial over* $\mathbb{F}_{q^2}$*. If* $b \neq a^q$ *then* $P(T)$ *has at most* 2 *zeroes over* $\mathbb{F}_{q^2}$

Lemma

Let $P(T) = aT^q + bT + c$ *be a polynomial over* $\mathbb{F}_{q^2}$*. If* $b^{q+1} \neq a^{q+1}$ *then* $P(T)$ *has at most* 1 *zero over* $\mathbb{F}_{q^2}$

Lemma

Let $a, b, S, T, \lambda \in \mathbb{F}_{q^2}$*, where* $a^q + a = 0, b^q + b = 0, S^q + S = 0, T^q + T = 0$ $\lambda \neq 0$*. Then*

- $(S + a)(T + b) = 0$ *has* $2q - 1$ *solutions over* $\mathbb{F}_{q^2}$*.*
- $(S + a)(T + b) = \lambda$ *where* $\lambda \in \mathbb{F}_q^*$ *has* $q - 1$ *solutions over* $\mathbb{F}_{q^2}$*.*
- $(S + a)(T + b) = \lambda$ *where* $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *has no solutions over* $\mathbb{F}_{q^2}$*.*

Choice of Hermitian form

We use the Hermitian form given by

$$B(x, y) := xJ\bar{y}^T$$

where

$$J = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Cardinali and Giuzzi [3, 5] and De Bruyn [1] use a different form. However, the resulting codes are equivalent.

Pivot sets

The main advantage of the Hermitian form given by J is that we may partition the matrices in L representing the totally isotropic spaces of $\mathbb{H}_{3,6}$ into 8 Schubert cells.

$$\left\{ \begin{bmatrix} * & * & * & 0 & 0 & 1 \\ * & * & * & 0 & 1 & 0 \\ * & * & * & 1 & 0 & 0 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} * & * & 0 & * & 0 & 1 \\ * & * & 0 & * & 1 & 0 \\ * & * & 1 & 0 & 0 & 0 \end{bmatrix} \right\}, \cdots$$

We classify the matrices according to their pivot columns (hence the name *pivot sets*).

Schubert cell structure

$$P_1 = \left\{ \begin{bmatrix} a_1 & a_2 & a_3 & 0 & 0 & 1 \\ -a_2^q & a_4 & a_5 & 0 & 1 & 0 \\ -a_3^q & -a_5^q & a_6 & 1 & 0 & 0 \end{bmatrix} \right\}$$

where $a_1^q + a_1 = a_4^q + a_4 = a_6^q + a_6 = 0, a_i \in \mathbb{F}_{q^2}$

$$P_2 = \left\{ \begin{bmatrix} b_1 & b_2 & 0 & b_3 & 0 & 1 \\ -b_2^q & b_4 & 0 & b_5 & 1 & 0 \\ -b_3^q & -b_5^q & 1 & 0 & 0 & 0 \end{bmatrix} \right\}$$

where $b_1^q + b_1 = b_4^q + b_4 = 0, b_i \in \mathbb{F}_{q^2}$

$$P_3 = \left\{ \begin{bmatrix} c_1 & 0 & c_2 & 0 & c_3 & 1 \\ -c_2^q & 0 & c_4 & 1 & 0 & 0 \\ -c_3^q & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \right\}$$

where $c_1^q + c_1 = c_4^q + c_4 = 0, c_i \in \mathbb{F}_{q^2}$

$$P_4 = \left\{ \begin{bmatrix} d_1 & 0 & 0 & d_2 & d_3 & 1 \\ -d_2^q & 0 & 1 & 0 & 0 & 0 \\ -d_3^q & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \mid d_1^q + d_1 = 0, d_i \in \mathbb{F}_{q^2} \right\}$$

Note that the submatrices outside the pivot columns are skew–Hermitian.

$$P_5 = \left\{ \begin{bmatrix} 0 & e_1 & e_2 & 0 & 1 & 0 \\ 0 & -e_2^q & e_3 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \mid e_1^q + e_1 = e_3^q + e_3 = 0, e_i \in \mathbb{F}_{q^2} \right\}$$

$$P_6 = \left\{ \begin{bmatrix} 0 & x_1 & 0 & x_2 & 1 & 0 \\ 0 & -x_2^q & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \mid x_1^q + x_1 = 0, x_i \in \mathbb{F}_{q^2} \right\}$$

$$P_7 = \left\{ \begin{bmatrix} 0 & 0 & y_1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \mid y_1^q + y_1 = 0, y_1 \in \mathbb{F}_{q^2} \right\}$$

$$P_8 = \left\{ \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \right\}$$

Example

To show the usefulness of this partitioning, we show:

Lemma

$$wt(det_{236} - det_{456}) = q^9 - q^7$$

Evaluating $det_{236} - det_{456}$ on P_1

The partition $P_1 = \left\{ \begin{bmatrix} a_1 & a_2 & a_3 & 0 & 0 & 1 \\ -a_2^q & a_4 & a_5 & 0 & 1 & 0 \\ -a_3^q & -a_5^q & a_6 & 1 & 0 & 0 \end{bmatrix} \mid a_1^q + a_1 = \right.$
$\left. a_4^q + a_4 = a_6^q + a_6 = 0, a_i \in \mathbb{F}_{q^2} \right\}$

Note that $f(M_W) = \begin{vmatrix} a_2 & a_3 & 1 \\ a_4 & a_5 & 0 \\ -a_5^q & a_6 & 0 \end{vmatrix} - \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} = a_4 a_6 + a_5^{q+1} - 1.$

For the q^5 values of a_1, a_2 and a_3, f is determined by the values of a_4, a_5 and a_6. We note that $f(M_W) = 0$ if $a_4 a_6 = -a_5^{q+1} - 1$. Through auxiliary lemmas we may prove that there are at most $q^8 + q^6$ solutions to the equation. Therefore $wt_{P_1}(f) = q^9 - q^8 - q^6$.

Evaluating $det_{236} - det_{456}$ on P_2

Along P_2, the matrices look as such $P_2 =$
$$\left\{ \begin{bmatrix} b_1 & b_2 & 0 & b_3 & 0 & 1 \\ -b_2^q & b_4 & 0 & b_5 & 1 & 0 \\ -b_3^q & -b_5^q & 1 & 0 & 0 & 0 \end{bmatrix} \mid b_1^q + b_1 = b_4^q + b_4 = 0, b_i \in \mathbb{F}_{q^2} \right\}$$

Note that $f(M_W) = \begin{vmatrix} b_2 & 0 & 1 \\ b_4 & 0 & 0 \\ -b_5^q & 1 & 0 \end{vmatrix} - \begin{vmatrix} b_3 & 0 & 1 \\ b_5 & 1 & 0 \\ 0 & 0 & 0 \end{vmatrix} = b_4.$

For the q^7 values of b_1, b_2, b_3 and b_5, f is determined by the value of b_4. For the $q-1$ nonzero values of b_4, f has a nonzero evaluation. Therefore $wt_{P_2}(f) = q^8 - q^7$.

Evaluating $det_{236} - det_{456}$ on P_3

Along P_3, the matrices look as such

$$P_3 = \left\{ \begin{bmatrix} c_1 & 0 & c_2 & 0 & c_3 & 1 \\ -c_2^q & 0 & c_4 & 1 & 0 & 0 \\ -c_3^q & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \middle| c_1^q + c_1 = c_4^q + c_4 = 0, c_i \in \mathbb{F}_{q^2} \right\}$$

Note that $f(M_W) = \begin{vmatrix} 0 & c_2 & 1 \\ 0 & c_4 & 0 \\ 1 & 0 & 0 \end{vmatrix} - \begin{vmatrix} 0 & c_3 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{vmatrix} = c_4$. For the q^5 values of c_1, c_2, and c_3, f is determined by the value of c_4. For the $q-1$ nonzero values of c_4, f has a nonzero evaluation. Therefore $wt_{P_3}(f) = q^6 - q^5$.

Evaluating $det_{236} - det_{456}$ on P_4

Along P_4, the matrices look as such

$$P_4 = \left\{ \begin{bmatrix} d_1 & 0 & 0 & d_2 & d_3 & 1 \\ -d_2^q & 0 & 1 & 0 & 0 & 0 \\ -d_3^q & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \mid d_1^q + d_1 = 0, d_i \in \mathbb{F}_{q^2} \right\}$$

For any matrix $M_W \in P_4$ then $f(M_W) = -1$ This implies that for all q^5 values of d_1, d_2 and d_3, $f(M_W) = -1 \neq 0$. Therefore $wt_{P_4}(f) = q^5$.

Evaluating $det_{236} - det_{456}$ on P_5, P_6, P_7, P_8

The evaluation is $f(M_W) = 0$ in all remaining pivot sets.

$$P_5 = \left\{ \begin{bmatrix} 0 & e_1 & e_2 & 0 & 1 & 0 \\ 0 & -e_2^q & e_3 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \mid e_1^q + e_1 = e_3^q + e_3 = 0, e_i \in \mathbb{F}_{q^2} \right\}$$

$$P_6 = \left\{ \begin{bmatrix} 0 & x_1 & 0 & x_2 & 1 & 0 \\ 0 & -x_2^q & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \mid x_1^q + x_1 = 0, x_i \in \mathbb{F}_{q^2} \right\}$$

$$P_7 = \left\{ \begin{bmatrix} 0 & 0 & y_1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \mid y_1^q + y_1 = 0, y_1 \in \mathbb{F}_{q^2} \right\}$$

$$P_8 = \left\{ \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \right\}$$

Calculating the Weight

Adding all the weights, we have
$wt(f) = wt_{P_1}(f) + wt_{P_2}(f) + wt_{P_3}(f) + wt_{P_4}(f) = q^9 - q^7$.

Results

Our main result is the following:

Theorem

The minimum distance of the Polar Hermitian Grassmann code $C(\mathbb{H}_{3,6})$ is $q^9 - q^7$.

Proof Sketch and Key Ideas

Definition

For $I \subseteq \{1,2,3,4,5,6\}$ denote by

$$I^* := \{7-j \mid j \notin I\}$$

Lemma

Let P denote the pivot set of a given partition P_i of $\mathbb{H}_{3,6}$. Let M_W be a matrix representative of $W \in P$. Then $det_{I^*}(M_W)$ and $det_I(M_W)$ are "transposes" of each other.

Proof Sketch and Key Ideas

On

$$P_1 = \left\{ \begin{bmatrix} a_1 & a_2 & a_3 & 0 & 0 & 1 \\ -a_2^q & a_4 & a_5 & 0 & 1 & 0 \\ -a_3^q & -a_5^q & a_6 & 1 & 0 & 0 \end{bmatrix} \right\}$$

where $a_1^q + a_1 = a_4^q + a_4 = a_6^q + a_6 = 0, a_i \in \mathbb{F}_{q^2}$

Let $I = \{2, 3, 4\}$. $I^* = \{7-1, 7-5, 7-6\} = \{1, 2, 6\}$

$det_I = \begin{vmatrix} a_2 & a_3 \\ a_4 & a_5 \end{vmatrix}$, $det_{I^*} = \begin{vmatrix} -a_2^q & a_4 \\ -a_3^q & -a_5^q \end{vmatrix}$

In this case $det_{I^*} = det_I^q$

On P_2 the relation becomes $det_{I^*} = -det_I^q$

Proof Sketch and Key Ideas

Goal: take $f = f_{123} det_{123} + f_{124} det_{124} + \cdots + f_{456} det_{456}$ and determine the least number of spaces where the evaluation is nonzero.

We sketch our proof of the minimum distance as follows:

- We use the automorphisms of $\mathbb{H}_{3,6}$ to assume that det_{123} has coefficient 1 and det_{234}, det_{134}, det_{136} have coefficient 0.
- The auxiliary lemmas imply that if det_{126}, det_{125}, det_{235} don't have coefficient 0 then the combination has more than $q^9 - q^7$ nonzero elements on the pivot sets.
- Likewise det_{124}, det_{135}, det_{236} may be assumed do not appear in f.
- Studying the equation $det(\mathrm{X}) + Tr(A\mathrm{X}) + \gamma = 0$ for X a 3×3 skew–Hermitian matrix, show that in order for $wt(f) \leq q^9 - q^7$ then f is equivalent to a combination with only five possible minors 123, 145, 246, 356 and 456.

Acknowledgements

This research is supported by NSF-DMS REU 1852171: REU Site: Combinatorics, Probability, and Algebraic Coding Theory

We thank Bart, Ilaria, Luca and Sudhir Ghorpade for their help and thoughtful discussions.

Have an excellent week!

References

[1] Bart De Bruyn, *On the Grassmann-embeddings of the Hermitian dual polar spaces*, Linear and Multilinear Algebra **56** (2008), no. 6, 665–677, available at `https://doi.org/10.1080/03081080701535856`. ↑12

[2] Bart De Bruyn and Harm Pralle, *The hyperplanes of dh(5, q2)* **20** (2008), no. 2, 239–264. ↑10

[3] Ilaria Cardinali and Luca Giuzzi, *Line Hermitian Grassmann codes and their parameters*, Finite Fields and Their Applications **51** (2018May), 407–432. ↑12

[4] ———, *Minimum distance of orthogonal line-Grassmann codes in even characteristic*, Journal of Pure and Applied Algebra **222** (2018Oct), no. 10, 2975–2988. ↑9

[5] ———, *Implementing line-Hermitian Grassmann codes*, Linear Algebra and its Applications **580** (2019), 96–120. ↑12