The structure of dual Grassmann codes

F. Piñero
Joint work with P. Beelen

June 30, 2014 / Aalborg University, Aalborg, Denmark

Grassmannian

What is the Grassmannian?

Definition

Let V be a subspace of $\mathbb{F}$ of dimension m. The Grassmannian is defined as

$$\mathcal{G}_{m,\ell}(V) := \{W \text{ a linear subspace of } V \mid \dim W = \ell\}$$

- Usually denoted by $\mathcal{G}_{m,\ell}$ (or $\mathcal{G}_{m,\ell}(\mathbb{F})$)
- It has several characterizations.

Grassmannian

Fortunately, the Grassmannian is well known!

- It is a projective variety.
- It has a nice embedding in $\mathbb{P}^{\binom{m}{\ell}-1}$

Plücker embedding

We embed $\mathcal{G}_{m,\ell}$ into $\mathbb{P}^{\binom{m}{\ell}-1}$ like this:

- Let $W \in \mathcal{G}_{m,\ell}$.
- Define W^M as a $\ell \times m$ matrix whose rowspace is W.
- For a subset I of ℓ columns, let W_I^M denote the minor given by I.

The map

$$W \mapsto (W_{I_1}^M : W_{I_2}^M : \cdots : W_{I_{\binom{m}{\ell}}}^M) \in \mathbb{P}^{\binom{m}{\ell}-1}$$

is well-defined and injective.
$I_1, I_2, \ldots I_{\binom{m}{\ell}}$ are all the subsets the set $\{1, 2, \ldots, m\}$ of size ℓ.
This is known as the *Plücker embedding*.

Plücker embedding

Embedding $\mathcal{G}_{m,\ell}$ into $\mathbb{P}^{\binom{m}{\ell}-1}$ is quite useful.

- we can perform geometry on $\mathcal{G}_{m,\ell}$.
- It is also "a" code given by $\mathcal{G}_{m,\ell}$.

Grassmann codes

The code was defined by Ryan in 1987. Fortunately, the code has been extensively studied.

- $\mathcal{C}(\ell, m)$ is a $[|\mathcal{G}_{m,\ell}|, \binom{m}{\ell}, q^{\ell\ell'}]_q$ code.
- Its automorphism group of $\mathcal{C}(\ell, m)$ is nice!
- We have identified the minimum weight codewords of $\mathcal{C}(\ell, m)$.
- We know some of the higher weights of the codewords.

Affine Grassmann codes

Affine Grassmann codes were introduced by Beelen, Ghorpade and Høholdt in 2009.

Definition

The Affine Grassmann code $\mathcal{C}^{\mathbb{A}}(\ell, m)$ is defined by evaluating all $r \times r$ minors ($0 \leq r \leq \ell$) at all $\ell \times \ell'$ matrices over $\mathbb{F}_q$.

Why Affine Grassmann?

- The evaluation points of $\mathcal{C}^{\mathbb{A}}(\ell, m)$ are all $\ell \times \ell'$ matrices over a field.
- For a matrix M, consider the $\ell \times m$ matrix $(I_\ell | M)$.
- The matrices $(I_\ell | M)$ represent different elements of $\mathcal{G}_{m,\ell}$.

We also know several things about this code.
Beelen, Ghorpade and Høholdt 2009.

- $\mathcal{C}^A(\ell, m)$ is a $[q^{\ell\ell'}, \binom{m}{\ell}, |GL_\ell(q)|]_q$ code.
- The automorphism group of $\mathcal{C}^{\mathbb{A}}(\ell, m)$ is also nice.
- $\mathcal{C}^{\mathbb{A}}(\ell, m)$ is also realized by evaluating all minors at all $\ell \times \ell'$ matrices.
- We also know the minimum distance codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)$.

We know somethings about the dual code $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$.
Beelen, Ghorpade and Høholdt 2012

- We know the minimum distance of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$.
  - $d = 4$ if $q = 2$
  - $d = 3$ otherwise
- In both cases the minimum weight codewords generate $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$.

Theorem

Let c be a codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ of minimum weight. Then supp(c) is in the orbit of the automorhism group of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ of one of the following:

- $\left\{ \begin{bmatrix} 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 1 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 0 & 1 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 1 & 1 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \right\}$
- $\left\{ \begin{bmatrix} 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 1 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 0 & 0 & \cdots \\ 1 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 1 & 0 & \cdots \\ 1 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \right\}$
- $\left\{ \begin{bmatrix} 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 1 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 0 & 1 & \cdots \\ 1 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 1 & 1 & \cdots \\ 1 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \right\}$

The nonbinary case is simpler

Theorem

Let c be a codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ of minimum weight. Then supp(c) is in the orbit of the automorhism group of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ of:

$$\left\{ \begin{bmatrix} 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} 1 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}, \begin{bmatrix} \frac{\alpha}{\alpha+1} & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \right\}, \frac{\alpha}{\alpha+1} \neq 0, 1$$

where the coefficients of c are

$$c'_0 = 1, c'_M = \alpha, c'_{\alpha M} = -(\alpha + 1)$$

What about the Grassmann codes?

$\mathcal{C}(\ell, m)$ may also be reconstructed in this manner.
First we need to know something about its minimum weight codewords.

Theorem

Let $\mathcal{C}(\ell, m)$ be the Grassmann code over $\mathbb{F}_2$. Then the minimum distance of $\mathcal{C}(\ell, m)^\perp$ is 3 and the positions are given by spaces of the form

$$\langle V, a\rangle, \langle V, b\rangle, \langle V, a+b\rangle.$$

Minimum weight codewords of $\mathcal{C}(\ell, m)^\perp$

Since the Plücker map is an embedding, $d(\mathcal{C}(\ell, m)^\perp) > 2$.

If $L = \langle V, a \rangle$, $N = \langle V, b \rangle$, $O = \langle V, a + b \rangle$ are three vector spaces of dimension ℓ then by the multilinearity of the determinant, we have a weight 3 codeword of $\mathcal{C}(\ell, m)^\perp$ with support given by L, N and O.

Now we will prove this is the only possiblilty.

Let L, N and O be the support of a codeword of $\mathcal{C}(\ell, m)^{\perp}$. After applying a suitable automorphism of $\mathcal{C}(\ell, m)^{\perp}$, we may assume the coefficients are $c_{L^M} = c_{O^M} = 1$ and $c_{N^M} = -1$

$$L^M := (I_\ell | 0)$$

$$N^M := \left(\begin{array}{ccccccc|ccc}
1 & 0 & \cdots & 0 & 0 & \cdots & 0 & n_{1,\ell+1} & \cdots & n_{1,j} \\
0 & 1 & \cdots & 0 & 0 & \cdots & 0 & n_{2,\ell+1} & \cdots & n_{2,j} \\
\vdots & 0 & \ddots & 0 & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\
\vdots & 0 & \cdots & 0 & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 0 & 0 & \cdots & 1 & n_{\ell,\ell+1} & \cdots & n_{\ell,j}
\end{array}\right)$$

$$O^M := \left(\begin{array}{ccccccc|ccc}
1 & 0 & \cdots & o_{1,i} & 0 & \cdots & 0 & 0 & \cdots & o_{1,j} \\
0 & 1 & \cdots & o_{2,i} & 0 & \cdots & 0 & 0 & \cdots & o_{2,j} \\
\vdots & 0 & \ddots & o_{i-1,i} & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \cdots & o_{i,j} \\
\vdots & 0 & \cdots & o_{i+1,i} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & o_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & o_{\ell,j}
\end{array}\right)$$

We look at the minors given by

$$I = \{1, 2, \ldots, \ell\} \setminus \{i\} \cup \{j\}$$

$$j > \ell + 1$$

$$N_I^M = [n_{i,j}] = [0]$$

$$O_I^M = [o_{i,j}]$$

Therefore $o_{i,j} = n_{i,j} = 0$.

$$O^M := \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & o_{1,i} & 0 & \cdots & 0 & 0 & \cdots & o_{1,j} \\ 0 & 1 & \cdots & o_{2,i} & 0 & \cdots & 0 & 0 & \cdots & o_{2,j} \\ \vdots & 0 & \ddots & o_{i-1,i} & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & o_{i+1,i} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & o_{\ell,j} \end{array}\right)$$

We look at the minors given by

$$I = \{1, 2, \ldots, \ell\} \setminus \{i'\} \cup \{j\}$$

$$j > \ell + 1, 1 \leq i' \leq \ell, i' \neq i$$

$$N_I^M = \begin{bmatrix} n_{i',j} & n_{i',i} \\ n_{i,j} & n_{i,i} \end{bmatrix} = \begin{bmatrix} n_{i',j} & 0 \\ 0 & 1 \end{bmatrix}$$

$$O_I^M = \begin{bmatrix} o_{i',j} & o_{i',i} \\ o_{i,j} & o_{i,i} \end{bmatrix} = \begin{bmatrix} o_{i',j} & o_{i',i} \\ 0 & 0 \end{bmatrix}$$

We must have $n_{i',j} = 0$.

$$N^M := \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & n_{1,\ell+1} & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 & n_{2,\ell+1} & \cdots & 0 \\ \vdots & 0 & \ddots & 0 & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & 0 & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & n_{\ell,\ell+1} & \cdots & 0 \end{array}\right)$$

We look at the minors given by

$$I = \{1, 2, \dots, \ell\} \setminus \{i', i\} \cup \{j, \ell + 1\}$$

$$j > \ell + 1, 1 \leq i' \leq \ell, i' \neq i$$

$$N_I^M = \begin{bmatrix} n_{i',j} & n_{i',\ell+1} \\ n_{i,j} & n_{i,\ell+1} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$O_I^M = \begin{bmatrix} o_{i',j} & o_{i',\ell+1} \\ o_{i,j} & o_{i,\ell+1} \end{bmatrix} = \begin{bmatrix} o_{i',j} & 0 \\ o_{i,j} & 1 \end{bmatrix}$$

We must have $o_{i',j} = 0$.

$$O^M := \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & o_{1,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & o_{2,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & o_{i-1,i} & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & o_{i+1,i} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right)$$

We look at the minors given by $\{1, 2, \ldots, \ell\} \setminus \{i'\} \cup \{\ell + 1\}$

$$1 \leq i' \leq \ell, i' \neq i$$

$$N_I^M = \begin{pmatrix} n_{i',i} & n_{i',\ell+1} \\ n_{i,i} & n_{i,\ell+1} \end{pmatrix} = \begin{pmatrix} 0 & n_{i',\ell+1} \\ 1 & 1 \end{pmatrix}$$

$$O_I^M = \begin{pmatrix} o_{i',i} & o_{i',\ell+1} \\ o_{i,i} & o_{i,\ell+1} \end{pmatrix} = \begin{pmatrix} o_{i',i} & 0 \\ o_{i,i} & 1 \end{pmatrix}$$

Therefore $o_{i',i} = -n_{i',\ell+1}$.

$$N^M := \left(\begin{array}{ccccccc|ccc}
1 & 0 & \cdots & 0 & 0 & \cdots & 0 & n_{1,\ell+1} & \cdots & 0 \\
0 & 1 & \cdots & 0 & 0 & \cdots & 0 & n_{2,\ell+1} & \cdots & 0 \\
\vdots & 0 & \ddots & 0 & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\
\vdots & 0 & \cdots & 0 & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 0 & 0 & \cdots & 1 & n_{\ell,\ell+1} & \cdots & 0
\end{array}\right)$$

$$O^M := \left(\begin{array}{ccccccc|ccc}
1 & 0 & \cdots & -n_{1,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\
0 & 1 & \cdots & -n_{2,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & 0 & \ddots & -n_{i-1,i} & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\
\vdots & 0 & \cdots & n_{i+1,i} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & n_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & 0
\end{array}\right)$$

$$L^M := (I_\ell | 0)$$

$$N^M := \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & -n_{1,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & -n_{2,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & -n_{i-1,i} & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & -n_{i+1,i} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -n_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right)$$

$$O^M := \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & -n_{1,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & -n_{2,i} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & -n_{i-1,i} & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & -n_{i+1,i} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -n_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right)$$

Theorem

The code $\mathcal{C}(\ell, m)^\perp$ *is generated by its weight* 3 *codewords.*

Let $V_{m-\ell}$ be a subspace of dimension $m - \ell$ of V.

$$\mathcal{G}^{\delta} := \{ W \in \mathcal{G}_{m,\ell} \mid \dim W \cap V_{m-\ell} = \delta \}$$

Remark

$\mathcal{G}^0$ is the vector spaces of the affine grassmannian code.

Remark

$\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ is generated by sums of weight 3 codewords of $\mathcal{C}(\ell, m)^{\perp}$.

Remark

For $\delta = 1, 2, \ldots m - \ell$ For each $W \in \mathcal{G}^{\delta}$ add a weight 3 check where the other 2 positions are in $\mathcal{G}^{\delta-1}$.

Let $W = \langle U \cup x \rangle$, $x \in V_{m-\ell}$. Let $y \notin V_{m-\ell}, U$. Then $W_1 = \langle U \cup y \rangle$ and $W_2 = \langle U \cup x + y \rangle$ satisfy the conditions of the theorem.

$\mathcal{G}^0$	$\mathcal{G}^1$	$\mathcal{G}^2$	$\mathcal{G}^3$	$\cdots$	$\mathcal{G}^{m-\ell-1}$	$\mathcal{G}^{m-\ell}$
$\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$	0	0	0	$\cdots$	0	0
M_1	$\mathbb{I}_{\#\mathcal{G}^1}$	0	0	$\cdots$	0	0
0	M_2	$\mathbb{I}_{\#\mathcal{G}^2}$	0	$\cdots$	0	0
0	0	M_3	$\mathbb{I}_{\#\mathcal{G}^3}$	$\cdots$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
0	0	0	0	$\cdots$	$M_{m-\ell}$	$\mathbb{I}_{\#\mathcal{G}^{m-\ell}}$

Theorem

The code $\mathcal{C}(\ell, m)^\perp$ is generated by its weight 3 codewords.

Theorem

The higher weights of $\mathcal{C}(\ell, m)^\perp$, except for $d_{\left[{m \atop \ell}\right]_q}$ satisfy

$$d_i - d_{i-1} \in \{1, 2\}.$$

Thank you for your attention.