On Polar Grassmann Codes

I. Cardinali

Abstract

In this note we offer a short summary of the content of the lecture on polar Grassmann codes given at the Indian Intitute of Technology, Mumbai, during the International Conference on Algebraic Geometry and Coding Theory in December 2013. More precisely, we consider the codes arising from the projective system determined by the image $\varepsilon_k^{gr}(\Delta_k)$ of the Grassmann embedding ε_k^{gr} of an orthogonal Grassmannian Δ_k and determine some of their parameters.

Keywords: Polar spaces, orthogonal Grassmannians, Dual polar spaces, embeddings, error correcting codes.

1 Introduction

This note contains a short summary of some new results on linear error correcting codes related to the Grassmann embedding ε_k^{gr} of orthogonal Grassmannians. It is a synthetic transposition of the lecture I gave in December 2013 during the International Conference on Algebraic Geometry and Coding Theory at the Indian Intitute of Technology held in Mumbai, India. These results are extensively presented in the papers [3] and [4]. In Section 2 we provide some preliminaries on the topic; in particular, Subsection 2.1 recalls some properties of orthogonal Grassmannians, while codes arising from projective systems are discussed in Subsection 2.2. Our results are outlined in Section 3. In Section 4 we give some open problems related to polar grassmann codes.

2 Preliminaries

2.1 Orthogonal Grassmannians and their embeddings

Let $V := V(2n+1, q)$ be a $(2n+1)$–dimensional vector space over a finite field $\mathbb{F}_q$ endowed with a non–singular quadratic form η of Witt index n. For $1 \leq k \leq n$ denote by $\mathcal{G}_k$ the k–Grassmannian of $\mathrm{PG}(V)$ and by Δ_k its k–polar Grassmannian. Recall that the k–polar Grassmannian Δ_k is the proper subgeometry of $\mathcal{G}_k$ whose points are the k–subspaces of V which are totally singular for η; the lines of Δ_k are

- for $k < n$: $\ell_{X,Y} := \{Z \mid X \subset Z \subset Y,\ \dim(Z) = k\}$, with $\dim X = k-1$, $\dim Y = k+1$ and Y totally singular;
- for $k = n$: $\ell_X := \{Z \mid X \subset Z \subset X^\perp,\ \dim(Z) = n,\ Z \text{ totally singular}\}$, with X a totally singular $(n-1)$–subspace of V and $X^\perp$ its orthogonal with respect to η.

When $k = n$ the points of ℓ_X form a conic in the projective plane $\mathrm{PG}(X^\perp/X)$. Clearly, Δ_1 is just the orthogonal polar space of rank n associated to η; the geometry Δ_n can be regarded as the dual of Δ_1 and is thus called *orthogonal dual polar space* of rank n.

Given a point–line geometry $\Gamma = (\mathcal{P}, \mathcal{L})$ we say that an injective map $e\colon \mathcal{P} \to \mathrm{PG}(V)$ is a *projective embedding* of Γ if the following two conditions hold:

(1) $\langle e(\mathcal{P})\rangle = \mathrm{PG}(V)$;

(2) e maps any line of Γ onto a projective line.

Following [21], (see also [5]), when condition (2) is replaced by

(2)' e maps any line of Γ onto a non–singular conic of $\mathrm{PG}(V)$,

we say that e is a *Veronese embedding* of Γ.

The dimension $\dim(e)$ of an embedding $e\colon \Gamma \to \mathrm{PG}(V)$, either projective or Veronese, is the dimension of the vector space V. If Σ is a proper subspace of $\mathrm{PG}(V)$ such that $e(\Gamma) \cap \Sigma = \emptyset$ and $\langle e(p_1), e(p_2)\rangle \cap \Sigma = \emptyset$ for any two distinct points p_1 and p_2 of Γ, then it is possible to define a new embedding e/Σ of Γ in the quotient space $\mathrm{PG}(V/\Sigma)$ called the *quotient of e over Σ* by $(e/\Sigma)(x) = \langle e(x), \Sigma\rangle/\Sigma$.

Let now $W_k := \bigwedge^k V$. The *Grassmann* or *Plüker* embedding $e_k^{gr} : \mathcal{G}_k \to \mathrm{PG}(W_k)$ maps the arbitrary k–subspace $\langle v_1, v_2, \ldots, v_k \rangle$ of V (that is a point of $\mathcal{G}_k$) to the point $\langle v_1 \wedge v_2 \wedge \cdots \wedge v_k \rangle$ of $\mathrm{PG}(W_k)$. Let $\varepsilon_k^{gr} := e_k^{gr}|_{\Delta_k}$ be the restriction of e_k^{gr} to Δ_k. For $k < n$, the mapping ε_k^{gr} is a projective embedding of Δ_k in the subspace $\mathrm{PG}(W_k^{gr}) := \langle \varepsilon_k^{gr}(\Delta_k) \rangle$ of $\mathrm{PG}(W_k)$ spanned by $\varepsilon_k^{gr}(\Delta_k)$. We call ε_k^{gr} the *Grassmann embedding of* Δ_k.

If $k = n$, then ε_n^{gr} is a Veronese embedding and maps the lines of Δ_n onto non–singular conics of $\mathrm{PG}(W_n)$.

The dual polar space Δ_n affords also a projective embedding of dimension 2^n, namely the spin embedding ε_n^{spin}.

Let ν_{2^n} be the usual quadratic Veronese map $\nu_{2^n} : V(2^n, \mathbb{F}) \to V(\binom{2^n+1}{2}, \mathbb{F})$. It is well known that ν_{2^n} defines a Veronese embedding of the point–line geometry $\mathrm{PG}(2^n - 1, \mathbb{F})$ in $\mathrm{PG}(\binom{2^n+1}{2} - 1, \mathbb{F})$, which will also be denoted by ν_{2^n}. The composition $\varepsilon_n^{\mathrm{vs}} := \nu_{2^n} \cdot \varepsilon_n^{spin}$ is a Veronese embedding of Δ_n in a subspace $\mathrm{PG}(W_n^{vs})$ of $\mathrm{PG}(\binom{2^n+1}{2} - 1, \mathbb{F})$: it is called the *Veronese–spin embedding* of Δ_n. Properties of Grassmann and Veronese–spin embeddings, fundamental in order to obtain our results, are extensively investigated in [5], [6] and [8].

Theorem 1. *If $\mathbb{F}$ is an arbitrary field with $char(\mathbb{F}) \neq 2$, then*

1. $\dim(\varepsilon_k^{gr}) = \binom{2n+1}{k}$ *for any* $n \geq 2$, $1 \leq k \leq n$.
2. $\varepsilon_n^{\mathrm{vs}} \cong \varepsilon_n^{gr}$ *for any* $n \geq 2$.

When $char(\mathbb{F}) = 2$ it is possible to determine two subspaces $\mathcal{N}_1 \supset \mathcal{N}_2$ of W_n^{vs} such that the following holds.

Theorem 2. *If $char(\mathbb{F}) = 2$ then*

1. $\dim(\varepsilon_k^{gr}) = \binom{2n+1}{k} - \binom{2n+1}{k-2}$ *for any* $1 \leq k \leq n$.
2. $\varepsilon_n^{\mathrm{vs}}/\mathcal{N}_1 \cong \varepsilon_n^{spin}$ *for any* $n \geq 2$.
3. $\varepsilon_n^{\mathrm{vs}}/\mathcal{N}_2 \cong \varepsilon_n^{gr}$ *if* $n \geq 2$.

2.2 Projective systems and Codes

Error correcting codes are an essential component to any efficient communication system, as they can be used in order guarantee arbitrarily low probability of mistake in the reception of messages without requiring noise–free

operation; see [15]. An $[N, K, d]_q$ projective system Ω is a set of N points in $\mathrm{PG}(K-1, q)$ such that for any hyperplane Σ of $\mathrm{PG}(K-1, q)$, we have $|\Omega \setminus \Sigma| \geq d$. Existence of $[N, K, d]_q$ projective systems is equivalent to that of projective linear codes with the same parameters. Indeed, given a projective system $\Omega = \{P_1, \ldots, P_N\}$, fix a reference system $\mathfrak{B}$ in $\mathrm{PG}(K-1, q)$ and consider the matrix G whose columns are the coordinates of the points of Ω with respect to $\mathfrak{B}$. Then, G is the generator matrix of an $[N, K, d]$ code over $\mathbb{F}_q$, say $\mathcal{C} = \mathcal{C}(\Omega)$, uniquely defined up to code equivalence. Furthermore, as any word of $\mathcal{C}(\Omega)$ is of the form $c = mG$ for some row vector $m \in \mathbb{F}_q^K$, it is straightforward to see that the number of zeroes in c is the same as the number of points x of Ω lying on the hyperplane of equation $m \cdot x = 0$ where $m \cdot x = \sum_{i=1}^{K} m_i x_i$ and $m = (m_i)_1^K$, $x = (x_i)_1^K$. In particular, the minimum distance of $\mathcal{C}$ turns out to be $d = min\{|\Omega| - |\Omega \cap \Sigma| \colon \Sigma \text{ is a hyperplane of } \mathrm{PG(k-1, q)}\}$. This provides a geometric interpretation of the meaning of minimum distance.

The link between incidence structures $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ and codes is deep and it dates at least to [17]; we refer the interested reader to [1, 2] and [20] for more details. Traditionally, two basic approaches have proved to be most fruitful: either consider the incidence matrix of a structure as a generator matrix for a binary code, see for instance [1] and [14], or consider an embedding of $\mathcal{S}$ in a projective space and study either the code arising from the projective system thus determined or its dual.

Codes based on projective Grassmannians have been first introduced in [18] as generalisations of Reed–Muller codes of the first order; see also [19]. We refer to [16, 11, 12, 13] for some developments.

3 Main results

We investigate linear codes, henceforth denoted by $\mathcal{C}_{k,n}$, associated with the projective system $\varepsilon_k^{gr}(\Delta_k)$ determined by the image of the Grassmann embedding ε_k^{gr} of Δ_k. We will refer to the codes $\mathcal{C}_{k,n}$ as to *polar Grassmann codes.*

Theorem 3. *Let $C_{k,n}$ be the code determined by the projective system $\bar{\varepsilon}(\Delta_k)$ for $1 \leq k < n$. Then, the parameters of $C_{k,n}$ are*

$$N = \prod_{i=0}^{k-1} \frac{q^{2(n-i)} - 1}{q^{i+1} - 1}, \quad K = \begin{cases} \binom{2n+1}{k} & \textit{for } q \textit{ odd} \\ \binom{2n+1}{k} - \binom{2n+1}{k-2} & \textit{for } q \textit{ even} \end{cases},$$

$$d \geq \psi_{n-k}(q) q^{k(n-k)} - 1.$$

where $\psi_{n-k}(q) \geq q+1$ is the maximum size of a (partial) spread of the parabolic quadric $Q(2(n-k), q)$.

As for the codes arising from dual polar spaces of small rank, we have the following result where the minimum distance is precisely computed.

Theorem 4. *(i) The code $\mathcal{C}_{2,2}$, arising from a dual polar space of rank 2, has parameters*

$$N = (q^2+1)(q+1), \qquad K = \begin{cases} 10 & \text{for } q \text{ odd} \\ 9 & \text{for } q \text{ even} \end{cases}, \qquad d = q^2(q-1).$$

(ii) The code $C_{3,3}$, arising from a dual polar space of rank 3, has parameters

$$\begin{array}{lll} N = (q^3+1)(q^2+1)(q+1), & K = 35, & d = q^2(q-1)(q^3-1) \text{ for } q \text{ odd} \\ & \text{and} & \\ N = (q^3+1)(q^2+1)(q+1), & K = 28, & d = q^5(q-1) \text{ for } q \text{ even.} \end{array}$$

In [4] we prove the following

Theorem 5. *The linear automorphism group of a polar Grassmann code is the orthogonal group $O(2n+1, q)$.*

Relying on some results from [4] and [7] we aim to determine the minimum distance and the minimum weight codewords of the polar line Grassmann codes in the smallest non–trivial case, that is $k = 2$ and $n = 3$, for q an odd prime power.

Theorem 6. *The minimum distance of the code $\mathcal{C}_{2,3}$ is $q^7 - q^5$.*

4 Open problems

Since polar Grassmann codes have been only very recently introduced, many questions are still open for them. We propose the following open problems.

1 Determine the minimum distance for the polar Grassmann code $\mathcal{C}_{k,n}$ of orthogonal type for arbitrary n and $k \leq n$. We are currently working on this problem and already got some partial answers in [4].

2 Investigate properties of the dual code of a polar Grassmann code $\mathcal{C}_{k,n}$.

3 Investigate properties and parameters of polar Grassmann codes of symplectic type, arising from the projective system determined by the image of a symplectic Grassmannian under the Grassmann embedding.

4 Investigate properties and parameters of polar Grassmanns code of Hermitian type, arising from the projective system determined by the image of a unitary Grassmannian under the Grassmann embedding.

References

[1] Assmus, E.F., and J.D. Key., "Designs and their codes", Cambridge University Press, Cambridge (1992).

[2] Cameron, P.J., and J.H. van Lint, "Designs, Graph, Codes and their Links", Cambridge University Press (1991).

[3] Cardinali, I., and L. Giuzzi, *Caps and codes from orthogonal Grassmannians*, Finite Fields Appl. 24 (2013), 148–169.

[4] I. Cardinali and L. Giuzzi *Polar line Grassmann codes of orthogonal type.* In preparation.

[5] Cardinali, I., and A. Pasini, *Veronesean embeddings of dual polar spaces of orthogonal type*, J. Combin. Theory Ser. A, **120** (2013), 1328-1350.

[6] Cardinali I., and A. Pasini, *Grassmann and Weyl Embeddings of Orthogonal Grassmannians*, J. Algebraic Combin. 38 (2013), no. 4, 863–888.

[7] I. Cardinali and A. Pasini, *Embeddings of Line-grassmannians of Polar Spaces in Grassmann Varieties.* Groups of Exceptional Type, Coxeter Groups and Related Geometries, Springer Proc. Math.. To appear.

[8] I. Cardinali and A. Pasini, *On certain submodules of Weyl modules for* $\mathrm{SO}(2n+1,\mathbb{F})$ *with* $\mathrm{char}(\mathbb{F}) = 2$. Journal of Group Theory. To appear.

[9] Couvreur, A., and I. Duursma, *Evaluation codes from smooth Quadric Surfaces and Twisted Segre Varieties*, preprint (arXiv 1101.4603v1).

[10] Ebert, G., K. Metsch, and T. Szöni, *Caps embedded in Grassmannians*, Geometriae Dedicata **70** (1998), 181-196.

[11] Ghorpade, S.R., and G. Lachaud, *Hyperplane sections of Grassmannians and the number of MDS linear codes*, Finite Fields Appl. **7** (2001), 468-506.

[12] Ghorpade, S.R., A.R. Patir, and H.K. Pillai, *Decomposable subspaces, linear sections of Grassmann varieties, and Higher weights of Grassmann codes*, Finite Fields Appl. **15** (2009), 54-68.

[13] S.R. Ghorpade and K.V. Kaipa, *Automorphism groups of Grassmann codes.* Finite Fields Appl. **23** (2013), 80–102.

[14] Y. Kou, S. Lin, M.P.C. Fossorier, *Low–Density Parity Check Codes Based on Finite Geometries: a Rediscovery and New Results*, IEEE Trans. Inform. Theory **47** (2001), 2711-2736.

[15] MacWilliams, F.J., and N.J.A. Sloane, "The theory of error correcting codes", North–Holland Publishing Co., Amsterdam–New York–Oxford (1977).

[16] Nogin, D.Yu., *Codes associated to Grassmannians*, in "Arithmetic, geometry and coding theory (Luminy, 1993)", de Gruyter (1996), 145-154.

[17] Paige, L.J., *A note on the Mathieu groups*, Canad. J. Math. **9** (1957), 15-18.

[18] Ryan, C.T., *An application of Grassmannian varieties to coding theory*, Congr. Numer. **57** (1987), 257-271.

[19] Ryan, C.T., *Projective codes based on Grassmann varieties*, *Congr. Numer.* **57** (1987), 273-279.

[20] Tang, H., J. Xu, S. Lin, and K.A.S. Abded–Ghaffar, *Codes on Finite Geometries*, IEEE Trans. on Information Theory **51**, No. 2 (2005), 572-596.

[21] Thas, J.A., and H. Van Maldeghem, *Generalized Veronesean embeddings of projective spaces*, Combinatorica **31** (5) (2011), 615-629.

Ilaria Cardinali
Department of Information Engineering
University of Siena
Via Roma 56, I-53100, Siena, Italy
ilaria.cardinali@unisi.it