Codes and designs in Grassmannian spaces

Christine Bachoc

Laboratoire A2X, Université Bordeaux I
bachoc@math.u-bordeaux.fr

Abstract

We introduce the notion of designs in the Grassmannian spaces, link it to a certain family of orthogonal polynomials of several variables, establish lower bounds for these designs and prove that these lower bounds are upper bounds for the size of codes in a certain sense.

1 Introduction.

The problem of packings, and related combinatorial questions, in the Grassmanian spaces $\mathcal{G}_{m,n}$ of m-dimensional subspaces of $\mathbb{R}^n$ have been investigated in a series of recent papers (see [4], [5]). Moreover, Grassmannian codes are now used in the transmission of information through the so-called *space-time codes*.

The results presented here are due to the author, together with Renaud Coulangeon, Gabriele Nebe, and Eichii Bannai (see references [2] and [1] where the proofs of the results summarized here can be found).

The notion of designs was developped in many situations, over spaces which are 2-point homogeneous, or more generally on which lives a Q-polynomial association scheme. Originaly this is the work of Delsarte, Goethals and Seidel. The Grassmannian space has none of these properties, although it is homogeneous for the action of the orthogonal group and symmetric.

Despite of that, with the help of group representation, we introduce a notion of designs, and link it to the zonal polynomials related to the Grassmannian space. These are symmetric polynomials of m variables, if m is the dimension of the subspaces of $\mathbb{R}^n$ under consideration, and are orthogonal. Then, we establish lower bounds for the size of these designs.

Our notion of codes in the Grassmannian space does not refer to the choice of a specific distance on this space. It is the natural definition in our context, because the lower bounds for the size of designs are upper bounds for that notion of codes.

2 Designs on Grassmannian spaces.

Let $\mathcal{G}_{m,n}$ denote the real Grassmannian space, which is the space of m-dimensional subspaces of $\mathbb{R}^n$, together with the transitive action of the real orthogonal group $\mathrm{O}(n)$. The starting point is the decomposition of the space of complex-valued squared module integrable functions $L^2(\mathcal{G}_{m,n})$ under the action of $\mathrm{O}(n)$. One has:

$$L^2(\mathcal{G}_{m,n}) = \oplus_\mu \mathrm{H}^\mu_{m,n} \tag{1}$$

where the sum is over the partitions $\mu = \mu_1 \geq \cdots \geq \mu_m \geq 0$ with even parts $\mu_i \equiv 0 \mod 2$, and the spaces $\mathrm{H}^{\mu}_{m,n}$ are isomorphic to the irreducible representation of $\mathrm{O}(n)$ canonically associated to μ, and denoted V_n^{μ} (see [9]). The degree of the partition μ is by definition $\deg(\mu) := \sum_i \mu_i$, and its depth, denoted $\mathrm{depth}(\mu)$ is the number of its non-zero parts.

Definition 2.1 *A finite subset X of $\mathcal{G}_{m,n}$ is called a t-design if one of the following equivalent properties is satisfied:*

(i) For all $f \in \mathrm{H}^{\mu}_{m,n}$ and all μ with $0 \leq \deg(\mu) \leq t$,
$\int_{\mathcal{G}_{m,n}} f(p)dp = \frac{1}{|X|}\sum_{x\in X} f(x)$.

(ii) For all $f \in \mathrm{H}^{\mu}_{m,n}$ and all μ with $2 \leq \deg(\mu) \leq t$, $\sum_{x\in X} f(x) = 0$.

There is a nice caracterization of the designs in terms of the zonal functions of $\mathcal{G}_{m,n}$. It is a classical fact that the orbits under the action of $\mathrm{O}(n)$ of the pairs (p, p') of elements of $\mathcal{G}_{m,n}$ are caracterized by their so-called principal angles $(\theta_1, \ldots, \theta_m) \in [0, \pi/2]^m$. We denote $y_i := \cos^2(\theta_i)$. The polynomial functions on $\mathcal{G}_{m,n} \times \mathcal{G}_{m,n}$ which are invariant under the simultanuous action of $\mathrm{O}(n)$ are the polynomials in the variables $(y_1, \ldots, y_m)$, and are isomorphic to the algebra $\mathbb{C}[Y_1, \ldots, Y_m]^{S_m}$ of symmetric polynomials in m variables. Moreover, there is a unique sequence of polynomials $P_\mu(Y_1, \ldots, Y_m)$ indexed by the partitions into even parts, such that $\mathbb{C}[Y_1, \ldots, Y_m]^{S_m} = \sum_\mu \mathbb{C}P_\mu$, $P_\mu(1, \ldots, 1) = 1$, and the function : $p \in \mathcal{G}_{m,n} \to P_\mu(y_1(p, p'), \ldots, y_m(p, p'))$ defines, for all $p' \in \mathcal{G}_{m,n}$, an element of $\mathrm{H}^{\mu}_{m,n}$. These polynomials have degree $\deg(\mu)/2$. They are explicitely calculated in [10].

Theorem 2.2 *Let $X \subset \mathcal{G}_{m,n}$ be a finite set. Then,*

(i) $\sum_{p,p'\in X} P_\mu(y_1(p, p'), \ldots, y_m(p, p')) \geq 0$.

(ii) The set $X \subset \mathcal{G}_{m,n}$ is a t-design if and only if for all μ, $2 \leq \deg(\mu) \leq t$,

$$\sum_{p,p'\in X} P_\mu(y_1(p, p'), \ldots, y_m(p, p')) = 0.$$

It is worth noticing that, in the case $m = 1$, this notion coincides with the notion of designs in the real projective space introduced in [7] (or equivalently to *antipodal* spherical designs); the corresponding polynomials are Jacobi polynomials.

3 Constructions of designs

In [2], we have pointed out two different constructions of designs in Grassmannian spaces. The first type arises by considering m-dimensional sections of a n-dimensional lattice. This construction is well-known in the case $m = 1$, and standard lattices like the root lattice E_8 or the Leech lattice Λ_{24} give rise to nice designs of the projective space. We show that in the general case $m \geq 1$ this is also the case. Another construction considers orbits on the Grassmannian of finite subgroups of $\mathrm{O}(n)$.

Theorem 3.1 *Let G be a finite subgroup of $O(n)$. Let $m_0 \leq n/2$ be a fixed integer. The following properties are equivalent:*

(i) For all $m \leq m_0$, and for all $p \in \mathcal{G}_{m,n}$, the orbit $G \cdot p$ of p under the action of G is a $t = 2k$-design.

(ii) The representation of G provided by the space V_n^μ for the even partitions μ with $2 \leq \deg(\mu) \leq 2k$ and $\operatorname{depth}(\mu) \leq m_0$ does not contain the trivial character.

Some examples of finite groups G satisfying the conditions of previous theorem are pointed out in [2]. A very nice example is also the Clifford group $\mathcal{C}_k$, of degree 2^k. After the results of [11], the tensor invariants of this group come from self-dual binary codes. Since the first non trivial such code arises in length 8, the Clifford group holds the property of the theorem for $t = 6$ (and for all depths). Hence, all its orbits on the Grassmannians are 6-designs. Examples of such sets arise in [5].

4 Bounds on codes and designs.

In order to give the best possible bounds, we need to introduce the oriented Grassmannian space $\mathcal{G}^\circ_{m,n}$ and its decomposition. We have:

$$\mathcal{G}^\circ_{m,n} \simeq SO(n)/SO(m) \times SO(n-m)) \simeq O(n)/SO(m) \times O(n-m),$$

which is a 2 to 1 covering of $\mathcal{G}_{m,n}$. The orbits under $O(n)$ of pairs $(\tilde{p}, \tilde{q}) \in \mathcal{G}^\circ_{m,n} \times \mathcal{G}^\circ_{m,n}$ can be likewise parametrized by $(m+1)$-tuples $(\epsilon, t_1, \cdots, t_m)$, where $t_1, \cdots, t_m$ are defined as above, and $\epsilon \in \{\pm 1\}$ measures the relative orientation of p and q.

The structure of $L^2(\mathcal{G}^\circ_{m,n})$ as an $O(n)$-module is well-known, and is given for instance in [9], p. 546. We have the following decomposition

$$\mathcal{L}^2(\mathcal{G}^\circ_{m,n}) = \bigoplus H^\mu_{m,n}$$

in pairwise orthogonal non isomorphic irreducible $O(n)$-submodules $H^\mu_{m,n}$, the sum being over partitions $\mu = \mu_1 \geq \mu_2 \geq \ldots \mu_m \geq 0$, with $\mu_i \equiv \mu_j \mod 2$ for all (i,j). We call these partitions *m-admissible*, or *admissible* for short. They split into *odd* and *even*, according to the parity of the μ_i. The class of the $\mathrm{O}(n)$-representation $\mathrm{H}^\mu_{m,n}$ is denoted V_n^μ, and its dimension is denoted d_μ. It is worth noticing that we recover $L^2(\mathcal{G}_{m,n})$ as a subspace, corresponding to the sum of the $H^\mu_{m,n}$ over the even partitions μ.

The already introduced polynomials P_μ zonal polynomials of the Grassmannian space are a special basis of the algebra $\mathbb{C}[Y_1, \cdots, Y_m]^{S_m}$; the zonal plynomials of the oriented Grassmannian form a basis of the algebra $\mathbb{C}[Y_1, \cdots, Y_m]^{S_m}[\theta]$, with $\theta^2 = Y_1 \cdots Y_m$. The polynomials associated to odd partitions belong to $\theta\mathbb{C}[Y_1, \cdots, Y_m]^{S_m}$ and will be denoted $\theta P_\mu(Y_1, \ldots, Y_m)$ where P_μ has degree $\frac{\deg(\mu)-m}{2}$.

We introduce now a notion of codes in the Grassmannian space $\mathcal{G}_{m,n}$.

Definition 4.1 *Let $f(Y_1, \cdots, Y_m)$ be a symmetric polynomial such that $f(1, \cdots, 1) = 1$. A finite subset $\mathcal{D}$ of the Grassmannian space $\mathcal{G}_{m,n}$ is a f-code, if for any pair (p,q) of distinct elements in $\mathcal{D}$ one has*

$$f(y_1(p,q), \cdots, y_m(p,q)) = 0.$$

It is worth noticing that, if $y_1(p,q)+\cdots+y_m(p,q)$ belongs to a given set S when (p,q) belongs to $\mathcal{D}^2$, $p\neq q$, then $\mathcal{D}$ is an f-code for $f=\prod_{s\in S}(Y_1+\cdots+Y_m-s)$ and the degree of f equals the cardinality of S. We recover here the notion of an s-code introduced in [6] (and maybe in previous work of Delsarte).

The following notion of *type* is consistent with [7] Definition 5.4.:

Definition 4.2 *The type of an f-code is* 1 *if $Y_1\cdots Y_m$ divides the polynomial $f(Y_1,\cdots,Y_m)$, and* 0 *otherwise.*

For any integer k, we define

$$H_k=\bigoplus_{\substack{|\mu|\leq k\\ \mu \text{ admissible}}} H^{\mu}_{m,n}.$$

It decomposes, according to the parity of the partitions, as $H_k=H_k^+\oplus H_k^-$, and we have, for the respective dimensions $d_k^{\pm}$ of $H_k^{\pm}$,

$$d_k^+:=\sum_{\substack{|\mu|\leq k\\ \mu \text{ even}\\ \mathrm{depth}(\mu)\leq m}} d_\mu, \text{ resp. } d_k^-:=\sum_{\substack{|\mu|\leq k\\ \mu \text{ odd}\\ \mathrm{depth}(\mu)\leq m}} d_\mu.$$

Then, we have the following results:

Theorem 4.3 *Let $\mathcal{D}\subset\mathcal{G}_{m,n}$ be a $2k$-design. Then*

$$|\mathcal{D}|\geq\max\{d_k^+,d_k^-\}. \tag{2}$$

If equality holds in (2), then $\mathcal{D}$ is an f-code for $f=\frac{1}{d_k^+}\sum_{\substack{|\mu|\leq k\\ \mu \text{ even}}} d_\mu P_\mu$ if $d_k^+\geq d_k^-$, or for $f=\frac{Y_1\cdots Y_m}{d_k^-}\sum_{\substack{|\mu|\leq k\\ \mu \text{ odd}}} d_\mu P_\mu$ if $d_k^+<d_k^-$.

Theorem 4.4 *Any f-code $\mathcal{D}$ in $\mathcal{G}_{m,n}$ satisfies*

$$|\mathcal{D}|\leq d_k^+ \tag{3}$$

where $k=2\deg f$. If moreover f is of type 1, then

$$|\mathcal{D}|\leq d_k^- \tag{4}$$

where $k=2\deg f-m$. Whenever equality holds in (3), resp. (4), then

$$f=\frac{1}{d_k^+}\sum_{\substack{|\mu|\leq k\\ \mu \text{ even}}} d_\mu P_\mu, \text{ resp. } f=\frac{Y_1\cdots Y_m}{d_k^-}\sum_{\substack{|\mu|\leq k\\ \mu \text{ odd}}} d_\mu P_\mu,$$

and $\mathcal{D}$ is a $2k$-design.

References

[1] C. Bachoc, E, Bannai, R. Coulangeon, *Codes and designs in Grassmannian spaces*, submitted

[2] Bachoc, C., Coulangeon, R and Nebe, G. *Designs in Grassmanian spaces and lattices*, J. Algebraic Combinatorics **16** (2002), 5-19.

[3] Bannai, E., and Damerell, R.M. *Tight spherical designs II*, J. London Math. Soc., (3) 21 (1980), 13-30.

[4] Conway, J. H., Hardin, R. H. and Sloane, N. J. A. *Packing Lines, Planes, etc., Packings in Grassmannian Spaces*, Experimental Mathematics, Vol. 5 (1996), 139-159.

[5] Calderbank, A. R., Hardin, R. H., Rains, E. M., Shor, P. W. and Sloane, N. J. A., *A group-theoretic framework for the construction of packings in Grassmannian spaces*, J. Algebraic Combin. 9 (1999), no. 2, 129–140.

[6] Delsarte, Ph., Goethals, J.M. and Seidel, J.J. *Spherical codes and designs*, Geom. Dedicata (6) (1977), 363-388.

[7] Delsarte, Ph., Goethals, J.M. and Seidel, J.J. *Bounds for systems of lines, and Jacobi polynomials*, Philips Res. Repts 30 (1975),91*-105*, Bouwkamp volume.

[8] Fulton, W. and Harris, J. *Representation Theory, a first course*, GTM 129 Springer 1991

[9] Goodman, R. and Wallach, N. R. *Representations and invariants of the classical groups*, Encyclopedia of Mathematics and its Applications 68, Cambridge University Press, 1998.

[10] James, A.T. and Constantine, A.G. *Generalized Jacobi polynomials as spherical functions of the Grassmann manifold*, Proc. London Math. Soc. (3) 29 (1974), 174-192.

[11] Nebe, G., Rains, E., and Sloane, N.J.A. *The invariants of the Clifford groups*, Designs, Codes, and Cryptography 24 (1) (2001), 99-122.