数理解析研究所講究録 1299 巻 2003 年 57-63

ON A GENERALISATION OF SPHERICAL CODES AND DESIGNS.

RENAUD COULANGEON

ABSTRACT. We introduced with C. Bachoc and G. Nebe a notion of design (resp. code) in Grassmannian spaces. This extends the classical notions of spherical design (resp. code), which in this setting corresponds to the Grassmannian space $\mathcal{G}_{1,n}$, the set of lines in $\mathbb{R}^n$. This paper will survey on various results and applications, in particular to the study of Rankin invariants of lattices. We also give some bounds for the size of designs and codes which were obtained in collaboration with E. Bannai.

1. INTRODUCTION.

This a survey on recent work with C. Bachoc, E. Bannai and G. Nebe. To start with, let us recall the classical notions of spherical designs and codes (see [5]). We endow the sphere S^{n-1} with its canonical $O(n)$-invariant measure dx, normalized so as $\int_{S^{n-1}} dx = 1$.

Definition 1.1. *A finite subset set X of S^{n-1} is a t-design, t a positive integer, if for any homogeneous polynomial f of degree at most t one has*

$$\int_{S^{n-1}} f(x)dx = \frac{1}{|X|}\sum_{x\in X} f(x) \tag{1}$$

Definition 1.2. *A finite subset set X of S^{n-1} is an s-code, s a positive integer, if the scalar products of pairwise distinct vectors in X take at most s values*

$$|\{x\cdot y, x\neq y\in X\}|\leq s \tag{2}$$

Examples of designs arise in the theory of Euclidean lattices: if L is a lattice in $\mathbb{R}^n$, *i.e.* a discrete subgroup of $\mathbb{R}^n$ of maximal rank, one defines the set $S(L)$ of minimal vectors of L as the (finite) set of nonzero vectors in L with minimal length. One can of course view $S(L)$, conveniently rescaled, as a finite subset of S^{n-1}. The following theorem, due to B. Venkov, is one of the motivation for our work on generalized designs:

Theorem 1.3 ([11]). *If $S(L)$ is a 4-design, then L achieves a local maximum of the Hermite function $\gamma(L) = \frac{\min L}{(\det L)^{1/n}}$*

Recall that $\min L$ stands for the minimal squared length of nonzero vectors in L, and $\det L = vol(\mathbb{R}^n/L)^2$, so that $\gamma(L)^{n/2}$ is proportional to the density of the sphere packing associated to L.

Our definition of designs in general Grassmanian spaces give rise to similar results for higher dimensional analogues of the Hermite invariants, the so-called Rankin invariants ([10]), see section 5.

It is natural to ask for a *lower* (resp. *upper*) bound for the size of a t-design (resp. s-code). Such bounds were exhibited in [5], and the notion of *tight*-design and code (*i.e.* achieving these bounds) was introduced. Moreover, a kind of duality between tight-designs and tight-codes was brought to the fore. In section 6, we give similar bounds for designs and codes in general Grassmanian spaces.

2. Grassmannnians.

The Grassmannian space $\mathcal{G}_{m,n}$ (*resp.* $\mathcal{G}^{\circ}_{m,n}$) is the set of m-dimensional subspaces (*resp.* oriented subspaces) of $\mathbb{R}^n$. They are homogeneous spaces isomorphic respectively to $O(n)/O(m)\times O(n-m)$ and $O(n)/SO(m)\times O(n-m)$, and $\mathcal{G}^{\circ}_{m,n}$ is a 2 to 1 covering of $\mathcal{G}_{m,n}$.

$$\begin{array}{c}\mathcal{G}^{\circ}_{m,n} \simeq O(n)/SO(m) \times O(n-m)\\ \downarrow{\scriptstyle (2:1)}\\ \mathcal{G}_{m,n} \simeq O(n)/O(m) \times O(n-m)\end{array}$$

Example: $m = 1$

$$\begin{array}{c}\mathcal{G}^{\circ}_{1,n} = S^{n-1}\\ \downarrow{\scriptstyle (2:1)}\\ \mathcal{G}_{1,n} = \mathbb{P}^{n-1}\end{array}$$

We need to characterize the relative positions of two m-dimensional subspaces of $\mathbb{R}^n$, or, in more sophisticated words, to characterize the $O(n)$-orbit of a couple $(p,q) \in {\mathcal{G}_{m,n}}^2$. If $m = 1$, the relative positions of two lines through 0 is determined by their angle. In general, we define a m-tuple of *principal angles* as follows: we fix a base point p_0, for instance $p_0 :=$ the m-dimensional subspace generated by the first m vectors of the canonical basis of $\mathbb{R}^n$. Then, each couple $(p,q) \in {\mathcal{G}_{m,n}}^2$ can be written as $(p,q) = (g.p_0, h.p_0)$ for suitable g and h in $O(n)$. We decompose the matrix $g^{-1}h$ into blocks

$$g^{-1}h = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

with $A \in M_m(\mathbb{R})$, and denote by $1 \geq y_1 \geq y_2 \geq \cdots \geq y_m \geq 0$ the eigenvalues of the real symmetric matrix AA^t. Finally, we let $t_i := \sqrt{y_i} = \cos\theta_i \in [0,1]$. Then, the $O(n)$-orbit of (p,q) is characterized by the m-tuple $(t_1, \cdots, t_m)$

$$O(n).(p,q) \leftrightarrow (t_1, \cdots, t_m). \tag{3}$$

Remark. it is readily seen that this definition of the principal angles is equivalent to the classical one, as given in [7], p.584, for instance.

As for the $O(n)$-orbit of a couple $(\tilde{p},\tilde{q}) \in {\mathcal{G}^{\circ}_{m,n}}^2$, one needs one more invariant, namely $\epsilon := \frac{\det A}{|\det A|}$:

$$O(n).(\tilde{p},\tilde{q}) \leftrightarrow (\epsilon, t_1, \cdots, t_m). \tag{4}$$

3. Some harmonic analysis. Zonal functions.

The space of square integrable functions on $\mathcal{G}_{m,n}$, resp $\mathcal{G}^{\circ}_{m,n}$ splits into $O(n)$-irreducible modules $H^{\mu}_{m,n}$, indexed by partitions $\mu = \mu_1 \geq \cdots \geq \mu_m$ of an integer k in at most m nonzero parts, as follows (see [8] p. 546 or [2]): we say that a partition $\mu = \mu_1 \geq \cdots \geq \mu_m \geq 0$ of an integer k is *admissible* if

$$\mu_i \equiv \mu_j \mod 2 \text{ for all } (i,j), \tag{5}$$

and that μ is *even* (resp. *odd*), if its components are even (resp. odd). The integer $k = \sum \mu_i$, denoted by $|\mu|$, is the degree of μ. We the have:

$$\begin{array}{ccc} L^2(\mathcal{G}^{\circ}_{m,n}) & = & \bigoplus_{\mu \text{ admissible}} H^{\mu}_{m,n} \\ \uparrow & & \\ L^2(\mathcal{G}_{m,n}) & = & \bigoplus_{\substack{\mu \text{admissible} \\ \text{and even}}} H^{\mu}_{m,n} \end{array}$$

EXAMPLE: $m = 1$, $\mu = k$, $H^k_{1,n} = \mathrm{Harm}_k[X_1, \cdots, X_n]$, the space of harmonic polynomials of degree k.

It is worth noticing that the $H^{\mu}_{m,n}$ do depend only on n and μ, that is to say, if $m \leq m'$ and μ is a partition with at most m nonzero parts, then $H^{\mu}_{m,n} \simeq H^{\mu}_{m',n}$.

To each irreducible constituent $H^{\mu}_{m,n}$ is attached a *zonal* function P_μ on $\mathcal{G}^{\circ}_{m,n} \times \mathcal{G}^{\circ}_{m,n}$, characterized by:

(i) $P_\mu(p,.) \in H^{\mu}_{m,n}$ for all $p \in \mathcal{G}^{\circ}_{m,n}$, $P_\mu(.,q) \in H^{\mu}_{m,n}$ for all $q \in \mathcal{G}^{\circ}_{m,n}$

(ii) $P_\mu(\sigma p, \sigma q) = P_\mu(p,q)$ for all $\sigma \in O(n)$, $(p,q) \in {\mathcal{G}^{\circ}_{m,n}}^2$.

If μ is even, one has

$$P_\mu(p,q) = p_\mu(y_1(p,q), \cdots, y_m(p,q)),$$

where $p_\mu(Y_1, \cdots, Y_m)$ is a symmetric polynomial of degree $\frac{|\mu|}{2}$, whereas if μ is odd

$$P_\mu(p,q) = (\epsilon t_1 \cdots t_m) p_\mu(y_1, \cdots, y_m),$$

with $p_\mu(Y_1, \cdots, Y_m)$ a symmetric polynomial of degree $\frac{|\mu|-m}{2}$.

From now on, we normalize the zonal functions so as:

$$P_\mu(p,p) = 1.$$

We then have the two following properties:

(i) $\langle P_\mu(p,.), P_\lambda(q,.)\rangle = \frac{\delta_{\lambda,\mu}}{d_\mu} P_\mu(p,q)$,
where $d_\mu = \dim H^{\mu}_{m,n}$.

(ii) $P_\lambda P_\mu = \sum_\tau c_{\lambda,\mu}(\tau) P_\tau$, with $c_{\lambda,\mu}(\tau) \geq 0$.

4. Designs.

For any integer $k \geq 1$, we define

$$H_k^+ := \bigoplus_{\substack{|\mu| \leq k \\ \mu \text{even}}} H_{m,n}^\mu \subset L^2(\mathcal{G}_{m,n}) \subset L^2(\mathcal{G}_{m,n}^\circ)$$

$$\text{and } H_k^- := \bigoplus_{\substack{|\mu| \leq k \\ \mu \text{odd}}} H_{m,n}^\mu \subset L^2(\mathcal{G}_{m,n})^\perp \subset L^2(\mathcal{G}_{m,n}^\circ).$$

Definition 4.1 ([2]). *A subset $\mathcal{D} \subset \mathcal{G}_{m,n}$ is a $2k$-design if*

$$\forall \varphi \in H_{2k}^+ \;,\; \int_{\mathcal{G}_{m,n}} \varphi(p) dp = \frac{1}{|\mathcal{D}|} \sum_{p \in \mathcal{D}} \varphi(p)$$

Notice that, since the definition is given in the setting of *non oriented* grassmannians, what we get for $m = 1$ is not exactly the definition of spherical designs, but more restrictively, the notion of *antipodal* design (see [5]).

There are several criteria to test whether a given subset of a Grassmannian space is a design. The first one involves the zonal functions P_μ mentioned above.

Proposition 4.2 ([2]). *The following properties, for a subset $\mathcal{D} \subset \mathcal{G}_{m,n}$, are equivalent:*

(i) *$\mathcal{D}$ is a $2k$-design.*
(ii) *$\forall \mu$ with $2 \leq |\mu| \leq 2k$, $\sum_{p \in \mathcal{D}} P_\mu(p, \cdot) = 0$.*
(iii) *$\forall \mu$ with $2 \leq |\mu| \leq 2k$, $\sum_{(p,q) \in \mathcal{D}^2} P_\mu(p, q) = 0$.*

In order to apply this proposition, one has to compute explicitly the polynomials P_μ. This is done in [9]. For $m = 1$, the P_μ are the classical Gegenbauer polynomials [5].

We also have criteria of a completely different kind, involving group theory. The orthogonal group $O(n)$ acts on the set of n by n symmetric matrices SM_n by $g.S = (g^t)^{-1} S g^{-1}$, which in turn induces a representation of $O(n)$ in $\mathrm{Hom}_k(SM_n)$, the space of homogeneous polynomials of degree k in the matrix argument $S = (S_{i,j}) \in SM_n$

$$g.P(S) := P(g^{-1}.S) = P(g^t S g). \tag{6}$$

We then have the following theorem:

Theorem 4.3 ([2]). *Let G be a finite subgroup of $O(n)$. Then, the following properties are equivalent:*

(i) *$\forall m \leq \frac{n}{2}$, $\forall p \in \mathcal{G}_{m,n}$, $G \cdot p$ is a $2k$-design.*
(ii) $\mathrm{Hom}_k(SM_n)^G = \mathrm{Hom}_k(SM_n)^{O(n)}$.

This applies in particular when $G = \mathrm{Aut}\, L$ is the automorphism group of a lattice L. For instance, if $L = \mathbb{D}_4, \mathbb{E}_6$ or $\mathbb{E}_7$, theorem (4.3) applies with $k = 2$, if $L = \mathbb{E}_8$, it applies with $k = 3$, and if $L = \Lambda_{24}$ (the Leech lattice), with $k = 5$ (see [2]).

5. Rankin invariants.

Besides the classical Hermite function γ ($= \gamma_1$ in what follows), which we mentioned in the introduction, Rankin [10] defined a collection of functions γ_m, in the following way : let L be a lattice in $\mathbb{R}^n$, endowed with the usual scalar product denoted $x \cdot y$, and $1 \leq m \leq \dim L$ an integer. One defines

$$\delta_m(L) = \inf_{p \in L(m)} \det p, \tag{7}$$

in which $L(m)$ stands for the set of m-dimensional sublattices of L, and

$$\gamma_m(L) = \delta_m(L)/(\det L)^{\frac{m}{n}} \tag{8}$$

For $m = 1$, $\gamma_1(L)$ is the classical Hermite invariant of L. In general, the function γ_m is bounded on the set of n-dimensional positive definite lattices ([10]), and the supremum, which actually is a maximum, is denoted by $\gamma_{m,n}$. The lattices achieving a local maximum for γ_m are called m-extreme (see [4] for a characterization of m-extreme lattices in terms of m-perfection and m-eutaxy).

We define the set of minimal m-sections of L as

$$\mathcal{S}_m(L) = \{p \in L(m) \mid \det p = \delta_m(L)\} \tag{9}$$

which is a finite set. The map $p \mapsto \mathbb{R}p$ (the m-dimensional subspace spanned by p) induces an embedding of $\mathcal{S}_m(L)$ in $\mathcal{G}_{m,n}$ (this is because $\mathbb{R}p/p$ is torsion-free, by the minimality of p). So, we can view $\mathcal{S}_m(L)$ as a subset of $\mathcal{G}_{m,n}$. We then have the following theorem, analogous to Venkov's theorem mentioned in the introduction:

Theorem 5.1 ([2]). *$\mathcal{S}_m(L)$ is a 4-design $\Rightarrow$ L is m-extreme.*

The proof relies on the characterization of m-extreme lattices in terms of m-perfection and m-eutaxy mentioned above. This theorem, together with theorem 4.3, allows to check that some classical lattices are extreme with respect to all Rankin invariants:

Proposition 5.2. *If $L = \mathbb{D}_4, \mathbb{E}_6, \mathbb{E}_7, \mathbb{E}_8$ or Λ_{24}, then L is m-extreme for any m, $1 \leq m \leq \frac{\dim L}{2}$.*

This kind of results would be out of reach without the help of theorem 4.3 and 5.1.

6. Codes in Grassmannian varieties. Bounds.

Definition 6.1 ([1]). *Let $f(Y_1, \cdots, Y_m)$ be a symmetric polynomial such that $f(1, \cdots, 1) = 1$.*

A subset $\mathcal{D} \subset \mathcal{G}_{m,n}$ is an f-code if for all $(p, q) \in \mathcal{D}^2$, $p \neq q$ one has

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

REMARK. For $m = 1$, one recovers the usual definition of an s-code, *i.e.* a set of points on the sphere such that the mutual distances take at most s distinct values.

Let $d_k^+ = \dim H_k^+$ and $d_k^- = \dim H_k^-$. These dimensions can be easily calculated from the dimensions d_n^μ of the irreducible components $H_{m,n}^\mu$, as given for instance in [6], chapter 24. They are involved in the following two theorems, which give bounds for the size of designs and codes in $\mathcal{G}_{m,n}$.

Theorem 6.2 ([1]). *Let $\mathcal{D} \subset \mathcal{G}_{m,n}$ be a $2k$-design. Then*

$$|\mathcal{D}| \geq \max(d_k^+, d_k^-).$$

If equality holds, then $\mathcal{D}$ is an f-code with respect to

$$f = \frac{1}{d_k^+} \sum_{\substack{|\mu| \leq k \\ \mu \text{ even}}} d_\mu p_\mu \quad \text{or} \quad \frac{y_1 \cdots y_m}{d_k^-} \sum_{\substack{|\mu| \leq k \\ \mu \text{ odd}}} d_\mu p_\mu$$

$$(d_k^+ > d_k^-) \qquad\qquad (d_k^- > d_k^+)$$

Definition 6.3 ([1]). *An f-code has type 1 if $Y_1 \cdots Y_m$ divides f, type 0 otherwise.*

Theorem 6.4 ([1]). *Any f-code $\mathcal{D} \subset \mathcal{G}_{m,n}$ satisfies*

$$|\mathcal{D}| \leq d_k^+,$$

where $k = 2 \deg f$. If moreover f has type 1, then $\mathcal{D} \subset \mathcal{G}_{m,n}$ satisfies

$$|\mathcal{D}| \leq d_k^-,$$

where $k = 2 \deg f - m$.

If equality holds, then

$$f = \frac{1}{d_k^+} \sum_{\substack{|\mu| \leq k \\ \mu \text{ even}}} d_\mu p_\mu \text{ (type 0)},$$

resp.

$$f = \frac{y_1 \cdots y_m}{d_k^-} \sum_{\substack{|\mu| \leq k \\ \mu \text{ odd}}} d_\mu p_\mu \text{ (type 1)}$$

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

Designs, resp. codes, achieving the bound of theorem 6.2, resp. 6.4, are called *tight*.

EXAMPLE. In [3], §5, an infinite family $\mathcal{D}_p$ of packings in $\mathcal{G}_{\frac{p-1}{2},p}$, p a prime which is either 3 or congruent to -1 modulo 8, is defined. It consists on $\frac{p(p+1)}{2} = d_{[0,\cdots,0]} + d_{[2,0,\cdots,0]} = d_2^+$ subspaces with same pairwise chordal distance $d^2 = \frac{(p+1)^2}{4(p+2)}$. Since $d^2 = \sum \sin^2\theta_i = \frac{p-1}{2} - \sum y_i$, $\mathcal{D}_p$ is an f-code, with $f = \frac{4(p+2)(\sum Y_i)-(p^2-5)}{p^2-5}$, and theorem 6.4 applies, so that:

Proposition 6.5 ([1]). *For any prime p which is either 3 or congruent to -1 modulo 8, $\mathcal{D}_p$ is a tight 4-design in $\mathcal{G}_{\frac{p-1}{2},p}$.*

References

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

[2] Bachoc, C., Coulangeon, R and Nebe, G. *Designs in Grassmannian spaces and lattices*, to appear in J. Algebraic Combin.

[3] 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.

[4] Coulangeon, R. *Réseaux k-extrêmes*, Proc. London Math. Soc. (3) 73 (1996), no. 3, 555-574.

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

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

[7] Golub, G. H. and Van Loan, C. F. *Matrix computations*, John Hopkins Univ. Press, 2nd ed., 1989.

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

[9] 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.

[10] Rankin, R. A. *On positive definite quadratic forms*, J. London Math. Soc. (28) (1953), 309–314.

[11] Venkov, B. *Réseaux et designs sphériques*, in Monographies de l'Enseignement Mathématique (37) (2001), 10–86.

R. Coulangeon, Laboratoire A2X, Université Bordeaux I, 351, cours de la Libération, 33405 Talence France

E-mail address: coulange@math.u-bordeaux.fr