Journal of Algebraic Combinatorics **10** (1999), 279–288

Spherical 7-Designs in 2^n-Dimensional Euclidean Space

V.M. SIDELNIKOV
Dept. of Mathematics and Mechanics, Moscow State University, Moscow, Russia

Received July 23, 1997; Revised July 15, 1998

Abstract. We consider a finite subgroup Θ_n of the group $O(N)$ of orthogonal matrices, where $N = 2^n$, $n = 1, 2 \ldots$. This group was defined in [7]. We use it in this paper to construct spherical designs in 2^n-dimensional Euclidean space R^N. We prove that representations of the group Θ_n on spaces of harmonic polynomials of degrees 1, 2 and 3 are irreducible. This and the earlier results [1–3] imply that the orbit $\Theta_{n,2}\mathbf{x}^t$ of any initial point $\mathbf{x}$ on the sphere S_{N-1} is a 7-design in the Euclidean space of dimension 2^n.

Keywords: spherical design, orthogonal matrix, Euclidean space

1. Introduction

A spherical t-design in N-dimensional Euclidean space $\mathbf{R}^N$ is a finite nonempty set X of points on the unit sphere $S_{N-1} = \{\mathbf{x} = (x_1, \ldots, x_N) \in R^N \mid x_1^2 + \cdots + x_N^2 = 1\}$ such that

$$\frac{1}{|S_{N-1}|}\int_{S_{N-1}} f(\mathbf{x})\, d\mathbf{x} = \frac{1}{|X|}\sum_{\mathbf{x}\in X} f(\mathbf{x})$$

for all polynomials $f(\mathbf{x})$ of degree at most t where $|S_{N-1}|$ denotes the surface area of the S_{N-1}. Account of basic properties of spherical t-designs may be found in [1].

Let Hom(k) be the space of all homogeneous N-variable polynomials of degree k over $\mathbf{R}$ and let Harm(k) be the space of all homogeneous harmonic polynomials of degree k, i.e. the space of all homogeneous polynomials $y = y(\mathbf{x})$ satisfying the potential equation $\frac{\partial^2 y}{\partial x_1^2} + \cdots + \frac{\partial^2 y}{\partial x_N^2} = 0$. The dimension of Harm$(k)$ is $\binom{N+k-1}{k} - \binom{N+k-3}{k-2}$ [5, 6]. In what follows we assume that $N > 2$.

The space Harm(k) is an irreducible invariant subspace of the representation of the orthogonal group $O(N)$ on Hom(k). Speaking more precisely, the space Hom(k) can be represented as the direct sum:

$$\mathrm{Hom}(k) = \mathrm{Harm}(k) + \mathrm{Harm}(k-2)|\mathbf{x}|^2 + \cdots + \mathrm{Harm}(k-2l)|\mathbf{x}|^{2l}, \quad l = \left[\frac{k}{2}\right].$$

This material is based upon work supported by the U.S. Civilian Research Development under Award No RM-346 and by Russian Fundamental Research Foundation under Award No 96 01-00931.

Each term in this sum is an invariant irreducible subspace of the representation of $O(N)$ on Hom(k), where $|\mathbf{x}|$ denotes the norm of the vector $\mathbf{x}$ and $|\mathbf{x}|^2$ is used as a shorthand for the polynomial $x_1^2 + \cdots + x_N^2$ [6, 7].

Since $\mathbf{\Theta}_n$ is a subgroup of the group $O(N)$ the spaces Harm$(k-2j)$ are also invariant spaces of the representation of $\mathbf{\Theta}_n$ on Hom(k) and they in turn can be decomposed into direct sum of some nontrivial invariant subspaces.

Next we state some basic results, that will be useful in what follows.

Theorem A [2, Th. 6.10 and Th. 3.1], [3, Th. 1] *Let G be a finite subgroup of the group $O(N)$ and let ρ_k be a representation of G on Harm(k). If all representations ρ_i for $i = 1, \ldots, t$ are irreducible then for any $\mathbf{x} \in S_{N-1}$ the set*

$$X = \{g\mathbf{x} \mid g \in G\} \subset S_{N-1}$$

is a spherical $2t$-design.

If the set X in addition satisfies $\sum_{\mathbf{x}\in X} f(\mathbf{x}) = 0$ for all $f(\mathbf{x}) \in$ Harm$(2t+1)$, then X is a spherical $(2t+1)$-design.

In [7] we constructed a finite group $\Sigma_{n,p}$ which for p being an odd prime is a group of $p^n \times p^n$-matrices over $\mathbf{C}$, and for $p = 2$ is a group of $2^n \times 2^n$-matrices over $\mathbf{R}$.

The group $\Sigma_{n,p}$, $p > 2$, has an isomorphic image in a certain group $\tilde{\Sigma}_{n,p}$ of $2p^n \times 2p^n$-matrices over $\mathbf{R}$ [7]. The group $\Sigma_{n,2}$ has a remarkable subgroup $\mathbf{\Theta}_n$ of index 2 comprising all matrices from $\Sigma_{n,2}$ with rational entries.

The order of the group $\mathbf{\Theta}_n$ is asymptotically $c2^{n(2n+1)}$, $c = 1.38\ldots$, $n \to \infty$.

We used the group $\mathbf{\Theta}_n$ to construct orbit codes $\mathcal{K}(\mathbf{x}^t) = \mathbf{\Theta}_n\mathbf{x}$ with $\mathbf{x} = \mathbf{o}_1$, where $\mathbf{o}_1 = (1, 0, \ldots, 0)$ (see [7]). The cardinality of the code $\mathcal{K}(\mathbf{o}_1)$ is asymptotically $2.38\ldots$, $2^{n(n+1)/2}$, $n \to \infty$, and its Euclidean code distance is 1. The order of the stabilizer of the point $\mathbf{o}_1$ in the group $\mathbf{\Theta}_n$ is $O(2^{n(3n+1)/2)})$.

1. Definition and properties of the group $\Sigma_{1,p}$ Let $\mathbf{F}_p$ be a p-element Galois field, let $f(x) \in \mathbf{F}_p[x]$ denotes the polynomial of the second degree, let

$$E_{f,p} = \text{diag}(\exp(2\pi i f(0)/p), \ldots, \exp(2\pi i f(p-1)/p)$$

be a diagonal matrix, where $i = \sqrt{-1}$, and let $A(s) = A_p(s) = \|w^s_{a,b}\|$ be a unitary symmetrical $p \times p$ matrix, where $a, b \in \mathbf{F}_p$, $s = 1, 2, \ldots, p-1$, and $w^s_{a,b} = p^{-1/2}\exp(2\pi i abs/p)$. Note, that $(A(s))^{-1} = A(-s)$. Consider a group

$$\Sigma_{1,p} = \langle A(s), E_{f,p};\, s = 1, 2, \ldots, p-1,\ f(x) \in \mathbf{F}_p[x], \deg\ f(x) \le 2\rangle,$$

generated by $p-1$ unitary matrices $A(s)$ and p^3 diagonal matrices $E_{f,p}$.

Theorem B [7] *The group $\Sigma_{1,p}$ is a finite group of order $\sigma_{1,p}$, where*
1. $\sigma_{1,p} = 4p^4(p^2-1)$ *whenever* $p = 3 \bmod 4$,
2. $\sigma_{1,p} = 2p^4(p^2-1)$ *whenever* $p = 1 \bmod 4$,
3. $\sigma_{1,p} = 2^4$ *whenever* $p = 2$.

The entries of the matrices in $\Sigma_{1,p}$ and in matrices of the group $\Sigma_{n,p}$ to be defined later are complex numbers whenever $p > 2$. There exists an isomorphic mapping ϕ of the group $\Sigma_{n,p}$ to the group $\tilde{\Sigma}_{n,p}$ of orthogonal $2p^n \times 2p^n$ matrices over **R**. There also exists a mapping ρ from U^{p^n-1} to the sphere S^{2p^n-1} such that for any matrix $P \in \Sigma_{n,p}$ we have $\lambda(\mathbf{x} - \mathbf{x}P) = \lambda'(\rho(\mathbf{x}) - \rho(\mathbf{x})\phi(P))$, where λ is the usual metric in $\mathbf{C}^{p^n}$ and λ' is the Euclidean metric in $\mathbf{R}^{2p^n}$. Thus, the maps ϕ and ρ are isomorphic and isometric transformations of codes on U^{p^n-1} into codes on S^{2p^n-1}.

2. **Definition of the group** $\Sigma_{n,p}, n > 1$ Let $D = \|d_{i,j}\|$ be a $n \times n$ matrix over Galois field $\mathbf{F}_p$, i.e., $D \in M_n(\mathbf{F}_p)$.

1. By $\mathbf{Ker}(D)$ we denote the linear space of zeroes of matrix D over the field $\mathbf{F}_p$, i.e. the set of all vectors $\mathbf{x}$ in n-dimensional space $(\mathbf{F}_p)^n$ such that $D\mathbf{x}^t = \mathbf{0}$. By $\mathbf{Im}(D)$ we denote the space spanned by columns of the matrix D, i.e. $\mathbf{Im}(D) = \{D\mathbf{x}^t; \mathbf{x} \in (\mathbf{F}_p)^n\}$.
2. Let $D, R, T \in M_n(\mathbf{F}_p), \alpha^t \in \mathbf{F}_p^n$ and $m = \dim \mathbf{Ker}(T)$. A $p^n \times p^n$ matrix $C(D, R, T, \alpha) = |v_{\mathbf{a},\mathbf{b}}|, \mathbf{a}, \mathbf{b} \in (\mathbf{F}_p)^n$, over the complex numbers, i.e. matrix from $M_{p^n}(\mathbf{C})$, is defined by

   $$v_{\mathbf{a},\mathbf{b}} = 0,$$

   whenever $R\mathbf{a} - T\mathbf{b} + \alpha \neq \mathbf{0}$, and by

   $$v_{\mathbf{a},\mathbf{b}} = p^{-m/2} \exp(2\pi i \mathbf{a} D \mathbf{b}^t / p),$$

   whenever

   $$R\mathbf{a} - T\mathbf{b} + \alpha = \mathbf{0}. \tag{1}$$

   Let $\mathbf{U}_n = \{\alpha_1, \ldots, \alpha_N\} = (\mathbf{F}_p)^n, N = p^n$, be the set of all elements of the space $(\mathbf{F}_p)^n$, listed in the lexicographical order. We use the set $\mathbf{U}_n$ for indexing rows and columns of the matrices $C(D, R, T, \alpha)$ in such a way that the entry in the intersection of the ith row and the jth column is equal to v_{α_i,α_j}.

   Note that the identity matrix $\tilde{E}$ in $M_{2^n}(\mathbf{R})$ can be represented as $\tilde{E} = C(0, Q, Q, 0)$, where Q is an arbitrary nondegenerate matrix in $M_n(\mathbf{F}_p)$. The matrix $C(0, E, E, -\alpha) = \Gamma_\alpha$ is a substitution matrix corresponding to the translation $\sigma : \mathbf{x} \to \mathbf{x} + \alpha$ in the space $(\mathbf{F}_p)^n$.
3. Denote by $B(D, R, T, \alpha)$ a matrix $C(D, R, T, \alpha)$ such that the matrices D, R, T and the vector α satisfy the following two conditions
   a. $\mathbf{Im}(R) = \mathbf{Im}(T)$ and $\alpha \in \mathbf{Im}(R)$.
   b. The bilinear form $\mathbf{x}D\mathbf{y}^t$ has for $m > 0$ the following property: for any not identically zero vector $\mathbf{x}_0$ in $\mathbf{Ker}(R)$ the linear function $\mathbf{x}_0 D\mathbf{y}^t$ mapping $\mathbf{y}$ to $\mathbf{Ker}(T)$ is not identically zero, i.e. $\mathbf{x}_0 D\mathbf{y}_0^t \neq 0$ for some $\mathbf{y}_0$ in $\mathbf{Ker}(T)$.
4. Let $f(\mathbf{x}) \in \mathbf{F}_p[\mathbf{x}], \mathbf{x} = (x_1, \ldots, x_n)$, be a polynomial of the second degree. By E_f we denote the diagonal matrix $E_f = \mathrm{diag}(\exp(2\pi i f(\alpha_1)/p), \ldots, \exp(2\pi i f(\alpha_\mathrm{N})/p))$.

Notice that

$$B(D, R, T, \alpha) = E_l B(D, R, T, 0)\Gamma_\beta,$$

where Γ_β is the substitution matrix corresponding to the translation $\sigma : \mathbf{x} \to \mathbf{x} + \beta$ in the space $\mathbf{F}_p^n$, β is an arbitrary vector in $\mathbf{F}_p^n$ satisfying $\beta T = -\alpha$ and $l = l(\mathbf{x}) = \mathbf{x} D \beta^t$ is the linear function.

5. Let $p = 2$, or $p = 1 \bmod 4$. We denote by $\Sigma_{n,p}$ the set of all unitary $p^n \times p^n$ matrices of the form

$$P = \pm E_{f_1} B(D, R, T, \alpha) E_{f_2}, \tag{2}$$

where $f_1(\mathbf{x})$ and $f_2(\mathbf{x})$ range over all pairs n-variate polynomials of degree at most 2, and matrices D, R, T and element α are chosen from the set of all quadruples $\{D, R, T, \alpha\}$, satisfying the properties 3.a. and 3.b. If $p = 3 \bmod 4$, then by $\Sigma_{n,p}$ we denote the set of all matrices of the form $i^\varepsilon P$, where ε is chosen in the set of numbers $\{1, 2, 3, 4\}$, and the matrix P is chosen in the set of all matrices of the form (2). The matrices in $\Sigma_{n,p}$ are all unitary as follows from Lemma A.

Lemma A [7] *The matrix $C(D, R, T, \alpha)$ is unitary iff conditions 3.a., 3.b hold, i.e., the matrix $C(D, R, T, \alpha)$ is unitary matrix iff it coincides with the matrix $B(D, R, T, \alpha)$.*

Theorem C [7] *The set $\Sigma_{n,p}$ of unitary matrices is closed under multiplication, i.e. $\Sigma_{n,p}$ is the finite group. The order of the group $\Sigma_{n,p}$ is*

$$\sigma_{n,p} = \vartheta(p)(p^n - 1) \cdot \ldots \cdot (p^n - p^{n-1}) \left(\sum_{m=0}^{n} p^{n-m} \begin{bmatrix} n \\ n-m \end{bmatrix}_p \tau_{m,p} \right) \tau_{n,p}/p \tag{3}$$

where $\vartheta(2) = 1$, $\vartheta(p) = 2$ whenever $p = 1 \bmod 4$, $\vartheta(p) = 4$, whenever $p = -1 \bmod 4$, $[{n \atop m}]_p = [{n \atop n-m}]_p = (p^n - 1) \cdot \ldots \cdot (p^n - p^{m-1})/(p^m - 1) \cdot \ldots \cdot (p^m - p^{m-1})$, $m \geq 1$, is a Gaussian coefficient, and $\tau_{n,2} = 2^{n(n+1)/2+1}$, $\tau_{n,p} = p^{n(n+3)/2+1}$, $p > 2$, is the number of n-variable polynomials of the second degree in $\mathbf{F}_p[\mathbf{x}]$, $\mathbf{x} = (x_1, \ldots, x_N)$, $N = p^n$.

In particular, $\sigma_{2,2} = 2304 = 2^8 \cdot 3^2$, $\sigma_{3,2} = 2^{14} \cdot 3^2 \cdot 5 \cdot 7$, $\sigma_{4,2} = 2^{22} \cdot 3^5 \cdot 5^2 \cdot 7$, $\sigma_{5,2} = 2^{32} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot 31$, $\sigma_{6,2} = 2^{44} \cdot 3^8 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 17 \cdot 31$.

Corollary A [7] *The order $\sigma_{n,p}$ of the group $\Sigma_{n,p}$ is $\sigma_{n,p} = O(p^{2n^2+3n+1})$ whenever $p > 2$, and $\sigma_{n,2} \sim c2^{n(2n+1)+1}$, $n \to \infty$. In this asymptotic $c = 1.77\ldots$.*

For $p = 2$ the set $\mathbf{\Theta}_n$ is defined as a set of matrices P of the form (2) with dim $\mathbf{Ker}(R)$ even, i.e the set $\mathbf{\Theta}_n \subset \Sigma_{n,2}$ is the set of all matrices over the rationals.

The structure of the group $\Sigma_{n,p}$ was studied by Lev Kazarin [9].

Theorem D [7] *The set $\mathbf{\Theta}_n$ is a subgroup of index 2 of the group $\Sigma_{n,2}$.*

2. 7-Designs

We also use the set $\mathbf{U}_n$ defined above for indexing unknown quantity x_α of 2^n-variable polynomials $f(\mathbf{x})$ in $\mathbf{R}[\mathbf{x}]$.

Lemma B *For any $n \geq 3$, the group $\mathbf{\Theta}_n$ has a triplewise transitive subgroup Υ of substitution matrices, i.e. for any two monomials $x_{\alpha_i} x_{\alpha_j} x_{\alpha_k}$ and $x_{\beta_i} x_{\beta_j} x_{\beta_k}$, where $\{\alpha_i, \alpha_j, \alpha_k\}$ and $\{\beta_i, \beta_j, \beta_k\}$ are both three-element subsets of the set $\mathbf{F}_2^n$, there is a substitution matrix Γ in the group Υ such that $\Gamma x_{\alpha_i} x_{\alpha_j} x_{\alpha_k} = x_{\beta_i} x_{\beta_j} x_{\beta_k}$.*

Proof: A substitution matrix is a matrix with rational entries. Therefore to prove the lemma it suffices to show that $\Upsilon \subset \Sigma_{n,2}$.

We shall show that the subgroup of $\Sigma_{n,2}$ of all substitution matrices $\Gamma(\sigma)$ corresponding to affine maps $\sigma : \mathbf{x} \to \mathbf{x}Q + \alpha$, where Q is a nondegenerate matrix over $\mathbf{F}_2$ and $\alpha \in \mathbf{F}_2^n$, has all stated properties. Denote this subgroup by Υ.

Direct calculations show that

$$\Gamma(\sigma) = B(0, E, Q, -\alpha),$$

hence the group Υ is a subgroup of $\Sigma_{n,2}$.

To show triplewise transitivity of the subgroup Υ, we prove that it contains substitution matrix corresponding to the affine map $\sigma : \mathbf{x} \to Q\mathbf{x} + \beta$, which transforms three-element set $\beta = \{\beta_1, \beta_2, \beta_3\}$ into the set $\{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2\}$, where $\mathbf{e}_i = (\underbrace{0, \dots, 0}_{i-1}, 1, 0, \dots, 0)$, $i = 1, \dots, n$.

Indeed, we first use the substitution matrix Γ_{β_3} to transform the set β into the set $\gamma = \{\mathbf{0}, \gamma_1, \gamma_2\}$, $\gamma_i = \beta_i + \beta_3$, $i = 1, 2$. Then use a linear map $\sigma' : \mathbf{x} \to Q\mathbf{x}$ with nondegenerate matrix Q such that $Q\gamma_i = \mathbf{e}_i$, $i = 1, 2$, to transform the set γ into the set $\{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2\}$. The required substitution matrix is $\Gamma = \Gamma(\sigma')\Gamma_{\beta_3}$. The proof is complete. □

Quadratic homogeneous harmonic polynomial in $N = 2^n$ variables looks as follows

$$F(\mathbf{x}) = \sum_{i<j} a_{\alpha_i,\alpha_j} x_{\alpha_i} x_{\alpha_j} + \sum_{i=1}^{N} a_{\alpha_i} x_{\alpha_i}^2, \quad \text{where} \quad \sum_{i=1}^{N} a_{\alpha_i} = 0$$

and a cubic one has the following form

$$F(\mathbf{x}) = \sum_{i<j<k} a_{\alpha_i,\alpha_j,\alpha_k} x_{\alpha_i} x_{\alpha_j} x_{\alpha_k} + \sum_{i<j} a_{\alpha_i,\alpha_j} x_{\alpha_i} x_{\alpha_j}^2 + \sum_{i>j} b_{\alpha_i,\alpha_j} x_{\alpha_i} x_{\alpha_j}^2 + \sum_{i=1}^{N} a_{\alpha_i} x_{\alpha_i}^3,$$

where

$$\sum_{j=1}^{i-1} a_{\alpha_i,\alpha_j} + \sum_{j=i+1}^{N} b_{\alpha_j,\alpha_i} + 3a_{\alpha_i} = 0 \ \text{ for all } \alpha_i.$$

This implies that the dimension of Harm(3) is $\binom{N}{3} + 2\binom{N}{2} + \binom{N}{1} - N = \binom{N+2}{3} - \binom{N}{1}$ which agrees with the above-mentioned relation.

It should be noted that

$$E_f F(\mathbf{x}) = F(E_f \mathbf{x}^t) = \sum_{i<j<k} (-1)^{f(\alpha_i)+f(\alpha_j)+f(\alpha_k)} a_{\alpha_i,\alpha_j,\alpha_k} x_{\alpha_i} x_{\alpha_j} x_{\alpha_k}$$
$$+ \sum_{i<j} (-1)^{f(\alpha_i)} a_{\alpha_i,\alpha_j} x_{\alpha_i} x_{\alpha_j}^2 + \sum_{1>j} (-1)^{f(\alpha_i)} b_{\alpha_i,\alpha_j} x_{\alpha_i} x_{\alpha_j}^2$$
$$+ \sum_{i=1}^{N} (-1)^{f(\alpha_i)} a_{\alpha_i} x_{\alpha_i}^3 .$$

Lemma C *For any $n > 1$*

$$\sum_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2} E_f x_{\beta_i} x_{\beta_j} x_{\beta_k} = \begin{cases} 2^{n(n+1)/2} x_{\mathbf{0}} x_{\mathbf{e}_1} x_{\mathbf{e}_2}, & \text{if } \{\beta_1, \beta_2, \beta_3\} = \{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2\}; \\ 0, & \text{if } \{\beta_1, \beta_2, \beta_3\} \neq \{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2\}, \end{cases}$$

where the sum in $\sum_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}$ ranges over the set of all diagonal matrices E_f with Boolean function $f(\mathbf{x}) = f_0 + \sum_{i=1}^{N} f_{\alpha_i} x_{\alpha_i} + \sum_{i<j} f_{\alpha_i,\alpha_j} x_{\alpha_i} x_{\alpha_j}$ satisfying

$$f(\mathbf{0}) + f(\mathbf{e}_1) + f(\mathbf{e}_2) = 0. \tag{4}$$

Proof: Let $B_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}$ be the linear space of all Boolean functions $f(\mathbf{x})$, $\deg f(\mathbf{x}) \leq 2$, such that (4) holds. The dimension of $B_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}$ is one less then the dimension of the space of all Boolean functions of second degree, i.e. it is equal to $n(n+1)/2$.

Consider a function $l(f) = l_{\beta_1,\beta_2,\beta_3}(f) = f(\beta_1) + f(\beta_2) + f(\beta_3)$ on the space $B_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}$. It is obvious, $l(f)$ is a linear function and in particular $l_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}(f)$ is identically zero. We have to prove that the function $l(f)$ is nondegenerate whenever $\{\beta_1, \beta_2, \beta_3\} \neq \{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2\}$. For this it suffices to show that in the space $B_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}$ there is a function $f(\mathbf{x})$ such that $l(f) = 1$.

Let $L_{\mathbf{e}_1,\mathbf{e}_2}$ be the two-dimensional linear subspace of the space $\mathbf{F}_2^n$ spanned by $\mathbf{e}_1, \mathbf{e}_2$. First we consider the case when the vectors $\{\beta_1, \beta_2, \beta_3\}$ are pairwise distinct and $\{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2\} \neq \{\beta_1, \beta_2, \beta_3\}$.

We consider two subcases:

a) $\{\beta_1, \beta_2, \beta_3\} \subset L_{\mathbf{e}_1,\mathbf{e}_2}$, e.g., $\beta_1 = \mathbf{e}_1$, $\beta_2 = \mathbf{e}_2$, $\beta_3 = \mathbf{e}_1 + \mathbf{e}_2$;
b) the vector $\beta_1 = (\beta_{1,1}, \ldots, \beta_{1,n})$ does not belong to $L_{\mathbf{e}_1,\mathbf{e}_2}$.

In the subcase a) the function $f(\mathbf{x}) = x_1 x_2$ will do since $f(\mathbf{0}) + f(\mathbf{e}_1) + f(\mathbf{e}_2) = 0$ and $f(\mathbf{e}_1 + \mathbf{e}_2) + f(\mathbf{e}_1) + f(\mathbf{e}_2) = 1$. If $\beta_1 = \mathbf{0}$, $\beta_2 = \mathbf{e}_2$, $\beta_3 = \mathbf{e}_1 + \mathbf{e}_2$ or $\beta_1 = \mathbf{0}$, $\beta_2 = \mathbf{e}_1$, $\beta_3 = \mathbf{e}_1 + \mathbf{e}_2$ then the function $f(\mathbf{x}) = x_1 + x_2$ has the required properties.

Now we pass to the subcase b). Consider a set $M = \{\beta_1', \beta_2', \beta_3'\}$, where $\beta_i' = (0, 0, \beta_{i,3}, \ldots, \beta_{i,n})$, $i = 1, 2, 3$. Under the hypothesis of this subcase β_1' is not identically zero vector. If either the elements of M are linearly independent or $\beta_1' = \beta_2' = \beta_3'$, then obviously there is a vector $\mathbf{l} = (0, 0, l_3, \ldots, l_n)$ such that $\langle \mathbf{l}, \beta_1' \rangle = \langle \mathbf{l}, \beta_2' \rangle = \langle \mathbf{l}, \beta_3' \rangle = 1$. In this case the function $f(\mathbf{x}) = \langle \mathbf{l}, \mathbf{x} \rangle$ satisfies both $f(\mathbf{0}) + f(\mathbf{e}_1) + f(\mathbf{e}_2) = 0$ and $f(\beta_1) + f(\beta_2) + f(\beta_3) = 1$.

If $\beta'_1 = \beta'_2 + \beta'_3$ and $\beta'_1 \neq 0$, $\beta'_2 \neq 0$, then there are two vectors $\mathbf{l}_i = (0, 0, l_{i,3}, \ldots, l_{i,n})$, $i = 1, 2$, such, that $\langle \mathbf{l}_1, \beta'_1 \rangle = \langle \mathbf{l}_1, \beta'_2 \rangle = 1$, $\langle \mathbf{l}_1, \beta'_3 \rangle = 0$ and $\langle \mathbf{l}_2, \beta'_1 \rangle = \langle \mathbf{l}_2, \beta'_3 \rangle = 1$, $\langle \mathbf{l}_2, \beta'_2 \rangle = 0$, since the vectors β'_1 and β'_2 are linearly independent. In this case the function $f(\mathbf{x}) = \langle \mathbf{l}_1, \mathbf{x} \rangle \langle \mathbf{l}_2, \mathbf{x} \rangle$ satisfies both $f(\mathbf{0}) + f(\mathbf{e}_1) + f(\mathbf{e}_2) = 0$ and $f(\beta_1) + f(\beta_2) + f(\beta_3) = 1$.

If $\beta'_1 = \beta'_2 + \beta'_3$ and $\beta'_1 = \beta'_2 \neq 0$, i.e. $\beta'_3 = 0$, then the vectors $\beta''_i = (\beta_{i,1}, \beta_{1,2}, 0, \ldots, 0)$, $i = 1, 2$, are distinct. For example, let $\beta''_1 \neq 0$. There exist two vectors $\mathbf{l}' = (l_1, l_2, 0, \ldots, 0)$ and $\mathbf{l} = (0, 0, l_3, \ldots, l_n)$ such, that $\langle \beta''_1, \mathbf{l}' \rangle = 1$, $\langle \beta''_2, \mathbf{l}' \rangle = 0$, and $\langle \mathbf{l}, \beta'_1 \rangle = 1$. The function $f(\mathbf{x}) =< \mathbf{l}', \mathbf{x} >< \mathbf{l}, \mathbf{x} >$ satisfies both $f(\mathbf{0}) + f(\mathbf{e}_1) + f(\mathbf{e}_2) = 0$ and $f(\beta_1) + f(\beta_2) + f(\beta_3) = 1$.

Now consider the case when there are at least two identical vectors in the set $\{\beta_1, \beta_2, \beta_3\}$. W.l.o.g. suppose that $\beta_2 = \beta_3$. Then $f(\beta_1) + f(\beta_2) + f(\beta_3) = f(\beta_1)$. Therefore we may consider a one-element set $\{\beta_1\}$ instead of a three-element one. In this case the proof that there is a function $f(\mathbf{x})$ in $B_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}$ such that $l(f) = f(\beta_1) = 1$, and $f(\mathbf{0}) + f(\mathbf{e}_1) + f(\mathbf{e}_2) = 0$ goes along the same lines but is a little bit easier. We leave this proof to reader.

Thus, we have proved that in all cases the function $l(f) = l_{\beta_1,\beta_2,\beta_3}(f)$ is not identically zero function provided $\{\beta_1, \beta_2, \beta_3\} \neq \{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2\}$.

The proof of the lemma follows from the identity

$$\sum_{B_{\mathbf{0},\mathbf{e}_1,\mathbf{e}_2}} (-1)^{l(f)} = 0, \tag{5}$$

which holds for any not identically zero function $l(f)$. This identity (5) follows from the fact that each nondegenerate linear function takes the value 0 in exactly one half of the points. The proof is complete. □

Theorem E *For any $n > 1$ the representations ρ_1, ρ_2, and ρ_3 of the group $\boldsymbol{\Theta}_{n,2}$ on* Harm(1), Harm(2), *and* Harm(3) *respectively are irreducible.*

Proof: First, consider the most complicated case, namely a representation ρ_3 on Harm(3). The main idea of the proof is as follows. Suppose, contrary to our claim, that Harm(3) is not irreducible. Then the Maschke theorem implies that Harm(3) is a direct sum of two nontrivial invariant subspaces, say H and H'. If we could prove, that each of H and H' contains a monomial $x_{\mathbf{0}} x_{\mathbf{e}_1} x_{\mathbf{e}_2}$, then we would get $H \cap H' \neq \{0\}$, a contradiction.

Thus, the proof of the theorem is reduced to the proof of the following statement. Any not identically zero invariant subspace H of Harm(3) contains the monomial $x_{\mathbf{0}} x_{\mathbf{e}_1} x_{\mathbf{e}_2}$. We proceed to prove this statement.

It should be noted that any harmonic polynomial which does not contain monomials of the form $x_{\alpha_i} x_{\alpha_j} x_{\alpha_k}$ with three-element set of indices $\alpha_i, \alpha_j, \alpha_k$, contains at least one monomial of the form $x_{\beta_i} x^2_{\beta_j}$ with not identically zero coefficient. Therefore no harmonic polynomial can be composed entirely by monomials of the form x^3_β.

First we shall prove that any not identically zero invariant subspace H has polynomial, which contains some monomial $x_{\alpha_i} x_{\alpha_j} x_{\alpha_k}$ with not identically zero coefficient and three-element set $\{\alpha_i, \alpha_j, \alpha_k\}$ of indices.

Suppose the contrary, i.e. that any polynomial $F(\mathbf{x})$ in H has not identically zero coefficients only for monomials of either form $x_{\beta_i}x^2_{\beta_j}$ or x^3_β. Since the group Υ is triplewise transitive (see Lemma C) we can assume that monomial $x_{\mathbf{0}}x^2_{\mathbf{e}_1}$ is one of them. In this case we prove, that there exist a polynomial $G(\mathbf{x}) \in H$ and a matrix $B \in \mathbf{\Theta}_n$ such that the polynomial $G(B\mathbf{x})$ has some monomial $x_{\alpha_i}x_{\alpha_j}x_{\alpha_k}$ with not identically zero coefficient and a three-element set $\{\alpha_i, \alpha_j, \alpha_k\}$ of indices.

For this we consider the polynomial

$$m(\mathbf{x}) = m_F(\mathbf{x}) = \sum_{\mathbf{0}} F(E_h\mathbf{x}^t), \tag{6}$$

where the sum $\sum_{\mathbf{0}}$ ranges over the linear space $L_{\mathbf{0}}$ of all Boolean functions of the form $h(\mathbf{x}) = \sum_{i=1}^N h_{\alpha_i}x_{\alpha_i} + \sum_{i<j} h_{\alpha_i,\alpha_j}x_{\alpha_i}x_{\alpha_j}$ (with $h(\mathbf{0}) = 0$). It is easy to show along the same lines as in the proof of Lemma 2, that

$$m(\mathbf{x}) = 2^{n(n+1)/2}\left(\sum_{\alpha\neq\mathbf{0}} a_{\mathbf{0},\alpha}x_{\mathbf{0}}x^2_\alpha + a_{\mathbf{0}}x^3_{\mathbf{0}}\right) \quad \text{and} \quad \sum_{\alpha\neq\mathbf{0}} a_{\mathbf{0},\alpha} + 3a_{\mathbf{0}} = 0. \tag{7}$$

Note that $m(\mathbf{x}) \neq 0$, provided $a_{\mathbf{0},\mathbf{e}_1} \neq 0$ and the last equality in (7) holds since $m(\mathbf{x})$ is a harmonic polynomial.

Consider a matrix $B = B(D, R, R, 0)$ in $\mathbf{\Theta}_n$, where $D = \operatorname{diag}(1, 1, 0, \ldots, 0)$ and $R = \operatorname{diag}(0, 0, 1, \ldots, 1)$. The matrix B can be represented as $B = \operatorname{diag}(A_2, \ldots, A_2)$ with a suitable numbering of rows and columns. Here A_2 is the 4×4 Hadamard matrix $A_2 = 1/2\|(-1)^{\langle\alpha_i,\alpha_j\rangle}\|$, $\alpha_1 = \mathbf{0}$, $\alpha_2 = \mathbf{e}_1$, $\alpha_3 = \mathbf{e}_2$, $\alpha_4 = \mathbf{e}_1 + \mathbf{e}_2$. Notice that entry $v_{\alpha,\beta}$ of the matrix $B = \|v_{\alpha,\beta}\|$ is not identically zero iff $\alpha + \beta \in \mathbf{L}_2$, where $\mathbf{L}_2 = \mathbf{L}_{\mathbf{e}_1,\mathbf{e}_2}$ is the two-dimensional subspace in $\mathbf{F}^n_2$ spanned by vectors $\mathbf{e}_1, \mathbf{e}_2$. In this case $v_{\alpha,\beta} = (-1)^{\alpha D\beta_t}$.

Let $a_{\mathbf{0}} = 0$. In this case we show, that the polynomial $m(B\mathbf{x})$ has a monomial $x_{\alpha_i}x_{\alpha_j}x_{\alpha_k}$ with not identically zero coefficient and three-element set $\{\alpha_i, \alpha_j, \alpha_k\}$ of indices.

Let $\beta = \{\beta_1, \beta_2, \beta_3\}$ be a three-element subset of the set $\{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_2\} = \mathbf{L}_2$ and let

$$S_i = (\{\beta_1, \beta_2, \beta_3\}) = \frac{1}{8}\sum{}'(-1)^{\langle\beta_i,\gamma_2\rangle+\langle\beta_i,\gamma_3\rangle}, \quad i = 1, 2, 3,$$

where the sum ranges over all permutation $(\gamma_1, \gamma_2, \gamma_3)$ of the triple $(\beta_1, \beta_2, \beta_3)$. Direct calculations show that

$$m_F(B\mathbf{x}^t)2^{-n(n+1)/2} = \sum_\beta (a_{\mathbf{0},\mathbf{e}_1}S_1(\beta) + a_{\mathbf{0},\mathbf{e}_2}S_2(\beta) + a_{\mathbf{0},\mathbf{e}_1+\mathbf{e}_2}S_3(\beta))x_{\beta_1}x_{\beta_2}x_{\beta_3} + \ldots, \tag{8}$$

where the sum $\sum_\beta$ ranges over all four distinct three-element subsets β of the set L_2, and dots stand for monomials $x_{\alpha_1}x_{\alpha_2}x_{\alpha_3}$ such that $\{\alpha_1, \alpha_2, \alpha_3\} \not\subset \mathbf{L}_2$.

Let $S(\beta) = (S_1(\beta), S_2(\beta), S_3(\beta))$. By easy calculations we have $S(\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2) = \frac{1}{8}(6, 2, 2)$, $S(\mathbf{0}, \mathbf{e}_1, \mathbf{e}_1 + \mathbf{e}_2) = S(\mathbf{0}, \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_2) = \frac{1}{8}(6, -2, -2)$, and $S(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_2) = \frac{1}{8}(6, 6, 6)$. The space $\mathbf{S}$, $\mathbf{S} \subset \mathbf{R}^3$, spanned by these three vectors has dimension 2. The vector $(0, -1, 1)$ is a basis of one-dimensional space $\mathbf{S}^\perp$ orthogonal to $\mathbf{S}$.

By assumption $a_{\mathbf{0},\mathbf{e}_1} \neq 0$, therefore $\mathbf{a} = (a_{\mathbf{0},\mathbf{e}_1}, a_{\mathbf{0},\mathbf{e}_2}, a_{\mathbf{0},\mathbf{e}_1+\mathbf{e}_2}) \notin \mathbf{S}^{\perp}$. It follows that in the four-element set $\mathbf{L}_2$ of vectors there is at least one, say β, such that $(S(\beta), \mathbf{a}) \neq 0$. Thus we get that the polynomial $m(B\mathbf{x}^t)$ (cf. (8)) has some monomial $x_{\beta_1}x_{\beta_2}x_{\beta_3}$, $\{\beta_1, \beta_2, \beta_3\} \subset \mathbf{L}_2$, with not identically zero coefficient and three-element set of indices $\beta_1, \beta_2, \beta_3$.

Let now $a_{\mathbf{0}} \neq 0$. Consider the subgroup Υ' of the group Υ, consisting of all substitution matrices, corresponding to linear maps $\sigma : \mathbf{x} \to Q\mathbf{x}$ in the space $(\mathbf{F}_2)^n$, where Q is a $n \times n$ nondegenerate matrix over the field $\mathbf{F}_2$. Notice, that $\mathbf{0}$ is a fixed point of the map σ, therefore the polynomials $x_{\mathbf{0}}$, $x_{\mathbf{0}}^2$ and $x_{\mathbf{0}}^3$ and only they are fixed points of any transformation in Υ'.

The polynomial

$$q(\mathbf{x}) = \sum_{P\in\Upsilon'} m_F(P\mathbf{x}^t) = a\sum_{\alpha\neq\mathbf{0}} x_{\mathbf{0}}x_{\alpha}^2 + bx_{\mathbf{0}}^3,\ a + 3b = 0,\ b = a_{\mathbf{0}}|\Upsilon'|, \tag{9}$$

is invariant with respect to all transformations in Υ'. Therefore under the hypothesis $a_{\mathbf{0}} \neq 0$ the factor a in this expression is not identically zero.

Next we show, that a nondegenerate polynomial $q(B\mathbf{x}^t)$ has monomial $x_{\beta_1}x_{\beta_2}x_{\beta_3}$, $\{\beta_1, \beta_2, \beta_3\} \subset \{\mathbf{0}, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_2\} = \mathbf{L}_2$, with three-element set of indices and not identically zero coefficient. The proof of this statement goes along the same lines as the proof of the previous case $a_{\mathbf{0}} = 0$. Namely, first we explicitly calculate a vector of coefficients $S(\beta) = (S_0(\beta), S_1(\beta), S_2(\beta), S_3(\beta))$, $\beta = \{\beta_1, \beta_2, \beta_3\}$, to be used in the expression for the coefficient corresponding to the monomial $x_{\beta_1}x_{\beta_2}x_{\beta_3}$ (cf. (8)). Notice, that now we have extended a set of coefficients $S_i(\beta)$, $i = 0, 1, 2, 3$, by a new one $S_0(\beta)$, determined by the relation $u(2B\mathbf{x}^t) = \sum_\beta S_0(\beta)x_{\beta_1}x_{\beta_2}x_{\beta_3}$, where $u(\mathbf{x}) = x_{\mathbf{0}}^3$.

Again, just as in the case $a_0 = 0$ the space $\mathbf{S}$, spanned by vectors from $S(\beta)$ has dimension 2. The space $\mathbf{S}^{\perp}$ of vectors $\mathbf{a} = (a_{\mathbf{0}}, a_{\mathbf{0},\mathbf{e}_1}, a_{\mathbf{0},\mathbf{e}_2}, a_{\mathbf{0},\mathbf{e}_1+\mathbf{e}_2})$ such that $(\mathbf{S}, \mathbf{a}) = 0$ also has dimension 2 and its basis is $(-1, 1, 0, 0)$, $(0, 0, -1, 1)$.

The vector $\mathbf{a} = \mathbf{a}(q) = (a_{\mathbf{0}}, a_{\mathbf{0},\mathbf{e}_1}, a_{\mathbf{0},\mathbf{e}_2}, a_{\mathbf{0},\mathbf{e}_1+\mathbf{e}_2})$ of coefficients of the polynomial $q(\mathbf{x})$ is equal to (b, a, a, a), $b \neq 0$, $a \neq 0$, and does not belong to $\mathbf{S}^{\perp}$. Therefore among four vectors $S(\beta)$, $\beta \in \mathbf{L}_2$, there must be at least one, such that $(S(\beta), \mathbf{a}(q)) \neq 0$, i.e. $q(B\mathbf{x}^t)$ has monomial $x_{\beta_i}x_{\beta_j}x_{\beta_k}$ with not identically zero coefficient and three-element set $\{\beta_i, \beta_j, \beta_k\}$ of indices.

Thus, in any nontrivial invariant subspace H there is a polynomial $g(\mathbf{x})$ having at least one monomial $x_{\alpha_i}x_{\alpha_j}x_{\alpha_k}$ with not identically zero coefficient and three-element set $\{\alpha_1, \alpha_2, \alpha_3\}$ of indices. In the group Υ there is a matrix Y, which transforms the monomial $x_{\alpha_i}x_{\alpha_j}x_{\alpha_k}$ into monomial $x_{\mathbf{0}}x_{\mathbf{e}_1}x_{\mathbf{e}_2}$. Therefore in any subspace H there is a polynomial which contains the monomial $x_{\mathbf{0}}x_{\mathbf{e}_1}x_{\mathbf{e}_2}$ with not identically zero coefficient. This and Lemma C imply, that H contains the monomial $x_{\mathbf{0}}x_{\mathbf{e}_1}x_{\mathbf{e}_2}$. This proves the theorem in the case of representation ρ_3.

The proof of irreducibility of the representations ρ_1 and ρ_2 is easier than the proof of irreducibility of the representation ρ_3 and goes along the same lines. In particular, in the case of the space Harm(2) (respectively Harm(1)), we prove, that any not identically zero invariant subspace contains the monomial $x_{\mathbf{0}}x_{\mathbf{e}_1}$ (respectively $x_{\mathbf{0}}$). The details are left to reader. The theorem is proved. □

Theorem F *For any* $\mathbf{x} \in S_{N-1}$ *the set* $\mathcal{K}(\mathbf{x}) = \mathbf{\Theta}_n \mathbf{x}^t$ (*the orbit of the group* $\mathbf{\Theta}_n$ *with the initial point* $\mathbf{x}$ *or the orbit code*) *is a* 7*-design.*

Proof: It follows from the Theorem A, Theorem E and the identity

$$\sum_{B \in \mathbf{\Theta}_n} F(B\mathbf{x}^t) = 0,$$

which holds for any polynomial $F(\mathbf{x})$ in $\mathrm{Hom}(2k+1)$, since the group $\mathbf{\Theta}_n$ contains a matrix $-E$, where E is the identity matrix.

One natural question is how one can select an initial point $\mathbf{x}$ in such a way that the number of elements of the design $\mathcal{K}_n(\mathbf{x})$ is minimal. Obviously $|\mathcal{K}_n(\mathbf{x})| = |\mathbf{\Theta}_n|/|\Omega(\mathbf{x})|$, where $\Omega(\mathbf{x})$ is the stabilizer of the point $\mathbf{x}$ in the group $\mathbf{\Theta}_n$. As shown in [7] (Lemma 6)

$$|\Omega(\mathbf{o}_1)| = (2^n - 1) \cdots (2^n - 2^{n-1})\tau_{n,2}/2,$$

where $\mathbf{o}_1 = (1, 0, \ldots, 0)$ and $\tau_{n,2} = 2^{n(n+1)/2+1}$ is the number of n-variable polynomials of the second degree over the field $\mathbf{F}_2$.

This implies that

$$|\mathcal{K}(\mathbf{o}_1)| = \sum_{m=0}^{n} 2^{n-m} \begin{bmatrix} n \\ m \end{bmatrix}_2 \tau_{m,2}$$

It should be noted that the cardinalities $|\mathcal{K}_n(\mathbf{o}_1)|$ of the designs $\mathcal{K}_n(\mathbf{o_1})$ for dimensions $N = 8, 16, 32$ ($n = 3, 4, 5$) coincide with the cardinalities of well-know designs derived from Barnes-Wall lattices [8].

Other natural question is whether there exists an initial point $\mathbf{x}$, for which the design $\mathcal{K}(\mathbf{x})$ has the strength larger than 7. This question will be studied by the author in forthcoming papers. □

Acknowledgments

The author wishes to thank L.S. Kazarin and N.P. Varnovsky for their useful suggestions. We also thank Prof. C. Godsil and anonymous reviewer for many valuable comments.

References

1. P. Delsarte, J.M. Goethals, and J.J. Seidel, "Spherical codes and designs," *Geometriae Dedicata* **6** (1977), 263–288.
2. J.M. Goethals and J.J. Seidel, "Spherical designs," *Proc. of Symposium in Pure Math.*, Vol. 34, pp. 255–272, 1979.
3. E. Bannai, "On some spherical t-designs," *J. Combinatorial Theory (A)* **26** (1979), 157–161.
4. E. Bannai, "Spherical t-designs which are orbits of finite groups," *J. Math. Soc.* **36**(2), 1984, 341–354.
5. S. Helgason, *Groups and Geometrical Analysis*, Academic Press, INC, 1984.
6. N. Ya. Vilenkin, *Special Functions and Theory of Representation of Groups*, Moscow, Nauka, 1965, (in Russian).
7. V.M. Sidelnikov, "On one finite matrix group and codes on Euclidean sphere," *Problems of Information Transmission* **33** (1997), 29–44.
8. J.H. Conway, and N.J.A. Sloane, *Sphere Packing, Lattices and Groups*, 2nd edition, Springer-Verlag, 1993.
9. Lev Kazarin, "On groups suggested by Sidelnikov," *Math. USSR Sbornik* (1998), to appear.