V. M. Sidel'nikov, Orbital spherical 11-designs in which the initial point is a root of an invariant polynomial,
Algebra i Analiz, 1999, Volume 11, Issue 4, 183–203

Алгебра и анализ
Том 11 (1999), вып. 4

ОРБИТНЫЕ СФЕРИЧЕСКИЕ 11-ДИЗАЙНЫ, У КОТОРЫХ НАЧАЛЬНАЯ ТОЧКА — КОРЕНЬ ИНВАРИАНТНОГО МНОГОЧЛЕНА

© В. М. Сидельников

В работе рассматриваются сферические t-дизайны на N-мерной евклидовой сфере S_{N-1}, которые являются орбитой $G\mathrm{x}_0$ конечной группы G ортогональных матриц с начальной точкой $\mathrm{x}_0 \in S_{N-1}$. Если в качестве начальной точки x_0 взять общий корень всех гармонических G-инвариантных многочленов $f(\mathrm{x})$ степени $\leqslant t$ с нулевым средним, т.е. тех $f(\mathrm{x})$, для которых $\int_{S_{N-1}} f(\mathrm{x})d\mu(\mathrm{x}) = 0$, то орбита будет t-дизайном [1].

Для групп $\Phi_{n,2}$ и $\Sigma_{n,2}$ ортогональных $2^n \times 2^n$-матриц, введенных в работе [13], показано, что пространство $\Phi_{n,2}$-инвариантных и $\Sigma_{n,2}$-инвариантных гармонических многочленов степеней $\leqslant 9$ с нулевым средним является одномерным. Найдена образующая $\Lambda(\mathrm{x})$ этого пространства. Показано, что $\Sigma_{n,2}$-инвариантных гармонических многочленов десятой степени нет. Если x_0 — корень $\Lambda(\mathrm{x})$, то орбита $\Phi_{n,2}\mathrm{x}_0$ является 9-дизайном, а орбита $\Sigma_{n,2}\mathrm{x}_0$ — 11-дизайном в 2^n-мерном евклидовом пространстве.

§1. Введение

Сферическим t-дизайном в N-мерном евклидовом пространстве $\mathbb{R}^N$ называется непустое конечное множество $X \subset S_{N-1}$, для которого выполнено соотношение

$$\frac{1}{|S_{N-1}|}\int\limits_{S_{N-1}} f(\mathrm{x})d\mu(\mathrm{x}) = \frac{1}{|X|}\sum_{x\in X} f(\mathrm{x})$$

для всех многочленов степени $\leqslant t$, где $S_{N-1} := \{(x_1,\dots,x_N) \in \mathbb{R}^N : x_1^2 + \dots + x_N^2 = 1\}$— единичная сфера в $\mathbb{R}^N$, $\mu(\mathrm{x})$ — обычная евклидова (т.е. инвариантная относительно ортогональной группы $O(N)$) мера на S_{N-1} и $|S_{N-1}| := \int_{S_{N-1}} d\mu(\mathrm{x})$ — площадь поверхности S_{N-1}. Читатель может ознакомиться с основными свойствами сферических t-дизайнов по работам [2, 4].

Работа поддержана Американским фондом US Civilian Research Development, грант № RM1-346 и РФФИ, грант № 96-01-00931.

Основные определения: $\mathrm{Hom}(k)$ — пространство однородных многочленов степени k над $\mathbb{R}$ от N переменных, $\mathrm{Harm}(k)$ — пространство однородных гармонических многочленов степени k, т.е. пространство однородных полиномов $y = y(\mathbf{x})$, для которых выполнено уравнение Лапласа $\frac{\partial^2 y}{\partial x_1^2} + \cdots + \frac{\partial^2 y}{\partial x_n^2} = 0$. Размерности пространств $\mathrm{Hom}(k)$ и $\mathrm{Harm}(k)$ равны $m(N,k) = \binom{N+k-1}{k}$ и $n(N,k) = \binom{N+k-1}{k} - \binom{N+k-3}{k-2}$ соответственно [7, 6].

Скалярное произведение (f,g) на $\mathrm{Hom}(k)$ определим обычным образом, а именно с помощью соотношения

$$(f,g) := \frac{1}{|S_{N-1}|} \int\limits_{S_{N-1}} f(\mathbf{x})g(\mathbf{x})d\mu(\mathbf{x}).$$

Пространство $\mathrm{Harm}(k)$ является неприводимым инвариантным подпространством представления ортогональной группы $O(N)$ на $\mathrm{Hom}(k)$. Говоря более точно, пространство $\mathrm{Hom}(k)$ может быть представлено как прямая сумма [7, 6]:

$$\begin{aligned}\mathrm{Hom}(k) &= \mathrm{Harm}(k) + r^2\,\mathrm{Harm}(k-2) + \dots \\ &+ r^{2l}\,\mathrm{Harm}(k-2l), \quad l = [k/2],\ r^2 := \sum_{i=1}^{N} x_i^2.\end{aligned} \tag{1}$$

Как следует из [6, гл. 2, теорема 2.1, следствие 2.4] и [7, гл. IX, §6, с. 441]:

i. Каждый многочлен $f(\mathbf{x})$ степени не выше t равен на S_{N-1} сумме $f(\mathbf{x}) = \sum_{i=0}^{t} a_i h_i(\mathbf{x})$ однородных гармонических многочленов $h_i(\mathbf{x})$ степеней i, т.е. равен некоторому гармоническому многочлену.

ii.

$$\int\limits_{S_{N-1}} h_j(\mathbf{x})d\mu(\mathbf{x}) = 0, \quad j > 0,\ h_j(x) \in \mathrm{Harm}(j). \tag{2}$$

Отсюда следует

Лемма А [3]. *Пусть* $H(t) = \mathrm{Harm}(1) + \cdots + \mathrm{Harm}(t)$, $t \geqslant 1$. *Множество* X *является* t*-дизайном тогда и только тогда, когда для любого* $h(\mathbf{x})$ *из* $H(t)$ *выполнено*

$$\sum_{\mathbf{x}\in X} h(\mathbf{x}) = 0.$$

Отметим, что пространство $H(t)$ состоит, как следует из (2), из гармонических многочленов $f(\mathbf{x})$ степени $\leqslant t$ с нулевым средним, т.е. многочленов, для которых $\int_{S_{N-1}} f(\mathbf{x})d\mu(\mathbf{x}) = 0$.

Пусть G — конечная группа ортогональных матриц и $\mathbf{a}$ — точка на S^{N-1}. Естественный класс дизайнов X составляют орбитные дизайны, т.е. множества вида $X := G\mathbf{a} := \{g\mathbf{a} \mid g \in G\}$, которые представляют собой орбиту начальной точки $\mathbf{a}$.

Как показано в [3–5], орбита $G\mathbf{a}$ является $2s$-дизайном при любом $\mathbf{a} \in S^{N-1}$, если естественное представление группы G на пространстве гармонических многочленов степени k является абсолютно неприводимым для каждого k, $k = 0, \dots, s$.

В работе [1, теорема 3.12] доказано, что орбита $G\mathbf{a}$ является t-дизайном при любом $\mathbf{a} \in S^{N-1}$, если и только если $H(t)$ не содержит G-инвариантных гармонических многочленов. Кроме того, там же показано, что если $H(t)$ содержит G-инвариантные многочлены, то их можно „убить", выбрав в качестве начальной точки $\mathbf{a}$ их общий корень. В этом случае орбита $G\mathbf{a}$ — t-дизайн.

В §2 настоящей работы указанные результаты работы [1] (применительно к орбитным дизайнам) приведены в несколько более общем и более удобном для использования виде.

В качестве примера приведем следующие хорошо известные результаты. Орбита $.0\mathbf{a}$ группы Конвея $.0$ всех ортогональных преобразований, оставляющих на месте решетку Лича, является 11-дизайном при любом начальном векторе $\mathbf{a}$, ибо первый $.0$-инвариантный многочлен с нулевым средним имеет степень 12 [10]. Если в качестве $\mathbf{a}$ взять вектор $\mathbf{e} = 32^{-1/2}(-3, 1^{23}) \in S_{23}$ (см. [11, гл. 4, §11]), то мы получим 11-дизайн, который содержит 196560 элементов. Заметим, что $2\mathbf{e}$ — один из векторов решетки Лича минимальной длины. Общее число таких векторов равно 196560, а группа $.0$ действует на них транзитивно [12, теорема 2.82].

Если же в качестве $\mathbf{a}$ взять корень единственного $.0$-инвариантного гармонического многочлена $\Omega(\mathbf{a})$ степени 12 с нулевым средним, то мы получим 15-дизайн в 24-мерном евклидовом пространстве, ибо в $H(15)$ нет $.0$-инвариантных гармонических многочленов степеней 13, 14, 15 [10]. В этом случае орбита $.0\mathbf{a}$, очевидно, содержит $|.0|/S(\mathbf{a})$ элементов, где $|.0| = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$ и $S(\mathbf{a})$ — стабилизатор элемента $\mathbf{a}$ [12]. Как предполагает автор, $|S(\mathbf{a})| = 1$ для любого корня $\Omega(\mathbf{a})$, поэтому число элементов у 15-дизайна $.0\mathbf{a}$ предположительно равно $|.0|$. Необходимо отметить, что „явный вид" инвариантного многочлена $\Omega(\mathbf{a})$ автору не известен.

Основным результатом работы является построение бесконечной серии 9-дизайнов и 11-дизайнов в 2^n-мерном евклидовом пространстве с помощью введенных в работе [13] групп $\Phi_{n,2}$ и $\Sigma_{n,2}$, $n = 1, 2, \ldots$, ортогональных $2^n \times 2^n$-матриц. Группа $\Phi_{n,2}$ является подгруппой индекса 2 группы $\Sigma_{n,2}$. Группа $\Phi_{n,2}$ при $n = 2$ является группой порядка 1152, которая порождена 16 матрицами $\mathrm{diag}(\pm1, \pm1, \pm1, \pm1)$, 24 матрицами P_π и матрицей Адамара $H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$, где P_π — подстановочная матрица, которая соответствует аффинному отображению $\mathrm{x} \xrightarrow{\pi} Q\mathrm{x}+\alpha$, ($Q \in M_n(\mathbf{F}_2)$ — невырожденная матрица, $\alpha \in \mathbf{F}_2^2$) пространства $\mathbf{F}_2^2$ в себя (см. §3).

Для того чтобы породить группу $\Sigma_{n,2}$, надо в наборе порождающих матриц заменить H на матрицу $H(\mathrm{e}_1) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$.

Мы доказываем, что пространство $\Phi_{n,2}$-инвариантных гармонических многочленов $f(\mathrm{x})$ степени $\leqslant 9$ с нулевым средним является одномерным с образующей $\Lambda^{(n)}(\mathrm{x})$ 8-й степени, которая имеет достаточно сложный вид (см. теорему 1). Пространство $\Sigma_{n,2}$-инвариантных гармонических многочленов $f(\mathrm{x})$ степени $\leqslant 11$ с нулевым средним также является одномерным с той же образующей $\Lambda^{(n)}(\mathrm{x})$. Поэтому орбиты $\Phi_{n,2}\mathrm{a}$ и $\Sigma_{n,2}\mathrm{a}$, где a — любой корень многочлена $\Lambda^{(n)}(\mathrm{x})$, являются 9-дизайном и 11-дизайном соответственно.

Отметим, что $\Lambda^{(2)}(\mathrm{x}) = \sum_{i=0}^{4} x_{\alpha_i}^8 + 7\sum_{\alpha_i \neq \alpha_j} x_{\alpha_i}^4 x_{\alpha_j}^4 + 168\prod_{i=1}^{4} x_{\alpha_i}^2 - \frac{7}{10}(\sum_{i=1}^{4} x_{\alpha_i}^2)^4$, где индексация переменных производится элементами двумерного пространства $\mathbf{F}_2^2 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ над полем $\mathbf{F}_2$ из двух элементов.

Одним из корней многочлена $\Lambda^{(2)}(\mathrm{x})$ является вектор $\mathrm{c}(x_0)$, где $\mathrm{c}(x) = \frac{\sin x}{\sqrt{3}}(0, 1, 1, 1) + \cos x(1, 0, 0, 0)$, и x_0 — корень уравнения $\Lambda^{(2)}(\mathrm{c}(x)) = \cos^8 x + \frac{14}{3}\cos^4 x \sin^4 + \frac{56}{9}\cos^2 x \sin^6 x + \frac{5}{9}\sin^8 x - \frac{7}{10} = 0$. Орбитные коды $\Phi_{n,2}\mathrm{c}(x_0)$ и $\Sigma_{n,2}\mathrm{c}(x_0)$ содержит 96 и 192 точек и являются 9- и 11-дизайнами на сфере в четырехмерном евклидовом пространстве.

Подобными методами можно построить 9- и 11-дизайны на сфере в восьмимерном евклидовом пространстве, которые содержат 15360 и 30720 точек (см. §6).

§2. Необходимые и достаточные условия, при которых орбита $G\mathrm{a}$ является t-дизайном

Рассмотрим линейное представление ι_k ортогональной группы $O(N)$ на $\mathrm{Hom}(k)$, $k > 0$, т.е. на однородных многочленах степени k. Пусть $\Omega'' = \{a_1(\mathrm{x}), \ldots, a_{m(N,k)}(\mathrm{x})\}$ — некоторый ортогональный базис $\mathrm{Hom}(k)$. Представление ι_k в базисе Ω'' представляет собой гомоморфизм группы $O(N)$ в группу ортогональных $\binom{N+k-1}{k} \times \binom{N+k-1}{k}$-матриц $T(g) = (t_{i,j}(g))$ с помощью отображения $a_i(\mathrm{x}) \to a_i(g^{-1}\mathrm{x}) = \sum_{j=1}^{m(N,k)} t_{i,j}(g^{-1})a_j(\mathrm{x})$. Ввиду (1) и того, что пространства $\mathrm{Harm}(i)$ являются $O(N)$-инвариантными, все матрицы $T(g)$ в соответствующем ортогональном базисе Ω' могут быть представлены как клеточно-диагональные с клетками $T_i(g)$ размера $n(N,i)\times n(N,i)$, $i = k, k-2, \dots, k-2[k/2]$. Отметим, что при $i = 0$ все матрицы $T_0(g)$ реализуют тождественное преобразование на одномерном пространстве $\mathrm{Harm}(0)$, в то время как при $i > 0$ ι_l — не тождественное неприводимое представление на пространстве $\mathrm{Harm}(i)$.

Пусть G — конечная подгруппа группы $O(N)$ и ρ_k — представление G на $\mathrm{Hom}(k)$.

В этом случае инвариантные подпространства $\mathrm{Harm}(i)$ не обязательно остаются неприводимыми для ρ_k и, вообще говоря, распадаются в прямую сумму неприводимых инвариантных подпространств $H_{i,j}$ размерности $\dim H_{i,j} = k_{i,j}$, $j = 1, \dots, N_i$, так, что $\mathrm{Harm}(i) = H_{i,1} + \dots + H_{i,N_i}$. По теореме Машке каждая матрица $T_i(g)$ в соответствующем ортогональном базисе Ω становится клеточно-диагональной с клетками $T_{ij}(g)$ размера $k_{i,j} \times k_{i,j}$. Линейные операторы $T_{ij}(g)$ реализуют неприводимое представление ρ_{ij} группы G на подпространстве $H_{i,j}$.

Лемма 1. *Пусть $f(\mathrm{x}) \in H_{i,j}$. Тогда*

$$\sum_{g\in G} f(g\mathrm{x}) = |G| f(\mathrm{x}) \quad \text{или} \quad \sum_{g\in G} f(g\mathrm{x}) = 0$$

в зависимости от того, представление ρ_{ij} — тождественное или нет на $H_{i,j}$.

Доказательство. Первое равенство очевидно. Второе следует из хорошо известного соотношения ортогональности для матричных элементов нетождественного неприводимого представления конечной группы (соотношение (5) из §4, гл. 8 в [9])

$$\sum_{g\in G} T_{ij}(g)\hat{f}(\mathrm{x}) = 0 \iff \sum_{g\in G} f(g\mathrm{x}) = 0$$

для $f(\mathrm{x}) \in H_{i,j}$, где $\hat{f}(\mathrm{x})$ — вектор, элементы которого являются координатами многочлена $f(\mathrm{x})$ в базисе Ω. ∎

Многочлен $h(\mathrm{x})$ из $H(t)$ будем называть G-инвариантным, если $f(g\mathrm{x}) = f(\mathrm{x})$ для всех $g \in G$.

Пусть $\mathrm{y} \in S_{N-1}$. Множество $X(\mathrm{y}) := \{g\mathrm{y} : g \in G\}$ называется орбитным кодом или орбитным дизайном с начальным вектором y. Очевидно, число элементов $X(\mathrm{y})$ равно $|G|/|S(\mathrm{y})|$, где $S(\mathrm{y})$ — стабилизатор точки y в группе G.

Лемма 2. i. *Множество* $X := X(\mathbf{x}_1, \ldots, \mathbf{x}_s) := \bigcup_{i=1}^{s} X(\mathbf{x}_i)$ *является* t*-дизайном тогда и только тогда, когда для любого* G*-инвариантного многочлена* $h(\mathbf{x})$ *из* $H(t)$ *выполнено*

$$\sum_{i=1}^{s} h(\mathbf{x}_i) = 0. \tag{3}$$

ii. *Орбитный код* $X(\mathbf{x}_1)$ *является* t*-дизайном при любом начальном векторе* $\mathbf{x}_1 \in S_{N-1}$ *тогда и только тогда, когда пространство* $H(t)$ *не содержит* G*-инвариантных многочленов.*

Доказательство. i. Пусть X — t-дизайн. Пространство $H(t)$, как следует из леммы 1, является прямой суммой пространства инвариантных многочленов H_0 и ортогонального к H_0 в $H(t)$ пространства H_1, т.е. любой $h(\mathbf{x})$ из $H(t)$ может быть представлен в виде $h(\mathbf{x}) = h_0(\mathbf{x}) + h_1(\mathbf{x})$, $h_0(\mathbf{x}) \in H_0$, $h_1(\mathbf{x}) \in H_1$ так, что

$$\sum_{\mathbf{x} \in X} h(\mathbf{x}) = \sum_{i=1}^{s} \sum_{g \in G} h(g\mathbf{x}_i) = |G| \sum_{i=1}^{s} h_0(\mathbf{x}_i) = 0.$$

Если X — не t-дизайн, то по лемме А найдется такой многочлен $h(\mathbf{x})$, что $\sum_{\mathbf{x} \in X} h(\mathbf{x}) = \sum_{i=1}^{s} \sum_{g \in G} h(g\mathbf{x}_i) = |G| \sum_{i=1}^{s} h_0(\mathbf{x}_i) \neq 0$, т.е. для $h_0(\mathbf{x})$ не выполнено (3).

ii. Из лемм А и (1) следует, если в $H(t)$ нет G-инвариантных многочленов, то для всех $h(\mathbf{x})$ выполнено $\sum_{\mathbf{x} \in X} h(\mathbf{x}) = 0$. Как следует из леммы 1, последнее равенство выполнено для всех $h(\mathbf{x})$ только при отсутствии G-инвариантных многочленов в $H(t)$. •

Таким образом, $X(\mathbf{x}_1, \ldots, \mathbf{x}_s)$ является t-дизайном, если и только если множество $\{\mathbf{x}_1, \ldots, \mathbf{x}_s\}$ — дизайн для пространства G-инвариантных многочленов из $H(t)$. Лемма 2 далее будет использована только при $s = 1$.

§3. Структура группы $\Sigma_{n,2}$

В качестве G мы будем рассматривать группу $\Sigma_{n,2}$, которая введена через матричные образующие в работе [13]. В работе [15] показано, что группа $\Sigma_{n,2}$ изоморфна полупрямому произведению экстраспециальной группы O_2 порядка 2^{2n+1} и ортогональной группы $O^+(2n, 2)$, которая действует на O_2 естественным образом. Отметим, что этот результат мы в работе использовать не будем. Очень коротко напомним определение $\Sigma_{n,2}$ [13].

Пусть $N := 2^n$ и $f(\mathbf{x})$ — булева функция от n переменных, $\mathbf{F}_2^n := \{\alpha_1, \ldots, \alpha_N\}$ — множество n-мерных двоичных векторов, упорядоченное каким-либо образом. Мы обозначаем через $\mathcal{E}$ группу, состоящую из диагональных матриц

$E_f := \mathrm{diag}((-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_N)})$, где $f(\mathbf{x})$ пробегает все булевы функции степени 2 или менее, и через $\mathcal{P}$ — группу, состоящую из подстановочных $2^n \times 2^n$-матриц $P(Q,\alpha) = P_\pi$, реализующих аффинные отображения $\mathbf{x} \xrightarrow{\pi} Q\mathbf{x} + \alpha$, где $Q \in M_n(\mathbf{F}_2)$ — невырожденная матрица, $\alpha \in \mathbf{F}_2^n$ и $M_n(\mathbf{F}_2)$ — множество всех матриц над полем $\mathbf{F}_2$. Пусть $D, R, T \in M_n(\mathbf{F}_2)$, $\mathrm{Im}\, R := R\mathbf{F}_2^n$ — пространство строк R, $\mathrm{Ker}\, R := \{\mathbf{x} : R\mathbf{x} = 0\}$, $\mathrm{Com}\, R$ — дополнение к пространству $\mathrm{Ker}\, R$.

Конечная группа $\Sigma_{n,2}$ определяется как группа, порожденная группой $\mathcal{U}$ и всевозможными матрицами $B(D,R,T) = (v_{\alpha,\beta})$, $\alpha, \beta \in \mathbf{F}_2^n$, такими, что $\mathrm{Im}\, R = \mathrm{Im}\, T$ и билинейная форма $\mathbf{x}D\mathbf{y}^T$ невырождена на $\mathrm{Ker}\, R \times \mathrm{Ker}\, T$.

По определению матрицы $B(D,R,T)$ ее элемент $v_{\alpha,\beta}$ является нулевым только тогда, когда $\alpha R \neq \beta T$, т.е. когда $\alpha = \alpha' + \alpha''$, $\beta = \beta' + \beta''$, $\alpha \in \ker R$, $\beta'' \in \mathrm{Ker}\, T$, $\alpha' \in \mathrm{Com}\, R, \beta' \in \mathrm{Com}\, T$ и $\alpha' R \neq \beta' T$. Если $\alpha R = \beta T$, то $v_{\alpha,\beta} := 2^{-m/2}(-1)^{\alpha D \beta^T}$, где $m := \dim \mathrm{Ker}\, R$.

Индексацию строк и столбцов матриц из $\Sigma_{n,2}$ осуществляем элементами пространства $\mathbf{F}_2^n$, упорядоченным указанным образом.

Порядок $\sigma_{n,2}$ группы $\Sigma_{n,2}$ асимптотически равен $c2^{n(2n+1)+1}$, $c = 1.38\ldots, n \to \infty$. Отметим, что $\sigma_{1,2} = 8$, $\sigma_{2,2} = 2304 = 2^8 \cdot 3^2$, $\sigma_{3,2} = 5160960 = 2^{14} \cdot 3^2 \cdot 5 \cdot 7$, $\sigma_{4,2} = 178362777600 = 2^{22} \cdot 3^5 \cdot 5^2 \cdot 7$, $\sigma_{5,2} = 96253116206284800 = 2^{32} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot 31$, $\sigma_{6,2} = 8196514963163795423232 00 = 2^{44} \cdot 3^8 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 17 \cdot 31$ [13].

Мы будем обозначать через $\Phi_{n,2}$ подгруппу индекса 2 группы $\Sigma_{n,2}$, которая образована элементами (матрицами) с рациональными коэффициентами. О свойствах группы $\Phi_{n,2}$ см. [13] и [15]. Пусть $H := 2^{-n/2}((-1)^{\langle a,b \rangle})$, где $a, b \in \mathbf{F}_2^n$, $\langle a,b \rangle$ — их скалярное произведение в пространстве $\mathbf{F}_2^n$, — матрица Адамара.

Лемма 3. *Группа $2^n \times 2^n$-матриц $\Sigma_n := \langle \mathcal{U}, H \rangle$, где $\mathcal{U} := \langle \mathcal{E}, \mathcal{P} \rangle$, совпадает с $\Sigma_{n,2}$ при нечетном n и с группой $\Phi_{n,2}$ при четном n.*

Доказательство. Как вытекает из определений

$$P(Q', \mathbf{O})B(D,R,T)P(Q,\mathbf{O}) = B(Q'DQ^T, Q'R, QT). \tag{4}$$

Пусть $\mathcal{N} := \{1, 2, \ldots, n\}$, $\mathcal{W} := \{i_1, \ldots, i_k\}$ — k-элементное подмножество $\mathcal{N}$ и $\overline{\mathcal{W}} := \mathcal{N} \setminus \mathcal{W}$. Обозначим через $I(\mathcal{W})$ диагональную $n \times n$-матрицу из $M_n(F_2)$, у которой на местах (i_j, i_j), $j = 1, \ldots, k$, стоят единицы, а на остальных местах диагонали — нули.

Ввиду условия $\mathrm{Im}\, R = \mathrm{Im}\, T$ можно подобрать невырожденные матрицы Q' и Q так, чтобы $Q'R = QT = I_{n-m}$, где $m = \mathrm{rang}\, R$ и $I_k := (\{1, \ldots, k\})$.

Покажем, что матрицу $B(D, I_{n-m}, I_{n-m})$ можно представить в виде

$$B(D, I_{n-m}, I_{n-m}) = E_{f_1} B(\widetilde{D}, I_{n-m}, I_{n-m}) E_{f_2}, \tag{5}$$

где $\widetilde{D} = (\widetilde{d}_{i,j})$ и $\widetilde{d}_{i,j} = 0$, если выполнено по крайней мере одно из соотношений $i \geqslant n-m$, $j \geqslant n-m$ и $f_i(\mathrm{x})$, $i = 1,2$, — некоторые булевы функции степени не выше 2. Другими словами, $\widetilde{D} = \mathrm{diag}(0,\ldots,0,\widehat{D})$ — матрица ранга m, у которой ненулевые элементы сосредоточены только в нижнем правом блоке размера $m \times m$, и $\widehat{D}$ — невырожденная $m \times m$-матрица.

Для этого билинейную форму $\mathrm{x}D\mathrm{y}^T$ представим в виде $\mathrm{x}D\mathrm{y}^T = \mathrm{x}'D\mathrm{y}'^T + \mathrm{x}'D\mathrm{y}''^T + \mathrm{x}''D\mathrm{y}'^T + \mathrm{x}''D\mathrm{y}''^T$, где $\mathrm{x} = \mathrm{x}' + \mathrm{x}''$, $\mathrm{y} = \mathrm{y}' + \mathrm{y}''$, $\mathrm{x}',\mathrm{y}' \in \mathrm{Ker}\, I_{n-m}$, $\mathrm{x}'',\mathrm{y}'' \in \mathrm{Com}\, I_{n-m}$ и $\mathrm{x}'' = \mathrm{y}''$ для ненулевых элементов $v_{\mathrm{x},\mathrm{y}}$. Отсюда $\mathrm{x}D\mathrm{y}^T = \mathrm{x}'D'\mathrm{y}'^T + \mathrm{x}'D\mathrm{x}''^T + \mathrm{y}''D\mathrm{y}'^T + \mathrm{x}''D\mathrm{x}''^T$. Положим $f_1(\mathrm{x}) = \mathrm{x}'D\mathrm{x}''^T + \mathrm{x}''D\mathrm{x}''^T$ и $f_2(\mathrm{y}) = \mathrm{y}''D\mathrm{y}''^T$. Отсюда следует соотношение (5).

Для невырожденной матрицы $Q = \mathrm{diag}(1,\ldots,1,\widehat{D}^{-1})$ ввиду $\mathrm{Im}\,\widetilde{D} = \mathrm{Ker}\, I_{n-m}$ выполнены соотношения $\widetilde{D}Q^T = I(\{n-m+1,\ldots,n\}) = \overline{I}_m$ и $I_{n-m}Q = I_{n-m}$. Таким образом, по построению $B(\widetilde{D}, I_{n-m}, I_{n-m})P(Q,\mathrm{O}) = B(\overline{I}_m, I_{n-m}, I_{n-m})$.

Следовательно, группа $\Sigma_{n,2}$ порождена матрицами $B(\overline{I}_m, I_{n-m}, I_{n-m})$, $m = 1,\ldots,n$ и группой $\mathcal{U}$.

Матрица $H(\mathcal{W}) := B(I(\mathcal{W}), I(\overline{\mathcal{W}}), I(\overline{\mathcal{W}}))$ является (при соответствующей перестановке ее строк и столбцов) блочно-диагональной, блоками которой служат $2^k \times 2^k$-матрицы Адамара $H_k := 2^{-k/2}((-1)^{\langle\alpha,\beta\rangle})$, $\alpha,\beta \in \mathbb{F}_2^k$. В частности, $H(\mathcal{N}) = H$. Как нетрудно установить,

$$H(\mathcal{W}_1)H(\mathcal{W}_2) = H(\mathcal{W}), \tag{6}$$

где $\mathcal{W} = \mathcal{W}_1 \oplus \mathcal{W}_2 = \mathcal{W}_1 \cup \mathcal{W}_2 \setminus \mathcal{W} \cap \mathcal{W}_2$ — симметрическая сумма множеств $\mathcal{W}_1$ и $\mathcal{W}_2$.

Отсюда, в частности, вытекает, что группа $\Sigma_{n,2}$ порождена группой $\mathcal{U}$ и матрицей $h(\mathcal{W})$ с одноэлементным множеством $\mathcal{W}$, а группа $\Phi_{n,2}$ — группой $\mathcal{U}$ и двухэлементным множеством $\mathcal{W}$.

Пусть $f(\mathrm{x}) = x_1x_2$. Прямые вычисления дают, что $H(\mathcal{N})E_fH(\mathcal{N}) = E_fH(\{1,2\})P(Q,\mathrm{O})E_f = E_fP(Q,\mathrm{O})E_f$, где $Q = \mathrm{diag}\left(\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),1,\ldots,1\right)$. Следовательно, с учетом (6) группе $\langle \mathcal{U}, H(\mathcal{N})\rangle$ принадлежат все матрицы $H(W)$, у которых множество W содержит четное число элементов. Отсюда вытекает, что $\Phi_{n,2} = \langle \mathcal{U}, H(\mathcal{N})\rangle$ при четном n.

При нечетном n, как следует из (6), группе $\langle \mathcal{U}, H(\mathcal{N})\rangle$ принадлежит матрица $H(\{1\}) = H(\mathcal{N})H\{2,\ldots,n\})$, что доказывает равенство $\Sigma_{n,2} = \langle \mathcal{U}, H(\mathcal{N})\rangle$ для нечетного n. •

Максимальность подгруппы $\mathcal{U}$ в $\Phi_{n,2}$ доказана также в [15].

§4. $\Phi_{n,2}$-инвариантные многочлены восьмой степени

Пусть $\alpha := (\alpha_1, \dots, \alpha_k)$ — набор элементов $\mathbf{F}_2^n$, который будем также рассматривать и как множество элементов. Положим $\mathbf{x}_\alpha := x_{\alpha_1}, \dots, x_{\alpha_k}$.

Пусть g — элемент группы $\Sigma_{n,2}$, G — подгруппа $\Sigma_{n,2}$ и $f(\mathbf{x})$ — многочлен. Положим $f^g(\mathbf{x}) := f(g\mathbf{x})$ и $f^G(\mathbf{x}) := |G|^{-1}\sum_{g\in G} f^g(\mathbf{x})$. Многочлен $f^G(\mathbf{x})$ будем называть усреднением $f(\mathbf{x})$ по подгруппе G. Как следует из леммы 1, $f^G(\mathbf{x}) = f(\mathbf{x})$, если $f(\mathbf{x})$ принадлежит пространству H_0 G-инвариантных многочленов, и $f^G(\mathbf{x}) = 0$, если $f(\mathbf{x})$ принадлежит пространству H_1 ортогональному к H_0.

Лемма 5. Случай i. *Одночлен $\mathbf{x}_\alpha = x_{\alpha_1}\dots x_{\alpha_8}$ восьмой степени является $\mathcal{E}$-инвариантным тогда и только тогда, когда выполнено одно из двух условий:*

i.1. *в наборе $\alpha = (\alpha_1, \dots, \alpha_8)$ каждый элемент встречается четное число раз;*

i.2. *множество $\alpha = \{\alpha_1, \dots, \alpha_8\}$ является смежным классом некоторого подпространства размерности 3, т.е., например, $\alpha_1 = \gamma$, $\alpha_2 = \alpha_1 + \gamma$, $\alpha_3 = \alpha_2 + \gamma$, $\alpha_4 = \alpha_3 + \gamma$, $\alpha_5 = \alpha_1 + \alpha_2 + \gamma$, $\alpha_6 = \alpha_1 + \alpha_3 + \gamma$, $\alpha_7 = \alpha_2 + \alpha_3 + \gamma$, $\alpha_8 = \alpha_1 + \alpha_2 + \alpha_3 + \gamma$.*

Случай ii. *Одночлен $\mathbf{x}_\beta = x_{\beta_1}\dots x_{\beta_{10}}$ десятой степени $\mathcal{E}$-инвариантен тогда и только тогда, когда выполнено одно из следующих трех условий:*

ii.1. *в наборе $\beta = (\beta_1, \dots, \beta_{10})$ каждый элемент встречается четное число раз;*

ii.2. *в наборе $\beta = (\beta_1, \dots, \beta_{10})$ один элемент, скажем β_i, встречается дважды, а остальные однократно, и набор α длины 8, полученный удалением в наборе β двух β_i, удовлетворяет условию* i.2;

ii.3. *в наборе $\beta = (\beta_1, \dots, \beta_{10})$ один элемент, скажем β_i, встречается трижды, а остальные однократно, и набор α длины 8, полученный удалением в β двух β_i, удовлетворяет условию* 1.2.

Доказательство. Случай i. Заметим, что

$$E_f\mathbf{x}_\alpha = (-1)^{f(\alpha_1)+\dots+f(\alpha_8)}x_{\alpha_1}\dots x_{\alpha_8}. \tag{7}$$

Отсюда вытекает, что $\mathbf{x}_\alpha\mathcal{E}$-инвариантен, если α удовлетворяет условию i.1 леммы. Предположим теперь, что набор α индексов монома $\mathbf{x}_\alpha$ состоит из элементов, среди которых имеется по меньшей мере один встречающийся нечетное число раз.

Как известно [8], для фиксированной булевой функции $g(\mathbf{x})$ равенство

$$\sum_{\mathbf{z}\in\mathbf{F}_2^n} f(\mathbf{z})g(\mathbf{z}) = 0 \tag{8}$$

для всех $f(\mathbf{x})$, $\deg f(\mathbf{x}) \leqslant 2$, выполнено тогда и только тогда, когда $\deg g(\mathbf{x}) \leqslant n-3$. Это утверждение на языке теории кодирования звучит следующим образом: кодом, двойственным к коду Рида-Маллера второго порядка, является код Рида-Маллера $n-3$ порядка (код RM_{n-3}). Равенство (8) по другому можно записать в виде

$$\sum_{\mathbf{a}\in\mathcal{M}} f(\mathbf{a}) = 0,$$

где $\mathcal{M}$ — множество решений уравнения $g(\mathbf{x}) = 1$.

Минимальное кодовое расстояние кода RM_{n-3} равно 8. Кодовые векторы веса 8 порождаются булевыми функциями вида $g(\mathbf{x}) = l_1(\mathbf{x})\cdots l_{n-3}(\mathbf{x})$, где $l_j(\mathbf{x}) = \widetilde{l}_j(\mathbf{x}) + l_j$ и $\widetilde{l}_j(\mathbf{x})$, $j = 1,\ldots,n-3$, — линейно независимые линейные функции и l_j — константы, и только ими. Множество векторов $\mathcal{M}$, на которых функция $g(\mathbf{x})$ принимает значение 1, является решениями системы уравнений $a_j(\mathbf{x}) = 1$, $i = 1,\ldots,n-3$, т.е. смежным классом некоторого линейного пространства размерности 3.

Случай ii. Очевидно, что $\mathbf{x}_\alpha$ $\mathcal{E}$-инвариантен, если α удовлетворяет условию **ii.1** леммы.

Для доказательства утверждений ii.2 и ii.3 следует только заметить, что код RM_{n-3} не содержит векторов веса 10, т.е. моном $\mathbf{x}_\beta$, у которого набор β состоит из различных элементов, не является $\mathcal{E}$-инвариантным. Поэтому случаи ii.2 и ii.3 по существу сводятся к случаю i.2. •

Рассмотрим многочлены

1. $\Gamma_3(\mathbf{x}) := \sum_\alpha \sum_{(3)} x_\alpha x_{\beta+\alpha} x_{\gamma+\alpha} x_{\delta+\alpha} x_{\beta+\gamma+\alpha} x_{\beta+\delta+\alpha} x_{\gamma+\delta+\alpha} x_{\beta+\gamma+\delta+\alpha}$, $n \geqslant 3$, где суммирование в сумме $\sum_\alpha$ производится по всем $\alpha \in \mathbf{F}_2^n$ и в сумме $\sum_{(3)}$ — по всем наборам $(\beta,\gamma,\delta) \in \mathbf{F}_2^n \times \mathbf{F}_2^n \times \mathbf{F}_2^n$, у которых β, γ, δ — линейно-независимые векторы. Отметим, что $\Gamma_3(\mathbf{x})$ — гармонический многочлен, а число слагаемых в двойной сумме $\sum_\alpha \sum_{(3)}$ равно $N(N-1)(N-2)(N-4)$. Если $n = 1, 2$, то полагаем, что $\Gamma_3(\mathbf{x}) = 0$.

2. $\Gamma_2(\mathbf{x}) := \sum_\alpha \sum_{(2)} x_\alpha x_{\beta+\alpha} x_{\gamma+\alpha} x_{\delta+\alpha} x_{\beta+\gamma+\alpha} x_{\beta+\delta+\alpha} x_{\gamma+\delta+\alpha} x_{\beta+\gamma+\delta+\alpha}$, $n \geqslant 2$, где суммирование в сумме $\sum_\alpha$ производится по всем α и в сумме $\sum_{(2)}$ — по всем наборам (β,γ,δ), для которых пространство, натянутое на векторы β, γ, δ, имеет размерность 2. Покажем, что для многочлена $\Delta(\mathbf{x}) = \sum x^2_{\alpha_1} x^2_{\alpha_2} x^2_{\alpha_3} x^2_{\alpha_4}$, где суммирование в $\sum$ производится по всем наборам $\boldsymbol{\alpha} = (\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ с попарно различными элементами таким, что $\alpha_1+\alpha_2+\alpha_3+\alpha_4 = \mathbf{0}$, выполнено

$$\Gamma_2(\mathbf{x}) = 7\Delta(\mathbf{x}).$$

Очевидно, многочлены $\Gamma_2(\mathbf{x})$ и $\Delta(\mathbf{x})$ содержат одни и те же мономы. Каждый моном в любом из этих многочленов встречается одинаковое число раз, поэтому $\Gamma_2(\mathbf{x}) = q\Delta(\mathbf{x})$. Вычислим число слагаемых Y_1, Y_2 у сумм, представляющих эти два многочлена, что позволит вычислить q.

Область суммирования суммы $\sum_{(2)}$ разбивается на семь непересекающихся множеств: тройки вида $(\alpha_1, \alpha_2, \alpha_3)$, $\alpha_1 + \alpha_2 + \alpha_3 = \mathbf{0}$, вида $(\mathbf{0}, \alpha_1, \alpha_2)$, $(\alpha_1, \mathbf{0}, \alpha_2)$, $(\alpha_1, \alpha_2, \mathbf{0})$ и вида $(\alpha_1, \alpha_1, \alpha_2)$, $(\alpha_1, \alpha_2, \alpha_2)$, $(\alpha_1, \alpha_2, \alpha_1)$, $\alpha_1 \neq \alpha_2, \alpha_1\alpha_2, \alpha_3 \neq \mathbf{0}$. Число троек каждого вида равно $(N-1)(N-2)$, т.е. сумма $\sum_\alpha \sum_{(2)}$ содержит $Y_1 = 7N(N-1)(N-2)$ слагаемых.

Очевидно, число $Y_2 = 2^n(2^n - 1)(2^n - 2)$, ибо $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$ и $\alpha_4 \neq \alpha_i$, $i = 1, 2, 3$, если $\alpha_1, \alpha_2, \alpha_3$ попарно различны, т.е. $q = 7$.

3. $\Gamma_1 := \sum_\alpha \sum_{(1)} x_\alpha x_{\beta+\alpha} x_{\gamma+\alpha} x_{\delta+\alpha} x_{\beta+\gamma+\alpha} x_{\beta+\delta+\alpha} x_{\gamma+\delta+\alpha} x_{\beta+\gamma+\delta+\alpha}$, $n \geqslant 1$, где суммирование в сумме $\sum_{(1)}$ производится по всем α и всем наборам (β, γ, δ), для которых пространство, натянутое на векторы β, γ, δ, имеет размерность 1. Покажем, что многочлен $\Gamma_1(\mathbf{x})$ может быть представлен в виде

$$\Gamma_1(\mathbf{x}) = 7 \sum x_{\alpha_1}^4 x_{\alpha_2}^4 = 7\Omega(\mathbf{x}),$$

где суммирование в сумме $\sum$ производится по всем наборам (α_1, α_2) с различными элементами.

Действительно, многочлены $\Gamma_1(\mathbf{x})$, $\Omega(\mathbf{x})$ образованы одними и теми же мономами $x_{\alpha_1}^4 x_{\alpha_2}^4$. Число слагаемых у суммы, представляющей многочлен $\Gamma_1(\mathbf{x})$, равно $7N(N-1)$, ибо имеется $N-1$ одномерных пространств $L = \{\mathbf{0}, \mathbf{a}\}$, $\mathbf{a} \neq \mathbf{0}$, и каждое из них может быть представлено как пространство, натянутое на векторы семи различных наборов (β, γ, δ): 1 набор $(\mathbf{a}, \mathbf{a}, \mathbf{a})$, $\mathbf{a} \neq \mathbf{0}$, и 3 набора (β, γ, δ) с двумя элементами $\mathbf{a}$ и одним $\mathbf{0}$, 3 набора (β, γ, δ) с одним элементом $\mathbf{a}$ и двумя $\mathbf{0}$. Число слагаемых у суммы $\sum x_{\alpha_1}^4 x_{\alpha_2}^4$ равно $N(N-1)$.

4. $\Gamma_0(\mathbf{x}) := \sum_\alpha \sum_{(0)} x_\alpha x_{\beta+\alpha} x_{\gamma+\alpha} x_{\delta+\alpha} x_{\beta+\gamma+\alpha} x_{\beta+\delta+\alpha} x_{\gamma+\delta+\alpha} x_{\beta+\gamma+\delta+\alpha}$, $n \geqslant 1$, где суммирование в сумме $\sum_{(0)}$ производится по всем α и всем наборам (β, γ, δ), для которых пространство, натянутое на векторы β, γ, δ, имеет размерность 0, т.е. сумма $\sum_{(0)}$ имеет одно слагаемое с $(\beta, \gamma, \delta) = (\mathbf{0}, \mathbf{0}, \mathbf{0})$. Число слагаемых в сумме $\sum_\alpha \sum_{(0)}$ равно N.

5. $\Phi(\mathbf{x}) := \sum' x_{\alpha_1}^2 x_{\alpha_2}^2 x_{\alpha_3}^2 x_{\alpha_4}^2$, где суммирование в $\sum'$ производится по всем наборам $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ с попарно различными элементами такими, что $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \neq 0$.

Далее будем полагать, что суммирование в $\sum$ производится по всем наборам $(\alpha_1 \dots \alpha_k)$ с попарно различными элементами и с соответствующим значением k.

6. $\Upsilon(\mathbf{x}) := \sum x_{\alpha_1}^2 x_{\alpha_2}^2 x_{\alpha_3}^4$.
7. $\Xi(\mathbf{x}) := \sum x_{\alpha_1}^2 x_{\alpha_2}^6$.

Следует заметить, что все эти многочлены являются многочленами вида $c_\beta \mathbf{x}_\beta^{\mathcal{U}}$ с соответствующими наборами β и постоянными c_β. Например, для $\Gamma_3(\mathbf{x})$ $\beta = (0, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_3, \mathbf{e}_2 + \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3)$.

Лемма 6. *Базис пространства $L_8(\mathcal{U})$ $\mathcal{U}$-инвариантных многочленов степени 8, где $\mathcal{U} := \langle \mathcal{E}, \mathcal{D} \rangle$, образован многочленами Γ_i, $i = 0, 1, 2, 3$, $\Phi(\mathbf{x})$, $\Upsilon(\mathbf{x})$, $\Xi(\mathbf{x})$.*

Доказательство. Пусть $P \in \mathcal{P}$ — подстановочная матрица, реализующая аффинное отображение $\mathbf{x} \xrightarrow{\pi} Q\mathbf{x} + \alpha$ пространства $\mathbf{F}_2^n$ в себя, и $E_f \in \mathcal{E}$. Так как $E_f P = P E_{f'}$, где $f'(\mathbf{x}) = f(\pi^{-1}\mathbf{x})$, то любой элемент U из $\mathcal{U}$ может быть представлен как $U = PE_f$.

Отсюда с учетом равенства $Px_{\beta_1} \dots x_{\beta_8} = x_{\pi(\beta_1)} \dots x_{\pi(\beta_8)}$ вытекает, что $\mathcal{U}$-инвариантными многочленами являются многочлены $\mathbf{x}_\beta^{\mathcal{P}} = |\mathcal{P}|^{-1} \sum_{P \in \mathcal{P}} P\mathbf{x}_\beta$, у которых $\mathbf{x}_\beta$ — один из $\mathcal{E}$-инвариантных мономов из леммы 5.

Если вычислить многочлен $\mathbf{x}_\beta^{\mathcal{P}}$ для всех типов $\mathcal{E}$-инвариантных мономов $\mathbf{x}_\beta$, перечисленных в лемме 5, и учесть, что группа $\mathcal{P}$, действующая на $\mathbf{F}_2^n$, является трижды транзитивной, то мы получим список многочленов из условия леммы. Очевидно, эти многочлены являются линейно-независимыми. Лемма доказана.

Замечание. Пусть G_0 — подгруппа группы G и $L_t(G)$ и $L_t(G_0)$ — пространства G-инвариантных и G_0-инвариантных многочленов из $H(t)$. Тогда $L_t(G) \subseteq L_t(G_0)$.

Лемма 7. *Пусть $n \geqslant 3$ и L — пространство, натянутое на шесть многочленов Γ_i, $i = 0, 1, 2$, $\Psi(\mathbf{x})$, $\Upsilon(\mathbf{x})$, $\Xi(\mathbf{x})$ от 2^n переменных. Тогда в пространстве $H(8) \cap L$ нет ненулевых $\Phi_{n,2}$-инвариантных многочленов, т.е. пространство $H(8) \cap L$ нульмерно.*

Доказательство. В работе [14] автора показано (с использованием результатов работ [3, 4]), что орбитный код $\Phi_{n,2}\mathbf{x}$ является 7-дизайном при любом $\mathbf{x} \in S_{N-1}$. Отсюда и из леммы 2 сразу вытекает, что в $H(7)$ нет $\Phi_{n,2}$-инвариантных многочленов. Поэтому если в $H(8)$ имеется ненулевой $\Phi_{n,2}$-инвариантный многочлен $I(\mathbf{x})$, то он принадлежит $\mathrm{Harm}(8)$. Обозначим через $\Pr(J(\mathbf{x}))$ проекцию однородного многочлена $J(\mathbf{x})$ степени 8 на подпространство $\mathrm{Harm}(8)$ (см. [2]).

Легко проверить, что

i. $\Xi(\mathbf{x}) + \Gamma_0(\mathbf{x}) = r^2(\sum x^6)$, где $r^2 = \sum x^2$;
ii. $\Upsilon(\mathbf{x}) + \Xi(\mathbf{x}) + \Gamma_1(\mathbf{x})/7 = r^2(\sum x_{\alpha_1}^2 x_{\alpha_2}^4)$;
iii. $3\Upsilon(\mathbf{x}) + \Gamma_2(\mathbf{x})/4 + \Phi(\mathbf{x}) = r^2(\sum x_{\alpha_1}^2 x_{\alpha_2}^2 x_{\alpha_3}^2)$.

Так как $\Pr(r^2\Pi(\mathbf{x})) = 0$ для любого $\Pi(\mathbf{x})$ степени 6, то из i, ii, iii вытекает, что среди 6 многочленов $\Pr(\Gamma_i(\mathbf{x}))$, $i = 0,1,2$, $\Pr(\Phi(\mathbf{x}))$, $\Pr(\Upsilon(\mathbf{x}))$, $\Pr(\Xi(\mathbf{x}))$ имеется не более трех линейно-независимых, и в качестве последних мы можем взять многочлены $\Pr(\Gamma_i(\mathbf{x}))$, $i = 0,1,2$.

Таким образом, мы показали с учетом замечания, что если в $H(8)\cap L$ имеется ненулевой $\Phi_{n,2}$-инвариантный многочлен $J(\mathbf{x})$, то он принадлежит подпространству, натянутому на многочлены $\Pr(\Gamma_i(\mathbf{x}))$, $i = 0,1,2$.

Проекция $\Pr(J(\mathbf{x}))$ может быть представлена в виде

$$\Pr(J(\mathbf{x})) = \sum_{k=0}^{4} h_k r^{2k}\Delta^k J(\mathbf{x}), \quad h_0 = 1, \tag{9}$$

где $\Delta = \frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_N^2}$ и h_k — некоторые константы (см. [6, с. 440]).

Пусть $I(\mathbf{x}) = a_0 \Pr(\Gamma_0(\mathbf{x})) + a_1 \Pr(\Omega(\mathbf{x})) + a_2 \Pr(\Delta(\mathbf{x}))$, где $\Omega(\mathbf{x}) = \frac{1}{7}\Gamma_1(\mathbf{x})$, $\Delta(\mathbf{x}) = \frac{1}{7}\Gamma_2(\mathbf{x})$.

Из [9], леммы 1 и из того, что в пространстве $H(7)$ отсутствуют $\Phi_{n,0}$-инвариантные многочлены, вытекает, что для $\Phi_{n,2}$-инвариантного гармонического многочлена $I(\mathbf{x})$ степени 8 выполнено

$$\begin{aligned} I(\mathbf{x}) &= (a_0 \Pr(\Gamma_0(\mathbf{x})) + a_1 \Pr(\Omega(\mathbf{x})) + a_2 \Pr(\Delta(\mathbf{x})))^{\Phi_{n,2}} \\ &= a_0\Gamma_0(\mathbf{x}) + a_1\Omega(\mathbf{x}) + a_2\Delta(\mathbf{x}) - b\Big(\sum_\alpha x_\alpha^2\Big)^4. \end{aligned}$$

С учетом соотношения $(\sum_\alpha x_\alpha^2)^3 = \sum_\alpha x_\alpha^6 + 3\sum_{\alpha\neq\beta} x_\alpha^2 x_\beta^4 + \sum x_{\alpha_1}^2 x_{\alpha_2}^2 x_{\alpha_3}^2$ коэффициенты a_i, b определяются из соотношения

$$\begin{aligned} \Delta I(\mathbf{x}) &= 8\cdot 7a_0 \sum_\alpha x_\alpha^6 + 24a_1 \sum_{\alpha\neq\beta} x_\alpha^2 x_\beta^4 \\ &\quad + 8a_2 \sum x_{\alpha_1}^2 x_{\alpha_2}^2 x_{\alpha_3}^2 - 8(N+6)b\Big(\sum_\alpha x_\alpha^2\Big)^3 \\ &= 0. \end{aligned}$$

Следовательно, если $I(\mathbf{x})$ — ненулевой многочлен, то $I(\mathbf{x}) = (\Gamma_0(\mathbf{x}) + 7\Omega(\mathbf{x}) + 7\Delta(\mathbf{x})) - 7(N+6)^{-1}(\sum_\alpha x_\alpha^2)^4 = \Gamma_0(\mathbf{x}) + \Gamma_1(\mathbf{x}) + \Gamma_2(\mathbf{x}) - 7(N+6)^{-1}(\sum_\alpha x_\alpha^2)^4$.

Таким образом, мы показали, что пространство $\Phi_{n,2}$-инвариантных многочленов не более, чем одномерно.

$I(\mathbf{x})$ — $\Phi_{n,2}$ — инвариантный многочлен, поэтому $I(H(\{1,\ldots,2i\})\mathbf{e}_1) = I(\mathbf{e}_1)$, $i = 0,\ldots,[n/2]$, где $H(\{1,\ldots,2i\})$ — блочно-диагональная матрица из $\Phi_{n,2}$, блоками которой являются $2^{2i} \times 2^{2i}$-матрицы Адамара ($H(\{1,\ldots,j\})$ определена в доказательстве леммы 4 и принадлежит $\Phi_{n,2}$ только при четных j). Следовательно, если одно из последних равенств не выполнено, то $I(\mathbf{x})$ — не $\Phi_{n,2}$-инвариантный многочлен.

Легко вычислить $I(\mathbf{e}_1) = I(H(\{1\})\mathbf{e}_1) = I(H(\{1,2\})\mathbf{e}_1) = 1 - 7(N+6)^{-1}$, $I(H(\{1,2,3\})\mathbf{e}_1) = 43/64 - 7(N+6)^{-1}$, $I(H(\{1,2,3,4\})\mathbf{e}_1) = 197/512 - 7(N+6)^{-1}$. Отсюда вытекает, что $I(\mathbf{x})$ не является $\Sigma_{n,2}$-инвариантным при $n \geqslant 3$ и не является $\Phi_{n,2}$-инвариантным при $n \geqslant 4$, ибо $H(\{1,2,3\}) \notin \Phi_{n,2}$.

Многочлен $I(\mathbf{x})$ не является $\Phi_{n,2}$-инвариантным при $n = 3$ по следующей причине. Пусть $\mathbf{c} = 2^{-3/2}(1,1,1,1,1,1,1,1)$. Тогда $21/64 = I(\mathbf{c}) \neq I(H(\{1,2\})\mathbf{c}) = 1/2$.

Таким образом, предположение о существовании $\Phi_{n,2}$-инвариантного ненулевого многочлена приводит к противоречию при $n \geqslant 3$, что доказывает лемму. •

Отметим, что в $H(8) \cup L$ существуют $\Phi_{n,2}$-инвариантные многочлены $I(\mathbf{x})$ при $n = 1,2$ (см. теорему 1).

Теорема 1. *Пространство $\mathcal{I}_n$ гармонических $\Phi_{n,2}$-инвариантных многочленов степени 8 при $n \geqslant 1$ является одномерным. Ее образующей является $\Lambda(\mathbf{x}) = \Lambda^{(n)}(\mathbf{x}) = \Gamma(\mathbf{x}) - 7/(N+6)(\sum_\alpha x_\alpha^2)^4 \in \mathrm{Harm}(8)$, где*

$$\Gamma(\mathbf{x}) = \sum_{\alpha,\beta,\gamma,\delta} x_\alpha x_{\beta+\alpha} x_{\gamma+\alpha} x_{\delta+\alpha} x_{\gamma+\beta+\alpha} x_{\gamma+\delta+\alpha} x_{\beta+\delta+\alpha} x_{\gamma+\beta+\delta+\alpha}$$
$$= \sum_{i=0}^{3} \Gamma_i(\mathbf{x}).$$

Доказательство. Докажем сначала, что $\Gamma(\mathbf{x})$ является Σ_n-инвариантным многочленом. По построению $\Gamma(\mathbf{x})$ — $\mathcal{U}$-инвариантный многочлен и по лемме 3 $\Sigma_n = \langle \mathcal{U}, H\rangle$, поэтому для доказательства этого достаточно показать, что $\Gamma(\mathbf{x}) = \Gamma(H\mathbf{x})$. Отметим, что $\Phi_{n,2} \subseteq \Sigma_n$, поэтому $\Gamma(\mathbf{x})$ будет являться и $\Phi_{n,2}$-инвариантным многочленом.

Имеем

$$
\begin{aligned}
&\Gamma(H\mathbf{x})\\
&= 2^{-4n} \sum_{\alpha,\gamma,\beta,\delta} \Big(\sum_{\theta_1} (-1)^{\langle \alpha,\theta_1\rangle} x_{\theta_1} \Big) \Big(\sum_{\theta_2} (-1)^{\langle \beta+\alpha,\theta_2\rangle} x_{\theta_2} \Big)\\
&\qquad \times \Big(\sum_{\theta_3} (-1)^{\langle \gamma+\alpha,\theta_3\rangle} x_{\theta_3} \Big) \Big(\sum_{\theta_4} (-1)^{\langle \delta+\alpha,\theta_4\rangle} x_{\theta_4} \Big)\\
&\qquad \times \Big(\sum_{\theta_5} (-1)^{\langle \beta+\gamma+\alpha,\theta_5\rangle} x_{\theta_5} \Big) \Big(\sum_{\theta_6} (-1)^{\langle \beta+\delta+\alpha,\theta_6\rangle} x_{\theta_6} \Big)\\
&\qquad \times \Big(\sum_{\theta_7} (-1)^{\langle \gamma+\delta+\alpha,\theta_7\rangle} x_{\theta_7} \Big) \Big(\sum_{\theta_8} (-1)^{\langle \beta+\gamma+\delta+\alpha,\theta_8\rangle} x_{\theta_8} \Big)\\
&= 2^{-3n} \sum_{\theta} \sum_{\beta,\gamma,\delta} (-1)^{\langle \beta,\theta_2+\theta_5+\theta_6+\theta_8\rangle + \langle \gamma,\theta_3+\theta_5+\theta_7+\theta_8\rangle + \langle \delta,\theta_4+\theta_6+\theta_7+\theta_8\rangle}\\
&\qquad \times x_{\theta_1} x_{\theta_2} x_{\theta_3} x_{\theta_4} x_{\theta_5} x_{\theta_6} x_{\theta_7} x_{\theta_8}\\
&= {\sum_{\theta}}' x_{\theta_1} x_{\theta_2} x_{\theta_3} x_{\theta_4} x_{\theta_5} x_{\theta_6} x_{\theta_7} x_{\theta_8},
\end{aligned}
$$

где суммирование в сумме $\sum_\theta$ производится по всем наборам $\theta = (\theta_1,\theta_2,\theta_3,\theta_4,\theta_5,\theta_6,\theta_7,\theta_8)$ таким, что $\sum_{i=1}^{8}\theta_i = 0$, а в сумме $\sum'_\theta$ по всем наборам θ, для которых $\theta_2+\theta_5+\theta_6+\theta_8 = 0$, $\theta_3+\theta_5+\theta_7+\theta_8 = 0$, $\theta_4+\theta_6+\theta_7+\theta_8 = 0$ и $\sum_{i=1}^{8}\theta_i = 0$.

Выписанная система линейных уравнений имеет ранг 4, и все ее решения могут быть записаны в виде $\theta_1 = \kappa$, $\theta_2 = \psi_1+\kappa$, $\theta_3 = \psi_2+\kappa$, $\theta_4 = \psi_1+\psi_2+\kappa$, $\theta_5 = \psi_3+\kappa$, $\theta_6 = \psi_1+\psi_3+\kappa$, $\theta_7 = \psi_2+\psi_3+\kappa$, $\theta_8 = \psi_1+\psi_2+\psi_3+\kappa$. Отсюда вытекает, что $\Gamma(\mathbf{x}) = \Gamma(H\mathbf{x})$.

Проверка равенства $\Delta\Lambda(\mathbf{x}) = 0$ с учетом равенств, полученных при доказательстве леммы 7, не может представить затруднений.

Пусть $n \geqslant 3$ и имеется другой $\Phi_{n,2}$-инвариантный гармонический многочлен $\Lambda'(\mathbf{x})$, не пропорциональный $\Lambda(\mathbf{x})$. Из леммы 7 вытекает, что одним из его слагаемых является многочлен Γ_3. Поэтому разность $a\Lambda(\mathbf{x})-b\Lambda'(\mathbf{x})$ с подходящими коэффициентами a и b будет ненулевым $\Phi_{n,2}$-инвариантным многочленом из пространства L. Это противоречит лемме 7, т.е. $\Lambda(\mathbf{x}) = d\Lambda'(\mathbf{x})$.

Так как $\Lambda^{(i)}(\mathbf{x})$, $i = 1,2$, — ненулевые $\Phi_{n,2}$-инвариантные многочлены, а из доказательства леммы 7 следует, что пространство гармонических многочленов L, к которому принадлежит $\Lambda^{(i)}(\mathbf{x})$, $i = 1,2$, не более чем одномерно, то одномерными являются и $\mathcal{I}_i$, $i = 1,2$, пространства $\Phi_{n,2}$-инвариантных гармонических многочленов. •

Как нетрудно вычислить, $\Lambda^{(1)}(\mathbf{x}) = x_{\alpha_1}^8 + x_{\alpha_2}^8 + 14x_{\alpha_1}^4 x_{\alpha_2}^4 - \frac{7}{8}(x_{\alpha_1}^2 + x_{\alpha_2}^2)^4$ и $\Lambda^{(2)}(\mathbf{x}) = \sum_{i=0}^4 x_{\alpha_i}^8 + 7\sum_{\alpha_i \neq \alpha_j} x_{\alpha_i}^4 x_{\alpha_j}^4 + 168\prod_{i=1}^4 x_{\alpha_i}^2 - \frac{7}{10}(\sum_\alpha x_\alpha^2)^4$.

Отметим, что при нечетных n многочлен $\Lambda(\mathbf{x})$ является одновременно $\Sigma_{n,2}$-инвариантным, ибо $\Sigma_n = \Sigma_{n,2}$ при нечетном n. При четном n имеем $\Sigma_n = \Phi_{n,2}$ и $\Lambda(\mathbf{x})$ не обязан быть $\Sigma_{n,2}$-инвариантным. Однако $\Sigma_{n,2}$-инвариантным будет многочлен $\Lambda'(\mathbf{x}) = \Lambda(\mathbf{x}) + \Lambda(H(\mathbf{e}_1)\mathbf{x})$, если он отличен от нуля. Последнее выполнено, ибо, используя явный вид многочлена $\Lambda(\mathbf{x})$, нетрудно вычислить, что $\Lambda'(\mathbf{e}_1) = 2\Lambda(\mathbf{e}_1) \neq 0$. Таким образом, $\Lambda(\mathbf{x})$ – $\Sigma_{n,2}$-инвариантный многочлен при всех n. Следует заметить, что $\Sigma_{n,2}$-инвариантные и $\Phi_{n,2}$-инвариантные многочлены десятой степени различны (см. §5).

§5. $\Sigma_{n,2}$-инвариантные гармонические многочлены десятой степени отсутствуют

Будем обозначать через L_1-пространство $\mathcal{U}$-инвариантных многочленов, которые получаются $\mathcal{U}$-усреднением одночленов, удовлетворяющих условию ii.1.

План доказательства отсутствия $\Sigma_{n,2}$-инвариантных гармонических многочленов 10-й степени. Мы доказываем, что

1. Пространство $\Sigma_{n,2}$-инвариантных многочленов вида $\mathbf{x}_\beta$, где β — удовлетворяет ii.2 или ii.3, принадлежит $(\mathbf{x},\mathbf{x})\,\mathrm{Hom}(8)$, т.е. $\Sigma_{n,2}$-инвариантные гармонические многочлены 10-й степени, если они существуют, принадлежат пространству L_1 (лемма 8).

2. Пространство $L_1 \cap \mathrm{Harm}(10) = \langle N_{10}, N_{6,4}, N_{4,2,2,2}^{(0)}\rangle$ не содержит $\Sigma_{n,2}$-инвариантных многочленов 10-й степени (лемма 9).

Пусть $n \geqslant 4$ и $\beta_0 = (0^3, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_3, \mathbf{e}_2 + \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3)$, $\beta_1 = (\mathbf{e}_4^2, 0, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_3, \mathbf{e}_2 + \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3)$ — наборы, которые удовлетворяют условию ii.3 и ii.2 леммы 5 соответственно, и $\beta = (0, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_3, \mathbf{e}_2 + \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3)$, $\omega = (\mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_4, \mathbf{e}_2 + \mathbf{e}_4, \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4)$. При $n \geqslant 3$ положим $I_{\beta_i} = c_i(\mathbf{x}_{\beta_i})^{\mathcal{U}}$, $i = 0, 1$, постоянную c_i выберем так, чтобы коэффициент при $\mathbf{x}_{\beta_i}$ был равен 1. При $n = 1, 2$ полагаем $I_{\beta_i} = 0$. Отметим, что $I_{\beta_0} + I_{\beta_1} = (\mathbf{x},\mathbf{x})I_\beta$ и $c_0 = (2^3-1)(2^3-2)(2^3-4)(2^n-8)\dots(2^n-2^{n-1})$, $c_1 = 8(2^3-1)(2^3-2)(2^3-4)(2^n-16)\dots(2^n-2^{n-1})$.

Лемма 8. $(\mathbf{x}_{\beta_i})^{\Sigma_{n,2}} \in \mathrm{Hom}(8)$, $i = 0, 1$.

Доказательство. Рассмотрим только случай $i = 0$. Случай $i = 1$ рассматривается совершенно аналогично.

Как нетрудно проверить, $(\mathbf{x}_{\beta_0})^{\mathcal{U}} = (\mathbf{x},\mathbf{x})\Gamma_3(\mathbf{x})$, поэтому далее будем полагать, что $n \geqslant 4$. Для матрицы $H(\mathbf{e}_4) \in \Sigma_{n,2}$, определенной в §3, имеем

$$\begin{aligned}
&H(\{\mathbf{e}_4\})\mathbf{x}_{\beta_0}\\
&\quad = 2^{-5}(x_0 + x_{e_4})^3(x_{e_1} + x_{e_1+e_4})(x_{e_2} + x_{e_2+e_4})(x_{e_3} + x_{e_3+e_4})\\
&\qquad \times (x_{e_1+e_2} + x_{e_1+e_2+e_4})(x_{e_1+e_3} + x_{e_1+e_3+e_4})(x_{e_2+e_3} + x_{e_2+e_3+e_4})\\
&\qquad \times (x_{e_1+e_2+e_3} + x_{e_1+e_2+e_3+e_4})\\
&\quad = 2^{-5}(\mathbf{x}_{\beta_0} + 3\mathbf{x}_{\gamma_0} + 3\mathbf{x}_{\delta_0} + \mathbf{x}_{\omega_0}) + S, \qquad (10)
\end{aligned}$$

где S — члены, которые не удовлетворяют условиям ii.1–ii.3, т.е. члены, которые при усреднении по $\mathcal{E}$ уйдут в 0, и $\gamma_0 = (\mathbf{e}_4^2, 0, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_3, \mathbf{e}_2 + \mathbf{e}_3, \mathbf{e}_1, +\mathbf{e}_2 + \mathbf{e}_3)$, $\delta_0 = (0^2, \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_4, \mathbf{e}_2 + \mathbf{e}_4, \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4)$, $\omega_0 = (\mathbf{e}_4^3, \mathbf{e}_1 + \mathbf{e}_4, \mathbf{e}_2 + \mathbf{e}_4, \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4)$. Наборы β_0 и ω_0 являются наборами, удовлетворяющими свойству ii.3, а наборы γ_0 и δ_0 — свойству ii.2.

Из (10) вытекает, что

$$(H(\{\mathbf{e}_4\})\mathbf{x}_{\beta_0})^{\mathcal{U}} = 2^{-5}(2c_0^{-1}I_{\beta_0} + 6c_1^{-1}I_{\beta_1}).$$

С другой стороны,

$$(I_{\beta_0})^{\Sigma_{n,2}} = ((H(\mathbf{e}_4)\mathbf{x}_{\beta_0})^{\mathcal{U}})^{\Sigma_{n,2}} = 2^{-5}(2c_0^{-1}I_{\beta_0}^{\Sigma_{n,2}} + 6c_1^{-1}I_{\beta_1}^{\Sigma_{n,2}}).$$

Прибавим к обеим частям равенства $2^{-5}(6c_1^{-1} - 2c_0^{-1})I_{\beta_0}^{\Sigma_{n,2}}$. В результате получим

$$\begin{aligned}
\Big(1 + \frac{1}{32}(6c_1^{-1} - 2c_0^{-1})\Big)(I_{\beta_0})^{\Sigma_{n,2}} &= \frac{6}{32}c_1^{-1}(I_{\beta_0} + I_{\beta_1})^{\Sigma_{n,2}}\\
&= \frac{6}{32}c_1^{-1}(\mathbf{x},\mathbf{x})(I_{\beta})^{\Sigma_{n,2}},
\end{aligned}$$

т. е. $I_{\beta_0}^{\Sigma_{n,2}} = c(\mathbf{x}_{\beta_i})^{\Sigma_{n,2}} \in (\mathbf{x},\mathbf{x})\,\mathrm{Hom}(8)$. Отметим, что $1 + \frac{1}{32}(6c_1^{-1} - 2c_0^{-1}) = 1 + \frac{1}{32}(6\cdot((2^3-1)(2^3-2)(2^3-4)(2^n-8)\dots(2^n-2^{n-1}))^{-1} - 2(8(2^3-1)(2^3-2)(2^3-4)(2^n-16)\dots(2^n-2^{n-1}))^{-1} \neq 0$. •

Переходим к изучению гармонических многочленов, которые могут быть получены из одночленов, которые удовлетворяют условию ii.1. Положим $M_{i,j,k} :=$

$(x^i_{\alpha_1} x^j_{\alpha_2} x^k_{\alpha_3})^{\mathcal{U}}$, где α_1, α_2, α_3, $(\alpha_s \in \mathbf{F}_2^n)$ — попарно различные индексы. Отметим, что многочлен $M_{i,j,k}$ не зависит от выбора набора $(\alpha_1, \alpha_2, \alpha_3)$. Совершенно также введем многочлены $M_{i,j}$ и M_i.

Положим $M^{(0)}_{4,2,2,2} := (x^4_{\alpha_1} x^2_{\alpha_2} x^2_{\alpha_3} x^2_{\alpha_4})^{\mathcal{U}}$, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, $M^{(1)}_{4,2,2,2} := (x^4_{\alpha_1} x^2_{\alpha_2} x^2_{\alpha_3} x^2_{\alpha_4})^{\mathcal{U}}$, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \neq 0$, где α_1, α_2, α_3, α_4 — попарно различные векторы; $M^{(0)}_{2,2,2,2,2} := (x^2_{\alpha_1} x^2_{\alpha_2} x^2_{\alpha_3} x^2_{\alpha_4} x^2_{\alpha_5})^{\mathcal{U}}$, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, $M^{(1)}_{2,2,2,2,2} := (x^2_{\alpha_1} x^2_{\alpha_2} x^2_{\alpha_3} x^2_{\alpha_4} x^2_{\alpha_5})^{\mathcal{U}}$, если для любого i четыре ненулевых вектора из множества $\{\alpha_1 - \alpha_i, \alpha_2 - \alpha_i, \alpha_3 - \alpha_i, \alpha_4 - \alpha_i, \alpha_5 - \alpha_i\}$ линейно-независимы, где α_1, α_2, α_3, α_4, α_5 — попарно различные векторы.

Лемма 9. *Пространство L_1 не содержит $\Sigma_{n,2}$-инвариантных многочленов.*

Доказательство. $\mathcal{U}$-инвариантные многочлены, получаемые усреднением по $\mathcal{U}$ из мономов, удовлетворяющих условию ii.1, следующие:

1. M_{10},	4. $M_{6,2,2}$,	7. $M^{(1)}_{4,2,2,2}$,
2. $M_{8,2}$,	5. $M_{4,4,2}$,	8. $M^{(0)}_{2,2,2,2,2}$,
3. $M_{6,4}$,	6. $M^{(0)}_{4,2,2,2}$,	9. $M^{(1)}_{2,2,2,2,2}$.

Очевидно, при подходящих константах $c_{i,j,k,\ldots}$ имеем

i. $(\mathbf{x},\mathbf{x})M_8 = c_8 M_{10} + c'_{10} M_{8,2}$.

ii. $(\mathbf{x},\mathbf{x})M_{6,2} = c_{6,2} M_{8,2} + c'_{6,2} M_{6,4} + c''_{6,2} M_{6,2,2}$.

iii. $(\mathbf{x},\mathbf{x})M_{4,4} = c_{4,4} M_{6,4} + c'_{4,4} M_{4,4,2}$.

iv. $(\mathbf{x},\mathbf{x})M_{6,2,2} = c_{6,2,2} M_{6,2,2} + c'_{6,2,2} M_{4,4,2} + c''_{6,2,2} M^{(0)}_{4,2,2,2} + c'''_{6,2,2} M^{(1)}_{4,2,2,2}$.

v. $(\mathbf{x},\mathbf{x})M^{(0)}_{2,2,2,2} = c_{2,2,2,2} M^{(0)}_{4,2,2,2} + c'_{2,2,2,2} M^{(0)}_{2,2,2,2,2}$.

vi. $(\mathbf{x},\mathbf{x})M^{(1)}_{2,2,2,2} c M^{(1)}_{4,2,2,2} + c' M^{(0)}_{2,2,2,2,2} + c'' M^{(1)}_{2,2,2,2,2}$.

Положим $N_{*,*,\ldots} = \mathrm{Pr}_{10}(M_{*,*,\ldots})$, где $\mathrm{Pr}_{10}(J(\mathbf{x}))$ — проекция многочлена $J(\mathbf{x})$ на $\mathrm{Harm}(10)$. Проекции левых частей равенств i–vi на $\mathrm{Harm}(10)$ равны 0. Поэтому 9 многочленов $N_{*,*,\ldots}$, как можно легко проверить, линейно выражаются через 3 многочлена N_{10}, $N_{6,4}$, $N^{(0)}_{4,2,2,2}$.

Таким образом, если имеется $\Sigma_{n,2}$-инвариантный гармонический многочлен $I(\mathbf{x})$, принадлежащий пространству, натянутому на 9 многочленов $N_{*,*,\ldots}$, то он имеет вид

$$\begin{aligned} I(\mathbf{x}) &= a_0 N_{10} + a_1 N_{6,4} + a_3 N^{(0)}_{4,2,2,2} \\ &= a_0 M_{10} + a_1 M_{6,4} + a_2 M^{(0)}_{4,2,2,2} + a_3 (\mathbf{x},\mathbf{x})^5 + b(\mathbf{x},\mathbf{x})\Lambda(\mathbf{x}). \end{aligned}$$

Последнее равенство вытекает из (9) и того, что $\mathrm{Harm}(8)$ содержит единственный инвариантный многочлен $\Lambda(\mathbf{x})$, а пространства $\mathrm{Harm}(j)$, $j = 1, \ldots, 7$, не содержат $\Sigma_{n,2}$-инвариантных многочленов [14]. Коэффициент b равен нулю, ибо в многочлен $\Lambda(\mathbf{x})$ входят мономы из $\Gamma_3(\mathbf{x})$, не выражающиеся через многочлены $M_{*,*,\ldots}$.

Коэффициенты a_i удовлетворяют условию $\Delta I(\mathbf{x}) = 10a_0M_8 + 12a_1M_{6,2} + 30a_1M_{4,4} + 12a_2M^{(0)}_{2,2,2,2} + 12a_2M_{4,2,2} + 10(N+8)a_3(\mathbf{x},\mathbf{x})^4 = 0$. Отметим, что $(\mathbf{x},\mathbf{x})^4 = M_8 + 4M_{6,2} + 6M_{4,4} + M^{(0)}_{2,2,2,2} + M^{(1)}_{2,2,2,2}$. Отсюда вытекает, что $a_3 = 0$, ибо при $a_3 \neq 0$ коэффициент при многочлене $M^{(1)}_{2,2,2,2}$ у $\Delta I(\mathbf{x})$, равный a_3, будет отличен от 0, а $M^{(1)}_{2,2,2,2}$ линейно не выражается через многочлены $M_{6,2}$, $M_{4,4}$, $M^{(0)}_{2,2,2,2}$, $M_{4,2,2}$. Коэффициенты a_i, $i = 0, 1, 2$, также равны 0, ибо многочлены $M_{6,2}, \ldots, M^{(0)}_{2,2,2,2}$ — линейно-независимы. •

Теорема 2. *При $n \geqslant 1$ множество $\Sigma_{n,2}$-инвариантных гармонических многочленов 10 степени пусто.*

Доказательство непосредственно вытекает из лемм 8 и 9. •

Отметим, что множество $\Phi_{n,2}$-инвариантных гармонических многочленов 10 степени не пусто по крайней мере для $n = 3, 4, 5, 6$.

§6. 9- и 11-дизайны в 2^n-мерном евклидовом пространстве

Теорема 3. *Пусть $\mathbf{a} \in S^{2n}$ — корень многочлена $\lambda^{(n)}(\mathbf{x})$. Тогда орбита $X = \Phi_{n,2}\mathbf{a}$ является 9-дизайном, орбита $X = \Phi_{n,2}\mathbf{a}$ — 11-дизайном.*

Доказательство. Так как $-E \in \Phi_{n,2}$, то для любого $f(\mathbf{x}) \in \mathrm{Hom}(2k+1)$ выполнено $f(\mathbf{x})^{\Phi_{n,2}} = 0$, т.е. $\Phi_{n,2}$-инвариантных многочленов нечетной степени не существует. Отсюда и из леммы 2 следует утверждение теоремы. •

Отметим, что у многочлена $\Lambda^{(n)}(\mathbf{x})$ всегда имеется корень на S^{N-1}, ибо он является многочленом с нулевым средним.

Укажем естественный способ (среди множества других возможных способов) вычисления некоторых корней многочлена $\Lambda^{(n)}(\mathbf{x})$. Предположим, что известны две точки $\mathbf{a}$ и $\mathbf{b}$ такие, что $\Lambda^{(n)}(\mathbf{a}) \geqslant 0$, $\Lambda^{(n)}(\mathbf{b}) \leqslant 0$. Пусть $\mathbf{x} = (1 + \sin 2x(\mathbf{a},\mathbf{b}))^{-1/2}(\mathbf{a}\sin x + \mathbf{b}\cos x)$ — точка на S^{N-1} и x_0 — любой корень тригонометрического многочлена $q(x) = (1 + \sin 2x(\mathbf{a},\mathbf{b}))^4\lambda^{(n)}(\mathbf{x})$, $0 \leqslant x_0 \leqslant \pi/2$. Тогда $\mathbf{x}_0 = (1 + \sin 2x_0(\mathbf{a},\mathbf{b}))^{-1/2}(\mathbf{a}\sin x_0 + \mathbf{b}\cos x_0)$ — корень $\Lambda^{(n)}(\mathbf{x})$.

Пусть $\mathbf{a} = N^{-1/2}(1, \ldots, 1)$. Как нетрудно вычислить, при $\Lambda^{(n)}(\mathbf{a}) = 1 - 7/(N+6) \geqslant 0$. Указать точку $\mathbf{b}$, для которой $\Lambda^{(n)}(\mathbf{b}) \leqslant 0$, значительно сложнее. Будем полагать, что далее координаты векторов $\mathbf{a}$ индексируются элементами $\mathbf{F}_2^n$, расположенными в лексикографическом порядке так, что первая координата занумерована нулевым вектором из $\mathbf{F}_2^n$.

Рассмотрим случай $n = 2$. Положим $\mathbf{i} = \frac{1}{\sqrt{3}}(0,1,1,1)$, $\mathbf{j} = (1,0,0,0)$. Рассмотрим многочлен $q(x) = \Lambda^{(2)}(\mathbf{i}\sin x + \mathbf{j}\cos x) = \cos^8 x + \frac{14}{3}\cos^4 x \sin^4 x + \frac{56}{9}\cos^2 x \sin^6 x + \frac{5}{9}\sin^8 x - \frac{7}{10}$. Так как $q(\pi/2) = \Lambda^{(2)}(\mathbf{i}) = -\frac{49}{270}$, $q(0) = \Lambda^{(2)}(\mathbf{j}) = \frac{3}{10}$, то многочлен $q(x)$ имеет корень x_0 на интервале $0 \leqslant x \leqslant \pi/2$.

Стабилизатор точки $\mathbf{a} = \mathbf{i}\sin x_0 + \mathbf{j}\cos x_0$ состоит из 6 элементов $P(Q,0)$, которые оставляют элемент с индексом $0 = (0,0)$ на месте.

Таким образом, мы построили 9-дизайн $\Phi_{2,2}\mathbf{a}$ и 11-дизайн $\Sigma_{2,2}\mathbf{a}$ на сфере S^3 в четырехмерном евклидовом пространстве, который содержит $|\Phi_{2,2}|/6 = 96$ и 192 элемента соответственно.

В случае $n = 3$ положим $\mathbf{b}_0 = 2^{-3/2}(-1,1,\dots,1)$, $\mathbf{a}_0 = (1,0,\dots,0)$. Как показывают вычисления, $\Lambda^{(3)}(\mathbf{b}_0) = -0,15625$, $\Lambda^{(3)}(\mathbf{a}_0) = 1/2$. Стабилизатор точки $\mathbf{c} = \mathbf{a}\sin x_0 + \mathbf{b}\cos x_0$, где x_0 — корень многочлена $q(x)$, состоит из 168 элементов вида $P(Q,0)$, т.е. орбитный 9-дизайн $\Phi_{3,2}\mathbf{c}$ на S^7 содержит 15360 элементов, а 11-дизайн $\Sigma_{3,2}\mathbf{c}_0$ — 30720 элементов.

Выражаю благодарность Л. С. Казарину, С. П. Стрункову за полезные советы.

Список литературы

[1] Goethals J.-M., Seidel J. J., *Cubature formulae, polytopes, and spherical designs*, Geometric Vein (C. Devis, B. Grunbaum, and F. A. Sherk, eds.), Springer-Verlag, New York–Berlin, 1981, pp. 203–218.

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

[3] Goethals J.-M., Seidel J. J., *Spherical designs*, Relations between Combinatorics and other Parts of Mathematics, Proc. Sympos. Pure Math., vol. 34, Amer. Math. Soc., Providence, RI, 1979, pp. 255–272.

[4] Bannai E., *On some spherical t-designs*, J. Combin. Theory Ser. A **26** (1979), 157–161.

[5] Bannai E., *Spherical t-designs which are orbits of finite groups*, J. Math. Soc. Japan **36** (1984), no. 2, 341–354.

[6] Стейн И., Вейс Г., *Введение в гармонический анализ на евклидовых пространствах*, Мир, М., 1974.

[7] Виленкин Н. Я., *Специальные функции и теория представлений групп*, Наука, М., 1965.

[8] MacWilliams F. J., Sloane N. J. A., *The theory of error-correcting codes*, North-Holland Math. Library, vol. 16, North-Holland Publishing Co., Amsterdam etc., 1977.

[9] Кострикин А. И., *Введение в алгебру*, Наука, М., 1977.

[10] Huffman W. C., Sloane N. J. A., *Most primitive groups have messy invariants*, Adv. Math. **32** (1979), 118–127.

[11] Конвей Дж., Слоэн Н., *Упаковки шаров, решетки и группы*, Мир, М., 1990.

[12] Горенстейн Д., *Конечные простые группы. Введение в их классификацию*, Мир, М., 1985.

[13] Сидельников В. М., *Об одной конечной матричной группе и кодах на евклидовой сфере*, Пробл. передачи информ. **33** (1997), № 1, 35–54.

[14] Sidel'nikov V. M., *Spherical 7-designs in 2^n-dimensional Euclidean space.* (Предложено в J. Algebraic Combin.).

[15] Казарин Л. С., *О группах, предложенных Сидельниковым*, Мат. сб. **189** (1998), № 7, 131–144.

Поступило 16 февраля 1998 г.