On unbalanced Boolean functions with best correlation immunity*

Denis S. Krotov Konstantin V. Vorob'ev

Sobolev Institute of Mathematics
Novosibirsk 630090, Russia

{krotov,vorobev}@math.nsc.ru

Submitted: Mar 6, 2019; Accepted: Feb 3, 2020; Published: Feb 21, 2020

Abstract

It is known that the order of correlation immunity of a nonconstant unbalanced Boolean function in n variables cannot exceed $2n/3 - 1$; moreover, it is $2n/3 - 1$ if and only if the function corresponds to an equitable 2-partition of the n-cube with an eigenvalue $-n/3$ of the quotient matrix. The known series of such functions have proportion $1 : 3$, $3 : 5$, or $7 : 9$ of the number of ones and zeros. We prove that if a nonconstant unbalanced Boolean function attains the correlation-immunity bound and has ratio $C : B$ of the number of ones and zeros, then CB is divisible by 3. In particular, this proves the nonexistence of equitable partitions for an infinite series of putative quotient matrices.

We also establish that there are exactly 2 equivalence classes of the equitable partitions of the 12-cube with quotient matrix $[[3, 9], [7, 5]]$ and 16 classes, with $[[0, 12], [4, 8]]$. These parameters correspond to the Boolean functions in 12 variables with correlation immunity 7 and proportion $7 : 9$ and $1 : 3$, respectively (the case $3 : 5$ remains unsolved). This also implies the characterization of the orthogonal arrays $\mathrm{OA}(1024, 12, 2, 7)$ and $\mathrm{OA}(512, 11, 2, 6)$.

Mathematics Subject Classifications: 06E30, 05B15, 05B30

1 Introduction

We study unbalanced Boolean functions with the maximum possible order of correlation immunity. A function $f : \{0, 1\}^n \to \{0, 1\}$ is called *unbalanced* if the number of its ones is different from 0, 2^{n-1}, and 2^n. It is called *t-th order correlation immune* if the number of ones (equivalently, zeros) $(x_1, \ldots, x_n) : f(x_1, \ldots, x_n) = 1$ is statistically independent on the values of any t arguments. Fon-Der-Flaass [5] proved that the correlation-immunity

*This work was funded by the Russian Science Foundation under grant 18-11-00136.

order of an unbalanced Boolean function in n variables cannot exceed $2n/3-1$; moreover, any unbalanced Boolean function f of correlation-immunity order $2n/3-1$ corresponds to an equitable 2-partition of the n-cube Q_n with quotient matrix $[[a,b],[c,d]]$, where $a+b=c+d=n$ and $a-c=-n/3$ (a formal definition can be found in Section 2; here, it is essential that the number of ones of f relates to the number of zeros as $c:b$). Nowadays, there are three known families of quotient matrices corresponding to such functions: $[[0,3T],[T,2T]]$, $[[T,5T],[3T,3T]]$ (found in [23]), $[[3T,9T],[7T,5T]]$ (found in [7]). For each of the matrices $[[0,3],[1,2]]$, $[[1,5],[3,3]]$, and $[[0,6],[2,4]]$, a function is unique up to equivalence. Kirienko [13] found that there are exactly two inequivalent unbalanced Boolean functions in 9 variables attaining the bound on the order of correlation immunity (the corresponding quotient matrix is $[[0,9],[3,6]]$). Fon-Der-Flaass [7] started the investigation of the equitable partitions of Q_{12} attaining the correlation-immunity bound. It was shown that equitable partitions with quotient matrix $[[1,11],[5,7]]$ do not exist, while equitable partitions with quotient matrix $[[3,9],[7,5]]$ were built (see the construction in Section 5). These results were also important from the framework of the study of parameters of equitable 2-partitions of the n-cube: they closed the smallest open cases remaining after the general paper [6]. After that, all quotient matrices of equitable 2-partitions of the n-cube were characterized for any n smaller than 24. For $n=24$, the remaining questionable matrices were $[[1,23],[9,15]]$, $[[2,22],[10,14]]$, $[[3,21],[11,13]]$, $[[5,19],[13,11]]$, $[[7,17],[15,9]]$, and it is notable that all these parameters correspond to unbalanced Boolean functions with extreme order of correlation immunity, $15=2n/3-1$.

In the present work, we prove a new property of the equitable partitions that meet the correlation-immunity bound with equality. In particular, our results imply the nonexistence of an equitable partition with quotient matrix $[[2,22],[10,14]]$ or $[[5,19],[13,11]]$, as well as any Boolean function with correlation immunity $2n/3-1$ and proportion between the number of ones and the number of zeros $5:11$, $13:19$, or any $C:B$ such that CB is not divisible by 3. Besides that, we provide a characterization of all inequivalent equitable partitions with the quotient matrices $[[3,9],[7,5]]$ and $[[0,12],[4,8]]$.

From the theoretical point of view, studying Boolean functions lying on the correlation-immunity bound with different proportions of the number of ones and zeros is the most intriguing part of our research. On the other hand, the functions of correlation-immunity order $2n/3-1$ with 2^{n-2} ones are of special interest because of the following two connections, and our classification related with the quotient matrix $[[0,12],[4,8]]$ makes a contribution to their study.

The first connection is with t-resilient functions. A function $f:\{0,1\}^n\to\{0,1\}^m$ is called *t-resilient* if for every $\bar{a}$ from $\{0,1\}^m$ the function

$$f_{\bar{a}}(\bar{x})=\begin{cases}1 & \text{if } f(\bar{x})=\bar{a}\\ 0 & \text{if } f(\bar{x})\neq\bar{a}\end{cases} \tag{1}$$

is correlation immune of order t with 2^{n-m} ones. The resilient functions are important for applications in cryptography, see e.g. [4]. If $m=2$, then $t\leqslant 2n/3-1$ [8]. If $m=2$ and $t=2n/3-1$, then the functions $f_{\bar{a}}$ belong to the class of functions we study and correspond to the equitable partitions of Q_n with quotient matrix $[[0,3T],[T,2T]]$, $T=n/3$.

The second connection is with orthogonal arrays. An *orthogonal array* $\mathrm{OA}(N, n, 2, t)$ (we consider only the binary orthogonal arrays) is a multiset of N vertices on the n-cube such that the number of its elements $(x_1, \ldots, x_n)$ with prescribed values in any t positions does not depend on those values, see e.g. [9]. (Often, the elements of an orthogonal array are considered as being arranged as the rows or the columns of an $N \times n$ or $n \times N$ array, respectively). An orthogonal array is *simple* if it is an ordinary set, without multiplicities more than one. It is straightforward that the simple $\mathrm{OA}(N, n, 2, t)$ are in one-to-one correspondence with the Boolean functions $\{0,1\}^n \to \{0,1\}$ of correlation-immunity order t with N ones (actually, the set of ones of such function forms the corresponding $\mathrm{OA}(N, n, 2, t)$). A result of Bierbrauer [1, Theorem 1] says for $\mathrm{OA}(N, n, q, t)$ that

$$N \geqslant q^n \left(1 - \frac{(q-1)n}{q(t+1)}\right); \tag{2}$$

moreover, for a non-simple array the inequality becomes strict, which is straightforward from the proof, see [1, p. 181, line 4] (note that for the simple binary orthogonal arrays, the bound was proved earlier by Friedman [8, Theorem 2.1]). The arrays $\mathrm{OA}(2^{n-2}, n, 2, 2n/3-1)$ lie on this bound; hence, they are simple and, as follows from the results of [5], correspond to the equitable partitions with quotient matrix $[[0, 3T], [T, 2T]]$, $T = n/3$. In particular, the results of our classification imply that there are exactly 16 inequivalent $\mathrm{OA}(1024, 12, 2, 7)$ and exactly 37 inequivalent $\mathrm{OA}(512, 11, 2, 6)$ (such arrays are obtained from $\mathrm{OA}(1024, 12, 2, 7)$ by shortening). The classification of orthogonal arrays with given parameters is a problem that attracts attention of many researchers, see the recent works [2], [3], and the bibliography there. We note that the preceding computational results were successful for smaller t and N than in our case. Futher discussion on the quotient matrix $[[0, 3T], [T, 2T]]$, related equitable partitions, orthogonal arrays, and Boolean functions can be found in [15].

With the other parameters considered in our paper, the situation is different. The Fon-Der-Flaass bound was generalized to the binary orthogonal arrays by Khalyavin [12], who proved that any $\mathrm{OA}(N, n, 2, t)$ with $N < 2^{n-1}$ satisfies $t \leqslant 2n/3 - 1$. However, this does not mean that any array lying on this bound is simple (e.g., there is a non-simple $\mathrm{OA}(24, 6, 2, 3)$ [24]). The classification of non-simple orthogonal arrays that meet the Fon-Der-Flaass–Khalyavin bound is a separate problem, which is not considered in the current research.

The introductory part of the paper continues with definitions and basic facts (Section 2) and Section 3, where we describe the computer tools used for the classification results. The main theoretical results of the paper are proved in Section 4. Theorem 5 states (in an equivalent formulation) that if the correlation-immunity order of an unbalanced Boolean function f lies on the Fon-Der-Flaass bound, then the number of ones of the derivative $f^{(i)}(\bar{x}) = f(\bar{x}) + f(\bar{x} + \bar{e}_i)$ of f in any basic direction $\bar{e}_i$, $i = 1, \ldots, n$, does not depend on the direction. As a consequence, we have a new necessary condition on the existence of such functions and corresponding equitable 2-partitions (Corollary 6). Section 5 contains the characterization of inequivalent equitable 2-partitions of the 12-cube

with quotient matrix $[[3,9],[7,5]]$, based on the combination of theoretical and computational results, and a description of the original Fon-Der-Flaass construction [7] of such partitions, including the representation via the Fourier transform. In Section 6, we describe the computational classification of the equitable partitions of the 12-cube with quotient matrix $[[0,12],[4,8]]$. The list of the all 16 inequivalent partitions is given in the appendix. As we mentioned above, the last partitions correspond to the order-7 correlation immune Boolean functions in 12 variables with 2^{10} ones, and to the orthogonal arrays $\mathrm{OA}(2^{10},12,2,7)$. In Section 7, we briefly discuss equitable partitions with quotient matrix $[[2,10],[6,6]]$ and the connection of such partitions with orthogonal arrays $\mathrm{OA}(1536,13,2,7)$.

2 Definitions and basic facts

Let $G=(V,E)$ be an undirected graph. A partition $(C_0,\dots,C_{\tau-1})$ of the vertex set V into τ *cells* is called an *equitable partition* (*equitable τ-partition*) with *quotient matrix* $M=(m_{ij})$ if for all $i,j\in\{0,\dots,\tau-1\}$ any vertex of C_i has exactly m_{ij} neighbors in C_j. Two partitions $(C_0,\dots,C_{\tau-1})$ and $(C'_0,\dots,C'_{\tau-1})$ of V are *equivalent* if there is a graph automorphism π such that $\pi(C_i)\in\{C'_0,\dots,C'_{\tau-1}\}$ for every i from $\{0,\dots,\tau-1\}$.

The *n-cube* $Q_n=(\mathrm{v}Q_n,\mathrm{E}Q_n)$ (also known as the Hamming graph $H(n,2)$) is a graph whose vertices are the words of length n over the alphabet $\{0,1\}$, also treated as vectors over the binary field $\mathrm{GF}(2)$. Two vertices are adjacent if and only if they differ in exactly one coordinate position, which is referred to as the *direction* of the corresponding edge. The *Hamming distance* $d(\bar x,\bar y)$ between vertices $\bar x$ and $\bar y$ is the number of coordinates in which they differ. The *weight* $\mathrm{wt}(\bar x)$ of a word $\bar x$ is the number of ones in it. By $(\bar x,\bar y)$, we denote the ordinary inner product of vectors: $(\bar x,\bar y)=x_1y_1+x_2y_2+\dots+x_ny_n$. For two vertices $\bar x=(x_1,\dots,x_n)$, $\bar y=(y_1,\dots,y_n)$, we will write $\bar x\preccurlyeq\bar y$ if $x_i\leqslant y_i$ for all i from 1 to n. We denote by $\bar e_i$ the word with all zeros except one 1 in the i-th position; by $\overline{0}$ and $\overline{1}$, the all-zero and all-one words, respectively. For $\bar x,\bar y\in\mathrm{v}Q_n$, the set $\Gamma^{\bar y}_{\bar x}=\{\bar z+\bar y:\bar z\preccurlyeq\bar x\}$ is a *k-face* of Q_n, where $k=\mathrm{wt}(\bar x)$ is the dimension of the face.

Any equitable 2-partition of Q_n satisfies the following necessary conditions on the coefficients of its quotient matrix $[[a,b],[c,d]]$ [6], [5]:

(a) a, b, c, d are nonnegative integers such that $a+b=c+d=n$, $b>0$, $c>0$;

(b) $\dfrac{b+c}{\gcd(b,c)}$ is a power of 2;

(c) if $b\neq c$, then $a-c\geqslant -\dfrac{n}{3}$.

Condition (c) is a special case of the bound $t\leqslant 2n/3-1$ on the order t of correlation immunity of an unbalanced Boolean function [5]. We say that an equitable 2-partition with quotient matrix $[[a,b],[c,d]]$ *attains the correlation-immunity bound* if $b\neq c$ and $a-c=-n/3$ (equivalently, $b+c=4n/3$). Besides (a)–(c), the only matrix for which the nonexistence of the corresponding equitable 2-partitions of Q_n was established, before

the current research, was $[[1,11],[5,7]]$ (usually, we also agree that $b \geqslant c$, because this can always be reached by choosing the order of cells), see [7]. In Section 4, we will prove a new necessary condition, which rejects the matrix $[[1,11],[5,7]]$ as well as an infinite number of other matrices satisfying (a)–(c).

Some of our results are formulated in terms of real-valued functions defined on the vertices of the n-cube. Two such functions $f_1, f_2 : \mathrm{v}Q_n \to \mathbb{R}$ are *equivalent* if there is a permutation π of n coordinate positions and a vector $\bar{y}$ such that $f_1(\bar{y}+\pi\bar{x}) = f_2(\bar{x})$ for all $\bar{x} \in \mathrm{v}Q_n$. The *norm* of a function f is $\|f\| = (\sum_{\bar{y}\in \mathrm{v}Q_n} f(\bar{y})^2)^{\frac{1}{2}}$.

Given an eigenvalue λ of the adjacency matrix of a graph $G = (V, E)$, a function $f : V \to \mathbb{R}$ is called an *eigenfunction* or a *λ-eigenfunction* of G if it is not constantly zero and for every $x \in V$

$$\lambda \cdot f(x) = \sum_{y\in V:(x,y)\in E} f(y).$$

Note that the tuple of values of a λ-eigenfunction is essentially an eigenvector of the adjacency matrix of G corresponding to the eigenvalue λ.

It is well known and easy to check that the eigenspectrum of Q_n is $\{\lambda_i(n) = n - 2i : i = 0, 1, \ldots, n\}$ and the set of functions $\{\chi_{\bar{y}}(\bar{x}) = (-1)^{(\bar{x},\bar{y})} : \mathrm{wt}(\bar{y}) = i\}$ is an orthogonal basis of the $\lambda_i(n)$-eigenspace of Q_n for $i = 0, 1, \ldots, n$. Therefore, for a function f defined on $\mathrm{v}Q_n$, the following identity holds

$$f(\cdot) = \sum_{\bar{y}\in \mathrm{v}Q_n} \widehat{f}(\bar{y})\chi_{\bar{y}}(\cdot),$$

where

$$\widehat{f}(\bar{y}) = \frac{1}{2^n} \sum_{\bar{z}\in \mathrm{v}Q_n} f(\bar{z})(-1)^{(\bar{z},\bar{y})}$$

is a *Fourier coefficient*, $\bar{y} \in \mathrm{v}Q_n$. By the weight of the coefficient $\widehat{f}(\bar{y})$, we will understand the weight of $\bar{y}$. The next properties of the basis $\{\chi_{\bar{y}} : \bar{y} \in \mathrm{v}Q_n\}$ follow instantly from its definition.

Proposition 1. *For $\bar{x}, \bar{y} \in \mathrm{v}Q_n$ the following equalities hold:*

(i) $\chi_{\bar{0}} \equiv 1$,

(ii) $\chi_{\bar{x}}\chi_{\bar{y}} = \chi_{\bar{x}+\bar{y}}$.

We will need the following well-known properties of the basis functions.

Proposition 2. (i) *For every $k \in \{0, \ldots, n-1\}$, every $\bar{y} \in \mathrm{v}Q_n$ of weight $n-k$, and every $(k+1)$-face Γ, it holds*

$$\sum_{\bar{x}\in\Gamma} \chi_{\bar{y}}(\bar{x}) = 0;$$

(ii) (see, e.g., [17, Ch. 5, Lemma 2]) *for every $\bar{x}$ and $\bar{y}$ from $\mathrm{v}Q_n$, it holds*

$$2^{n-\mathrm{wt}(\bar{x})} \sum_{\bar{z}\preccurlyeq\bar{x}} \widehat{\chi}_{\bar{y}}(\bar{z}) = \sum_{\bar{z}\preccurlyeq\bar{x}+\bar{1}} \chi_{\bar{y}}(\bar{z}). \tag{3}$$

Proof. (i) Let $\Gamma = \Gamma_{\bar{z}}^{\bar{z}'}$ for some words $\bar{z}$ of weight $k+1$ and $\bar{z}'$. Since $\mathrm{wt}(\bar{y}) = n-k$, there is some coordinate position j where $\bar{z}$ and $\bar{y}$ both have 1. Thus, for every $\bar{x} \in \Gamma$, we have $\chi_{\bar{y}}(\bar{x}) + \chi_{\bar{y}}(\bar{x} + \bar{e}_j) = 0$.

(ii) By the definition of a Fourier coefficient, $\widehat{\chi}_{\bar{y}}(\bar{z})$ equals 1 if $\bar{z} = \bar{y}$ and 0 otherwise. Thus, the left side of (3) is equal to $2^{n-\mathrm{wt}(\bar{x})}$ if $\bar{y} \preccurlyeq \bar{x}$ and zero otherwise. In the right side, we also have $\sum_{\bar{z} \preccurlyeq \bar{x}+\bar{1}} 1 = 2^{n-\mathrm{wt}(\bar{x})}$ if $\bar{y} \preccurlyeq \bar{x}$. In the remaining case $\bar{y} \succ \bar{x}$, we have 0 by arguments similar to (i). □

For a given set V of v elements, a (t,k,v)-*covering*, $t \leqslant k \leqslant v$, is a set S of k-subsets of V such that for every t-subset T of V there exists K from S such that $T \subseteq K$. The following facts are trivial and well known, see e.g. [22].

Proposition 3. *If S be a (t,k,v)-covering of a set V of size v, then*

(i) $|S| \geqslant \frac{\binom{v}{t}}{\binom{k}{t}}$;

(ii) *for every $a \in V$, the set $S_a = \{K \backslash \{a\} : a \in K \in S\}$ is a $(t-1,k-1,v-1)$-covering of $V \setminus \{a\}$.*

Given an equitable 2-partition (C_0, C_1) of Q_n with quotient matrix $[[a,b],[c,d]]$, by its *associated function* we will understand the function $f : \mathrm{v}Q_n \to \mathbb{R}$ defined as follows:

$$f(\bar{x}) = \begin{cases} b, & \bar{x} \in C_0 \\ -c, & \bar{x} \in C_1. \end{cases}$$

Lemma 4 ([5, 7])**.** *Let (C_0, C_1) be an equitable 2-partition of Q_n with quotient matrix $[[a,b],[c,d]]$ and associated function $f : \mathrm{v}Q_n \to \mathbb{R}$. Then the following identities take place:*

$$\begin{aligned} \widehat{f}(\bar{x}) &= 0 \qquad \text{for all } \bar{x} \text{ such that } \mathrm{wt}(\bar{x}) \neq \frac{b+c}{2}, \\ (b-c)\widehat{f}(\bar{x}) &= \sum_{\bar{y},\bar{z}:\, \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{y})\widehat{f}(\bar{z}) \qquad \text{for all } \bar{x} \neq \bar{0}, \\ bc &= \sum_{\bar{y}} \widehat{f}(\bar{y})^2. \end{aligned}$$

Proof. Counting the values of f over the neighbours of a given vertex, we find that f is an $(n-b-c)$-eigenfunction of Q_n. Thus, all its nonzero Fourier coefficients have weight $\frac{b+c}{2}$. By the definition of the associated function, we know that $(f-b)(f+c) = 0$. Therefore,

$$\left(\sum_{\bar{y} \in \mathrm{v}Q_n} \widehat{f}(\bar{y})\chi_{\bar{y}} - b\chi_{\bar{0}} \right) \left(\sum_{\bar{y} \in \mathrm{v}Q_n} \widehat{f}(\bar{y})\chi_{\bar{y}} + c\chi_{\bar{0}} \right) = 0.$$

After removing parentheses and using Proposition 1, we obtain the remaining equalities. □

The *kernel* of an equitable 2-partition $C = (C_0, C_1)$ is the set

$$\ker(C) = \{\bar{y} \in \mathrm{v}Q_n : C_0 = C_0 + \bar{y}\} = \{\bar{y} \in \mathrm{v}Q_n : f(\bar{x} + \bar{y}) = f(\bar{x}) \text{ for all } \bar{x} \in \mathrm{v}Q_n\}$$

of all periods of the cells or, equivalently, of the associated function f.

3 Computational tools

Exact covering. The approaches we apply for enumerating equitable partitions of Q_{12} (the approaches are completely different for the quotient matrices $[[3, 9], [7, 5]]$ and $[[0, 12], [4, 8]]$) include solving instances of the exact covering problem. In general, the exact covering problem can be formulated as follows. Given elements $a_1, \ldots, a_k$, natural numbers $\alpha_1, \ldots, \alpha_k$, and a collection $\mathcal{A} = \{A_1, \ldots, A_m\}$ of subsets of the set $\{a_1, \ldots, a_k\}$, find a subcollection $\mathcal{A}'$ of $\mathcal{A}$ such that each element a_i is contained in exactly α_i sets from $\mathcal{A}'$. Most mathematical packages include methods for finding an exact cover in the case $\alpha_1 = \cdots = \alpha_k = 1$, which is solved much effectively in practice than the general problem. However, our approaches need finding exact covers with different multiplicities. We exploited the `libexact` package [11], which can be used in `c/c++` programs.

Isomorphism. To find the number of equivalence classes of 2-partitions of the vertices of Q_n from a considered class, or any intermediate objects, we use the standard technique described in [10, Sect. 3.3]. Namely, sets of vertices of Q_n are represented by graphs in such a manner that two objects are equivalent if and only if the corresponding graphs are isomorphic. A famous package to work with the graph isomorphism is `nauty` [18]. The same approach allows to find the automorphism group of any object we deal with.

Double counting. The following nice approach, described in [10, Sect. 10.2], allows to partially validate the results of the exhaustive search. Assume that we have finished the classification of some objects and have found a representative of every equivalence class. Knowing the order of the automorphism group of each representative, we can calculate the total number of different objects. If this number does not coincide with the number of objects found by the exhaustive search, then the search was erroneous. This approach catches many kinds of systematic and random mistakes, but only works if the result of the search is not empty. We checked the results of every step of our classification by this double-counting method.

4 New necessary condition

In this section we provide a new necessary condition of the existence of equitable 2-partitions of Q_n attaining the bound [5] on correlation immunity. Given an equitable partition of a n-cube, we will say that an edge of the graph is *composite* if it is incident to vertices from different cells of the partition.

Theorem 5. *Let (C_0, C_1) be an equitable partition of Q_n with quotient matrix $[[a,b],[c,d]]$, $b \neq c$, attaining the correlation-immunity bound, i.e., $a - c = -\frac{n}{3}$. Let $f : \mathrm{v}Q_n \to \mathbb{R}$ be the function associated to this partition. The following statements are true:*

(i) *the value $\sum_{\bar{x}:\, x_i=0} \widehat{f}(\bar{x})^2$ does not depend on $i \in \{1,\dots,n\}$;*

(ii) *the number of composite edges of direction i does not depend on $i \in \{1,\dots,n\}$.*

Proof. (i) Since our partition attains the bound on correlation immunity, we have $a-c = -\frac{n}{3}$. By Lemma 4, we know that $\widehat{f}(\bar{x}) = 0$ if $\mathrm{wt}(\bar{x}) \neq \frac{2n}{3}$, and for every $\bar{x} \neq \overline{0}$, the following equality holds:

$$(b-c)\widehat{f}(\bar{x}) = \sum_{\bar{y},\bar{z}:\, \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{y})\widehat{f}(\bar{z}); \qquad \text{hence,} \quad \widehat{f}(\bar{x})^2 = \frac{1}{b-c} \sum_{\bar{y},\bar{z}:\, \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}).$$

Take some $i \in \{1,\dots,n\}$. Consider the square of the norm of the subfunction corresponding to $x_i = 0$, where $\bar{x} = (x_1,\dots,x_n)$. Our goal is to show that this norm does not depend on the choice of i.

$$\sum_{\bar{x}:\, x_i=0} \widehat{f}(\bar{x})^2 = \sum_{\bar{x}:\, x_i=0} \frac{1}{b-c} \sum_{\bar{y},\bar{z}:\, \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}) = \frac{1}{b-c} \sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}\\ x_i=0}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z})$$

$$= \frac{1}{3(b-c)} \left(\sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}\\ x_i=0}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}) + \sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}\\ y_i=0}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}) + \sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}\\ z_i=0}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}) \right).$$

We state that

$$\sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}\\ x_i=0}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}) + \sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}\\ y_i=0}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}) + \sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}\\ z_i=0}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}) = \sum_{\substack{\bar{x},\bar{y},\bar{z}:\\ \bar{x}+\bar{y}+\bar{z}=\overline{0}}} \widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z}).$$

Indeed, for every nonzero term $\widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z})$, each of the words $\bar{x}$, $\bar{y}$, $\bar{z}$ has exactly $\frac{n}{3}$ zeros and the positions of the zeros do not intersect for $\bar{x}$, $\bar{y}$, and $\bar{z}$ (which follows from $\bar{x}+\bar{y}+\bar{z} = \overline{0}$). Therefore, every nonzero summand $\widehat{f}(\bar{x})\widehat{f}(\bar{y})\widehat{f}(\bar{z})$ in the right side occurs exactly in one sum in the left side of the equality. This observation proves the last equality and the first claim of the theorem.

(ii) Let us count the number of composite edges of an arbitrary direction $i \in \{1,\dots,n\}$. Clearly, this value equals

$$\frac{1}{2(b-c)^2} \sum_{\bar{x} \in \mathrm{v}Q_n} \big(f(\bar{x}+\bar{e}_i) - f(\bar{x})\big)^2.$$

Using the Fourier transform, we have that

$$\sum_{\bar{x} \in \mathrm{v}Q_n} \big(f(\bar{x}+\bar{e}_i) - f(\bar{x})\big)^2 = \sum_{\bar{x} \in \mathrm{v}Q_n} \left(2 \sum_{\bar{y} \in \mathrm{v}Q_n:\, y_i=1} \widehat{f}(\bar{y})(-1)^{(\bar{x},\bar{y})} \right)^2.$$

After removing parentheses, dividing by 2^{n+2}, and changing the order of summing, we have

$$\frac{1}{2^n}\sum_{\bar{y}\in \mathrm{V}Q_n:y_i=1}\ \sum_{\bar{y}'\in \mathrm{V}Q_n:y'_i=1}\widehat{f}(\bar{y})\widehat{f}(\bar{y}')\sum_{\bar{x}\in \mathrm{V}Q_n}(-1)^{(\bar{x},\bar{y}+\bar{y}')}=\sum_{\bar{y}\in \mathrm{V}Q_n:y_i=1}\widehat{f}(\bar{y})^2=\sum_{\bar{y}\in \mathrm{V}Q_n}\widehat{f}(\bar{y})^2-\sum_{\bar{y}\in \mathrm{V}Q_n:y_i=0}\widehat{f}(\bar{y})^2.$$

By claim (i), the proof is done. □

Corollary 6. *If there exists an equitable partition of Q_n with quotient matrix $[[a,b],[c,d]]$ attaining the correlation-immunity bound, $b\neq c$, then either $\frac{b}{\gcd(b,c)}$ or $\frac{c}{\gcd(b,c)}$ is divisible by 3.*

Proof. Let (C_0,C_1) be an equitable 2-partition of Q_n with quotient matrix $[[a,b],[c,d]]$, $b\neq c$, attaining the correlation immunity bound. From the definition of an equitable partition, we see that there are $\frac{c}{b+c}2^n$ vertices in C_0. Consequently, there are exactly $\frac{bc}{b+c}2^{n-1}$ composite edges in the graph. By Theorem 5 we conclude that

$$\frac{bc}{n(b+c)}2^{n-1}\in\mathbb{N}.$$

Since our partition attains the bound on correlation immunity, we have $a-c=-\frac{n}{3}$. The degree of the n-cube equals $n=a+b$; so, we have $n=\frac{3}{4}(b+c)$. Substituting this expression to the number of edges, we prove the required statement. □

Corollary 6 implies the nonexistence of an infinite sequence of putative parameters of equitable 2-partition of Q_n for which this question was open before. In particular, it gives an alternative proof of the nonexistence of equitable 2-partitions of Q_{12} with quotient matrix $[[1,11],[5,7]]$, which was shown in [7], and the nonexistence of 2-partitions of Q_{24} with quotient matrices $[[2,22],[10,14]]$ and $[[5,19],[13,11]]$:

Corollary 7 (example)**.** *There are no equitable 2-partitions of Q_n with quotient matrices $[[T,11T],[5T,7T]]$ $(T=n/12)$ and $[[5T,19T],[13T,11T]]$ $(T=n/24)$.*

5 The equitable partitions with quotient matrix $[[3,9],[7,5]]$

In this Section we characterize all inequivalent 2-partitions of Q_{12} with quotient matrix $[[3,9],[7,5]]$.

5.1 General properties

Let (C_0,C_1) be an equitable 2-partition with quotient matrix $[[3,9],[7,5]]$. By direct counting, we have $|C_0|=7\cdot 256$ and $|C_1|=9\cdot 256$. Let f be the associated function:

$$f(\bar{x})=\begin{cases}9, & \bar{x}\in C_0\\ -7, & \bar{x}\in C_1.\end{cases}$$

By Lemma 4, we know that f is an eigenfunction corresponding to the eigenvalue $\lambda_8(12) = -4$ and all its nonzero Fourier coefficients have weight 8. Therefore, Proposition 2(i) guarantees that the sum of values of f over any 5-face equals 0. Consequently, any 5-face contains exactly 18 vertices from C_1 and 14 vertices from C_0. Proposition 2(ii) gives us the identity

$$16 \cdot \widehat{f}(\bar{x}) = \sum_{\bar{z} \preccurlyeq \bar{x}+\overline{1}} f(\bar{z}) \qquad \text{for all } \bar{x} \text{ such that } \mathrm{wt}(\bar{x}) = 8.$$

In the right side of the equality we have the sum of values of f over some 4-face of Q_{12}. This means that $\widehat{f}(\bar{x}) \in \{\frac{1}{16}(9m - 7(16-m)) : m = 0, 1, \ldots, 16\} = \{m - 7 : m = 0, 1, \ldots, 16\}$. In particular, $\widehat{f}(\bar{x})$ is integer.

Let us take an arbitrary $\bar{x}$ of weight 9 and use Proposition 2(ii) one more time:

$$\sum_{\bar{z} \preccurlyeq \bar{x}} \widehat{f}(\bar{z}) = \frac{1}{8} \sum_{\bar{z} \preccurlyeq \bar{x}+\overline{1}} f(\bar{z}).$$

Since the value from the right side of the equation belongs to $\{\frac{1}{8}(9m - 7(8-m)) : m = 0, 1, \ldots, 8\} = \{2m - 7 : m = 0, 1, \ldots, 8\}$, the sum $\sum_{\bar{z} \preccurlyeq \bar{x}} \widehat{f}(\bar{z})$ is odd. For a given $\bar{x} \in \mathrm{v}Q_n$ of weight 9, there is at least one $\bar{z} \preccurlyeq \bar{x}$ of weight 8 such that $\widehat{f}(\bar{z})$ is odd. In other words, the set of quadruples of zero coordinates of the weight-8 vertices $\bar{z}$ for which $\widehat{f}(\bar{z})$ is odd forms a $(3, 4, 12)$-covering T. Our next goal is to describe the set of possible values $\widehat{f}$ can take.

Applying Lemma 4 to our function, we have

$$\widehat{f}(\bar{x}) = 0, \qquad \text{if } \mathrm{wt}(\bar{x}) \neq 8, \tag{4}$$

$$2\widehat{f}(\bar{x}) = \sum_{\bar{y},\bar{z}\colon \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{y})\widehat{f}(\bar{z}), \qquad \text{if } \bar{x} \neq \overline{0}, \tag{5}$$

$$\sum_{\bar{x}} \widehat{f}(\bar{x})^2 = 63. \tag{6}$$

Suppose there is $\bar{y}$ such that $|\widehat{f}(\bar{y})| \geqslant 2$. Without loss of generality we take

$$\bar{y} = (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0).$$

By Theorem 5 we have

$$\sum_{\bar{x}\colon x_{12}=0} \widehat{f}(\bar{x})^2 = 21.$$

By Proposition 3(ii), the elements of our covering T containing the 12-th coordinate position form a $(2, 3, 11)$-covering by odd values of $\widehat{f}$ of the set $\{1, 2, \ldots, 11\}$. Since the sum of squares equals 21 and $|\widehat{f}(\bar{y})| \geqslant 2$, we conclude that the size of this covering is not bigger than 17. By Proposition 3(i), it must be at least 19, and we get a contradiction.

The arguments above prove the following statement.

Lemma 8. *Let f be the associated function of an equitable 2-partition of Q_{12} with quotient matrix $[[3, 9], [7, 5]]$. Then $\widehat{f}(\bar{x}) \in \{-1, 0, 1\}$ for every $\bar{x} \in \mathrm{v}Q_n$.*

5.2 Configurations of overcovered triples

As follows from Lemma 8 above, for every triple $\{i,j,k\}$ of different coordinates the number of nonzeros $\bar{x} = (x_1, \dots, x_{12})$ of $\widehat{f}$ such that $x_i = x_j = x_k = 0$ is odd. Since the nonzero $\bar{x}$ has exactly 4 zero coordinates (the quadruple of these coordinates will be referred to as *block*), we have a covering of all triples by 63 blocks, a $(3,4,12)$ covering. Consider the multiset A of all triples where the multiplicity of a triple is the number of blocks covering this triple (we know this number is odd). Reducing the multiplicities by 1, we get a multiset B with the coefficients equal to the number of "overcovering" of the corresponding triple. All these coefficients are even, and hence we can divide them by 2, obtaining a multicet C. The elements of C will be called *bitriples* (naturally, one bitriple in C corresponds to two triples in B). Taking into account the multiplicities, we have exactly 16 bitriples. Indeed, 63 blocks cover $4 \cdot 63 = 252 = 220 + 2 \cdot 16$ triples in total; each of $12 \cdot 11 \cdot 10/3! = 220$ 3-subsets of the set of coordinates is covered, plus each of 16 bitriples is covered twice.

Lemma 9. *Every coordinate belongs to exactly* 4 *bitriples.*

Proof. Every coordinate belongs to 21 blocks, which cover $21 \cdot 3 = 63$ triples with given coordinate, taking into account the multiplicities. The number of different such triples is $11 \cdot 10/2 = 55$. So, we have $(63 - 55)/2$ bitriples (recall that each of bitriples corresponds to two overcoverings, by the definition). □

Lemma 10. (i) *Every two different coordinates belong to an odd number of blocks,* (ii) *at least* 5*.*

Proof. Assume that the 1-st and 2-nd coordinates meet in exactly $21 - k$ blocks. We know that the number of all blocks is 63; exactly $63 - 42 = 21$ of them contain the first coordinate; exactly $21 - k$ of them contain the first and the second coordinates. Hence, exactly k blocks contain the first coordinate and do not contain the second. Similarly, exactly k blocks contain the second coordinate and do not contain the first.

The sum of all 63 values of f is 9 or -7 (the value of f in $\overline{0}$).

(a) The value of f at $10\overline{0}$ is also 9 or -7; therefore, among the 42 nonzeros with 1 in the first coordinate, either $a := 17$, or $a := 21$, or $a := 25$ values -1 and 25, 21, or 17 values $+1$, respectively (for example, if $f(\overline{0}) = -7$ and $f(10\overline{0}) = 9$, then among 42 nonzeros with 1 in the first coordinate, 25 should have the value -1 and 17 the value 1, for the sum change by 16 during the sign inverse, which corresponds to the translation of the partition by the vector $10\overline{0}$).

(b) The value of f at $01\overline{0}$ is also 9 or -7, therefore, among the 42 nonzeros with 1 in the second coordinate, either $b := 17$, or $b := 21$, or $b := 25$ values -1 and 25, 21, or 17 values $+1$, respectively.

(c) The value of f at $11\overline{0}$ is also 9 or -7, therefore, among the $2k$ nonzeros with different values in the first and the second coordinate, either $c = k - 4$, or $c = k$, or $c = k + 4$ values -1 and $k + 4$, k, or $k - 4$ values $+1$, respectively.

In the arguments (a), (b), (c), every nonzero occurs twice or does not occur at all (if it starts with 00). Indeed, if we denote by $\alpha_{i,j}$ the number of nonzeros $\bar{x} = (x_1, \dots, x_{12})$

such that $x_1 = i$, $x_2 = j$, and $f(\bar{x}) = -1$, then we get $a = \alpha_{1,0} + \alpha_{1,1}$, $b = \alpha_{0,1} + \alpha_{1,1}$, $c = \alpha_{0,1} + \alpha_{1,0}$. Hence, $a + b + c = 2(\alpha_{1,0} + \alpha_{0,1} + \alpha_{1,1})$ is even. On the other hand, $a + b + c \in \{k + 30, k + 34, k + 38, k + 42, k + 46, k + 50, k + 54\}$. It follows that k is even and $21 - k$ is odd.

(ii) follows from covering of all 10 triples that include the given pair. □

Corollary 11. *Each two different coordinates belong to an even number of bitriples,* 0*,* 2*, or* 4*.*

Proof. Without loss of generality, consider the first two coordinates. every 4-block containing them covers exactly two triples they belong to. So, the number of such 4-blocks is the half of the number of different triples of form $\{1, 2, i\}$, $i > 2$, plus the number, say k, of bitriples of such form. That is, $(12 - 2)/2 + k$. By Lemma 10, this number is odd. Hence, k is even. □

Our next goal is to describe possible bitriple systems up to equivalence. We first assume that there is at least one bitriple of multiplicity 1.

Lemma 12. *If there is a bitriple of multiplicity* 1*, then it belongs to the collection of* 8 *bitriples* $\{4 \pm 3, 5 \pm 3, 6 \pm 3\}$*, up to a coordinate permutation.*

Proof. Without loss of generality assume that we have a bitriple $\underline{\{1, 2, 3\}}$ of multiplicity 1. By Corollary 11, there is another bitriple with 1 and 2. Without loss of generality it is $\underline{\{1, 2, 9\}}$. By Corollary 11, there is another bitriple with 1 and 3. It cannot be $\{1, 9, 3\}$, because in that case any choice of the forth bitriple with 1 contradicts Corollary 11. So, it is $\underline{\{1, 8, 3\}}$, without loss of generality (we did not use 8 before). By Corollary 11, the fourth element with 1 is $\underline{\{1, 8, 9\}}$.

Again by Corollary 11 and since the multiplicity of $\{1, 2, 3\}$ is 1, there is another bitriple with 2 and 3. If it is $\{9, 2, 3\}$, then we have bitriples $\{1, 2, 3\}$, $\{1, 2, 9\}$, $\{9, 2, 3\}$ with 9, and the fourth bitriple with 9 contradicts Corollary 11. A similar argument rejects $\{8, 2, 3\}$ (with respect to 3). So, without loss of generality, we have $\underline{\{7, 2, 3\}}$.

Now, the fourth bitriple with 3 must be $\underline{\{7, 8, 3\}}$; the fourth bitriple with 2 must be $\underline{\{7, 2, 9\}}$; the fourth bitriple with 5 must be $\underline{\{7, 8, 9\}}$. □

Lemma 13. *If there is a bitriple of multiplicity* 1*, then the multiset of bitriples is one of the following, up to a coordinate permutation:*

$$\big\{\{4 \pm 3, 5 \pm 3, 6 \pm 3\},\ \{7 \pm 3, 8 \pm 3, 9 \pm 3\}\big\}, \tag{7}$$

$$\big\{\{4 \pm 3, 5 \pm 3, 6 \pm 3\},\ 4{\cdot}\{4, 5, 6\},\ 4{\cdot}\{10, 11, 12\}\big\}, \tag{8}$$

$$\big\{\{4 \pm 3, 5 \pm 3, 6 \pm 3\},\ 2{\cdot}\{4, 5, 9 \pm 3\},\ 2{\cdot}\{10, 11, 9 \pm 3\}\big\}, \tag{9}$$

$$\big\{\{4 \pm 3, 5 \pm 3, 6 \pm 3\},\ 2{\cdot}\{4, 5, 6\},\ 2{\cdot}\{4, 11, 12\},\ 2{\cdot}\{10, 5, 12\},\ 2{\cdot}\{10, 11, 6\}\big\}. \tag{10}$$

Proof. By Lemma 12, we have the first 8 bitriples. If there is another, 9-th bitriple of multiplicity 1, then by the same lemma we have (7). If there is no 9-th bitriple of multiplicity 1, then the remaining bitriples have multiplicity 2 or 4, and a simple exhaust search results in (8)–(10). □

If there is no bitriple of multiplicity 1, then the multiplicities of bitriples are 2 or 4. In this case, we can again divide them by 2, which results in a multiset of 8 triples, call them *bibitriples*. Every coordinate is covered by exactly 2 bibitriples. So, if there is no bibitriples of multiplicity 2, then the 8 bibitriples form a 1-$(12, 3, 2)$ design. If there is exactly one bibitriple of multiplicity 2, the remaining 6 form a 1-$(9, 3, 2)$ design. If there is exactly two bibitriples of multiplicity 2, the remaining 6 form a 1-$(6, 3, 2)$ design. The remaining case is 4 bibitriples of multiplicity 2. The number of 1-$(v, 2, 2)$ designs is known for $v = 12, 9, 6$, see http://oeis.org/A110100. In particular, up to permutation of the coordinates, we have 23, 6, and 2 solutions, respectively.

Finally, we know that the multiset of bibitriples is one of $36 = 4 + 23 + 6 + 2 + 1$ equivalence classes.

5.3 Coverings by 4-ples

For each multiset of bitriples, we can find all possible systems of quadruples such that every triple is included $1+2m$ times, where m is its multiplicity in the multiset of bitriples. To do this, we have to solve the corresponding instance of the exact cover problem. This can be done in seconds on a modern computer (we used the `libexact` [11] package with `c++`). The result is as follows.

Proposition 14. *There are exactly* 180 *equivalence classes of* $(3, 4, 12)$ *coverings such that the overcovered triples correspond to one of the* 36 *equivalence classes of bitriples mentioned above. Only* 5 *of* 36 *equivalence classes of bitriples can be realized in this way; namely,* (7) (112 *inequivalent coverings found*), (8) (1 *covering*), (10) (51 *coverings*),

$$4 \times \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{10, 11, 12\}\}$$

(1 *covering*), *and*

$$2 \times \{\{1, 2, 3\}, \{1, 5, 6\}, \{2, 4, 6\}, \{3, 4, 5\}, \{7, 8, 9\}, \{7, 11, 12\}, \{8, 10, 12\}, \{9, 10, 11\}\}$$

(15 *coverings*).

5.4 Finding signs of the Fourier coefficients

So, we have got 180 candidates for the set of nonzeros. To find the Fourier coefficient in each nonzero, we will exploit equations (5), (6). In particular, for $\bar{x} \neq \overline{0}$, we have

$$2\widehat{f}(\bar{x}) = \sum_{\bar{y},\bar{z}\colon \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{y})\widehat{f}(\bar{z}), \qquad \text{or}$$

$$\widehat{f}(\bar{x}) = \sum_{\bar{y},\bar{z}\colon \bar{y}\prec\bar{z},\, \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{y})\widehat{f}(\bar{z}), \qquad \text{in particular} \tag{11}$$

$$\widehat{f}(\bar{x}) \equiv \sum_{\bar{y},\bar{z}\colon \bar{y}\prec\bar{z},\, \bar{y}+\bar{z}=\bar{x}} \widehat{f}(\bar{y})\widehat{f}(\bar{z}) \bmod 2, \tag{12}$$

where $\prec$ denotes lexicographic preceding. The last equation immediately gives a necessary condition on the set of nonzeros (indeed, for every nonzero $\bar{x}$, we have $\widehat{f}(\bar{x}) \equiv 1 \bmod 2$; so, both parts of (12) do not depend on the sign of $\widehat{f}$). This condition rejects 173 of 180 coverings, as shown in the following computational proposition.

Proposition 15 (computational results)**.** *Among the* 180 *coverings found in Proposition 14, exactly* 7 *coverings can correspond to the nonzeros of a* $\{-1,0,1\}$*-valued function* $\widehat{f}$ *satisfying* (12)*. All these* 7 *coverings correspond to the set* (7) *of bitriples.*

Now assume that F is the set of nonzeros of $\widehat{f}$ and that the function $\phi : F \to \{0,1\}$ defines the sign of $\widehat{f}$ in each nonzero:

$$\widehat{f}(\bar{x}) = \begin{cases} (-1)^{\phi(\bar{x})} & \text{if } \bar{x} \in F, \\ 0 & \text{if } \bar{x} \notin F. \end{cases} \tag{13}$$

We will show that the 63 values of ϕ satisfy a system of $2^{12}-1$ linear equations over $GF(2)$, one equations for each $\bar{x} \neq \overline{0}$.

Consider any zero $\bar{x}$ of $\widehat{f}$ different from $\overline{0}$, i.e., $\widehat{f}(\bar{x}) = 0$, $\bar{x} \neq \overline{0}$. By (12), the number of pairs $\{\bar{y}, \bar{z}\}$ of elements from F such that $\bar{y} + \bar{z} = \bar{x}$ is even (the pairs are unordered; so, we can always assume $\bar{y} \prec \bar{z}$). Denote this number by $p(\bar{x})$. From (12) we see that for $p(\bar{x})/2$ pairs we have $\widehat{f}(\bar{y})\widehat{f}(\bar{z}) = 1$ and for the rest $p(\bar{x})/2$ pairs $\widehat{f}(\bar{y})\widehat{f}(\bar{z}) = -1$. It follows that the number of -1s among all such xs and xs has the same parity as $p(\bar{x})/2$. Let us write this fact as an equation.

$$\sum_{\bar{y},\bar{z}\in F:\, \bar{y}\prec\bar{z},\, \bar{y}+\bar{z}=\bar{x}} (\phi(\bar{y}) + \phi(\bar{z})) \equiv \frac{p(\bar{x})}{2} \bmod 2, \qquad \bar{x} \notin F \cup \{\overline{0}\}. \tag{14}$$

Next, consider an arbitrary nonzero $\bar{x} \in F$. For simplicity assume that $\widehat{f}(\bar{x}) = 1$. From (12) we see that $p(\bar{x})$ is odd, and we find from (12) that the number of -1s among all considered $\widehat{f}(\bar{y})$ and $\widehat{f}(\bar{z})$ is $\frac{p(\bar{x})-1}{2}$ if $\widehat{f}(\bar{x}) = 1$ and $\frac{p(\bar{x})+1}{2}$ if $\widehat{f}(\bar{x}) = -1$. We derive the following identity.

$$\phi(\bar{x}) + \sum_{\bar{y},\bar{z}\in F:\, \bar{y}\prec\bar{z},\, \bar{y}+\bar{z}=\bar{x}} (\phi(\bar{y}) + \phi(\bar{z})) \equiv \frac{p(\bar{x})-1}{2} \bmod 2, \qquad \bar{x} \in F. \tag{15}$$

We see that the 63 values of ϕ satisfy the system of 4095 equations (14), (15) over the finite field GF(2) of order 2 (some of the equations (14) are trivial, $0 = 0$; so, the actual system to solve has less than 800 equations). This system can be solved for all of the 7 remaining candidates for F.

Proposition 16 (computational results)**.** *Among the* 7 *sets considered in Proposition 15, the system of equations* (14), (15) *is consistent for exactly* 2 *sets. In each of these* 2 *cases, the rank of the system is* 44*; so, the number of solutions is* $2^{63-44} = 2^{19}$*.*

It remains, among the 2^{19} solutions in each of 2 cases, to choose the functions that correspond to the Fourier transform of $\{-7, 9\}$-valued functions. It is doable in a reasonable time; however, the following observation reduces the number of calculations even more.

Lemma 17. *For each i from 1 to 12, define the coordinate function $\psi_i : F \to \{0, 1\}$ by the identity $\psi_i(\bar{v}) = v_i$, where $\bar{v} = (v_1, \dots, v_{12})$.*

(i) *If some $\phi : F \to \{0, 1\}$ satisfies all equations (14), (15) then $\phi + \psi_i$ does.*

(ii) *Moreover, if $\widehat{f}$, see (13), is the Fourier transform of a $\{-7, 9\}$-valued function, then adding ψ_i to ϕ does not change this property.*

Proof. (i) It is easy to see that the number of $\bar{y}$s and $\bar{z}$s involved in (14) that have 1 in the i-th position is even. Indeed, if $x_i = 0$, then $y_i + z_i = 0$ for every pair $(\bar{y}, \bar{z})$ under the sum. If $x_i = 1$, then $y_i + z_i = 1$, but the number $p(\bar{x})$ of the pairs involved in the sum is even. Hence, adding ψ_i does not change the parity of the left side of (14).

The similar argument works for (15) with the only difference that $p(\bar{x})$ is even, which is compensated by involving $\bar{x}$ in the left side.

(ii) It is straightforward from the definition of the Fourier transform that the sum $\phi' = \phi + \psi_i$ corresponds to the translation $f'(\bar{v}) = f(\bar{v} + \bar{e}_i)$, where $\bar{e}_i$ has 1 in the i-th position and 0 in the others. □

So, the affine space of the all solutions ϕ can be partitioned into the cosets of the span $\langle \psi_1, \dots, \psi_{12} \rangle$ (the span has dimension 11 in one of the remaining cases and dimension 10 in the other), and it is sufficient to test one representative from every coset. Finally we have found 6 admissible representatives in one of the cases and 12 in the other. It occurs that in each of two cases, the equitable partitions found are equivalent.

Theorem 18. *There are exactly 2 inequivalent equitable partitions of Q_{12} with quotient matrix $[[3, 9], [7, 5]]$. Each of them has the automorphism group of order 48; the sizes of orbits under the action of the automorphism group are 48^{30}, 24^{14}, 8^2 for the smallest cell (in the notation $[\text{orbit size}]^{[\text{number of orbits}]}$) and 48^{40}, 24^{16} for the largest cell. One partition is coordinate transitive (that is, the 12 coordinates form one orbit under the action of the automorphism group) and the size of its kernel is 2. The other partition has two coordinate orbits of size 6 and the kernel of size 4.*

5.5 Fon-Der-Flaass construction

In this section, we define the equitable partitions constructed by Fon-Der-Flaass [7] and describe the corresponding Fourier transforms.

First, we color the vertices of Q_6 into three colors as follows (symbol $*$ can be replaced by each of 0 and 1; so, a word like $0{*}{*}100$ represent a set from 4 vertices, which is referred to as a 2-*face*).

Black:	000000,	111111,	000111,	111000.
White:	100000,	011111,	000011,	111100,
	010000,	101111,	000101,	111010,
	001000,	110111,	000110,	111001.
Gray:	0∗∗100,	1∗∗011,	1001∗∗,	0110∗∗,
12	∗0∗010,	∗1∗101,	010∗1∗,	101∗0∗,
2-faces	∗∗0001,	∗∗1110,	001∗∗1,	110∗∗0.

Next, color Q_{12} as $f_{12}(\bar{u},\bar{v}) := f_6(\bar{u}+\bar{v})$.

It remains to separate gray vertices into white and black. For every 2-face B from the twelve 2-faces above, with $*$s in the i-th and j-th position, we color $(\bar{u},\bar{v}) = (u_1,\dots,v_6)$ such that $\bar{u}+\bar{v} \in B$ with respect to the parity $u_1+u_2+u_3+u_4+u_5+u_6+v_i+v_j$ (by black/white or white/black; so we have the choice for each 2-face). In such a way, we obtain 2^{12} different black/white colorings of the vertices of Q_{12}; the corresponding vertex partitions are equitable with quotient matrix $[[3,9],[7,3]]$ [7].

By Proposition 2(ii) the Fourier coefficient at $\bar{z}$ (e.g., $\bar{z} = 010011101111$) is proportional (with 1/16) to the sum of f over the corresponding 4-face (e.g., respectively, $*0**000*0000$). So, the coefficients are straightforward to find. We omit technical details and describe the 2^{12} possibilities corresponding to the 2^{12} partitions constructed above. The nonzeros of one possible Fourier transform, with the corresponding signs, are the following:

$\begin{bmatrix}\bar{u}\\ \bar{v}\end{bmatrix}$: $\begin{bmatrix}\mathbf{00}1\,111\\ \mathbf{00}1\,111\end{bmatrix}-\begin{bmatrix}\mathbf{010}\,111\\ \mathbf{010}\,111\end{bmatrix}-\begin{bmatrix}\mathbf{100}\,111\\ \mathbf{100}\,111\end{bmatrix}-\begin{bmatrix}111\,\mathbf{00}1\\ 111\,\mathbf{00}1\end{bmatrix}+\begin{bmatrix}111\,\mathbf{010}\\ 111\,\mathbf{010}\end{bmatrix}+\begin{bmatrix}111\,\mathbf{100}\\ 111\,\mathbf{100}\end{bmatrix}+$

$\begin{bmatrix}\mathbf{011}\,\mathbf{011}\\ \mathbf{011}\,\mathbf{011}\end{bmatrix}+\begin{bmatrix}\mathbf{011}\,\mathbf{101}\\ \mathbf{011}\,\mathbf{101}\end{bmatrix}+\begin{bmatrix}\mathbf{011}\,\mathbf{110}\\ \mathbf{011}\,\mathbf{110}\end{bmatrix}+\begin{bmatrix}\mathbf{101}\,\mathbf{011}\\ \mathbf{101}\,\mathbf{011}\end{bmatrix}+\begin{bmatrix}\mathbf{101}\,\mathbf{101}\\ \mathbf{101}\,\mathbf{101}\end{bmatrix}+\begin{bmatrix}\mathbf{101}\,\mathbf{110}\\ \mathbf{101}\,\mathbf{110}\end{bmatrix}+\begin{bmatrix}\mathbf{110}\,\mathbf{011}\\ \mathbf{110}\,\mathbf{011}\end{bmatrix}+\begin{bmatrix}\mathbf{110}\,\mathbf{101}\\ \mathbf{110}\,\mathbf{101}\end{bmatrix}+\begin{bmatrix}\mathbf{110}\,\mathbf{110}\\ \mathbf{110}\,\mathbf{110}\end{bmatrix}+$

$\begin{bmatrix}\mathbf{000}\,\mathbf{110}\\ \mathbf{111}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{001}\,\mathbf{111}\\ \mathbf{110}\,\mathbf{110}\end{bmatrix}+\begin{bmatrix}\mathbf{010}\,\mathbf{111}\\ \mathbf{101}\,\mathbf{110}\end{bmatrix}-\begin{bmatrix}\mathbf{011}\,\mathbf{110}\\ \mathbf{100}\,\mathbf{111}\end{bmatrix}-\begin{bmatrix}\mathbf{100}\,\mathbf{111}\\ \mathbf{011}\,\mathbf{110}\end{bmatrix}-\begin{bmatrix}\mathbf{101}\,\mathbf{110}\\ \mathbf{010}\,\mathbf{111}\end{bmatrix}-\begin{bmatrix}\mathbf{110}\,\mathbf{110}\\ \mathbf{001}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{111}\\ \mathbf{000}\,\mathbf{110}\end{bmatrix}+$

$\begin{bmatrix}\mathbf{000}\,\mathbf{101}\\ \mathbf{111}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{001}\,\mathbf{111}\\ \mathbf{110}\,\mathbf{101}\end{bmatrix}-\begin{bmatrix}\mathbf{010}\,\mathbf{111}\\ \mathbf{101}\,\mathbf{101}\end{bmatrix}+\begin{bmatrix}\mathbf{011}\,\mathbf{101}\\ \mathbf{100}\,\mathbf{111}\end{bmatrix}-\begin{bmatrix}\mathbf{100}\,\mathbf{111}\\ \mathbf{011}\,\mathbf{101}\end{bmatrix}-\begin{bmatrix}\mathbf{101}\,\mathbf{101}\\ \mathbf{010}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{110}\,\mathbf{101}\\ \mathbf{001}\,\mathbf{111}\end{bmatrix}-\begin{bmatrix}\mathbf{111}\,\mathbf{111}\\ \mathbf{000}\,\mathbf{101}\end{bmatrix}+$

$\begin{bmatrix}\mathbf{000}\,\mathbf{011}\\ \mathbf{111}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{001}\,\mathbf{111}\\ \mathbf{110}\,\mathbf{011}\end{bmatrix}-\begin{bmatrix}\mathbf{010}\,\mathbf{111}\\ \mathbf{101}\,\mathbf{011}\end{bmatrix}-\begin{bmatrix}\mathbf{011}\,\mathbf{011}\\ \mathbf{100}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{100}\,\mathbf{111}\\ \mathbf{011}\,\mathbf{011}\end{bmatrix}+\begin{bmatrix}\mathbf{101}\,\mathbf{011}\\ \mathbf{010}\,\mathbf{111}\end{bmatrix}-\begin{bmatrix}\mathbf{110}\,\mathbf{011}\\ \mathbf{001}\,\mathbf{111}\end{bmatrix}-\begin{bmatrix}\mathbf{111}\,\mathbf{111}\\ \mathbf{000}\,\mathbf{011}\end{bmatrix}+$

$\begin{bmatrix}\mathbf{110}\,\mathbf{000}\\ \mathbf{111}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{001}\\ \mathbf{110}\,\mathbf{110}\end{bmatrix}-\begin{bmatrix}\mathbf{111}\,\mathbf{010}\\ \mathbf{110}\,\mathbf{101}\end{bmatrix}+\begin{bmatrix}\mathbf{110}\,\mathbf{011}\\ \mathbf{111}\,\mathbf{100}\end{bmatrix}-\begin{bmatrix}\mathbf{111}\,\mathbf{100}\\ \mathbf{110}\,\mathbf{011}\end{bmatrix}+\begin{bmatrix}\mathbf{110}\,\mathbf{101}\\ \mathbf{111}\,\mathbf{010}\end{bmatrix}-\begin{bmatrix}\mathbf{110}\,\mathbf{110}\\ \mathbf{111}\,\mathbf{001}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{111}\\ \mathbf{110}\,\mathbf{000}\end{bmatrix}-$

$\begin{bmatrix}\mathbf{101}\,\mathbf{000}\\ \mathbf{111}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{001}\\ \mathbf{101}\,\mathbf{110}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{010}\\ \mathbf{101}\,\mathbf{101}\end{bmatrix}-\begin{bmatrix}\mathbf{101}\,\mathbf{011}\\ \mathbf{111}\,\mathbf{100}\end{bmatrix}-\begin{bmatrix}\mathbf{111}\,\mathbf{100}\\ \mathbf{101}\,\mathbf{011}\end{bmatrix}+\begin{bmatrix}\mathbf{101}\,\mathbf{101}\\ \mathbf{111}\,\mathbf{010}\end{bmatrix}+\begin{bmatrix}\mathbf{101}\,\mathbf{110}\\ \mathbf{111}\,\mathbf{001}\end{bmatrix}-\begin{bmatrix}\mathbf{111}\,\mathbf{111}\\ \mathbf{101}\,\mathbf{000}\end{bmatrix}-$

$\begin{bmatrix}\mathbf{011}\,\mathbf{000}\\ \mathbf{111}\,\mathbf{111}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{001}\\ \mathbf{011}\,\mathbf{110}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{010}\\ \mathbf{011}\,\mathbf{101}\end{bmatrix}+\begin{bmatrix}\mathbf{011}\,\mathbf{011}\\ \mathbf{111}\,\mathbf{100}\end{bmatrix}+\begin{bmatrix}\mathbf{111}\,\mathbf{100}\\ \mathbf{011}\,\mathbf{011}\end{bmatrix}-\begin{bmatrix}\mathbf{011}\,\mathbf{101}\\ \mathbf{111}\,\mathbf{010}\end{bmatrix}-\begin{bmatrix}\mathbf{011}\,\mathbf{110}\\ \mathbf{111}\,\mathbf{001}\end{bmatrix}-\begin{bmatrix}\mathbf{111}\,\mathbf{111}\\ \mathbf{011}\,\mathbf{000}\end{bmatrix}-.$

In each of the last six groups, all the signs can be inversed. Additionally, in each of the last six groups, one can apply the coordinate permutation (4 10)(5 11)(6 12) to all 8 nonzeros. The last transformation, applied to one group, switches between the two equivalence classes of the equitable partitions.

6 [[0, 12], [4, 8]] and related structures: classification

The equitable partitions of the 12-cube with quotient matrix $[[0,12],[4,8]]$ (or, equivalently, the orthogonal arrays $\mathrm{OA}(1024,12,2,7)$, as was mentioned in the introduction) can be classified utilizing rather straightforward approach, a local exhaustive search, us-

ing the exact-covering software. Let S be the quotient matrix $[[0, 12], [4, 8]]$. We say that the pair of disjoint sets P_0, P_1 of vertices is an r-local (equitable) partition if $P_0 \cup P_1$ are the all words of weight at most r and the neighborhood of every vertex of weight less than r satisfy the local condition from the definition of the equitable partition.

So, there are exactly two 0-local partitions, $(\{\overline{0}\}, \emptyset)$ and $(\emptyset, \{\overline{0}\})$. For each of them, there is only one 1-local partition, up to isomorphism.

Proposition 19. *Up to isomorphism, there are exactly* 94 *two-local partitions* (P_0, P_1) *with* $\overline{0} \in P_0$*, and exactly* 6*, with* $\overline{0} \in P_1$*.*

Proof. Let $\overline{0} \in P_0$. In this case, all weight-1 words are in P_1. Consider the graph Γ on the 12 weight-1 words, where two vertices are adjacent if in the 12-cube they are adjacent to a common weight-2 word from P_0. So, the weight-2 words from P_0 are in one-to-one correspondence with the edges of Γ (indeed, a weight-2 word has exactly 2 weight-1 neighbors). Next, we see that Γ is a cubic graph (indeed, every weight-1 word is in P_1 and hence has exactly 4 neighbors from P_0; one of them is $\overline{0}$, the other 3 correspond to edges of Γ). The number of unlabelled connected cubic graphs on 4, 6, 8, and 12 vertices is 1, 2, 5, 85, respectively, see http://oeis.org/A002851. So, the number of connected and disconnected cubic graphs on 12 vertices is $85 + 5 + 3 + 1 = 94$.

Let $\overline{0} \in P_1$. Without loss of generality, all weight-1 words with 1 in the first 8 coordinates are assumed to be in P_1, the other 4 in P_0. The last four words have no neighbors in P_0; so, any weight-2 word in P_0 has two weight-1 neighbors in P_1 and can be considered as an edge of some graph Γ' on 8 vertices (weight-1 words of P_1). From the quotient matrix, we see that Γ' is regular of degree 4; so, its complement is cubic. There are 1 disconnected and 5 connected cubic graphs of order 8. □

The search of the 3-local partitions was done by solving instances of the exact covering problem. We fix some 2-local partition (P_0, P_1) and consider the weight-2 words in P_1 as the "points". To each "point" $\bar{x}$, we assign the multiplicity $\mu = 4 - \lambda$, where λ is the number of its weight-1 neighbors from P_0. To each weight-3 word $\bar{y}$ that has no neighbors from P_0, we assign a "set" $s(\bar{y})$ of 3 "points", namely the 3 weight-2 neighbors of $\bar{y}$. With the chosen "points", their multiplicities, and the "sets", we have an instance $\mathrm{Cov}(P_0, P_1)$ of the exact-covering problem. Straightforwardly from the definitions, we have the following one-to-one correspondence.

Proposition 20. *Given a* 2*-local partition* (P_0, P_1)*, the* 3*-local partitions* (R_0, R_1) *such that* $P_0 \subset R_0$ *and* $P_1 \subset R_1$ *are in one-to-one correspondence with the solutions* S *of* $\mathrm{Cov}(P_0, P_1)$*. Namely,* $S = \{s(\bar{y}) \mid \bar{y} \in R_0 \backslash P_0\}$*.*

In such a way, for each of $94+6$ non-isomorphic 2-local partitions, using `libexact`, we found all 3-local continuations. After the isomorph rejection, we found all non-isomorphic 3-local partitions. The same approach allows to proceed the next step in finding the 4-local partitions. The results are checked using the double-counting approach (see Section 3).

Proposition 21 (computational results)**.** *The number of non-isomorphic* 3*-local partitions* (P_0, P_1) *with* $\overline{0} \in P_0$ *and* $\overline{0} \in P_1$ *is* 34 *and* 222*, respectively. For* 4*-local partitions, the number is* 37 *and* 81*, respectively.*

The remaining part of the classification is based on the fact that the sum of the values of the $\{12, -4\}$-valued eigenfunction corresponding to a putative equitable partition (with considered parameters) over any 5-face is zero. Using this condition, one can uniquely reconstruct an eigenfunction by its values on the words of weight at most 4 (actually, it is sufficient to know the values on the weight-4 words, see [25, Theorem 3]). It occurs that every 4-local partition continues to a complete equitable partition (we have no theoretical proof of this fact).

Theorem 22 (computational results)**.** *There are exactly* 16 *equivalence classes of equitable partitions* (P_0, P_1) *of the* 12*-cube with quotient matrix* $[[0, 12], [4, 8]]$*. In one of them,* P_0 *is a linear (or affine) subspace of the* 12*-cube; two are "full-rank", i.e., the affine span of* P_0 *is the whole* 12*-cube; the other* 13 *are "semilinear", that is, the affine span of* P_0 *consists of a half of the vertices of the* 12*-cube. See the appendix for the list of representatives.*

Remark 23. For the classification, it is sufficient to consider only the local partitions that meet $\overline{0} \in P_0$, or only the local partitions that meet $\overline{0} \in P_1$. However, as the both ways were successful, we described in Propositions 19 and 21 the intermediate results for each of them.

Remark 24. The local search algorithm described in this section can be applied for finding equitable partitions with different parameters (in different graphs). However, we failed in the classification of the equitable partition of the 12-cube with quotient matrices $[[2, 10], [6, 6]]$ and $[[3, 9], [7, 5]]$ using the same approach. The corresponding instances of the exact-covering problem occur to be too large to solve with known tools.

The equitable partitions considered in the current section are related with several classes of combinatorial configurations. The following lemma summarizes several known results about such relations.

Lemma 25. *The objects from the following classes are in one-to-one correspondence:*

(I) *the equitable partitions of the* n*-cube with quotient matrix* $\begin{pmatrix} 0 & n \\ c & n-c \end{pmatrix}$, $c < n$;

(II) *the orthogonal arrays* $OA(N, n, 2, t)$*, where* $t = \dfrac{n+c}{2} - 1$ *and* $N = 2^n\Big(1 - \dfrac{n}{2(t+1)}\Big)$ *(so, the parameters attain the bound* (2)*)*;

(III) *the orthogonal arrays* $OA(N/2, n-1, 2, t-1)$;

(IV), (V) *the equitable partitions of the* $(n-1)$*-cube with quotient matrices* $\begin{pmatrix} 0 & c-1 & n-c \\ c-1 & 0 & n-c \\ c & c & n-2c-1 \end{pmatrix}$ *and* $\begin{pmatrix} c-1 & n-c & 0 \\ c & n-2c-1 & c \\ 0 & n-c & c-1 \end{pmatrix}$, *respectively*;

(VI) *the completely regular codes in* Q_{n-1} *with the intersection array* $(n-c, c; c, n-c)$.

By the definition, a *completely regular code* with the intersection array $(c_1, \dots, c_r; b_0, \dots, b_{r-1})$ is a set of vertices such that the distance partition with respect to it is equitable with tridiagonal quotient matrix, $(c_1, \dots, c_r)$ and $(b_0, \dots, b_{r-1})$ being the subdiagonal and the superdiagonal; so, the correspondence between (V) and (VI) is straightforward. The connection between (I) and (II) is noted in [19, 20]. (III), (IV), and (VI) are related in [16]. It is known [21, Proposition 2.3] that for odd t, the arrays $\mathrm{OA}(N/2, n-1, 2, t-1)$ are in one-to-one correspondence with the self-complementary arrays $\mathrm{OA}(N, n, 2, t)$ (a set C of vertices of Q_n is *self-complementary* if $C = C + \overline{1}$); on the other hand, the array of type (II) must be self-complementary because of the distance invariance of equitable partitions, see e.g. [14].

Once, for $n = 12$ and $c = 4$ we have representatives of all 16 equivalence classes of partitions of type (I), it is rather straightforward to find the number of equivalence classes of objects of types (II)–(VI).

Theorem 26. *There are exactly* 16 *inequivalent orthogonal arrays* $OA(1024, 12, 2, 7)$. *There are exactly* 37 *inequivalent objects from each of the following families: orthogonal arrays* $OA(512, 11, 2, 6)$*; completely regular codes in* Q_{11} *with the intersection array* $(8, 4; 4, 8)$*; equitable partitions of* Q_{11} *with quotient matrices* $[[0, 3, 8], [3, 0, 8], [4, 4, 3]]$ *and* $[[3, 8, 0], [4, 3, 4], [0, 8, 3]]$*, respectively.*

Remark 27. Unifying the first two cells of a 3-partition with quotient matrix $[[0, 3, 8], [3, 0, 8], [4, 4, 3]]$, we obtain an equitable 2-partition with quotient matrix $[[3, 8], [8, 3]]$. However, not all 2-partitions with quotient matrix $[[3, 8], [8, 3]]$ can be obtained in such a way.

7 $[[2, 10], [6, 6]]$: discussion, connection with $\mathrm{OA}(1536, 13, 2, 7)$

The remaining quotient matrix related with equitable partitions of $H(n, 2)$ that attain the correlation-immunity bound and were not discussed in details above is $[[2, 10], [6, 6]]$. The corresponding equitable partitions are of some special combinatorial interest because the first cell of such partition induces a collection of disjoint cycles in the Hamming graph. We failed to make the complete classification of such partitions using any approach described here directly. However, the computational algorithm from Section 6 can be modified, dividing the classification into more steps depending on the value of some coordinate. This way can be successful, but requires relatively large amount of computational resources. Hopefully, the classification will be finished within several months, and at this moment we can only announce that there are more than 80 equivalence classes of such partitions. In this section, we briefly discuss the length of cycles induced by such a partition and mention the relation with the quotient matrix $[[0, 13], [3, 10]]$, which corresponds to the orthogonal arrays $\mathrm{OA}(1536, 13, 2, 7)$.

7.1 Cycle lengths

As one can see from the first coefficient of the quotient matrix $[[2, 10], [6, 6]]$, the first cell of a corresponding equitable partition induces a regular subgraph of Q_{12} of degree 2, i.e.,

the union of disjoint cycles. Any theoretical information on the structure of a partition could simplify the classification; so, it is important to understand if the size of cycles is a constant or it can vary. In the following proposition, we show that there are partitions that induce both 4-cycles and 8-cycles. Another conclusion that can be made from it is that the simple construction [6, Prop. 1(c)] that multiplies the quotient matrix by an integer number can produce inequivalent equitable partitions if one varies the addition, treating the vertex set of the n-cube as different $\mathbb{Z}_4$ modules.

Proposition 28. *For every i from $\{0,1,2,3\}$, there is an equitable partition of Q_{12} with quotient matrix $[[2,10],[6,6]]$ such that the first cell induces $128\cdot(3-i)$ cycles of length 4 and $64\cdot i$ cycles of length 8.*

Proof. (i) We start with $i=0$ and construct a required partition (D_0,D_1) using the doubling construction [6, Proposition 1(c)]: if (P_0,P_1) is an equitable partition of Q_6 with quotient matrix $[[1,5],[3,3]]$, then (D_0,D_1) is defined by

$$D_i=\{(\bar{x},\bar{y}) \mid \bar{x}+\bar{y}\in P_i\}.$$

Now consider an arbitrary vertex $(\bar{x},\bar{y})$ from D_0. Let $\bar{z}=\bar{x}+\bar{y}\in P_0$, and let $\bar{z}+\bar{e}_j$ be the only neighbor of $\bar{z}$ from P_0. Then $(\bar{x},\bar{y})$, $(\bar{x}+\bar{e}_j,\bar{y})$, $(\bar{x}+\bar{e}_j,\bar{y}+\bar{e}_j)$, $(\bar{x},\bar{y}+\bar{e}_j)$ belong to D_0 and form a 4-cycle. So, every element of D_0 lies in a cycle of length 4 with elements from D_0.

(ii) Let $i=3$. Again, we start with the partition (P_0,P_1) and use the same construction but with different addition:

$$D_i=\{(\bar{x},\bar{y}) \mid \bar{x}\oplus\bar{y}\in P_i\}.$$

Here, the sum of $(x_1,\dots,x_6)\oplus(y_1,\dots,y_6)$ is defined by pairs of coordinates: $(x_{2j-1},x_{2j})\oplus(y_{2j-1},y_{2j})=\phi(\phi^{-1}(x_{2j-1},x_{2j})+\phi^{-1}(y_{2j-1},y_{2j}))$, where ϕ: $0\to 00$, $1\to 01$, $2\to 11$, $3\to 10$ is the *Gray map* from $\mathbb{Z}_4=\mathbb{Z}/4\mathbb{Z}$ to $\mathrm{GF}(2)^2$. It is straightforward that the construction doubled the parameters of the quotients matrices for this modification as well as in the case of usual addition. Again, consider an arbitrary vertex $(\bar{x},\bar{y})$ such that $\bar{z}=\bar{x}+\bar{y}$ and $\bar{z}+\bar{e}_j$ are from from P_0. We see that $(\bar{x},\bar{y})$, $(\bar{x}\oplus\bar{e}_j,\bar{y})$, $(\bar{x}\oplus\bar{e}_j,\bar{y}\ominus\bar{e}_j)$, $(\bar{x}\oplus\bar{e}_j\oplus\bar{e}_j,\bar{y}\ominus\bar{e}_j)$, $(\bar{x}\oplus\bar{e}_j\oplus\bar{e}_j,\bar{y}\ominus\bar{e}_j\ominus\bar{e}_j)$, $(\bar{x}\ominus\bar{e}_j,\bar{y}\ominus\bar{e}_j\ominus\bar{e}_j)$, $(\bar{x}\ominus\bar{e}_j,\bar{y}\oplus\bar{e}_j)$, $(\bar{x},\bar{y}\oplus\bar{e}_j)$ belong to D_0 and form a 8-cycle. So, every element of D_0 lies in a cycle of length 8 with elements from D_0.

(iii) For arbitrary i, we use the same construction with the "mixed" addition, the $\mathbb{Z}_4$ addition in the first $2i$ coordinates and the usual addition in the remaining ones. The first cell P_0 of (P_0,P_1) consists of 12 edges, 2 edges of each direction. The edges of the first $2i$ directions correspond to 8-cycles in D_0, while the remaining edges correspond to 4-cycles. Counting the number of cycles is straightforward. □

7.2 [[0, 13], [3, 10]] and OA(1536, 13, 2, 7)

The parameters of orthogonal arrays $\mathrm{OA}(1536,13,2,7)$ lie on the Bierbrauer–Friedman bound (2); hence, such arrays are simple. Moreover, as was observed in [19, 20], any

array on this bound corresponds to an equitable 2-partition with the first coefficient of the quotient matrix being 0. It is straightforward to see that the quotient matrix corresponding to $\mathrm{OA}(1536, 13, 2, 7)$ is $[[0, b], [c, d]] = [[0, 13], [3, 10]]$ (indeed, $0+b = c+d = 13$ and $c : (b+c) = 1536 : 2^{13}$); equitable partitions with this quotient matrix are known to exist [6, Proposition 2] and moreover, the recent classification result [16] says that they are all equivalent. By the argument similar to Remark 27, the "projection" of such a partition gives an equitable partition of Q_{12} with quotient matrix $[[2, 10], [6, 6]]$. It occurs that only 3 (of more than 80) inequivalent equitable partitions with quotient matrix $[[2, 10], [6, 6]]$ are related with $\mathrm{OA}(1536, 13, 2, 7)$ in such a way. Further studying of the exceptional properties of these three partitions can potentially give a tip how to construct other orthogonal arrays attaining bound (2) from equitable partitions. For example, putative $\mathrm{OA}(7 \cdot 2^{20}, 25, 2, 15)$ are equivalent to putative equitable partitions with quotient matrix $[[0, 25], [7, 18]]$ and related to equitable partitions with quotient matrix $[[6, 18], [14, 10]]$, which are known to exist (this matrix is a multiple of $[[3, 9], [7, 5]]$, considered in the current paper); so, one can try to construct $\mathrm{OA}(7 \cdot 2^{20}, 25, 2, 15)$ starting from $2 \times [[3, 9], [7, 5]]$.

Appendix

Below we list all 16 inequivalent equitable partitions (P_0, P_1) with quotient matrix $[[0, 12], [4, 8]]$. The parameters are listed in the following order: rank, i.e., the dimension of the affine span of P_0 (10, 11, or 12); the order of the automorphism group, i.e., of the stabilizer of P_0 in $\mathrm{Aut}(Q_{12})$; the orbit sizes, for P_0, then for P_1; the subspace Ker (the "kernel", given by a basis) and a set Repr (the set of representatives of cosets of the kernel) such that $P_0 = \{k+r | k \in \mathrm{Ker}, r \in \mathrm{Repr}\}$ (the kernel Ker is the maximal subspace for which such decomposition is possible). The binary words of length 12 are represented by hexadecimal numbers, e.g. 0a1 = 0000 1010 0001.

1. Rank: 10, $|\mathrm{Aut}| = 84934656$, orbits: 1024; 3072;
   Ker: ⟨003, 005, 009, 030, 050, 090, 300, 500, 900, 111⟩,
   Repr: {000}.

2. Rank: 11, $|\mathrm{Aut}| = 1179648$, orbits: 1024; 1024, 2048;
   Ker: ⟨300, 500, 900, 111, 222, 444, 888, 00f⟩,
   Repr: {000, 003, 005, 081}.

3. Rank: 11, $|\mathrm{Aut}| = 393216$, orbits: 1024; 1024, 2048;
   Ker: ⟨300, 500, 900, 111, 222, 444, 888, 003⟩,
   Repr: {000, 005, 009, 048}.

4. Rank: 11, $|\mathrm{Aut}| = 147456$, orbits: $2\times128, 768$; $2\times128, 768, 2\times1024$;
   Ker: ⟨300, 500, 900, 111, 222, 444, 888⟩,
   Repr: {000, 003, 005, 006, 00a, 00c, 00f, 018}.

5. Rank: 11, $|\mathrm{Aut}| = 49152$, orbits: 2×512; $2\times6, 3\times512, 1024$;
   Ker: ⟨900, c00, 300, 444, 222, 099⟩,
   Repr: {000, 003, 005, 006, 00a, 00c, 017, 018, 030, 03c, 04b, 050, 0a0, 0c0, 188, 809}.

6. Rank: 11, $|\mathrm{Aut}| = 24576$, orbits: 2×512; $2\times512, 2\times1024$;
   Ker: $\langle$900, 300, 500, 144, 111, 0aa$\rangle$,
   Repr: {000, 003, 005, 006, 00a, 00c, 018, 01e, 027, 030, 060, 081, 096, 0c0, 488, 828}.

7. Rank: 11, $|\mathrm{Aut}| = 196608$, orbits: 2×512; $2\times512, 2048$;
   Ker: $\langle$900, c00, 300, 033, 066, 0cc$\rangle$,
   Repr: {000, 003, 006, 00c, 012, 018, 048, 069, 224, 428, 4e1, 805, 809, 80a, 811, 814}.

8. Rank: 11, $|\mathrm{Aut}| = 9216$, orbits: $64, 3\times192, 384$; $64, 128, 3\times192, 6\times384$;
   Ker: $\langle$900, 300, 500, 144, 4bb$\rangle$,
   Repr: {000, 003, 005, 006, 00a, 00c, 017, 018, 02e, 030, 035, 03c, 04b, 050, 059, 05a,
   060, 069, 072, 081, 09c, 0a0, 0c0, 809, 811, 812, 821, 822, 828, 882, 888, 890}.

9. Rank: 11, $|\mathrm{Aut}| = 24576$, orbits: $2\times256, 512$; $2\times256, 3\times1024$;
   Ker: $\langle$900, 300, 500, 0aa, 055$\rangle$,
   Repr: {000, 003, 005, 006, 00a, 00c, 018, 027, 030, 036, 03c, 060, 06c, 081, 0b1, 0c0,
   166, 2b4, 40f, 809, 811, 812, 814, 821, 822, 824, 828, 82d, 842, 848, 884, 890}.

10. Rank: 11, $|\mathrm{Aut}| = 147456$, orbits: 1024; $256, 768, 2\times1024$;
    Ker: $\langle$900, 300, 500, 847, 1b8$\rangle$,
    Repr: {000, 003, 005, 006, 00c, 018, 01b, 022, 02b, 02d, 030, 035, 048, 059, 05a, 060,
    069, 071, 081, 08b, 090, 0c0, 809, 80a, 811, 812, 814, 821, 824, 850, 882, 884}.

11. Rank: 11, $|\mathrm{Aut}| = 147456$, orbits: $256, 768$; $256, 768, 2048$;
    Ker: $\langle$900, 300, 500, 0aa, 055$\rangle$,
    Repr: {000, 003, 006, 00c, 00f, 012, 018, 021, 030, 036, 039, 048, 060, 081, 084, 0c0,
    1b1, 21e, 2cc, 472, 496, 805, 809, 80a, 811, 814, 822, 824, 828, 82d, 842, 890}.

12. Rank: 11, $|\mathrm{Aut}| = 18432$, orbits: $256, 2\times384$; $2\times256, 2\times384, 2\times768$;
    Ker: $\langle$900, c00, 300, fff$\rangle$,
    Repr: {000, 003, 006, 00c, 00f, 011, 017, 018, 028, 02b, 02d, 030, 035, 036, 03a, 044,
    04b, 04d, 053, 056, 059, 05a, 05c, 060, 063, 066, 06a, 071, 081, 082, 09a, 0c0,
    155, 178, 1b1, 1c6, 247, 2cc, 41b, 46c, 472, 805, 809, 80a, 812, 814, 81d, 81e,
    821, 822, 824, 82e, 841, 842, 848, 850, 884, 888, 88b, 890, 896, 8a0, 8c3, 8d8}.

13. Rank: 11, $|\mathrm{Aut}| = 6144$, orbits: $4\times128, 2\times256$; $4\times64, 6\times128, 8\times256$;
    Ker: $\langle$900, c00, 300, fff$\rangle$,
    Repr: {000, 003, 006, 00c, 00f, 011, 017, 018, 028, 02b, 02d, 030, 035, 036, 03a, 044,
    04b, 04e, 053, 055, 059, 05a, 05c, 060, 063, 069, 072, 081, 082, 099, 09a, 0c0,
    133, 1e4, 247, 256, 26a, 278, 427, 439, 46c, 4c3, 805, 809, 80a, 812, 814, 81d,
    81e, 821, 822, 824, 82e, 841, 842, 848, 84d, 850, 871, 874, 884, 888, 890, 8a0}.

14. Rank: 11, $|\mathrm{Aut}| = 18432$, orbits: $256, 768$; $3\times256, 3\times768$;
    Ker: $\langle$900, c00, 300, fff$\rangle$,
    Repr: {000, 003, 006, 00c, 00f, 011, 018, 01d, 027, 028, 02d, 030, 033, 036, 03a, 044,
    04b, 04e, 053, 055, 056, 059, 05a, 060, 063, 069, 06a, 081, 082, 08b, 09a, 0c0,
    199, 21b, 21e, 22b, 235, 23c, 247, 278, 2a3, 46c, 472, 4b2, 805, 809, 80a, 812,
    814, 817, 821, 822, 824, 82e, 841, 842, 848, 850, 871, 884, 888, 890, 8a0, 8c6}.

15. Rank: 12, $|\mathrm{Aut}| = 32768$, orbits: 1024; 1024, 2048;
Ker: $\langle$111, 222, 444, 888, 003, 840$\rangle$,
Repr: {000, 04c, 009, 005, 054, 090, 030, 060, 051, 066, 06a, 01d, 03a, 036, 02c, 07c}.

16. Rank: 12, $|\mathrm{Aut}| = 49152$, orbits: 1024; 3072;
Ker: $\langle$00f, 0f0, f00, 333$\rangle$,
Repr: {000, 005, 050, 500, 550, 505, 055, 555, 021, 028, 041, 048, 210, 280, 410, 480,
102, 802, 104, 804, 126, 146, 826, 846, 261, 461, 268, 468, 612, 614, 682, 684,
016, 086, 206, 406, 160, 860, 062, 064, 601, 608, 620, 640, 111, 118, 181, 811,
881, 818, 188, 888, 013, 083, 130, 830, 301, 308, 516, 586, 165, 865, 651, 658}.

Acknowledgements

The authors thank Evgeny Bespalov, Vladimir Potapov, and Olli Pottonen for useful discussions and the referees for helpful comments.

References

[1] J. Bierbrauer. Bounds on orthogonal arrays and resilient functions. *J. Comb. Des.*, 3(3):179–183, 1995. doi:10.1002/jcd.3180030304.

[2] P. Boyvalenkov, T. Marinova, and M. Stoyanova. Nonexistence of a few binary orthogonal arrays. *Discrete Appl. Math.*, 217(2):144–150, 2017. doi:10.1016/j.dam.2016.07.023.

[3] D. A. Bulutoglu and K. J. Ryan. Integer programming for classifying orthogonal arrays. *Australas. J. Comb.*, 7(3):362–385, 2018.

[4] C. Carlet. Vectorial Boolean functions for cryptography. In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, volume 134 of *Encycl. Math. Appl.*, chapter 9, pages 398–469. Cambridge Univ. Press, 2010. doi:10.1017/CBO9780511780448.012.

[5] D. G. Fon-Der-Flaass. A bound on correlation immunity. *Sib. Èlektron. Mat. Izv.*, 4:133–135, 2007. Online: http://mi.mathnet.ru/eng/semr149.

[6] D. G. Fon-Der-Flaass. Perfect 2-colorings of a hypercube. *Sib. Math. J.*, 48(4):740–745, 2007. doi:10.1007/s11202-007-0075-4.

[7] D. G. Fon-Der-Flaass. Perfect colorings of the 12-cube that attain the bound on correlation immunity. *Sib. Èlektron. Mat. Izv.*, 4:292–295, 2007. In Russian. English translation: https://arxiv.org/abs/1403.8091.

[8] J. Friedman. On the bit extraction problem. In *Foundations of Computer Science, IEEE Annual Symposium on*, pages 314–319, Los Alamitos, CA, USA, 1992. IEEE Computer Society. doi:10.1109/SFCS.1992.267760.

[9] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays. Theory and Applications*. Springer Series in Statistics. Springer, New York, NY, 1999. doi:10.1007/978-1-4612-1478-6.

[10] P. Kaski and P. R. J. Östergård. *Classification Algorithms for Codes and Designs*, volume 15 of *Algorithms Comput. Math.* Springer, Berlin, 2006. doi:10.1007/3-540-28991-7.

[11] P. Kaski and O. Pottonen. `libexact` User's Guide, Version 1.0. Technical Report 2008-1, Helsinki Institute for Information Technology HIIT, 2008.

[12] A. V. Khalyavin. Estimates of the capacity of orthogonal arrays of large strength. *Mosc. Univ. Math. Bull.*, 65(3):130–131, 2010. doi:10.3103/S0027132210030101.

[13] D. Kirienko. On new infinite family of high order correlation immune unbalanced Boolean functions. In *Proceedings 2002 IEEE International Symposium on Information Theory, Lausanne, Switzerland, June 30 – July 5, 2002*, page 465. IEEE, 2002. doi:10.1109/ISIT.2002.1023737.

[14] D. S. Krotov. On weight distributions of perfect colorings and completely regular codes. *Des. Codes Cryptography*, 61(3):315–329, 2011. doi:10.1007/s10623-010-9479-4.

[15] D. S. Krotov. On $(2n/3-1)$-resilient $(n,2)$-functions. In *IEEE International Symposium on Information Theory, Paris, France, July 7–12, 2019*, pages 2957–2961. IEEE, 2019. doi:10.1109/ISIT.2019.8849584.

[16] D. S. Krotov. On the OA(1536,13,2,7) and related orthogonal arrays. *Discrete Math.*, 343:111659/1–11, 2020. doi:10.1016/j.disc.2019.111659.

[17] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam, Netherlands: North Holland, 1977.

[18] B. D. McKay and A. Piperno. Practical graph isomorphism, II. *J. Symb. Comput.*, 60:94–112, 2014. doi:10.1016/j.jsc.2013.09.003.

[19] V. N. Potapov. On perfect colorings of Boolean n-cube and correlation immune functions with small density. *Sib. Èlektron. Mat. Izv.*, 7:372–382, 2010. In Russian, English abstract. Online: http://mi.mathnet.ru/eng/semr248.

[20] V. N. Potapov. On perfect 2-colorings of the q-ary n-cube. *Discrete Math.*, 312(6):1269–1272, 2012. doi:10.1016/j.disc.2011.12.004.

[21] E. Seiden and R. Zemach. On orthogonal arrays. *Ann. Math. Stat.*, 37(5):1355–1370, 1966. doi:10.1214/aoms/1177699280.

[22] D. R. Stinson. Coverings. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, Discrete Mathematics and Its Applications, pages 275–280. CRC press, Boca Raton, New York, London, Tokio, 1996.

[23] Yu. Tarannikov. On resilient Boolean functions with maximal possible nonlinearity. Cryptology ePrint Archive 2000/005, 2000. https://eprint.iacr.org/2000/005.

[24] Yu. V. Tarannikov. Private communication. June 2018.

[25] A. Yu. Vasil'eva. On reconstructive sets of vertices in the Boolean cube. *J. Appl. Ind. Math.*, 6(3):393–402, 2012. doi:10.1134/S1990478912030155.