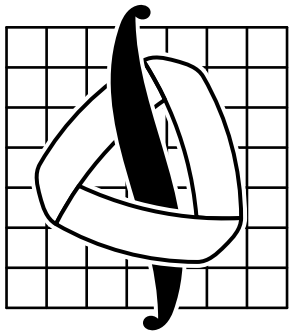
MOSCOW STATE UNIVERSITY M.V. LOMONOSOV



Department of Mechanics and Mathematics

Chair of Discrete Mathematics

Diploma paper on:

On some metrical properties of Boolean functions

Completed by:
student of 510 group
Alexey GRONSKIY

Scientific supervision:
Prof. Alexander UGOL'NIKOV

Moscow, 2011

Contents

Introduction

The significance of metrical properties of Boolean functions in discrete mathematics is approved by their numerous applications in different sub-domains, like coding theory. The notion of ρ-*complete system* of Boolean functions (look the Def. 1.3), investigated in this work, is connected with metrical structure of the space of Boolean functions.

This work is the further development of the research started in V.V. Malykhin's diploma paper ([3]).

The major object — ρ-*complete system* of Boolean functions in the space $[P_2]_{x_1,\ldots,x_n}$, and the connected notion of *distance vector* from the system of Boolean functions to the given Boolean function — are defined in section 1 (see also [3]).

With the introduced notions the following research directions are connected:

1. Investigating the properties of ρ-complete systems and distance vectors.
2. Finding necessary and sufficient conditions of ρ-completeness of the system.
3. Classification of ρ-complete systems according to different factors.
4. Finding the relationship of these objects with other notions of discrete mathematics.

In the section 2 necessary and sufficient conditions of ρ-completeness are described, and the new (against [3]) definitions of *strongly* ρ-*complete* and *weakly* ρ-*complete* systems are given. They play a significant role in the further research.

The section 3 gives the examples of ρ-complete systems and distance vectors, explores their simple properties.

In the section 4 a classifying factor for the set of complete systems is chosen. It is a certain collection of operations on the systems of Boolean functions. In the presence of this collection the set of complete systems breaks up into the equivalence classes, which then are described for the case of $[P_2]_{x_1,x_2}$. In the same section the relation between the notions of strong and week ρ-completeness in $[P_2]_{x_1,x_2}$ is shown.

For the cases $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$ we make an attempt of similar classification. The section 5 is devoted to this.

The relationship of the investigated mathematical objects with other notions of maths is discussed in 6.

Finally, the notes on the possible further research, which are not completed, are placed into the section 7.

1 Definitions and designations

1.1 Designations and abbreviations

The following is used in this work:

$[P_2]_{x_1,\ldots,x_n}$ — the set of Boolean functions, depending on n variables $x_1, \ldots, x_n$ (see also [6])

E, E^k — sets $\{0,1\}$ and $\{0,1\}^k$ correspondingly ($k \geqslant 1$)

$f^{(n)}(\widetilde{x})$ — Boolean function with n arguments

$\mathbb{Z}_+$ — set of non-negative whole numbers

$\widetilde{\alpha}$, $\widetilde{x}$ — ordered sets of elements from E (Boolean vectors)

$\boldsymbol{\gamma}$, $\mathbf{r}$ — vectors

γ_i, r_i — denote i-th coordinates of vectors $\boldsymbol{\gamma}$, $\mathbf{r}$

$\mathfrak{A}$, $\mathfrak{B}$ — finite ordered sets (systems) of Boolean functions

$\mathfrak{A}^*$ — system, which consists of functions which are dual to the functions of $\mathfrak{A}$

$A_{\mathfrak{A}}$, $A_{\mathfrak{B}}$ — matrices of systems $\mathfrak{A}$ and $\mathfrak{B}$ (look p. 6)

$\operatorname{rk} A$ — rank of matrix A

C_n^k — the binomial coefficient

$L^{(n)}$ — the class of linear Boolean functions of n variables (look 1.2)

$T_a^{(n)}$ — class of Boolean functions of n variables preserving the constant a (look 1.2)

$\|\widetilde{\alpha}\|$ — Hamming weight of vector $\widetilde{\alpha}$

$\square$ — end of proof

$\left.\begin{array}{l} A := B \\ B =: A \end{array}\right\}$ — "A is set equal to B by definition"

On standard logical operation ($\oplus$, &, $\vee$ etc.) look [6].

1.2 General notes

Zhegalkin polynomial (ZhP) of n-ary Boolean function $f(x_1, \ldots, x_n)$ is its representation in basis of $\{\&, \oplus, 1\}$:

$$f(x_1, \ldots, x_n) = a \oplus \bigoplus_{\substack{0 \leqslant i_1 < \ldots < i_k \leqslant n \\ 1 \leqslant k \leqslant n}} a_{i_1,\ldots,i_k} x_{i_1} \,\&\, \ldots \,\&\, x_{i_k},$$

where $a, a_{i_1,\ldots,i_k} \in E$.

Let $n \geqslant 1$. *Linear function* of n variables is $f(x_1, \ldots, x_n)$, which has the ZhP of the

following form:

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n,$$

where $a_i \in E$, $0 \leqslant i \leqslant n$.

Let $n \geqslant 1$, $a \in E$. Function of n variables $f(x_1, \ldots, x_n)$ *preserves the constant* a, if this relation is true: $f(a, \ldots, a) = a$.

Let $n \geqslant 1$, $1 \leqslant i \leqslant n$. *Selecting function (selector) of the variable* x_i is such function $e_{x_i}(\widetilde{x}) \in [P_2]_{x_1,\ldots,x_n}$ that for any set $\widetilde{\alpha} \in E^n$ the following relation is true $e_{x_i}(\widetilde{\alpha}) = \alpha_i$.

1.3 Basic definitions

We contemplate n-ary Boolean functions. Let $f, g \in [P_2]_{x_1,\ldots,x_n}$. We introduce the notion of the distance between these functions.

Definition 1.1. We will call the value

$$\rho(f, g) = \sum_{\widetilde{\alpha} \in E^n} (f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha})) \in \mathbb{Z}_+$$

the distance from f to g.

Note that for any f, g the distance $\rho(f, g)$ complies with $0 \leqslant \rho(f, g) \leqslant 2^n$.

For example, in $[P_2]_{x_1,x_2}$ the distance between $f(x_1, x_2) = 1$ and $g(x_1, x_2) = x_1 \oplus x_2$ equals $\rho(f, g) = 1 + 0 + 0 + 1 = 2$.

Having lexicographically ordered all the vectors $\widetilde{\alpha} \in E^n$: $\widetilde{\alpha}_1 = (0, \ldots, 0), \ldots, \widetilde{\alpha}_{2^n} = = (1, \ldots, 1)$, we can introduce the value-vector $\widetilde{\chi}_f$ of function f:

$$\widetilde{\chi}_f = (f(\widetilde{\alpha}_1), \ldots, f(\widetilde{\alpha}_{2^n}))^T$$

We remind, that *Hamming distance* between the Boolean vectors $\widetilde{x}, \widetilde{y} \in E^n$ is

$$d(\widetilde{x}, \widetilde{y}) = \sum_{i=1}^{n} (x_i \oplus y_i) = \|\widetilde{x} \oplus \widetilde{y}\|$$

So, $\rho(f, g)$ is exactly the Hamming distance between $\widetilde{\chi}_f$ and $\widetilde{\chi}_g$.

We naturally spread the introduced notion of the distance into the case of many functions.

Definition 1.2. Let $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$ be a system of k Boolean functions $g_1, \ldots, g_k$, than the vector compounded of distances from f to each of $g_i \in \mathfrak{A}$, will be denoted as

$$\boldsymbol{\rho}(\mathfrak{A}, f) = \big(\rho(g_1, f), \ldots, \rho(g_k, f)\big)^T \in \mathbb{Z}_+^k$$

and called *the distance* from f to system $\mathfrak{A}$.

The following properties are obvious:

1° For all $f, g \in [P_2]_{x_1,\ldots,x_n}$, holds true $\rho(f,g) \geqslant 0$. The equality holds if and only if $f = g$.

2° For all $f, g \in [P_2]_{x_1,\ldots,x_n}$ holds true $\rho(f,g) = \rho(g,f)$.

3° For all $f, g, h \in [P_2]_{x_1,\ldots,x_n}$ holds the triangle inequality:

$$\rho(f,g) + \rho(g,h) \leqslant \rho(f,h)$$

Definition 1.3. System $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$, containing k functions, is called ρ-*complete for the system* $\mathfrak{B} \subset [P_2]_{x_1,\ldots,x_n}$, if there does not exist any pair of non-equal $f_1, f_2 \in \mathfrak{B}$ such that $\boldsymbol{\rho}(\mathfrak{A}, f_1) = \boldsymbol{\rho}(\mathfrak{A}, f_2)$.

Specially, we will call a system ρ-*complete* (without designating the second system), if it is ρ-complete for the whole $[P_2]_{x_1,\ldots,x_n}$.

Note 1.4. In future, if nothing opposite is stated, we will call such systems simply *complete*, omitting ρ.

2 Necessary and sufficient conditions of completeness

In this section the questions of necessary and sufficient conditions of completeness will be discussed.

For the discussion it is useful to introduce the *matrix terminology*.

2.1 Matrix terminology

Assume we are given the system of k Boolean functions: $\mathfrak{A} = \{f_1(\widetilde{x}), \ldots, f_k(\widetilde{x})\} \subset$ $\subset [P_2]_{x_1,\ldots,x_n}$, where $k \geqslant 1$. We order (lexicographically ascending) all the Boolean vectors of n elements: $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_{2^n}$ and observe the matrix $B = (b_{ij})$, such that holds true

$$b_{ij} = f_i(\widetilde{\alpha}_j), \tag{2.1}$$

where $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant 2^n$. We define the mapping $\tau\colon E \to \{-1, 1\}$, which acts like

$$\tau(x) = \begin{cases} -1, & x = 1 \\ 1, & x = 0 \end{cases}$$

Then, for the above-introduced system $\mathfrak{A}$ we define a matrix $A_{\mathfrak{A}}$:

$$A_{\mathfrak{A}} = (a_{ij}),\ 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant 2^n,\ a_{ij} = \boldsymbol{\tau}(b_{ij})$$

We will say that $\mathfrak{A}$ *has a corresponding matrix* $A_{\mathfrak{A}}$ and call $A_{\mathfrak{A}}$ *the matrix of the system* $\mathfrak{A}$.

We will call matrices, whose entries are ± 1, *signed-unit matrices.*

Thus, $A_{\mathfrak{A}}$ is a matrix of size $k \times 2^n$, whose entries are ± 1.

We are going to prove a technical statement, which shows that a distance vector from the system to Boolean function f is the liner function of the value-vector of f.

Statement 2.1. *Following the introduced designators, the next relation holds true:*

$$\boldsymbol{\rho}(\mathfrak{A}, f) = A_{\mathfrak{A}} \cdot \widetilde{\chi}_f + \mathbf{r}_{\mathfrak{A}} \tag{2.2}$$

where the remainder vector $\mathbf{r}_{\mathfrak{A}}$ *depends only on the system* $\mathfrak{A}$ *and is represented as follows:*

$$\mathbf{r}_{\mathfrak{A}} = (I_{k\times 2^n} - A_{\mathfrak{A}}) \begin{pmatrix} 1/2 \\ 1/2 \\ \vdots \\ 1/2 \end{pmatrix},$$

where $I_{k\times 2^n}$ *is a matrix of size* $k \times 2^n$ *with all entries equal to* 1.

Proof. Let $\mathbf{r}_{\mathfrak{A}} = \boldsymbol{\rho}(\mathfrak{A}, f) - A_{\mathfrak{A}} \cdot \widetilde{\chi}_f$. Now we will prove that the vector $\mathbf{r}_{\mathfrak{A}}$ does not depend on f and its i-th entry equals the total number of (-1) entries in i-th row of $A_{\mathfrak{A}}$.

Let $1 \leqslant i \leqslant k$, and f_i be i-th function of $\mathfrak{A}$. Let $\mathbf{A}_i$ be i-th row of the matrix $A_{\mathfrak{A}}$, the entries of $\mathbf{A}_i$ are by definition equal to $\boldsymbol{\tau}(f_i(\widetilde{\alpha}_j))$. Rewriting $(r_{\mathfrak{A}})_i$ in the following representation

$$(r_{\mathfrak{A}})_i = \sum_{1\leqslant j\leqslant 2^n} [f_i(\widetilde{\alpha}_j) \oplus f(\widetilde{\alpha}_j)] - \mathbf{A}_i \cdot \widetilde{\chi}_f = \sum_{1\leqslant j\leqslant 2^n} [f_i(\widetilde{\alpha}_j) \oplus f(\widetilde{\alpha}_j) - \boldsymbol{\tau}(f_i(\widetilde{\alpha}_j)) \cdot f(\widetilde{\alpha}_j)]$$

and trivially checking, that in both cases $f(\widetilde{\alpha}_j) = 0, 1$ j-th term of this sum equals $f_i(\widetilde{\alpha}_j)$, we conclude that $(r_{\mathfrak{A}})_i$ does not depend on f. The sum itself is the total number of vectors $\widetilde{\alpha}$, for which $f_i(\widetilde{\alpha}) = 1$, i.e. the number of (-1) entries in i-th row of $A_{\mathfrak{A}}$.

Let k_+ and k_- be the total numbers of, respectively, $(+1)$ entries and (-1) entries

in i-th row of the $A_{\mathfrak{A}}$ matrix. Solving the system

$$\begin{cases} k_+ + k_- = 2^n \\ k_+ - k_- = \left(A \cdot (1, \ldots, 1)^T\right)_i \end{cases}$$

we obtain

$$(r_{\mathfrak{A}})_i = k_- = \frac{1}{2}(2^n - A \cdot (1, \ldots, 1)^T)_i$$

and hence

$$\mathbf{r}_{\mathfrak{A}} = (I_{k \times 2^n} - A_{\mathfrak{A}}) \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right)^T \qquad \square$$

2.2 Necessary and sufficient condition of ρ-completeness

In work [3] the author gives the most general necessary and sufficient condition of completeness of the system with matrix A. We give it here with the proof.

Statement 2.2. *$\mathfrak{A}$ is complete if and only if there does not exist any vector $\boldsymbol{\gamma} \in \{0, 1, -1\}^{2^n}$, $\boldsymbol{\gamma} \neq \mathbf{0}$, such that*

$$A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = \mathbf{0}$$

Proof. *Sufficiency.* Assume that the system is not complete and we found $f, g \in [P_2]_{x_1,\ldots,x_n}$, $f \neq g$, such that holds true the following:

$$\boldsymbol{\rho}(\mathfrak{A}, f) = \boldsymbol{\rho}(\mathfrak{A}, g)$$

We will show that, the vector $\boldsymbol{\gamma}$ with above-mentioned properties exist, thus coming to a contradiction. Due to the representation (2.2) the following holds true

$$A_{\mathfrak{A}}\widetilde{\chi}_f + \mathbf{r}_{\mathfrak{A}} = A_{\mathfrak{A}}\widetilde{\chi}_g + \mathbf{r}_{\mathfrak{A}},$$

or, in other terms,

$$A_{\mathfrak{A}} \cdot (\widetilde{\chi}_f - \widetilde{\chi}_g) = \mathbf{0}$$

Consequently, letting $\boldsymbol{\gamma} = (\widetilde{\chi}_f - \widetilde{\chi}_g) \neq \mathbf{0}$ (non-zero since the functions are not equal), we get the contradiction.

Necessity. Assume that the system is complete and there exists $\boldsymbol{\gamma} \in \{0, 1, -1\}^{2^n}$, $\boldsymbol{\gamma} \neq \mathbf{0}$ such that holds true the relation $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = \mathbf{0}$.

Since $\gamma_i \in \{0, 1, -1\}$, we can give two vectors $\widetilde{\varphi}, \widetilde{\psi}$ such that $\widetilde{\varphi} - \widetilde{\psi} = \boldsymbol{\gamma}$. The following holds true:

$$A_{\mathfrak{A}} \cdot (\widetilde{\varphi} - \widetilde{\psi}) = \mathbf{0},$$

from which we proceed to the following:

$$A_{\mathfrak{A}}\widetilde{\varphi} + \mathbf{r}_{\mathfrak{A}} = A_{\mathfrak{A}}\widetilde{\psi} + \mathbf{r}_{\mathfrak{A}},$$

which is equivalent to

$$\boldsymbol{\rho}(\mathfrak{A}, f) = \boldsymbol{\rho}(\mathfrak{A}, g),$$

where functions f, g have respectively the value-vectors $\widetilde{\chi}$, $\widetilde{\psi}$, and since $\boldsymbol{\gamma} \neq \mathbf{0}$, the relations $\widetilde{\chi} \neq \widetilde{\psi}$ and $f \neq g$ are true. The obtained contradiction with completeness of the system proves necessity and theorem. □

Definition 2.3. Vector $\boldsymbol{\gamma} \in \{0, 1, -1\}^{2^n}$, $\boldsymbol{\gamma} \neq \mathbf{0}$, for which $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = \mathbf{0}$, is called *eigenvector of the system* $\mathfrak{A}$.

The statement 2.2 leads to the following sufficient condition of completeness:

Corollary 2.4. *If* $\operatorname{rk} A_{\mathfrak{A}} = 2^n$*, then* $\mathfrak{A}$ *is complete.*

The given does not imply that $\operatorname{rk} A_{\mathfrak{A}} < 2^n$ entails incompleteness of $\mathfrak{A}$. So it is worth introducing the notions of minimal, strongly complete and weakly complete functions.

Definition 2.5. Complete system $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$ is called *minimal*, if after deletion of any function from it the system becomes incomplete.

Definition 2.6. System $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$ is called *strongly* ρ*-complete*, if it is minimal and $\operatorname{rk} A_{\mathfrak{A}} = 2^n$. System $\mathfrak{A}$ is called *weakly* ρ*-complete*, if it is ρ-complete, but $\operatorname{rk} A_{\mathfrak{A}} < 2^n$.

Note that the definition of the weak completeness does not require minimality of the system.

It can be easily seen that strongly complete systems should contain 2^n different functions and have square matrix, while weakly complete systems may contain less than 2^n functions.

The question on the more efficient necessary and sufficient conditions is still open. Partially it is solved in theorems 4.9 and 5.5.

3 Some general statements

In this section we will give some statements of general character.

Examples of regularly structured distance vectors are given in 3.1.

The simplest properties of distance vectors are given in 3.2. Note that besides the the interest itself, the statements given in this section play the role of technical ones on which the further discussion is based.

Some properties of complete systems are enumerated in 3.3. These properties will play the role in future, when we choose the classifying operations set for description of complete systems classes in $[P_2]_{x_1,\ldots,x_n}$.

3.1 Examples of distance vectors

Let $\mathfrak{A}_0 = L^{(n)} \cap T_0^{(n)} \subset [P_2]_{x_1,\ldots,x_n}$ be the set of n-ary linear functions which preserve the 0 constant. From the stated in 1.2 we can conclude that the system $\mathfrak{A}_0$ consists exactly of the functions taking the form $a_1x_1 \oplus \ldots a_nx_n,\ a_i \in E$, hence the total number of the functions in $\mathfrak{A}_0$ equals 2^n. The work [3] contains the proof of completeness of $\mathfrak{A}_0$.

Let the functions of the system $\mathfrak{A}_0$ be designated as $g_i,\ 1 \leqslant i \leqslant 2^n$ and the functions $g_1, g_2, \ldots, g_{2^n}$ be ordered as follows: first ordered in groups, ascending by the number of essential variables, and in each group in lexicographical order with respect to $x_1, x_2, \ldots, x_n$ (this can be done, because each of the functions of $\mathfrak{A}_0$, which essentially depends on m variables $x_{i_1}, \ldots, x_{i_m},\ i_k \neq i_l$ with $k \neq l$, has the form $g(x_{i_1}, \ldots, x_{i_m}) = = x_{i_1} \oplus \ldots \oplus x_{i_m}$).

Let $n \geqslant 1$. The following statements are correct.

Statement 3.1. *Let $f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$ be n-ary Boolean function. Then the distance vector from f to the system $\mathfrak{A}_0$ has the form*

$$\boldsymbol{\rho}(\mathfrak{A}_0, f) = (2^{n-1}, \ldots, 2^{n-1}, 0)^T$$

Proof. a) For the function $g_{2^n}(\widetilde{x}) = x_1 \oplus \ldots \oplus x_n,\ g_{2^n} \in \mathfrak{A}_0$ is obvious that the following holds true $\rho(g_{2^n}, f) = 0$.
b) Assume now that the number of the function g_k satisfies the inequality $1 \leqslant k < 2^n$. For every such function $g_k(\widetilde{x}) = x_{i_1} \oplus \ldots \oplus x_{i_m}$ from $\mathfrak{A}_0$, depending on m variables (it is assumed that all $i_1, \ldots, i_m$ are different) the following relation is true

$$\rho(g_k, f) = \sum_{\widetilde{\alpha}} [(\alpha_1 \oplus \ldots \oplus \alpha_n) \oplus g_k(\widetilde{\alpha})] = \sum_{\widetilde{\alpha}} [\alpha_{j_1} \oplus \ldots \oplus \alpha_{j_{n-m}}],$$

where $j_1, \ldots, j_{n-m}$ are numbers of the non-essential variables of g_k. The last sum is number of vectors $\widetilde{\alpha}$ which contain among $\alpha_{j_1}, \ldots, \alpha_{j_{n-m}}$ an odd number of 1-s, i.e.

$$\rho(g_k, f) = 2^m(C_{n-m}^1 + C_{n-m}^3 + \ldots + C_{n-m}^l) = 2^m \cdot 2^{n-m-1} = 2^{n-1}$$

where $l = \max\limits_{2i+1 \leqslant n-m} (2i+1)$. □

Statement 3.2. *Let $f(x_1,\ldots,x_n)=x_1\vee\ldots\vee x_n$ be n-ary Boolean function. Then the distance vector from f to the system $\mathfrak{A}_0$ has the form*

$$\boldsymbol{\rho}(\mathfrak{A}_0,f)=(2^n-1,2^{n-1}-1,\ldots,2^{n-1}-1)^T$$

PROOF. a) For the function $g_1(\widetilde{x})=0,\ g_1\in\mathfrak{A}_0$, it's obvious that the equality $\rho(g_1,f)=2^n-1$ holds true, because in this case $\rho(g_1,f)$ is exactly the total number of non-zero Boolean vectors of the length n

b) Assume now that the number of the function g_k satisfies the inequality $1<k\leqslant 2^n$. For every such function $g_k(\widetilde{x})=x_{i_1}\oplus\ldots\oplus x_{i_m}$ from $\mathfrak{A}_0$, depending on m variables (all the $i_1,\ldots,i_m$ are different) the following holds true

$$\rho(g_k,f)=\sum_{\widetilde{\alpha}}[(\alpha_1\vee\ldots\vee\alpha_n)\oplus g_k(\widetilde{\alpha})]=\sum_{\widetilde{\alpha}\neq\widetilde{0}}[\alpha_{i_1}\oplus\ldots\oplus\alpha_{i_m}\oplus 1],$$

but the last sum is the total number of vectors $\widetilde{\alpha}$, which contain among entries $\alpha_{i_1},\ldots,\alpha_{i_m}$ even number of 1-s. Thus, taking into account that the variables with indices not from the set $\{i_1,\ldots,i_m\}$ do not influent the sum and that the zero vector is considered in (a), we get

$$\rho(g,f)=2^{n-m}\cdot(C_m^0+C_m^2+\ldots+C_m^l)-1=2^{n-1}-1$$

where $l=\max\limits_{2i\leqslant n-m}(2i)$. □

Statement 3.3. *Let $f(x_1,\ldots,x_n)=x_1\,\&\ldots\&\,x_n$ be n-ary Boolean function. Then the distance vector from f to the system $\mathfrak{A}_0$ has the form*

$$\boldsymbol{\rho}(\mathfrak{A}_0,f)=(1,\underbrace{2^{n-1}-1,\ldots,2^{n-1}-1}_{C_n^1},\underbrace{2^{n-1}+1,\ldots,2^{n-1}+1}_{C_n^2},$$
$$\underbrace{2^{n-1}-1,\ldots,2^{n-1}-1}_{C_n^3},\ldots,\underbrace{2^{n-1}+(-1)^n,\ldots,2^{n-1}+(-1)^n}_{C_n^n})^T$$

PROOF. a) For the function $g_1(\widetilde{x})=0$, $g_1\in\mathfrak{A}_0$ it's obvious that $\rho(g_1,f)=1$, because in this case $\rho(g_1,f)$ is exactly the total number of unit vectors of the length n.

b) Assume now that the number of the function g_k satisfies the inequality $1<k\leqslant$ $\leqslant 2^n$. For every such function $g_k(\widetilde{x})=x_{i_1}\oplus\ldots\oplus x_{i_m}$, which depends on m variables (all the $i_1,\ldots,i_m$ are different), the following holds true (here $(m+1)_{(2)}$ designates the

remainder of $(m+1)$ in modulus 2):

$$\rho(g_k, f) = \sum_{\widetilde{\alpha}} [\alpha_1\alpha_2 \ldots \alpha_n \oplus g(\widetilde{\alpha})] = \sum_{\widetilde{\alpha}\neq\widetilde{1}} [\alpha_{i_1} \oplus \ldots \oplus \alpha_{i_m}] + (m+1)_{(2)}$$

Note that the first summand is the number of vectors (except the unit vector), containing an odd number of unit entries among $\alpha_{i_1}, \ldots, \alpha_{i_m}$. Now consider two cases:

1) m is even:

$$\rho(g, f) = 2^{n-m}(C_m^1 + C_m^3 + \ldots + C_m^{m-1}) + 1 = 2^{n-1} + 1$$

2) m is odd:

$$\rho(g, f) = 2^{n-m}(C_m^1 + C_m^3 + \ldots + C_m^{m-2}) + (2^{n-m} - 1)C_m^m + 0 = 2^{n-1} - 1$$

Hereby, vector $\boldsymbol{\rho}(\mathfrak{A}_0, f)$ is compounded of groups, which consist of $(2^{n-1}+1)$ and $(2^{n-1}-1)$, the groups are going by-turn on after another (the exception is the 1st entry $\boldsymbol{\rho}(\mathfrak{A}_0, f)$, which is a "group" consisting of single 1). The length of the m-th group is equal to the total number of m-ary functions in $\mathfrak{A}_0$ which is C_n^m. □

3.2 Properties of distance vectors

In this section we give several statements, which both present a self-interest and play the role of a basis for the further considerations. From here on we observe functions and systems of functions belonging to $[P_2]_{x_1,\ldots,x_n}$.

The relation between $\boldsymbol{\rho}(\mathfrak{A}, f)$ and $\boldsymbol{\rho}(\mathfrak{A}, \bar{f})$ clarifies by the following.

Statement 3.4. *For any functions g, f holds true*

$$\rho(g, f) + \rho(g, \bar{f}) = 2^n \tag{3.1}$$

Proof. The expression

$$\rho(g, f) = \sum_{\widetilde{\alpha}} (f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha})) =: A$$

is the total number of vectors $\widetilde{\alpha}$ for which $f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha}) = 1$, and the expression

$$\rho(g, \bar{f}) = \sum_{\widetilde{\alpha}} (\overline{f(\widetilde{\alpha})} \oplus g(\widetilde{\alpha})) = \sum_{\widetilde{\alpha}} (f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha}) \oplus 1) = \sum_{\widetilde{\alpha}} (\overline{f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha})}) =: B$$

is the total number of vectors $\widetilde{\alpha}$ for which $\overline{f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha})} = 1$ or, in other terms, $f(\widetilde{\alpha}) \oplus$

$\oplus g(\widetilde{\alpha}) = 0$. Hence, $A + B = 2^n$, which was to be proved. □

Corollary 3.5. *For every system $\mathfrak{A}$ and every function f the following relation holds true:*

$$\boldsymbol{\rho}(\mathfrak{A}, f) + \boldsymbol{\rho}(\mathfrak{A}, \bar{f}) = (2^n, \ldots, 2^n)^T \tag{3.2}$$

Proof. Equality (3.1) holds true for each component of $\boldsymbol{\rho}(\mathfrak{A}, f)$, hence the (3.2) holds true, too. □

Statement 3.6. *Let for to systems $\mathfrak{A} = \{g_i\}$, $\mathfrak{B} = \{h_i\}$ of the same size k be satisfied the condition $g_i = \bar{h}_i$, $1 \leqslant i \leqslant k$. Then for arbitrary function f holds true*

$$\boldsymbol{\rho}(\mathfrak{A}, f) + \boldsymbol{\rho}(\mathfrak{B}, f) = (2^n, \ldots, 2^n)^T$$

The proof of 3.6 is similar to the one of the corollary 3.5.

3.3 Properties of systems of functions

Here will be given the statements used in future.

Suppose that $\mathfrak{A} = \{g_1, \ldots, g_k\} \subset [P_2]_{x_1,\ldots,x_n}$. We define $\mathfrak{A}' = \{g_1, \ldots, \bar{g}_i, \ldots, g_k\}$. We will say that the system $\mathfrak{A}'$ is obtained from $\mathfrak{A}$ *by replacing g_i with its negation.* The following statement is correct.

Statement 3.7. *Let $\mathfrak{A}'$ be obtained from $\mathfrak{A}$ by replacing $g_i \in \mathfrak{A}$ with its negation. Then*

1) *If $\mathfrak{A}$ is complete, then $\mathfrak{A}'$ is complete, too.*

2) *If $\mathfrak{A}$ is not complete, then $\mathfrak{A}'$ is not complete, too.*

3) *If $\mathfrak{A}$ is strongly complete, then $\mathfrak{A}'$ is strongly complete, too.*

4) *If $\mathfrak{A}$ is weakly complete, then $\mathfrak{A}'$ is weakly complete, too.*

Proof. 1) Suppose that $\mathfrak{A}$ is complete. We utilize the completeness criterion from the statement 2.2 and assume that $\mathfrak{A}'$ has an eigenvector $\boldsymbol{\gamma}'$. The replacement of $g_i \in \mathfrak{A}$ with $\bar{g}_i$ corresponds to multipilcation of the i-th row in matrix $A_{\mathfrak{A}}$ by (-1). Taking into account this relation between $A_{\mathfrak{A}}$ and $A_{\mathfrak{A}'}$ we easily see that $A_{\mathfrak{A}'} \cdot \boldsymbol{\gamma}' = \mathbf{0}$ implies $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma}' = \mathbf{0}$, so the eigenvector of $\mathfrak{A}'$ is at the same time the eigenvector of the initial system$\mathfrak{A}$. We get the contradiction with the completeness of $\mathfrak{A}$.

2) Suppose that $\mathfrak{A}$ is not complete, while the obtained system $\mathfrak{A}'$ is complete. Then, according to item 1), the system $\mathfrak{A}''$, obtained from $\mathfrak{A}'$ by replacing the i-th function with its negation is complete. But since $\bar{\bar{g}}_i = g_i$ we get that $\mathfrak{A}'' = \mathfrak{A}$, and the contradiction.

3) Replacement of $g_i \in \mathfrak{A}$ with $\bar{g}_i$ corresponds to multiplication of the i-th row in $A_{\mathfrak{A}}$ by (-1). Obviously, this operation does not change the rank of the matrix, hence, $\mathfrak{A}'$ is strongly complete, too.

4) Analogically to item 3). □

Suppose next that $\mathfrak{A} = \{g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n)\} \subset [P_2]_{x_1,\ldots,x_n}$. We define $\mathfrak{A}' = \{g_1(x_1, \ldots, \bar{x}_i, \ldots, x_n), \ldots, g_k(x_1, \ldots, \bar{x}_i, \ldots, x_n)\}$. We will say that the system $\mathfrak{A}'$ is obtained from $\mathfrak{A}$ *by replacing variable* x_i *with its negation*. The following holds true.

Statement 3.8. *Let* $\mathfrak{A}'$ *be obtained from* $\mathfrak{A}$ *by replacing* x_i *with its negation. Then*

1) *If* $\mathfrak{A}$ *is complete, then* $\mathfrak{A}'$ *is complete, too.*

2) *If* $\mathfrak{A}$ *is not complete, then* $\mathfrak{A}'$ *is not complete, too.*

3) *If* $\mathfrak{A}$ *is strongly complete, then* $\mathfrak{A}'$ *is strongly complete, too.*

4) *If* $\mathfrak{A}$ *is weakly complete, then* $\mathfrak{A}'$ *is weakly complete, too.*

Proof. From the definition of $A_{\mathfrak{A}}$ follows that the considered operation of replacement of the variable with its negation corresponds to a certain permutation σ of columns of the matrix.

1) Suppose that $\mathfrak{A}$ is complete. Assume that the system $\mathfrak{A}'$ has the eigenvector $\boldsymbol{\gamma}'$. We consider vector $\boldsymbol{\gamma} = \sigma^{-1}(\boldsymbol{\gamma}')$ where application of the permutation to a vector means the permutation of its components. Then, obviously, $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = \mathbf{0}$, i.e. γ is the eigenvector of $\mathfrak{A}$, that means, $\mathfrak{A}$ is not complete. We got the contradiction.

2) Suppose that $\mathfrak{A}$ is not complete, while the obtained system $\mathfrak{A}'$ is complete. Than the system $\mathfrak{A}''$, obtained from $\mathfrak{A}'$ be means of the same operation, is complete, according what is proven in item 1). But since $\bar{\bar{x}}_i = x_i$ we get that $\mathfrak{A}'' = \mathfrak{A}$, and the contradiction.

3) The permutation of the columns of the matrix $A_{\mathfrak{A}}$ does not change the rank of this matrix. Hence, $\mathfrak{A}'$ is strongly complete.

4) Analogically to item 3). □

An easy consequence of statements 3.7, 3.8 is the following one.

Corollary 3.9. *A system* $\mathfrak{A}$ *is complete if and only if the dual system* $\mathfrak{A}^*$ *is complete.*

Suppose next that $\mathfrak{A} = \{g_1, \ldots, g_k\} \subset [P_2]_{x_1,\ldots,x_n}$ and we are given a function $f \in \in [P_2]_{x_1,\ldots,x_n}$. We define $\mathfrak{A}' = \{g_1 \oplus f, \ldots, g_k \oplus f\}$. We will say that the system $\mathfrak{A}'$ is obtained from the system $\mathfrak{A}$ *by addition of* f *modulo* 2. The following statement is correct.

Statement 3.10. *Let* $\mathfrak{A}'$ *be obtained from* $\mathfrak{A}$ *by addition of* f *modulo* 2. *Then*

1) *If* $\mathfrak{A}$ *is complete, then* $\mathfrak{A}'$ *is complete, too.*

2) *If* $\mathfrak{A}$ *is not complete, then* $\mathfrak{A}'$ *is not complete, too.*

3) *If* $\mathfrak{A}$ *is strongly complete, then* $\mathfrak{A}'$ *is strongly complete, too.*

4) *If* $\mathfrak{A}$ *is weakly complete, then* $\mathfrak{A}'$ *is weakly complete, too.*

PROOF. The operation is equivalent to the addition modulo 2 of the vector $\widetilde{\chi}_f$ to each of the vectors $\widetilde{\chi}_{g_k}$, $g_k \in \mathfrak{A}$. This, by-turn, is equivalent to component-wise multiplication of each row of $A_{\mathfrak{A}}$ by vector $\mathbf{v} = \tau(\widetilde{\chi}_f)$, or, in other words, multiplication by (-1) of those matrix columns which have indices from a certain set of indices $J = \{j\colon v_j = -1\}$.

1) Suppose that $\mathfrak{A}$ is complete. Assume that the system $\mathfrak{A}'$ has the eigenvector $\boldsymbol{\gamma}'$. We consider a vector $\boldsymbol{\gamma}$ with components $\gamma_i = v_i \cdot \gamma'_i$. Then $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = A_{\mathfrak{A}'} \cdot \boldsymbol{\gamma}' = \mathbf{0}$, i.e. $\mathfrak{A}$ is not complete. We got a contradiction.

2) Suppose that $\mathfrak{A}$ is not complete, while the obtained system $\mathfrak{A}'$ is complete. Than the system $\mathfrak{A}''$, obtained from $\mathfrak{A}'$ be means of the same operation, is complete, according what is proven in item 1). But since for every function $g_i \in \mathfrak{A}$ holds true $g_i \oplus f \oplus f = g_i$, then $\mathfrak{A}'' = \mathfrak{A}$ and we get a contradiction.

3) According to the note above, the considered operation is the multiplication of certain columns of $A_{\mathfrak{A}}$ by (-1), which does not change the rank of the matrix. Hence, $\mathfrak{A}'$ is strongly complete.

4) Analogically to item 3). □

Suppose next that

$$\mathfrak{A} = \{g_1(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n)\} \subset [P_2]_{x_1,\ldots,x_n}$$

We define

$$\mathfrak{A}' = \{g_1(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n)\}$$

(i.e. among the arguments of the functions of the system variables x_i and x_j are replaced with each other). We will say that the system $\mathfrak{A}'$ is obtained from $\mathfrak{A}$ *by transposition of variables* x_i and x_j. The following statement is correct.

Statement 3.11. *Let* $\mathfrak{A}'$ *be obtained from* $\mathfrak{A}$ *by transposition of variables* x_i *and* x_j. *Then*

1) *If* $\mathfrak{A}$ *is complete, then* $\mathfrak{A}'$ *is complete, too.*

2) *If* $\mathfrak{A}$ *is not complete, then* $\mathfrak{A}'$ *is not complete, too.*

3) *If* $\mathfrak{A}$ *is strongly complete, then* $\mathfrak{A}'$ *is strongly complete, too.*

4) *If* $\mathfrak{A}$ *is weakly complete, then* $\mathfrak{A}'$ *is weakly complete, too.*

PROOF. From the definition of $A_{\mathfrak{A}}$ follows that the considered operation of replacement of the variable with its negation corresponds to a certain permutation σ of

columns of the matrix.

The further proof is similar to the proof of the statement 3.8. □

Suppose next that $\mathfrak{A} = \{g_1, \ldots, g_i, \ldots, g_j, \ldots, g_k\} \subset [P_2]_{x_1,\ldots,x_n}$. We define $\mathfrak{A}' = \{g_1, \ldots, g_j, \ldots, g_i, \ldots, g_k\}$ (where functions g_i and g_j are replaced with each other). We will say that the system $\mathfrak{A}'$ is obtained from $\mathfrak{A}$ *by transposition of variables* g_i and g_j. We will call a sequence of transpositions a *permutation of functions.* the following statement is true.

Statement 3.12. *Let* $\mathfrak{A}'$ *be obtained from* $\mathfrak{A}$ *by permutation of functions. Then* 1) *If* $\mathfrak{A}$ *is complete, then* $\mathfrak{A}'$ *is complete, too.*

2) *If* $\mathfrak{A}$ *is not complete, then* $\mathfrak{A}'$ *is not complete, too.*

3) *If* $\mathfrak{A}$ *is strongly complete, then* $\mathfrak{A}'$ *is strongly complete, too.*

4) *If* $\mathfrak{A}$ *is weakly complete, then* $\mathfrak{A}'$ *is weakly complete, too.*

Proof. We note that the operation permutation of functions corresponds to permutation of rows of matrix $A_{\mathfrak{A}}$. Further proof of all the four items is obvious. □

4 Structure of the set of complete systems in $[P_2]_{x_1,x_2}$

In this section we define the classifying collection of operations and perform the classification of complete systems of Boolean functions of two variables.

Definition 4.1. We define a set of operations $\mathscr{F} = \{\mathrm{F}, \mathrm{V}, \mathrm{S}, \mathrm{T}, \mathrm{P}\}$ on the system $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$ in the following way (on the basis of notions given in 3.3):

1. Replacement of function $g \in \mathfrak{A}$ with its negation $\bar{g}$. Designation of the operation: $\mathrm{F}_g(\mathfrak{A})$.

2. Replacement of the variable x_i with its negation $\bar{x}_i$. Designation of the operation: $\mathrm{V}_{x_i}(\mathfrak{A})$.

3. Addition modulo 2 of the function f to each of the functions of the system $\mathfrak{A}$. Designation of the operation: $\mathrm{S}_f(\mathfrak{A})$ or, for the sake of shortness, $\mathfrak{A} \oplus f$.

4. Transposition of variables x_i and x_j. Designation of the operation: $\mathrm{T}_{x_i,x_j}(\mathfrak{A})$.

5. Permutation σ of functions in the system $\mathfrak{A}$. Designation of the operation $\mathrm{P}_\sigma(\mathfrak{A})$.

We call the systems $\mathfrak{A}$ and $\mathfrak{B}$ *similar* (designation $\mathfrak{A} \sim \mathfrak{B}$), if $\mathfrak{B}$ can be obtained from $\mathfrak{A}$ by means of finite sequence of operations from $\mathscr{F}$. Note that the introduced relation is reflexive (obvious), symmetric (because if $\mathfrak{B}$ can be obtained from $\mathfrak{A}$ by means of finite sequence of operations from $\mathscr{F}$, then $\mathfrak{A}$ can be obtained from $\mathfrak{B}$ by

means of finite sequence of inverse operations), and transitive (obvious). Thus, the introduced relation satisfies the definition of the equivalence relation. So we will also use the notion of *equivalent* systems as a synonym.

Statement 4.2. *Each of two sets - strongly complete systems and weakly complete systems - is partitioned into classes of equivalence by the equivalence relation.*

Proof. According to the proven in 3.3, operations from $\mathscr{F}$ preserve strong and weak completeness of system. □

For the sake of convenience we rename the variables: $x := x_1, y := x_2$.

4.1 Theorem of classification of strongly complete systems in $[P_2]_{x_1,x_2}$

We consider strongly complete systems in $[P_2]_{x_1,x_2}$. These systems have square matrices of the order $2^2 = 4$ (look p. **??**) and contain 4 functions.

One of the main results of this work is the following theorem.

Theorem 4.3. *The set of the strongly complete systems in $[P_2]_{x_1,x_2}$ is partitioned by the relation $\sim$ into four equivalence classes B_1, B_2, B_3, B_4, where*

$$B_1 = \Big[\{0, x, y, xy\}\Big]_{\mathscr{F}}, \qquad B_2 = \Big[\{0, x, y, x \oplus y\}\Big]_{\mathscr{F}},$$
$$B_3 = \Big[\{0, x, xy, y \oplus xy\}\Big]_{\mathscr{F}}, \qquad B_4 = \Big[\{0, x, xy, x \oplus y \oplus xy\}\Big]_{\mathscr{F}}$$

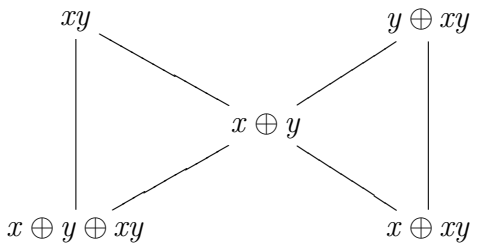
Lemma 4.4. *Let $\mathfrak{A} \subset [P_2]_{x_1,x_2}$ be strongly complete system, $\mathfrak{A} = \{f_1, f_2, f_3, f_4\}$, where $f_1 = 0$ and $f_i \in T_0$, $i = 2, 3, 4$. Then there exist a pair of numbers $i \neq j$, $1 \leqslant i, j \leqslant 4$ such that one of the following equalities holds true*

$$f_i = x \oplus f_j, \quad \text{or} \quad f_i = y \oplus f_j. \tag{4.1}$$

For the sake of convenience we introduce these designators for selecting functions: $e_{x_1} = x$, $e_{x_2} = y$.

Proof. In case when selecting functions exist among f_2, f_3, f_4, lemma is correct, since the zero-function belongs to the system $\mathfrak{A}$.

Next we assume that $\mathfrak{A}$ does not contain selective functions. Suppose that there are no pairs possessing the property (4.1). For the sake of clearness, on the graph we show pairs of functions of x, y preserving 0 and not having the property (4.1):



It is seen that we have two triples of functions, among which there are no pairs with (4.1) property: $\{xy, x \oplus y, x \oplus y \oplus xy\}$ and $\{y \oplus xy, x \oplus xy, x \oplus y\}$. In the first case the matrix of the system is singular (arrow shows linear transformations of rows of the matrix):

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -2 \\ 0 & -2 & -2 & 0 \\ 0 & -2 & -2 & -2 \end{pmatrix}$$

In the second case, similarly:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & -2 & -2 & 0 \end{pmatrix}$$

So in both cases the system is not complete. The obtained contradiction proves the lemma. □

The following statement is correct.

Lemma 4.5. *Let $\mathfrak{A} \subset [P_2]_{x_1,x_2}$ be a strongly complete system. Then $\mathfrak{A}$ belongs to one of four sets:*

$$\begin{aligned} B_1 &= \Big[\{0, x, y, xy\}\Big]_{\mathscr{F}} & B_2 &= \Big[\{0, x, y, x \oplus y\}\Big]_{\mathscr{F}} \\ B_3 &= \Big[\{0, x, xy, y \oplus xy\}\Big]_{\mathscr{F}} & B_4 &= \Big[\{0, x, xy, x \oplus y \oplus xy\}\Big]_{\mathscr{F}} \end{aligned} \tag{4.2}$$

For simplicity of the further calculations we make an agreement: anywhere we use one of the operations $\mathrm{F}, \mathrm{V}, \mathrm{S}, \mathrm{T}$ we will implicitly add the operation P. Hereby, we will perform all further transformations of the systems without explicit mention of permutation of functions.

Proof. *Step 1.* Utilizing operations F and S we can transform the system to another one $\mathfrak{A}_1$, which satisfies the conditions of lemma 4.4. The system $\mathfrak{A}_1$ has the

matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & & & \\ 1 & & * & \\ 1 & & & \end{pmatrix}$$

Step 2. From lemma 4.4 follows that among the last three functions of the system we can find a function of a form $(x \oplus g, g)$ or $(y \oplus g, g)$. If the second case holds, we proceed to the first case by the operation of transposition of variables. We will denote the resulting system as $\mathfrak{A}_2$.

Step 3. By means of the operation S_g (where g is the one from Step 2) we obtain a system $\mathfrak{A}_3 = \{0, x, *, *\}$ with matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & & * & \\ 1 & & & \end{pmatrix}$$

From the non-singularity of the matrix follows that among the rest two rows should be the one with (-1) int the second column. Such a row corresponds to some function, which takes the value 1 on the vector $(x, y) = (0, 1)$: possible variants are y, $x \oplus y$, $y \oplus xy$, $x \oplus y \oplus xy$.

Next we consider sub-cases:

1) The system contains function y: then the matrix of the system has the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & * & * & * \end{pmatrix}$$

taking the non-singularity of the matrix into account, we see that the last row can have one of the forms:

$\tau(\widetilde{\chi}_f)$	$f(x, y)$
$(1, 1, 1, -1)$	xy
$(1, -1, -1, 1)$	$x \oplus y$
$(1, 1, -1, 1)$	$x \oplus xy$
$(1, -1, 1, 1)$	$y \oplus xy$
$(1, -1, -1, -1)$	$x \oplus y \oplus xy$

1.1) Let the last row have the form $(1, 1, 1, -1)$. It corresponds to a function xy,

and the system $\{0, x, y, xy\}$ belongs to B_1.

1.2) Let the last row have the form $(1, -1, -1, 1)$. It corresponds to a function $x \oplus y$, and the system $\{0, x, y, x \oplus y\}$ belongs to B_2.

1.3) Let the last row have the form $(1, 1, -1, 1)$. It corresponds to a function $x \oplus xy$. We next perform a chain of transformations

$$\{0, x, y, x \oplus xy\} \xrightarrow{\mathrm{V}_y} \{0, x, \bar{y}, xy\} \xrightarrow{\mathrm{F}_y} \{0, x, y, xy\},$$

from which follows that the initial system belongs to B_1.

1.4) Let the last row have the form $(1, -1, 1, 1)$. It corresponds to a function $y \oplus xy$. We next perform the operation $\mathrm{T}_{x,y}$ and reduce to the case 1.3). Hence the system belongs to B_1.

1.5) Let the last row have the form $(1, -1, -1, -1)$. It corresponds to a function $x \oplus y \oplus xy$. We next perform a chain of transformations

$$\begin{aligned}\{0, x, y, x \oplus y \oplus xy\} \xrightarrow{\mathrm{F}_{x\oplus y\oplus xy}} \{0, x, y, x \oplus y \oplus xy \oplus 1\} = \\ = \{0, x, y, \bar{x}\,\bar{y}\} \xrightarrow{\mathrm{F}_x} \{0, \bar{x}, y, \bar{x}\,\bar{y}\} \xrightarrow{\mathrm{F}_y} \\ \xrightarrow{\mathrm{F}_y} \{0, \bar{x}, \bar{y}, \bar{x}\,\bar{y}\} \xrightarrow{\mathrm{V}_x, \mathrm{V}_y} \{0, x, y, xy\},\end{aligned}$$

and reduce to the case 1.3). Hence the system belongs to B_1.

2) The system contains function $x \oplus y$: then the matrix of the system has the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & * & * & * \end{pmatrix}$$

taking the non-singularity of the matrix into account, we see that the last row can have one of the forms:

$\tau(\widetilde{\chi}_f)$	$f(x, y)$
$(1, -1, 1, -1)$	y
$(1, 1, -1, 1)$	$x \oplus xy$
$(1, -1, 1, 1)$	$y \oplus xy$
$(1, 1, 1, -1)$	xy
$(1, -1, -1, -1)$	$x \oplus y \oplus xy$

2.1) Let the last row have the form $(1, -1, 1, -1)$. It corresponds to a function y, this case has already been considered in 1.2)

2.2) Let the last row have the form $(1, 1, -1, 1)$. It corresponds to a function $x \oplus xy$.

We next perform a chain of transformations

$$\{0, x, x \oplus y, x \oplus xy\} \xrightarrow{\mathrm{S}_x} \{0, x, y, xy\},$$

hence the system belongs to B_1.

2.3) Let the last row have the form $(1, -1, 1, 1)$. It corresponds to a function $y \oplus xy$. We next perform a chain of transformations

$$\{0, x, x \oplus y, y \oplus xy\} \xrightarrow{\mathrm{S}_x} \{0, x, y, x \oplus y \oplus xy\}$$

thus reducing this case to 1.5).

2.4) Let the last row have the form $(1, 1, 1, -1)$. It corresponds to a function xy. We next perform a chain of transformations

$$\{0, x, x \oplus y, xy\} \xrightarrow{\mathrm{S}_x} \{0, x, y, x \oplus xy\}$$

thus reducing this case to 1.3).

2.5) Let the last row have the form $(1, -1, -1, -1)$. It corresponds to a function $x \oplus y \oplus xy$. We next perform a chain of transformations

$$\{0, x, x \oplus y, x \oplus y \oplus xy\} \xrightarrow{\mathrm{S}_x} \{0, x, y, y \oplus xy\}$$

thus reducing this case to 1.4).

3) The system contains function $y \oplus xy$: then the matrix of the system has the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & * & * & * \end{pmatrix}$$

taking the non-singularity of the matrix into account, we see that the last row can have one of the forms:

$\tau(\widetilde{\chi}_f)$	$f(x, y)$
$(1, -1, 1, -1)$	y
$(1, -1, -1, 1)$	$x \oplus y$
$(1, 1, -1, 1)$	$x \oplus xy$
$(1, 1, 1, -1)$	xy

3.1) Let the last row have the form $(1, -1, 1, -1)$. It corresponds to a function y, this case has already been considered in 1.4).

3.2) Let the last row have the form $(1,-1,-1,1)$. It corresponds to a function $x \oplus y$, this case has already been considered in 2.3).

3.3) Let the last row have the form $(1,1,-1,1)$. It corresponds to a function $x \oplus xy$. We next perform a chain of transformations

$$\{0, x, y \oplus xy, x \oplus xy\} \xrightarrow{\mathrm{S}_x} \{0, x, xy, x \oplus y \oplus xy\},$$

hence the system belongs to B_4.

3.4) Let the last row have the form $(1,1,1,-1)$. It corresponds to a function xy. In this case the system belongs to B_3.

4) The system contains function $x \oplus y \oplus xy$: then the matrix of the system has the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \\ 1 & * & * & * \end{pmatrix}$$

taking the non-singularity of the matrix into account, we see that the last row can have one of the forms:

$\tau(\widetilde{\chi}_f)$	$f(x,y)$
$(1,-1,1,-1)$	y
$(1,-1,-1,1)$	$x \oplus y$
$(1,1,-1,1)$	$x \oplus xy$
$(1,1,1,-1)$	xy

4.1) Let the last row have the form $(1,-1,1,-1)$. It corresponds to a function y, this case has already been considered in 1.5).

4.2) Let the last row have the form $(1,-1,-1,1)$. It corresponds to a function $x \oplus y$, this case has already been considered in 2.5).

4.3) Let the last row have the form $(1,1,-1,1)$. It corresponds to a function $x \oplus xy$. We next perform a chain of transformations

$$\{0, x, x \oplus y \oplus xy, x \oplus xy\} \xrightarrow{\mathrm{S}_x} \{0, x, xy, y \oplus xy\}$$

hence the system belongs to B_3.

4.4) Let the last row have the form $(1,1,1,-1)$. It corresponds to a function xy. In this case the system belongs to B_4.

All the possible cases have been examined, the lemma is proven. □

The following fact holds true.

Lemma 4.6. *The sets B_1, B_2 and $C = B_3 \cup B_4$ are mutually nonintersecting.*

PROOF. Let $\varkappa_1(\mathfrak{A}) := \min(s, 2^n - s)$, where s is the total number of logical conjunctions of order n (max. possible) in all the Zhegalkin polynomials of the functions from $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$, taken together. For instance, for the system $\mathfrak{A} = \{x, xy, x \oplus xy, y \oplus \oplus xy\} \subset [P_2]_{x_1,x_2}$ we obtain $\varkappa_1(\mathfrak{A}) = \min(3, 1) = 1$.

We next show that $\varkappa_1(\mathfrak{A})$ is an invariant of the sets B_1, B_2, C with respect to operations from $\mathscr{F}$.

Consider the operations:

a) F_f is the addition of a unit (modulo 2) to $f \in \mathfrak{A}$, and thus does not change the total number of above-mentioned conjunctions in Zhegalkin polynomials and thus preserves $\varkappa_1(\mathfrak{A})$.

b) V_{x_i} is the replacement of all the entries of x_i with $(x_i \oplus 1)$. Apparently, this does not change the total number of conjunctions of maximal order in Zhegalkin polynomial (here we essentially utilize the maximality of the order) and thus preserves $\varkappa_1(\mathfrak{A})$.

c) S_g may change the total number of above-mentioned conjunctions in the only one case: if g contains such conjunction in its Zhegalkin polynomial. But in this case, if the total number of such conjunctions in all Zhegalkin polynomials was equal to s then in new system there will be $(2^n - s)$ such conjunctions (since $\mathfrak{A}$ contains 2^n functions), so $\varkappa_1(\mathfrak{A}) = \varkappa_1(\mathfrak{A}')$.

d) T_{x_i,x_j}, apparently, does not change the total number of such conjunctions in Zhegalkin polynomials and thus preserves $\varkappa_1(\mathfrak{A})$.

e) P_σ, apparently, does not change the total number of such conjunctions in Zhegalkin polynomials and thus preserves $\varkappa_1(\mathfrak{A})$.

For the case $\mathfrak{A} \subset [P_2]_{x_1,x_2}$ the number $\varkappa_1(\mathfrak{A})$ can take the values of $0, 1, 2$. We are left to note that

$$\varkappa_1(\mathfrak{A}) = 1 \text{ if } \mathfrak{A} \in B_1, \quad \varkappa_1(\mathfrak{A}) = 0 \text{ if } \mathfrak{A} \in B_2, \quad \varkappa_1(\mathfrak{A}) = 2 \text{ if } \mathfrak{A} \in C,$$

which proves the lemma. □

Note 4.7. From the proof it follows that the total number of logical conjunctions xy in Zhegalkin polynomials for the systems from B_3 and B_4 always equals 2.

We next prove the following statement.

Lemma 4.8. $B_3 \cap B_4 = \varnothing$.

PROOF. We consider the Zhegalkin polynomials of the function of the system $\mathfrak{A} \subset \subset [P_2]_{x_1,x_2}$. Let p be the total number of entries of variable symbols into formulae of

Zhegalkin polynomials of the functions of $\mathfrak{A}$. We define $\varkappa_2(\mathfrak{A})$ as evenness of p:

$$\varkappa_2(\mathfrak{A}) = \begin{cases} 1, & \text{if } p \text{ is odd} \\ 0, & \text{if } p \text{ is even} \end{cases}$$

We next prove that for the sets B_3 and B_4 this value is invariant with respect to the operations from $\mathscr{F}$.

Consider the possible cases:

a) F_f is the addition of a unit (modulo 2) to $f \in \mathfrak{A}$ and thus does not change the number of entries of variable symbols.

b) V_{x_i} is the replacement of all the entries of x_i with $(x_i \oplus 1)$. Without loss of generality we let $x_i = x$. Number of entries of variable x in Zhegalkin polynomials does not change after the operation. Number of entries of variable y in Zhegalkin polynomials changes only at the expense of transformations of xy into $(x \oplus 1)y = xy \oplus \oplus y$. According to the note 4.7 the number of xy is even, hence the number of entries of variable y changes by an even value, so $\varkappa_2(\mathfrak{A}) = \varkappa_2(\mathscr{F}_{x_i}(\mathfrak{A}))$.

c) S_g changes the number of entries of all variables by an even value, because there are four functions in $\mathfrak{A} \subset [P_2]_{x_1,x_2}$.

d) T_{x_i,x_j}, by definition preserves $\varkappa_2(\mathfrak{A})$.

e) P_σ, by definition preserves $\varkappa_2(\mathfrak{A})$.

For finishing the proof we are left to note that

$$\varkappa_2(\mathfrak{A}) = 0 \text{ with } \mathfrak{A} \in B_3, \quad \varkappa_2(\mathfrak{A}) = 1 \text{ with } \mathfrak{A} \in B_4 \qquad \square$$

Proof (Of theorem 4.3). The statements of lemmas 4.5, 4.6, 4.8 prove the theorem 4.3. $\square$

4.2 Equivalence of the notions of completeness and strong completeness in $[P_2]_{x_1,x_2}$

The question of relation between the notions of completeness and strong completeness $[P_2]_{x_1,x_2}$ is answered by the following theorem.

Theorem 4.9. *Let $\mathfrak{A} \subset [P_2]_{x_1,x_2}$. The system $\mathfrak{A}$ is complete if and only if $\mathfrak{A}$ is strongly complete.*

In other words, this means that in $[P_2]_{x_1,x_2}$ *there are no weakly complete systems.* This fact is quite remarkable as to some extent it isolates the case $n = 2$ for $[P_2]_{x_1,\ldots,x_n}$.

Proof. *Sufficiency.* Obvious.

Necessity. Utilizing the operations from $\mathscr{F}$ we can transform (without changing the type of completeness) the given system $\mathfrak{A}$ to the equivalent one $\mathfrak{A}_1$ with the matrix:

$$A_{\mathfrak{A}_1} = A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & * & * & * \\ \vdots & & & \vdots \\ 1 & * & * & * \end{pmatrix}$$

We have to check that if $\mathfrak{A}$ is not strongly complete (the matrix A is singular), then $\mathfrak{A}$ is not complete, i.e. it has an eigenvector $\boldsymbol{\gamma}$:

$$A \cdot \boldsymbol{\gamma} = \mathbf{0} \tag{4.3}$$

We next will perform linear transformations on the rows of the matrix and find the searched vector $\boldsymbol{\gamma}$ utilizing the fact that if a matrix M' is obtained from M by linear transformations on the rows and if $M' \cdot \boldsymbol{\gamma} = 0$, then $M \cdot \boldsymbol{\gamma} = 0$, too.

We will, possibly, permutate the columns of the matrix, implicitly supposing that the entries of the searched vector are permutated respectively.

Since the rank of a singular matrix in our case cannot exceed 3, the following cases are possible:

1) $\operatorname{rk} A = 1$: in this case all the rows of the matrix can be linearly expressed through the first one. Vector $\boldsymbol{\gamma} = (1, 1, -1, -1)^T$, obviously, satisfies (4.3).

2) $\operatorname{rk} A = 2$: subtracting the first row from each of the others (and, possibly, permutating the columns) we reduce the matrix of the system (4.3) to the form

$$A' = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & \alpha_1 & \alpha_2 \\ 0 & -2 & \alpha_1 & \alpha_2 \\ 0 & -2 & \alpha_1 & \alpha_2 \end{pmatrix}$$

where $\alpha_i \in \{-2, 0\}$. It is easy to see that depending on the value of α_1 either $\boldsymbol{\gamma} = (0, 1, -1, 0)^T$ or $\boldsymbol{\gamma} = (1, 0, -1, 0)^T$ satisfy (4.3).

3) $\operatorname{rk} A = 3$: subtracting the first row from each of the others, then, possibly, permutating the rows and columns, then subtracting the second row from the rows below

it we can get the following matrices

$$A'_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & \alpha_1 & \alpha_2 \\ 0 & 0 & 0 & \pm 2 \\ & & 0 & \end{pmatrix} \qquad A'_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & \alpha_1 & \alpha_2 \\ 0 & 0 & \beta_1 & \beta_2 \\ & & 0 & \end{pmatrix} \qquad A'_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & -2 & \alpha_1 \\ 0 & 0 & 0 & \pm 2 \\ & & 0 & \end{pmatrix}$$

where $\alpha_i \in \{-2, 0\}$, $\beta_i \in \{2, -2, 0\}$.

In case of matrix A'_1 depending on the value of α_1 either $\boldsymbol{\gamma} = (0, 1, -1, 0)^T$ or $\boldsymbol{\gamma} = = (1, 0, -1, 0)^T$ satisfy (4.3).

In case of matrix A'_2: if only single of β_i is zero, then we get the case similar to A'_1.

Let both β_i be non-zero of the same sign. In such case if $\alpha_1 = \alpha_2$, then vector $\boldsymbol{\gamma} = = (0, 0, 1, -1)^T$ satisfies (4.3). If $\alpha_1 \neq \alpha_2$, then one of α_i (without loss of generality, let it be α_1) equals 0, and the other (let it be α_2) equals -2, then vector $\boldsymbol{\gamma} = (1, -1, -1, 1)^T$ satisfies (4.3).

Let both β_i be non-zero of different signs (without loss of generality, $\beta_1 = 2, \beta_2 = -2$). In this case from the way we obtained this matrix (subtraction of the first row, then permutation, then subtraction of the second row from the rows below) follows that $\alpha_1 \neq \alpha_2$, because in opposite case we could not obtain the configuration $\beta_1 = 2, \beta_2 = -2$. So, $\alpha_1 \neq \alpha_2$ and vector $\boldsymbol{\gamma} = (1, 1, -1, -1)^T$ satisfies (4.3).

In case of matrix A'_3: $\boldsymbol{\gamma} = (1, -1, 0, 0)^T$ satisfies (4.3).

The necessity is proven. □

4.3 Theorem of classification of complete systems in $[P_2]_{x_1,x_2}$

The subsequence of theorems 4.3 and 4.9 is

Theorem 4.10. *The set of the complete systems in $[P_2]_{x_1,x_2}$ is partitioned by the relation $\sim$ into four equivalence classes B_1, B_2, B_3, B_4, where*

$$B_1 = \Big[\{0, x, y, xy\}\Big]_{\mathscr{F}}, \qquad B_2 = \Big[\{0, x, y, x \oplus y\}\Big]_{\mathscr{F}},$$
$$B_3 = \Big[\{0, x, xy, y \oplus xy\}\Big]_{\mathscr{F}}, \qquad B_4 = \Big[\{0, x, xy, x \oplus y \oplus xy\}\Big]_{\mathscr{F}}$$

5 On the relation between the notions of completeness and strong completeness

The theorem 4.9 answers the question on how completeness and strong completeness are related in $[P_2]_{x_1,x_2}$. For the spaces of higher dimensions $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$ the answer is given in this section.

5.1 Non-equivalence of the notions of completeness and strong completeness in $[P_2]_{x_1,\ldots,x_3}$

We next cite an example showing that in $[P_2]_{x_1,\ldots,x_3}$ weakly complete systems exist(i.e. the notions of completeness and strong completeness are not equivalent in $[P_2]_{x_1,\ldots,x_3}$).

Statement 5.1. *Weakly complete systems exist in* $[P_2]_{x_1,\ldots,x_3}$.

Proof. We consider a system $\mathfrak{A}$, containing 7 functions and having a matrix

$$A = A_{\mathfrak{A}} = \begin{pmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

The functional form of the system will be cited below. This system is obviously not strongly complete. We next prove that it s complete.

We designate as A' a sub-matrix of A, which is made up of the first seven columns, and next prove that A' is non-singular.

$$\det A' = \det \begin{pmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 \end{pmatrix} = \det \begin{pmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 0 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 0 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 \end{pmatrix}$$

Thus the question on the non-singularity of A' is reduced to the same question of the principal minor of the 6-th order, which is obviously non-singular, hence A' is non-singular, too.

From the proven follows that rk $A = 7$, and the vector columns compounding A' are the basis in $\mathbb{R}^7$. Hence the vector column $(1,1,1,1,1,1,1)^T$ taking the last column of A can be linearly expressed through the first seven columns uniquely.

We are left to note that

$$5\cdot\begin{pmatrix}1\\1\\1\\1\\1\\1\\1\end{pmatrix}=\begin{pmatrix}-1&1&1&1&1&1&1\\1&-1&1&1&1&1&1\\1&1&-1&1&1&1&1\\1&1&1&-1&1&1&1\\1&1&1&1&-1&1&1\\1&1&1&1&1&-1&1\\1&1&1&1&1&1&-1\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\\1\\1\\1\end{pmatrix}$$

Hereby in the capacity of solutions of homogeneous system with the matrix A can be taken the vectors

$$\boldsymbol{\gamma}=\beta\cdot(1,1,1,1,1,1,1,-5)^T,\quad \beta\in\mathbb{R}$$

and only them which eliminates an existence of non-trivial solution vector with entries from $\{1,-1,0\}$. The condition of completeness criterion (statement 2.2) is satisfied, hence the system $\mathfrak{A}$ is complete. □

5.2 Non-equivalence of the notions of completeness and strong completeness in $[P_2]_{x_1,\ldots,x_n}$, $n\geqslant 3$

The example cited in the proof of statement 5.1 represents a special case of a more generalized construction, which we will give below. We premise several auxiliary statements to it.

Lemma 5.2. *A square matrix $A=(a_{ij})_{i,j=1}^N$ such that*

$$a_{ij}=\begin{cases}0, & i=j\\ \lambda, & i\neq j\end{cases}$$

where $\lambda\neq 0$ is non-singular.

Proof. Without loss off generality we let $\lambda=1$. Assume that the matrix is singular. Then one of its rows can be linearly expressed through the others. Without loss of generality, this row is the first one, being linearly expressed through the others with coefficients $k_2,k_3,\ldots,k_N$. Considering by-turn the components of these rows, we get

$$\sum_{i=2}^{N}k_i=0;\quad \sum_{i=3}^{N}k_i=1;\quad \ldots\quad \sum_{\substack{i=2\\ i\neq j}}^{N}k_i=1;\quad \ldots\quad \sum_{i=2}^{N-1}k_i=1$$

Subtracting by-turn from the first equality each of the others, we get $k_i=-1$, $i=$

$= 2, \ldots, N$, what is obviously wrong. This contradiction proves the lemma. $\square$

Lemma 5.3. *Let $N \geqslant 5$. Then there exists a signed-unit matrix $A = (a_{ij})$ of size $(N-1) \times N$, such that a homogeneous linear system with this matrix does not have solution vectors with entries from $\{1, -1, 0\}$.*

Proof. We specify the matrix A of size $(N-1) \times N$ in the following way:

$$a_{ij} = \begin{cases} -1, & i = j \\ 1, & i \neq j \end{cases}$$

Hereby, the matrix A has the following form:

$$A = \left.\begin{pmatrix} -1 & 1 & \ldots\ldots\ldots & 1 \\ 1 & -1 & 1 & \ldots\ldots & 1 \\ \cdots & 1 & -1 & 1 & \cdots & 1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & \\ \underbrace{\ldots\ldots\ldots\ldots\ldots\ldots\ldots}_{N} & & & 1 & -1 & 1 \end{pmatrix}\right\} (N-1)$$

We designate as A' a sub-matrix of size $(N-1) \times (N-1)$, which is made up of the first $(N-1)$ columns of the matrix A.

The matrix A' is non-singular. To prove this, we by-turn add the first row to each of the others and get the matrix

$$\left(\begin{array}{c|ccc} -1 & * & * \ldots & * \\ \hline 0 & & & \\ 0 & & A'' & \\ \vdots & & & \\ 0 & & & \end{array}\right)$$

where the sub-matrix A'' of size $(N-2) \times (N-2)$ satisfies the conditions of statement 5.2 with $\lambda = 2$ and thus is non-singular. The non-singularity of A' is proven.

From the proven follows that the vector columns of A' make up a basis in $\mathbb{R}^{N-1}$ and thus the last column (unit column) of matrix A can be linearly expressed though the first $(N-1)$ columns uniquely. It is left to note that the coefficients of this linear expressions are mutually identical and equal to $1/(N-3)$, what implies that there is no non-trivial linear combinaton of the columns of A with coefficients from $\{1, -1, 0\}$,

because all such coefficient vector have the following form

$$\boldsymbol{\gamma} = \beta \cdot (1, 1, \ldots, 1, -(N-3))^T, \quad N \geqslant 5, \quad \beta \in \mathbb{R}$$

The searched matrix is now found. □

Note 5.4. Note that the condition $N \geqslant 5$ is essential. Without it the last step of the proof becomes wrong.

Theorem 5.5. *Let $n \geqslant 3$. Weakly complete systems exist in $[P_2]_{x_1,\ldots,x_n}$*

Proof. The inequality $2^n \geqslant 8$ holds true. Hence, according to lemma 5.3, we can find a signed-unit matrix with 2^n columns of a rank less than 2^n, for which the completeness criterion holds true (statement 2.2).

The system of functions, to which this matrix corresponds, is weakly complete by definition. □

Theorems 4.9 and 5.5 answer the question whether the sufficient condition of completeness of a system $\mathfrak{A}$ in $[P_2]_{x_1,\ldots,x_n}$

$$\operatorname{rk} A_{\mathfrak{A}} = 2^n$$

is at the same time the necessary condition. For $n = 2$, the answer is positive, for $n \geqslant 3$ — negative.

5.3 Examples of weakly complete systems

In $[P_2]_{x_1,\ldots,x_3}$: the matrix cited in the proof of statement 5.1 is the matrix of a weakly complete system $\mathfrak{A}$, which has the form

$$\mathfrak{A} = \{\bar{x}\bar{y}\bar{z}, \bar{x}\bar{y}z, \bar{x}y\bar{z}, \bar{x}yz, x\bar{y}\bar{z}, x\bar{y}z, xy\bar{z}\}.$$

In case of $[P_2]_{x_1,\ldots,x_n}$ with arbitrary $n \geqslant 3$: the matrix cited in the proof of statement 5.5 is the matrix of a weakly complete system $\mathfrak{B}$, which consists of all conjunctions of n variables, except a one:

$$\mathfrak{B} = \{x_1^{\sigma_1} x_2^{\sigma_2} \ldots x_n^{\sigma_n} \mid (\sigma_1, \sigma_2, \ldots, \sigma_n) \neq (1, \ldots, 1)\}.$$

6 Connection with Hadamard matrices

In this section we examine the connection with so called *Hadamard matrices*.

A square matrix $H = (h_{ij})_{i,j=1}^{k}$, $h_{ij} \in \{-1, 1\}$ is called an *Hadamard matrices*, if its columns (or, what is the same, rows) are orthogonal, i.e.

$$HH^T = kI$$

For more info on Hadamard matrices look [4], [5].

Hadamard matrices play a significant role in Coding Theory ([4]), helping, for example, to build the codes lying on the Plotkin boundary ([4], Theorem 2.0.5).

For an arbitrary square matrix, the necessary condition for it to be a Hadamard matrix is that its order should be a multiple of 4 (look [5]). Nevertheless, at the moment there exist no methods of constructing Hadamard matrices of any order which is a multiple of 4.

The connection between matrices of certain strongly complete systems and Hadamard matrices makes a presumption of existence of methods of constructing Hadamard matrices in terms of strongly complete systems of Boolean functions.

We will call a system $\mathfrak{A} \subset [P_2]_{x_1,\dots,x_n}$ *Hadamard system*, is the matrix $A_{\mathfrak{A}}$ is a Hadamard one.

Let $n \geqslant 1$. We next give a criterion of hadamarity a system $\mathfrak{A}$, containing 2^n functions from $[P_2]_{x_1,\dots,x_n}$.

Statement 6.1. *The system $\mathfrak{A} \in [P_2]_{x_1,\dots,x_n}$, containing 2^n different functions, is an Hadamard system if and only if $\rho(f_1, f_2) = 2^{n-1}$ for any pair of functions $f_1 \neq f_2$, $f_1, f_2 \in \mathfrak{A}$.*

Proof. We note that for any pair $\mathbf{v}_1, \mathbf{v}_2$ (the can be identical) of rows of the matrix $A_{\mathfrak{A}}$, corresponding to functions f_1, f_2, their scalar multiplication is the difference between the number of identical entries of $\mathbf{v}_1, \mathbf{v}_2$ and the number of non-identical entries of vectors $\mathbf{v}_1, \mathbf{v}_2$, thus the following chain is correct

$$(\mathbf{v}_1, \mathbf{v}_2) = \|\overline{\widetilde{\chi}_{f_1} \oplus \widetilde{\chi}_{f_2}}\| - \|\widetilde{\chi}_{f_1} \oplus \widetilde{\chi}_{f_2}\| = 2^n - 2\|\widetilde{\chi}_{f_1} \oplus \widetilde{\chi}_{f_2}\| = 2^n - 2\rho(f_1, f_2),$$

from where, utilizing the property of Hadamard matrices ($(\mathbf{v}_1, \mathbf{v}_2) = 0$), we get the statement. □

Note that by definition of Hadamard matrices, only a strongly complete system can be an Hadamard system.

Statement 6.2. *Let $\mathfrak{A}$ be a system of functions with a square matrix of size $2^n \times \times 2^n$. Then the operations of $\mathscr{F}$ (Definition 4.1) preserve the hadamarity of the system $\mathfrak{A}$.*

PROOF. Operations F, V, S, T, P are equivalent to, respectively, multiplication of a certain row of $A_{\mathfrak{A}}$ by -1, some permutation of columns of $A_{\mathfrak{A}}$, multiplication of certain columns of $A_{\mathfrak{A}}$ by -1, some permutation of columns of $A_{\mathfrak{A}}$, some permutation of rows of $A_{\mathfrak{A}}$.

All these operation preserve the orthogonality of columns. □

Corollary 6.3. *In any closed (with respect to $\mathscr{F}$) class of systems in $[P_2]_{x_1,\dots,x_n}$, $n \geqslant 2$ all the systems have simultaneously Hadamard matrices, or simultaneously not Hadamard matrices.*

We will call the equivalence class of systems, whose systems are Hadamard systems, an *Hadamard class.*

We remind that according to Theorem 4.3 the set of strongly complete systems in $[P_2]_{x_1,x_2}$ is partitioned into four equivalence classes with respect to $\mathscr{F}$:

$$B_1 = \Big[\{0, x, y, xy\}\Big]_{\mathscr{F}}, \qquad B_2 = \Big[\{0, x, y, x \oplus y\}\Big]_{\mathscr{F}},$$
$$B_3 = \Big[\{0, x, xy, y \oplus xy\}\Big]_{\mathscr{F}}, \qquad B_4 = \Big[\{0, x, xy, x \oplus y \oplus xy\}\Big]_{\mathscr{F}}$$

There is only one Hadamard class in this list:

$$B_2 = \Big[\{0, x, y, x \oplus y\}\Big]_{\mathscr{F}}$$

We next consider ways of obtaining Hadamard matrices of higher orders.

Tensor (*Kronecker*) *multiplication* (look. [4]) $A \otimes B$ of matrices $A_{n\times m}$ and $B_{k\times l}$ is a block matrix

$$C = A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{pmatrix}$$

of size $nk \times ml$.

The following statement is proven in [4].

Statement 6.4. *If A and B are Hadamard matrices, then $A \otimes B$ is a Hadamard matrix, too.*

The work [3] gave quite complicated proof of the fact that the system $L^{(n)} \cap T_0^{(n)}$ strongly complete. We give a simpler proof.

Statement 6.5. *The system $\mathfrak{A}_0(n) = L^{(n)} \cap T_0^{(n)} \subset [P_2]_{x_1,\dots,x_n}$, $n \geqslant 2$ is strongly complete.*

PROOF. The system $\mathfrak{A}_0(2)$, which generates the class B_2, satisfies this statement. As it is noted above, it has Hadamard matrix (let us designate it A_2). From the statement 6.4 follows that tensor multiplication of A_2 by the matrix

$$X = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

applied $k \geqslant 0$ times, generated an Hadamard matrix $C = X^{\otimes k} \otimes A_2$ of size 2^{k+2} and thus corresponds to a certain strongly complete system in $[P_2]_{x_1,\ldots,x_n}$, $n = k+2$. We next prove that the obtained system is $\mathfrak{A}_0(n)$.

For this we note that the operation of tensor multiplication of the matrix X by a matrix Y_s of any system $\mathfrak{B}(s)$ of functions of variables $x_1, x_2, \ldots, x_s$ produces a matrix of the form

$$Y_{s+1} = \begin{pmatrix} Y_s & Y_s \\ Y_s & -Y_s \end{pmatrix}$$

which corresponds to a system of functions of $(s+1)$ variables $x_0, x_1, \ldots, x_s$ (for the sake of convenience we designate the new variable as x_0):

$$\mathfrak{B}(s+1) = \mathfrak{B}'(s+1) \cup \mathfrak{B}''(s+1)$$

where $\mathfrak{B}'(s+1) = \mathfrak{B}(s)$ (does not depend on the new variable x_0) and $\mathfrak{B}''(s+1) = x_0 \oplus \oplus \mathfrak{B}(s)$.

Starting with $\mathfrak{A}_0(2)$ and constructing new systems in the above-described way we will get at the each step the class of linear systems, preserving 0. □

We pose the following question: is the class generated by the system $\mathfrak{A}_0(n)$ is the only one hadamard class?

Remind that a *normalized* Hadamard matrix is a Hadamard matrix with units int the first row and column. In terms of systems of Boolean functions a normalized matrix is the one of a system of functions which preserve 0 and among which the zero-function is contained.

We define a group G of matrix transformations as a group which contains transformations generated by inversions (i.e. multiplications by -1) of arbitrary row or column and by permutations of an arbitrary pair of rows or columns.

Two Hadamard matrices are called *equivalent* if one of them can be obtained from the other by means of a transformation from G.

In [5] it is stressed out, that, generally speaking, among the normalized Hadamard matrices there do exist non-equivalent Hadamard matrices (of order 16 and higher, the example is in the Appendix).

The following holds true (we give it here without proof).

Statement 6.6. *Let $n \geqslant 4$, $\mathfrak{A}_0(n) = L^{(n)} \cap T_0^{(n)} \subset [P_2]_{x_1,\ldots,x_n}$. There exists a system $\mathfrak{B} \subset [P_2]_{x_1,\ldots,x_n}$, which is not equivalent to $\mathfrak{A}_0$ and has an Hadamard matrix, too.*

The following question is still open: whether all the Hadamard matrices of the order 2^3 are generated by the systems of $\left[L^{(3)} \cap T_0^{(3)}\right]_{\mathscr{F}}$. It is known (look [2]), that there is a single equivalence class of Hadamard matrices of the order 8 but we cannot say whether this class is equal (in a matrix form) to the set of matrices of the system $\left[L^{(3)} \cap T_0^{(3)}\right]_{\mathscr{F}}$.

Hereby, one of the problems in this direction is to determine whether the group F of matrix transformations generated by operations from $\mathscr{F}$ is a proper subgroup of G (in this case the equivalent Hadamard matrices may correspond to non-equivalent systems), or $G = F$ (int this case the equivalence in the sense of Hadamard matrices is identical to equivalence in the sense of systems of Boolean functions).

7 Notes on the further ways of research, problems

7.1 On "projections" of complete systems from $[P_2]_{x_1,\ldots,x_{n+1}}$ into $[P_2]_{x_1,\ldots,x_n}$

We will call *minimization* of complete systems a process of deletion certain functions from the system so as to make it strongly complete.

Statement 7.1. *Suppose we are given a strongly complete system $\mathfrak{A}_{n+1}$ in $[P_2]_{x_1,\ldots,x_{n+1}}$. Then substitution of a constant in place of a certain variable into all the functions of the system $\mathfrak{A}_{n+1}$ will produce a complete system, and further minimization will produce a strongly complete system $\mathfrak{A}_n \subset [P_2]_{x_1,\ldots,x_n}$.*

Proof. Without loss of generality we will substitute a constant 0.

We next show that the sub-matrix of $A_{\mathfrak{A}_{n+1}}$, (the latter has full rank 2^{n+1}, according to the conditions) made up of their first 2^n columns, has the rank 2^n, which is maximum possible for this sub-matrix. This will prove the statement.

Representing the rows of the matrix $A_{\mathfrak{A}_{n+1}}$ as vectors in the space $\mathbb{R}^{2^{n+1}}$, which make up its basis, we see that the rows of the above-introduced sub-matrix are projections of these vectors into some sub-space $\mathbb{R}^{2^n}$.

But the projections of the basis vectors of a linear space V into its sub-space W make up a system of vector, whose linear span is W. In our case $V = \mathbb{R}^{2^{n+1}}$, $W = \mathbb{R}^{2^n}$.

Hence, in the projected system of vectors we can choose 2^n linearly independent vectors, i.e. the rank of the considered sub-matrix is 2^n. □

7.2 Obtaining the complete systems of higher orders

Statement 7.2. *If a system* $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$ *is strongly complete, then* $\mathfrak{A}' = \mathfrak{A} \cup (\mathfrak{A} \oplus \oplus x_{n+1}) \subset [P_2]_{x_1,\ldots,x_{n+1}}$ *is strongly complete, too.*

Proof. Obvious, considering the matrix of the obtained system. □

Utilizing this method, we obtain from B_1, B_2, B_3, B_4 the following strongly complete systems in $[P_2]_{x_1,\ldots,x_3}$:

$$\{0, \quad x, \quad y, \quad z, \quad xy, \quad x \oplus z, \quad y \oplus z, \quad xy \oplus z\}$$
$$\{0, \quad x, \quad y, \quad z, \quad x \oplus y, \quad x \oplus z, \quad y \oplus z, \quad x \oplus y \oplus z\}$$
$$\{0, \quad x, \quad z, \quad x \oplus z, \quad xy, \quad xy \oplus y, \quad xy \oplus z, \quad xy \oplus y \oplus z\}$$
$$\{0, \quad x, \quad z, \quad x \oplus z, \quad xy, \quad xy \oplus z, \quad xy \oplus x \oplus y, \quad xy \oplus x \oplus y \oplus z\}$$

These systems generate mutually non-equivalent classes in $[P_2]_{x_1,\ldots,x_3}$.

A special form of the system generating B_1 gives an idea of its expansion for higher orders as $K_{(n)}$.

The system

$$\{0, x, y, z, xy, xz, yz, xyz\}$$

is strongly complete, as it is proven in [3].

For the further considerations we will use the parameter $\varkappa_1(\mathfrak{A})$ introduced on the page p. 22.

The proof of the statement 4.6 shows that for any system from $[P_2]_{x_1,\ldots,x_n}$ the value of $\varkappa_1$ is invariant with respect to operations from $\mathscr{F}$.

Note that among the systems, considered in this section

$$\{0, \quad x, \quad y, \quad z, \quad xy, \quad x \oplus z, \quad y \oplus z, \quad xy \oplus z\}$$
$$\{0, \quad x, \quad y, \quad z, \quad x \oplus y, \quad x \oplus z, \quad y \oplus z, \quad x \oplus y \oplus z\}$$
$$\{0, \quad x, \quad z, \quad x \oplus z, \quad xy, \quad xy \oplus y, \quad xy \oplus z, \quad xy \oplus y \oplus z\}$$
$$\{0, \quad x, \quad z, \quad x \oplus z, \quad xy, \quad xy \oplus z, \quad xy \oplus x \oplus y, \quad xy \oplus x \oplus y \oplus z\}$$
$$\{0, \quad x, \quad y, \quad z, \quad xy, \quad xz, \quad yz, \quad xyz\}$$

the four former ones have $\varkappa_1 = 0$, the fifth one has $\varkappa_1 = 1$.

A system with $\varkappa_1 = 2$ can be obtained from the generating system for B_3 class: we multiply it by z, join to it a selecting function z and join the result with initial system:

$$\{0, x, z, xy, y \oplus xy, xz, xyz, yz \oplus xyz\}$$

Another example with $\varkappa_1 = 2$ can be similarly obtained from the generating system for B_4 class:

$$\{0, x, z, xy, x \oplus y \oplus xy, xz, xyz, xz \oplus yz \oplus xyz\}$$

The latter examples make us surmise the following: if a strongly complete system $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$ contains zero-function and preserves 0 constant, then the system $\mathfrak{A}' = \mathfrak{A} \cup (\mathfrak{A} \,\&\, x_{n+1}) \cup \{x_{n+1}\} \subset [P_2]_{x_1,\ldots,x_{n+1}}$ is strongly complete, too.

Note 7.3. Every class of equivalent systems contains the system, preserving zero, and containing zero-function, to which the statement 7.4 can be applied.

We call a system, which contains zero-function and which preserves 0 constant, a *normalized* system. Any system has the normalized equivalent one.

Statement 7.4. *Let a normalized system $\mathfrak{A} \subset [P_2]_{x_1,\ldots,x_n}$ be strongly complete. Then the system $\mathfrak{A}' = \mathfrak{A} \cup \{\mathfrak{A} \,\&\, x_{n+1}\} \cup \{x_{n+1}\} \subset [P_2]_{x_1,\ldots,x_{n+1}}$, whose duplicated functions are deleted, is strongly complete.*

Proof. The proof will be performed in a matrix form. We will construct the matrix of $\mathfrak{A}'$. Joining the matrices of $\mathfrak{A}$, $\mathfrak{A} \,\&\, x_{n+1}$ and $\{x_{n+1}\}$ in $[P_2]_{x_1,\ldots,x_{n+1}}$, we obtain:

$$B = \left(\begin{array}{ccc|ccc} & A & & & A & \\ \hline & 0 & & & A & \\ \hline 1 & \ldots & 1 & -1 & \ldots & -1 \end{array}\right),$$

where the non-singular square matrix A of the order 2^n is the matrix of the system $\mathfrak{A}$, containing the row $(1, \ldots, 1)$, because $\mathfrak{A}$ is normalized.

The matrix B has 2^{n+1} columns and $2^{n+1} + 1$ rows, two of which are equal to $(1, \ldots, 1)$ (they correspond to two zero-functions in $\mathfrak{A}'$). Deleting one of these duplicates, we get the matrix

$$A' = \left(\begin{array}{ccc|ccc} 1 & \ldots & 1 & -1 & \ldots & -1 \\ \hline 1 & \ldots & 1 & 1 & \ldots & 1 \\ \hline & \widetilde{A} & & & \widetilde{A} & \\ \hline & 1 & & & \widetilde{A} & \end{array}\right),$$

where $\widetilde{A}$ is the result of deletion of the row $(1,\dots,1)$ from A. $\widetilde{A}$ Has the rank 2^n-1.

We next prove from the contrary that A' is non-singular. Assume that there does exist a vector of coefficients $\mu_1,\dots,\mu_{2^{n+1}}$ such that the linear combination of row vectors $\mathbf{a}_i$ of the matrix A' with these coefficients equals 0:

$$\sum_{i=1}^{2^{n+1}} \mu_i \mathbf{a}_i = \mathbf{0}$$

We partition the set of indexes of the rows of A' into three sets: $\Omega_1=\{1,2\}$, $\Omega_2=$ $=\{3,\dots,3+2^n\}$ and $\Omega_3=\{(3+2^n)+1,\dots,2^{n+1}\}$. We designate as $\mathbf{x}_i$ and $\mathbf{y}_i$ the sub-vectors of the vector $\mathbf{a}_i$, which are made up of, respectively, the former 2^n and the latter 2^n entries. The following facts are correct (obviously):

$$\sum_{\Omega_2} \mu_i \mathbf{x}_i = \sum_{\Omega_2} \mu_i \mathbf{y}_i =: \mathbf{b}, \tag{7.1}$$

$$\sum_{\Omega_1\cup\Omega_3} \mu_i \mathbf{x}_i = (x,\dots,x) =: \mathbf{x}, \quad x\in\mathbb{R}. \tag{7.2}$$

Finally, is there is a non-zero coefficient among μ_i, $i\in\Omega_3$, then

$$\sum_{\Omega_1\cup\Omega_3} \mu_i \mathbf{y}_i =: \mathbf{y} \neq (y,\dots,y) \quad \text{for none of } y\in\mathbb{R}. \tag{7.3}$$

The letter follows from the fact the each of the vectors $\mathbf{y}_1,\mathbf{y}_2$ has identical entries, and none of linear combinations of the rows of the matrix $\widetilde{A}$ can be a vector with identical components, because $\widetilde{A}$ is the result of deletion of a row $(1,\dots,1)$ from non-singular matrix A.

From the expressions (7.1)–(7.3) follows that if there is a non-zero coefficient among μ_i, $i\in\Omega_3$, then

$$\sum_{i=1}^{2^{n+1}} \mu_i \mathbf{x}_i = \mathbf{b}+\mathbf{x}, \quad \sum_{i=1}^{2^{n+1}} \mu_i \mathbf{y}_i = \mathbf{b}+\mathbf{y}$$

Our assumption implies $\mathbf{b}+\mathbf{x}=\mathbf{b}+\mathbf{y}=\mathbf{0}$, from where follows $\mathbf{x}=\mathbf{y}$. The left part is a vector with identical components, and the right part is not and we get a contradiction.

Hence, all the coefficients μ_i, $i\in\Omega_3$ equal zero. Then it is easy to see that an assumption about the equality to zero of the linear combination of the rows of A' is reduced to the form

$$(\mu_1+\mu_2,\dots,\mu_1+\mu_2)+\mathbf{b} = (-\mu_1+\mu_2,\dots,-\mu_1+\mu_2)+\mathbf{b} = \mathbf{0},$$

hence, $\mu_1=-\mu_1=0$. Then an assumption about the equality to zero of the linear

combination of the rows of A' is reduced to the form

$$(\mu_2, \ldots, \mu_2) + \mathbf{b} = 0,$$

which is equivalent to

$$(\mu_2, \ldots, \mu_2) + \sum_{\Omega_2} \mu_i \mathbf{x}_i = 0,$$

which implies $\mu_2 = 0$, $\mu_i = 0, i \in \Omega_2$, because the left side of the latter equality is the linear combination of rows of a non-singular matrix A.

We have proven that all $\mu_i = 0$ and thus A' is non-singular, that means strong completeness of $\mathfrak{A}'$. $\square$

Conclusion

Theorems 4.3, 4.9, 4.10 fully reveal the structure of complete systems in $[P_2]_{x_1,x_2}$.

The attempts of research of the structure of complete systems in case of $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$ were made.

We performed the research on the relation between the notions of strong and weak completeness, gave the examples showing the existence of weakly complete systems in $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$ (Theorem 5.5).

The direction of finding the weakly complete systems is one of the most interesting as it allows to encode every Boolean function with a vector of the length less than 2^n.

Some technical statements were proven, showing the relation between Hadamard matrices and strongly complete systems.

Utilizing the methods and instruments, introduced in this work, we reproved the statements of [3] in significantly easier way.

Some classes of complete systems were found in $[P_2]_{x_1,\ldots,x_3}$. Which can help in expanding the structure of complete systems into the cases $n \geqslant 3$.

We drafted the range of questions, which should be investigated on our way (relation between equivalence of Hadamard matrices and equivalence of complete systems, the expansion into the spaces $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$).

Appendix. Example of two non-equivalent Hadamard matrices of the order 16

$$A_{16}^1 = \begin{pmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
+ & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - \\
+ & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + \\
+ & + & + & + & - & - & - & - & + & + & + & + & - & - & - & - \\
+ & - & + & - & - & + & - & + & + & - & + & - & - & + & - & + \\
+ & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + \\
+ & - & - & + & - & + & + & - & + & - & - & + & - & + & + & - \\
+ & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - \\
+ & - & + & - & + & - & (+) & (-) & - & + & - & + & - & + & (-) & (+) \\
+ & + & - & - & + & + & - & - & - & - & + & + & - & - & + & + \\
+ & - & - & + & + & - & (-) & (+) & - & + & + & - & - & + & (+) & (-) \\
+ & + & + & + & - & - & - & - & - & - & - & - & + & + & + & + \\
+ & - & + & - & - & + & (-) & (+) & - & + & - & + & + & - & (+) & (-) \\
+ & + & - & - & - & - & + & + & - & - & + & + & + & + & - & - \\
+ & - & - & + & - & + & (+) & (-) & - & + & + & - & + & - & (-) & (+)
\end{pmatrix}$$

$$A_{16}^2 = \begin{pmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
+ & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - \\
+ & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + \\
+ & + & + & + & - & - & - & - & + & + & + & + & - & - & - & - \\
+ & - & + & - & - & + & - & + & + & - & + & - & - & + & - & + \\
+ & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + \\
+ & - & - & + & - & + & + & - & + & - & - & + & - & + & + & - \\
+ & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - \\
+ & - & + & - & + & - & (-) & (+) & - & + & - & + & - & + & (+) & (-) \\
+ & + & - & - & + & + & - & - & - & - & + & + & - & - & + & + \\
+ & - & - & + & + & - & (+) & (-) & - & + & + & - & - & + & (-) & (+) \\
+ & + & + & + & - & - & - & - & - & - & - & - & + & + & + & + \\
+ & - & + & - & - & + & (+) & (-) & - & + & - & + & + & - & (-) & (+) \\
+ & + & - & - & - & - & + & + & - & - & + & + & + & + & - & - \\
+ & - & - & + & - & + & (-) & (+) & - & + & + & - & + & - & (+) & (-)
\end{pmatrix}$$

References

[1] *O.A. Logachiov, A.A.Salnikov, V.V.Yashchenko* Boolean functions in Coding Theory and Crypthology // Moscow, MCCME, 2004

[2] *F.J. McWilliams, N.J.A.Sloan* Theory of self-correcting codes // Moscow, "Sviaz", 1979

[3] *V.V. Malykhin* Diploma thesis. // Moscow, MSU, Dept. of Mech. and Math., 2008

[4] *V.M.Sidelnikov* Coding Theory // Moscow, 2007

[5] *M.Hall* Combinatorics // Moscow, "Mir", 1970

[6] *S.V. Yablonsky* Introduction to Discrete Mathematics // Moscow, 1979