On some metrical properties of Boolean functions

ρ-completeness and its properties

Alexey Gronskiy, supervision by Prof. Alexander Ugolnikov

ETHZ, May 2012

1. **Introduction**
   - Short history
   - The basic definitions and directions of research
2. **Basics**
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - Strong and weak completeness
3. **Classification of complete systems in** $[P_2]_{x_1,x_2}$
   - Classifying operations
   - Theorems
4. **Weakly complete systems,** $[P_2]_{x_1,\ldots,x_n}$**,** $n \geqslant 3$
5. **Relation with other objects, further research**
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

1. **Introduction**
   - Short history
   - The basic definitions and directions of research
2. **Basics**
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - Strong and weak completeness
3. **Classification of complete systems in $[P_2]_{x_1,x_2}$**
   - Classifying operations
   - Theorems
4. **Weakly complete systems, $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$**
5. **Relation with other objects, further research**
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

V. Malykhin, 2008

This work is the further development of the research started in V.V. Malykhin's diploma paper, concerning so called basis systems.

In his work, he first introduced the notion and gave some exapmles of basis systems.

1. **Introduction**
    - Short history
    - The basic definitions and directions of research
2. **Basics**
    - Matrix terminology
    - Necessary and sufficient conditions of completeness
    - Strong and weak completeness
3. **Classification of complete systems in $[P_2]_{x_1,x_2}$**
    - Classifying operations
    - Theorems
4. **Weakly complete systems, $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$**
5. **Relation with other objects, further research**
    - Relation with Hadamard matrices
    - Expansion to higher orders
    - Conclusion anf future

Designators

$[P_2]_{x_1,\dots,x_n}$: the set of n-ary Boolean functions

E, E^k: sets $\{0,1\}$ and $\{0,1\}^k$, respectively, $(k \geqslant 1)$

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

$\mathbb{Z}_+$: set of non-negative integers

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

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

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

Distance vector

We examine n-ary Boolean functions (the space $[P_2]_{x_1,\dots,x_n}$), depending on $x_1, \dots, x_n$.

Definition

For given $f, g \in [P_2]_{x_1,\dots,x_n}$, 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.

Distance vector-2

Definition

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 $\mathfrak{A}$.

ρ-complete system

Definition

System $\mathfrak{A} \subset [P_2]_{x_1,\dots,x_n}$, containing k functions, is called ρ-complete for the system $\mathfrak{B} \subset [P_2]_{x_1,\dots,x_n}$, if there does not exist any pair $f_1 \neq f_2, f_1, f_2 \in \mathfrak{B}$ 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 $[P_2]_{x_1,\dots,x_n}$.

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

ρ-complete system

Definition

System $\mathfrak{A} \subset [P_2]_{x_1,\dots,x_n}$, *containing* k *functions, is called ρ-complete for the system* $\mathfrak{B} \subset [P_2]_{x_1,\dots,x_n}$, *if there does not exist any pair* $f_1 \neq f_2, f_1, f_2 \in \mathfrak{B}$ *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 $[P_2]_{x_1,\dots,x_n}$.

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

Possible directions

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.
5. Finding the relationship between the form of distance vector and the complexity of function.

Possible directions

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.
5. Finding the relationship between the form of distance vector and the complexity of function.

Possible directions

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.
5. Finding the relationship between the form of distance vector and the complexity of function.

Possible directions

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.
5. Finding the relationship between the form of distance vector and the complexity of function.

Possible directions

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.
5. Finding the relationship between the form of distance vector and the complexity of function.

1. Introduction
    - Short history
    - The basic definitions and directions of research

2. **Basics**
    - **Matrix terminology**
    - Necessary and sufficient conditions of completeness
    - Strong and weak completeness

3. Classification of complete systems in $[P_2]_{x_1,x_2}$
    - Classifying operations
    - Theorems

4. Weakly complete systems, $[P_2]_{x_1,\dots,x_n}$, $n \geqslant 3$

5. Relation with other objects, further research
    - Relation with Hadamard matrices
    - Expansion to higher orders
    - Conclusion anf future

Matrix of the system-1

System of k Boolean functions: $\mathfrak{A} = \{f_1(\widetilde{x}), \ldots, f_k(\widetilde{x})\} \subset [P_2]_{x_1,\ldots,x_n}$, where $k \geqslant 1$.

All the Boolean vectors of n elements: $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_{2^n}$ — lexicographically ascending.

Observe the matrix $B = (b_{ij})$, such that holds true

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

Matrix of the system-2

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

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

where $\tau(x) := (-1)^x$.

Definition

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

Example

Suppose $\mathfrak{A} = \{1, xy, x \oplus y\}$

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

Why needed?

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

1. Introduction
   - Short history
   - The basic definitions and directions of research
2. Basics
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - Strong and weak completeness
3. Classification of complete systems in $[P_2]_{x_1,x_2}$
   - Classifying operations
   - Theorems
4. Weakly complete systems, $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$
5. Relation with other objects, further research
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

NS-conditions of completeness

Statement

$\mathfrak{A}$ is complete if and only if there does not exist any vector $\boldsymbol{\gamma} \in \{0, 1, -1\}^{2^n}$, $\boldsymbol{\gamma} \neq \mathbf{0}$ (we will call it eigenvector), such that

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

Statement (Corollary)

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

NS-conditions of completeness

Statement

$\mathfrak{A}$ is complete if and only if there does not exist any vector $\boldsymbol{\gamma} \in \{0, 1, -1\}^{2^n}$, $\boldsymbol{\gamma} \neq \mathbf{0}$ (we will call it eigenvector), such that

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

Statement (Corollary)

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

1. Introduction
   - Short history
   - The basic definitions and directions of research
2. **Basics**
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - **Strong and weak completeness**
3. Classification of complete systems in $[P_2]_{x_1,x_2}$
   - Classifying operations
   - Theorems
4. Weakly complete systems, $[P_2]_{x_1,\dots,x_n}$, $n \geqslant 3$
5. Relation with other objects, further research
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

Strong and weak completeness

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

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

Definition

System $\mathfrak{A} \subset [P_2]_{x_1,\dots,x_n}$ 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 $\operatorname{rk} A_{\mathfrak{A}} < 2^n$.

1. Introduction
   - Short history
   - The basic definitions and directions of research
2. Basics
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - Strong and weak completeness
3. **Classification of complete systems in $[P_2]_{x_1,x_2}$**
   - Classifying operations
   - Theorems
4. Weakly complete systems, $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$
5. Relation with other objects, further research
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

We need to make the structure of the complete systems set simpler. We next introduce the classifying operations and prove the first theorems of classification.

The operations on the systems

We define a set of operations $\mathscr{F} = \{\mathrm{F}, \mathrm{V}, \mathrm{S}, \mathrm{T}, \mathrm{P}\}$ on the system $\mathfrak{A} \subset [P_2]_{x_1,\dots,x_n}$ in the following way:

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 $\mathrm{P}_\sigma(\mathfrak{A})$.

The operations on the systems

We define a set of operations $\mathscr{F} = \{\mathrm{F}, \mathrm{V}, \mathrm{S}, \mathrm{T}, \mathrm{P}\}$ on the system $\mathfrak{A} \subset [P_2]_{x_1,\dots,x_n}$ in the following way:

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 $\mathrm{P}_\sigma(\mathfrak{A})$.

The operations on the systems

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:

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 $\mathrm{P}_\sigma(\mathfrak{A})$.

The operations on the systems

We define a set of operations $\mathscr{F} = \{\mathrm{F}, \mathrm{V}, \mathrm{S}, \mathrm{T}, \mathrm{P}\}$ on the system $\mathfrak{A} \subset [P_2]_{x_1,\dots,x_n}$ in the following way:

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 $\mathrm{P}_\sigma(\mathfrak{A})$.

The operations on the systems

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:

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 $\mathrm{P}_\sigma(\mathfrak{A})$.

Equivalence of systems

Definition

$\mathfrak{A}$ and $\mathfrak{B}$ are similar ($\mathfrak{A} \sim \mathfrak{B}$), if

$$\mathfrak{B} = \varphi_1 \circ \ldots \circ \varphi_k(\mathfrak{A}), \quad \varphi_i \in \mathscr{F}$$

$\sim$ is reflexive, symmetric and transitive. Thus, the introduced relation is equivalence relation.

Statement

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

1. Introduction
   - Short history
   - The basic definitions and directions of research
2. Basics
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - Strong and weak completeness
3. **Classification of complete systems in $[P_2]_{x_1,x_2}$**
   - Classifying operations
   - Theorems
4. Weakly complete systems, $[P_2]_{x_1,\dots,x_n}$, $n \geqslant 3$
5. Relation with other objects, further research
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

Strongly complete systems in $[P_2]_{x_1,x_2}$

Theorem

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

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

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

Completeness and strong completeness in $[P_2]_{x_1,x_2}$

Theorem

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 $[P_2]_{x_1,\ldots,x_n}$.

Complete systems in $\left[P_2\right]_{x_1,x_2}$

Theorem

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

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

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

Theorem

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

Example: weakly complete system $\mathfrak{B}$, which consists of all conjunctions of n variables, except a one:

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

1. Introduction
   - Short history
   - The basic definitions and directions of research
2. Basics
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - Strong and weak completeness
3. Classification of complete systems in $[P_2]_{x_1,x_2}$
   - Classifying operations
   - Theorems
4. Weakly complete systems, $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$
5. **Relation with other objects, further research**
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

Definition

Hadamard matrix is an $n \times n$ matrix H with ± 1 entries, for which holds true:

$$HH^T = nI$$

1. Some strongly complete systems have Hadamard matrices
2. The operations from $\mathscr{F}$ preserve "hadamarity" of the matrix of the system
3. The question: whether the Hadamard matrix equivalence is the same as the systems equivalence

1. Introduction
    - Short history
    - The basic definitions and directions of research
2. Basics
    - Matrix terminology
    - Necessary and sufficient conditions of completeness
    - Strong and weak completeness
3. Classification of complete systems in $[P_2]_{x_1,x_2}$
    - Classifying operations
    - Theorems
4. Weakly complete systems, $[P_2]_{x_1,\dots,x_n}$, $n \geqslant 3$
5. **Relation with other objects, further research**
    - Relation with Hadamard matrices
    - **Expansion to higher orders**
    - Conclusion anf future

There are several statements concerning the ways of obtaining the classes of complete systems in $[P_2]_{x_1,\ldots,x_{n+1}}$ from the classes in $[P_2]_{x_1,\ldots,x_n}$.
Theoretically, this can help to perfrom a classification in case of $n \geqslant 3$, but the existance of weakly complete systems makes it difficult.

1. Introduction
   - Short history
   - The basic definitions and directions of research
2. Basics
   - Matrix terminology
   - Necessary and sufficient conditions of completeness
   - Strong and weak completeness
3. Classification of complete systems in $[P_2]_{x_1,x_2}$
   - Classifying operations
   - Theorems
4. Weakly complete systems, $[P_2]_{x_1,\ldots,x_n}$, $n \geqslant 3$
5. Relation with other objects, further research
   - Relation with Hadamard matrices
   - Expansion to higher orders
   - Conclusion anf future

Conclusion

Theorems of classification of strongly complete and complete functions 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 $[P_2]_{x_1,\dots,x_n}$, $n \geqslant 3$ were made.

Explored the relation between the notions of strong and weak completeness, gave the examples of weakly complete systems in $[P_2]_{x_1,\dots,x_n}$, $n \geqslant 3$

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

Unknown

1. What is the minimal number of functions in a weakly complete system (assessment)?
2. How can we easily determine whether the given vector is the distance vector?
3. What is the number of equivalence classes in $[P_2]_{x_1,\ldots,x_n}$?
4. Connection between the distance vector and the complexity of Boolean functions complexity?
5. Etc...

Thank you!