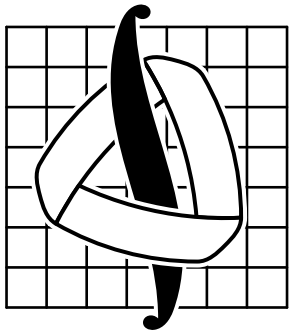
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА



Механико-математический факультет

Кафедра дискретной математики

Дипломная работа на тему:

О некоторых метрических свойствах булевых функций

Выполнил:
студент 510 группы
Гронский А.Ю.

Научный руководитель:
проф. Угольников А.Б.

Москва, 2011 год

Содержание

Введение

О значимости метрических свойств булевых функций в дискретной математике и её приложениях говорит большое количество применений этого понятия в разных разделах, в частности, в теории кодирования. Понятие ρ-*полной системы* булевых функций (см. определение 1.4), исследуемое в работе, связано с метрической структурой пространства булевых функций.

Данная работа является дальнейшем развитием темы, начало разработки которой содержится в дипломной работе В.В. Малыхина «О некоторых метрических свойствах булевых функций»([3]).

Основной объект — ρ-*полная система* булевых функций в пространстве $P_2(n)$, а также связанное с ним понятие *вектора расстояний* от системы булевых функций до заданной булевой функции — определяются в разделе 1 (также см. [3]).

С введенными понятиями связаны следующие направления исследований:

1. Рассмотрение свойств ρ-полных систем и векторов расстояний.
2. Установление необходимых и достаточных условий ρ-полноты системы.
3. Классификация ρ-полных систем по различным факторам.
4. Установление связей введенных объектов с другими математическими объектами.

В разделе 2 описываются необходимые и достаточные условия ρ-полноты, а также даются новые по сравнению с [3] определения *сильно* ρ-*полной* и *слабо* ρ-*полной* систем, играющие существенную роль в дальнейших рассмотрениях.

В разделе 3 даются примеры полных систем, векторов расстояний, рассматриваются их простейшие свойства.

В разделе 4 в качестве классифицирующего фактора для множества полных систем выбирается некоторый набор операций над системами булевых функций, относительно которого множество полных систем распадается на классы подобия, которые описываются полностью для случая $P_2(2)$. В этом же разделе описана связь понятий сильной и слабой ρ-полноты в $P_2(2)$.

Для случаев $P_2(n)$, $n \geqslant 3$, делаются попытки аналогичной классификации, дающие направление для дальнейших исследований, также рассматривается связь сильной и слабой ρ-полноты. Этой тематике посвящен раздел 5.

Связь изучаемых математических объектов с другими математическими объектами, которая в какой-то мере раскрывает потенциальные применения рассматриваемых объектов, отражена в разделе 6.

Замечания о дальнейших путях исследований, носящие незавершенный характер, вынесены в раздел 7.

1. Определения и обозначения

1.1. Обозначения и сокращения

В данной работе применяются следующие обозначения и сокращения:

$P_2(n)$ — пространство булевых функций, зависящих от n переменных (по поводу функций алгебры логики см. также [6])

E, E^k — множество $\{0,1\}$ и $\{0,1\}^k$ соответственно ($k \geqslant 1$)

$f^{(n)}(\widetilde{x})$ — n-местная (принимающая n аргументов) булева функция

$\mathbb{Z}_+$ — множество неотрицательных целых чисел

$\widetilde{\alpha}$, $\widetilde{x}$ — упорядоченные наборы элементов из E (булевы векторы)

$\boldsymbol{\gamma}$, $\mathbf{r}$ — векторы (множество, над которым они определяются, ясно из контекста или оговаривается явно)

γ_i, r_i — обозначают i-ые координаты векторов $\boldsymbol{\gamma}$, $\mathbf{r}$, если из контекста ясно, что речь идет о векторах

$\mathfrak{A}$, $\mathfrak{B}$ — конечные упорядоченные наборы (системы) булевых функций

$\mathfrak{A}^*$ — система, состоящая из функций, двойственных к функциям системы $\mathfrak{A}$

$A_{\mathfrak{A}}$, $A_{\mathfrak{B}}$ — матрицы систем булевых функций $\mathfrak{A}$ и $\mathfrak{B}$ (см. стр. 7)

$\operatorname{rk} A$ — ранг матрицы A

C_n^k — количество неупорядоченных выборок k элементов из n элементов

$L^{(n)}$ — класс линейных булевых функций n переменных (см. 1.2)

$T_a^{(n)}$ — класс булевых функций n переменных, сохраняющих константу a (см. 1.2)

$\|\widetilde{\alpha}\|$ — вес Хэмминга булева вектора $\widetilde{\alpha}$, равный количеству единичных компонент в $\widetilde{\alpha}$

$\square$ — конец доказательства

$\left.\begin{matrix} A := B \\ B =: A \end{matrix}\right\}$ — «A по определению полагается равным B»

Подробнее о стандартных операциях, принятых в алгебре логики ($\oplus$, $\&$, $\vee$ и т.д.) см. [6].

1.2. Общие замечания

Полиномом Жегалкина n-местной функции $f(x_1, \ldots, x_n)$ (представлением булевой функции в виде полинома Жегалкина) называется ее представление в базисе $\{\&, \oplus, 1\}$:

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

где $a, a_{i_1,\ldots,i_k} \in E$.

Пусть $n \geqslant 1$. *Линейной функцией* n переменных называется функция $f(x_1, \ldots, x_n)$, представление которой в виде полинома Жегалкина имеет вид

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

где $a_i \in E$, $0 \leqslant i \leqslant n$. Класс линейных функций n переменных в работе обозначается как $L^{(n)}$.

Пусть $n \geqslant 1, a \in E$. Функция n переменных $f(x_1, \ldots, x_n)$ *сохраняет константу* a, если выполняется равенство $f(a, \ldots, a) = a$. Класс функций n переменных, сохраняющих константу a, будем обозначать $T_a^{(n)}$.

Пусть $n \geqslant 1$, $1 \leqslant i \leqslant n$. *Селекторной функцией переменной* x_i называется функция $e_{x_i}(\widetilde{x}) \in P_2(n)$ такая, что на любом наборе $\widetilde{\alpha} \in E^n$ выполняется равенство $e_{x_i}(\widetilde{\alpha}) = \alpha_i$.

1.3. Основные определения

Рассматриваются булевы функции от n переменных. Пусть $f, g \in P_2(n)$. Для таких функций можно ввести понятие расстояния между ними следующим образом:

Определение 1.1. Будем называть величину

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

расстоянием от функции f до функции g.

Отметим, что внешняя сумма — обыкновенная, не по модулю 2. Таким образом, для любых f, g расстояние $\rho(f, g)$ между ними удовлетворяет неравенству $0 \leqslant \leqslant \rho(f, g) \leqslant 2^n$.

Например, в $P_2(2)$ расстояние между функциями $f(x_1, x_2) = 1$ и $g(x_1, x_2) = x_1 \oplus x_2$ равно $\rho(f, g) = 1 + 0 + 0 + 1 = 2$.

Если упорядочить в лексикографическом порядке все наборы вида $\widetilde{\alpha} \in E^n$: $\widetilde{\alpha}_1 = = (0, \ldots, 0), \ldots, \widetilde{\alpha}_{2^n} = (1, \ldots, 1)$, то можно ввести вектора значений $\widetilde{\chi}_f$ функции f:

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

Напомним, что *расстоянием Хэмминга* между булевыми векторами $\widetilde{x}, \widetilde{y} \in E^n$ называется величина

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

Введенное расстояние $\rho(f, g)$ между функциями f и g есть расстояние Хэмминга между векторами значений $\widetilde{\chi}_f$ и $\widetilde{\chi}_g$. Ввиду этого мы иногда будем допускать использование записи

$$\rho(f, g) = d(\widetilde{\chi}_f, \widetilde{\chi}_g)$$

Вышеприведенное понятие естественно распространить на случай нескольких функций.

Определение 1.2. Пусть $\mathfrak{A} \subset P_2(n)$ — система из k булевых функций $g_1, \ldots, g_k$, тогда вектор, имеющий компонентами расстояния от f до всех $g_i \in \mathfrak{A}$, будем обозначать

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

и называть *расстоянием* от f до системы $\mathfrak{A}$.

Замечание 1.3. Мы будем рассматривать системы булевых функций с точностью до перестановки в ней функций, поэтому и вектор расстояний определен с точностью до перестановки компонент. В работе не рассматриваются вопросы, для которых порядок элементов в векторе расстояний важен, поэтому данное ослабление не критично для дальнейших рассмотрений.

Очевидны свойства (следуют из аналогичных свойств расстояния Хэмминга):

1° Для любых $f, g \in P_2(n)$, выполняется $\rho(f, g) \geqslant 0$. Равенство достигается тогда и только тогда, когда f и g равны. Равенство функций f и g следует понимать в смысле равенства их векторов значений.

2° Для любых $f, g \in P_2(n)$ верно $\rho(f, g) = \rho(g, f)$.

3° Для любых $f, g, h \in P_2(n)$ выполняется неравенство треугольника:

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

Определение 1.4. Система функций $\mathfrak{A} \subset P_2(n)$, состоящая из k функций, называется ρ-*полной для системы* $\mathfrak{B} \subset P_2(n)$, если не существует пары функций $f_1, f_2 \in \mathfrak{B}$ таких, что $\boldsymbol{\rho}(\mathfrak{A}, f_1) = \boldsymbol{\rho}(\mathfrak{A}, f_2)$. Другими словами, система $\mathfrak{A}$ ρ-полна для системы $\mathfrak{B}$, если отображение из $\mathfrak{B}$ в $\mathbb{Z}_+^k$, действующее по правилу

$$f \mapsto \boldsymbol{\rho}(\mathfrak{A}, f), \quad \text{где } f \in \mathfrak{B}$$

инъективно.

В частности, будем называть систему функций ρ-*полной* (без указания второй системы), если она полна для всего множества $P_2(n)$.

Замечание 1.5. В дальнейшем, если не оговорено иное, будем такие системы называть просто *полными*. Термин «полнота» в смысле, используемом в теории функциональных систем, будем оговаривать особо.

2. Необходимое и достаточное условие полноты

В этом разделе будут рассмотрены вопросы, связанные с необходимым и достаточным условием полноты заданной системы булевых функций.

Для рассмотрения вопроса о необходимом и достаточном условии полноты системы булевых функций полезной оказывается *матричная терминология.*

2.1. Матричная терминология

Пусть дана система из k булевых функций $\mathfrak{A} = \{f_1(\widetilde{x}), \ldots, f_k(\widetilde{x})\} \subset P_2(n)$, где $k \geqslant 1$. Упорядочим всевозможные наборы длины n в лексикографическом порядке по возрастанию: $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_{2^n}$ и рассмотрим матрицу $B = (b_{ij})$, такую, что

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

где $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant 2^n$. Определим отображение $\tau\colon E \to \{-1, 1\}$, действующее по правилу

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

Для определенной выше системы $\mathfrak{A}$ определим матрицу $A_{\mathfrak{A}}$:

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

Будем говорить, что системе $\mathfrak{A}$ *соответствует матрица* $A_{\mathfrak{A}}$.

Таким образом, $A_{\mathfrak{A}}$ — матрица размера $k \times 2^n$, состоящая из ± 1.

Докажем техническое утверждение.

Предложение 2.1. *В введенных выше терминах справедливо представление*

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

где

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

а $I_{k\times 2^n}$ *— матрица размера* $k \times 2^n$*, состоящая из единиц.*

Доказательство. Очевиден тот факт, что $(r_{\mathfrak{A}})_i$ — количество чисел (-1) в i-ой строке матрицы $A_{\mathfrak{A}}$. Пусть k_+ и k_- — количество соответственно $(+1)$ и (-1) в i-ой строке. Тогда, решая систему

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

получим

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

откуда

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

2.2. Необходимое и достаточное условие ρ-полноты

В работе [3] приводится самая общая формулировка необходимого и достаточного условия полноты системы функций с матрицей A. Приведем его здесь с доказательством.

Предложение 2.2. $\mathfrak{A}$ *— полна тогда и только тогда, когда не существует вектора* $\boldsymbol{\gamma} \in \{0, 1, -1\}^{2^n}$*,* $\boldsymbol{\gamma} \neq \mathbf{0}$*, такого, что*

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

Доказательство. Пусть найдутся такие $f, g \in P_2(n)$, что

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

Это эквивалентно (в силу представления (2.2)) следующему равенству

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

или, что равносильно,

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

Откуда, положив $\boldsymbol{\gamma} = (\widetilde{\chi}_f - \widetilde{\chi}_g)$, получаем требуемый критерий. □

Таким образом, получаем следующее достаточное условие полноты:

Следствие 2.3. *Если* $\operatorname{rk} A_{\mathfrak{Q}} = 2^n$, *то система* $\mathfrak{A}$ — *полна.*

Из вышесказанного не следует, что $\operatorname{rk} A_{\mathfrak{Q}} < 2^n$ влечет неполноту системы $\mathfrak{A}$, поэтому целесообразно ввести понятия сильно полной и слабо полной систем.

Определение 2.4. Система $\mathfrak{A} \subset P_2(n)$ называется *сильно* ρ-*полной*, если $\operatorname{rk} A_{\mathfrak{Q}} = 2^n$. Система $\mathfrak{A}$ назывется *слабо* ρ-*полной*, если она является ρ-полной, но $\operatorname{rk} A_{\mathfrak{Q}} < 2^n$.

Из определений видно, что сильно полные системы должны содержать самое меньшее 2^n различных функций и в этом случае иметь квадратную матрицу, в то время как для слабо полных допускается и меньшее, чем 2^n, количество функций (равное рангу матрицы). В дальнейшем, говоря о сильно полных системах, будем подразумевать, что в них содержится 2^n различных функций и матрица квадратная.

Вопрос о необходимом условии полноты системы в общем случае открыт. Частично его решение дано в теоремах 4.8 и 5.5.

3. Некоторые общие утверждения

В данном разделе будут пречислены утверждения, носящие общий характер.

Примеры регулярно устроенных векторов расстояний рассмотрены в разделе 3.1. Они играют следующую роль: такие примеры указывают на существование просто устроенных векторов расстояний, что при дальнейшем рассмотрении может дать некоторые правила, описывающие произвольные вектора расстояний.

Простейшие свойства векторов расстояний описаны в разделе 3.2. Отметим, что помимо самостоятельного значения свойств, помещенные в этот раздел утверждения играют роль технических утвреждений для дальнейших рассмотрений.

Некоторые свойства полных систем функций перечислены в разделе 3.3. Эти свойства понадобятся в дальнейшем, при выборе классифицирующего набора операций для описания классов полных систем в $P_2(n)$.

3.1. Примеры векторов расстояний

Пусть $\mathfrak{A}_0 = L^{(n)} \cap T_0^{(n)} \subset P_2(n)$ — линейные функции n переменных, сохраняющие константу 0. Из сказанного в 1.2 следует, что в систему $\mathfrak{A}_0$ входят в точности функции, имеющие вид $a_1 x_1 \oplus \ldots a_n x_n,\ a_i \in E$, значит, количество функций в системе $\mathfrak{A}_0$ равно 2^n. В работе [3] доказано, что система $\mathfrak{A}_0$ полна.

Обозначим функции системы $\mathfrak{A}_0$ как g_i, $1 \leqslant i \leqslant 2^n$ и установим нумерацию функций $g_1, g_2, \ldots, g_{2^n}$ следующим образом: сначала — по возрастанию количества существенных переменных, а среди групп с одинаковым количеством существенных переменных — в лексикографическом порядке по $x_1, x_2, \ldots, x_n$ (это можно сделать, т.к. каждая функция из $\mathfrak{A}_0$, существенно зависящая от m переменных $x_{i_1}, \ldots, x_{i_m}$, $i_k \neq i_l$ при $k \neq l$, имеет вид $g(x_{i_1}, \ldots, x_{i_m}) = x_{i_1} \oplus \ldots \oplus x_{i_m}$).

Пусть $n \geqslant 1$. Справедливы следующие утверждения.

Предложение 3.1. *Пусть $f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$ есть n-местная булева функция. Тогда вектор расстояний от f до системы $\mathfrak{A}_0$ имеет вид*

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

Доказательство. а) Для функции $g_{2^n}(\widetilde{x}) = x_1 \oplus \ldots \oplus x_n$, $g_{2^n} \in \mathfrak{A}_0$, очевидно, выполнено равенство $\rho(g_{2^n}, f) = 0$.

б) Пусть теперь номер функции g_k удовлетворяет неравенству $1 \leqslant k < 2^n$. Для любой такой функции $g_k(\widetilde{x}) = x_{i_1} \oplus \ldots \oplus x_{i_m}$ из $\mathfrak{A}_0$, зависящей от m переменных (предполагается, что все $i_1, \ldots, i_m$ различны) выполнено соотношение

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

где $j_1, \ldots, j_{n-m}$ — номера переменных, от которых g_k не зависит существенно. Последняя сумма есть количество наборов $\widetilde{\alpha}$, в которых среди $\alpha_{j_1}, \ldots, \alpha_{j_{n-m}}$ содержится нечетное число единиц, т.е.

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

где $l = \max\limits_{2i+1 \leqslant n-m} (2i+1)$, что доказывает предложение. □

Предложение 3.2. *Пусть $f(x_1, \ldots, x_n) = x_1 \vee \ldots \vee x_n$ есть n-местная булева функция. Тогда вектор расстояний от f до системы $\mathfrak{A}_0$ имеет вид*

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

Доказательство. Доказательство почти аналогично предложению 3.1:

а) Для функции $g_1(\widetilde{x}) = 0$, $g_1 \in \mathfrak{A}_0$, очевидно, выполнено равенство $\rho(g_1, f) = 2^n - 1$, т.к. в этом случае расстояние — это в точности количество различных ненулевых наборов длины n

б) Пусть теперь номер функции g_k удовлетворяет неравенству $1 < k \leqslant 2^n$. Для любой такой функции $g_k(\widetilde{x}) = x_{i_1} \oplus \ldots \oplus x_{i_m}$ из $\mathfrak{A}_0$, зависящей от m переменных

(все $i_1, \ldots, i_m$ различны) выполнено соотношение

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

но последняя сумма есть количество наборов $\widetilde{\alpha}$, в которых среди $\alpha_{i_1}, \ldots, \alpha_{i_m}$ содержится четное число единиц, т.е.

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

где $l = \max\limits_{2i \leqslant n-m} (2i)$, что доказывает предложение. □

Предложение 3.3. *Пусть* $f(x_1, \ldots, x_n) = x_1 \,\&\, \ldots \,\&\, x_n$ — *n-местная булева функция. Тогда вектор расстояний от* f *до системы* $\mathfrak{A}_0$ *имеет вид*

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

Доказательство. Доказательство почти аналогично предыдущим:
а) Для функции $g_1(\widetilde{x}) = 0$, $g_1 \in \mathfrak{A}_0$ очевидно, что $\rho(g_1, f) = 1$, т.к. в таком случае расстояние — это в точности количество единичных наборов длины n.
б) Пусть теперь номер функции g_k удовлетворяет неравенству $1 < k \leqslant 2^n$. Для любой такой функции $g_k(\widetilde{x}) = x_{i_1} \oplus \ldots \oplus x_{i_m}$, зависящей от m переменных (предполагается, что все $i_1, \ldots, i_m$ различны), выполнено соотношение (здесь $(m+1)_{(2)}$ — остаток $(m+1)$ по модулю 2):

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

Заметим, что первое слагаемое есть количество наборов, кроме единичного, содержащих нечетное число единиц среди $\alpha_{i_1}, \ldots, \alpha_{i_m}$. Рассмотрим два случая:

1) m — четное:

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

2) m — нечетное:

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

Таким образом, вектор $\boldsymbol{\rho}(\mathfrak{A}_0, f)$ составляют группы, состоящие из чисел $(2^{n-1}+$ $+1)$ и $(2^{n-1}-1)$, идущие поочередно друг за другом (исключение составляет 1-ая координата вектора $\boldsymbol{\rho}(\mathfrak{A}_0, f)$, представляющая собой группу, состоящую из одной единицы). Длина m-ой группы равна количеству функций функций от m переменных в $\mathfrak{A}_0$ т.е. C_n^m. □

3.2. Свойства векторов расстояний

В этом разделе приведем ряд предложений, имеющих как самостоятельное значение, так и необходимых для дальнейших рассмотрений. Далее в разделе рассматриваются функции и системы функций, принадлежащие $P_2(n)$.

Связь $\boldsymbol{\rho}(\mathfrak{A}, f)$ и $\boldsymbol{\rho}(\mathfrak{A}, \overline{f})$ проясняется следующим фактом.

Предложение 3.4. *Для любых функций g, f выполняется равенство*

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

Доказательство. Действительно, выражение

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

есть количество наборов $\widetilde{\alpha}$, на которых $f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha}) = 1$, а выражение

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

есть количество наборов $\widetilde{\alpha}$, для которых $\overline{f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha})} = 1$, или, что то же самое, $f(\widetilde{\alpha}) \oplus g(\widetilde{\alpha}) = 0$. Но других наборов, кроме учтенных в A и B, нет, следовательно, $A + B = 2^n$, что и требовалось доказать. □

Следствие 3.5. *Для любой системы $\mathfrak{A}$ и любой булевой функции f выполнено соотношение*

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

Доказательство. Равенство (3.1) верно для каждой компоненты вектора $\boldsymbol{\rho}(\mathfrak{A}, f)$, откуда следует равенство (3.2). □

Предложение 3.6. *Если $\mathfrak{A} = \{g_i\}$, $\mathfrak{B} = \{h_i\}$, причем $g_i = \overline{h}_i$, то для произвольной функции f выполняется равенство*

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

Доказательство. Доказательство аналогично следствию 3.5. □

3.3. Свойства систем функций

Здесь будут приведены утверждения, которые важны для выбора операций $\mathscr{F}$ (см. стр. 14).

Предложение 3.7. *Замена произвольной функции в полной системе на ее отрицание сохраняет полноту.*

Доказательство. Замена k-ой функции $g_k \in \mathfrak{A}$ на ее отрицание $\overline{g}_k$ эквивалентна домножению k-ой строки матрицы $A_{\mathfrak{A}}$ на (-1). Обозначим полученную систему $\mathfrak{A}'$.

Воспользуемся критерием полноты системы из предложения 2.2 и предположим, что для $A_{\mathfrak{A}'}$ нашелся вектор $\boldsymbol{\gamma}$ из предложения 2.2. Учитывая связь $A_{\mathfrak{A}}$ и $A_{\mathfrak{A}'}$, нетрудно видеть, что из $A_{\mathfrak{A}'} \cdot \boldsymbol{\gamma} = \mathbf{0}$ следует $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = \mathbf{0}$. Противоречие с полнотой системы $\mathfrak{A}$. □

Предложение 3.8. *Замена всех вхождений произвольной переменной x_i в полной системе $\mathfrak{A} \subset P_2(n)$ на ее отрицание сохраняет полноту.*

Доказательство. Из построения матрицы $A_{\mathfrak{A}}$ следует, что замена переменной на ее отрицание эквивалентна некоторой перестановке σ ее столбцов.

Предположим, что для $A_{\mathfrak{A}'}$ существует вектор $\boldsymbol{\gamma}'$ из предложения 2.2. Рассмотрим вектор $\boldsymbol{\gamma} = \sigma^{-1}(\boldsymbol{\gamma}')$ (с переставленными компонентами). Тогда, очевидно, $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = \mathbf{0}$. Противоречие с полнотой $\mathfrak{A}$. □

Простым следствием предложений 3.7 и 3.8 является следующее утверждение.

Следствие 3.9. *Система $\mathfrak{A}$ полна тогда и только тогда, когда полна двойственная ей система $\mathfrak{A}^*$.*

Предложение 3.10. *Прибавление по модулю 2 некоторой функции g одновременно ко всем функциям системы сохраняет ее полноту.*

Доказательство. Операция эквивалентна прибавлению по модулю 2 вектора $\widetilde{\chi}_g$ ко всем векторам $\widetilde{\chi}_f$, $f \in \mathfrak{A}$. Это, в свою очередь, равносильно покомпонентному умножению каждой строки матрицы $A_{\mathfrak{A}}$ на вектор $\mathbf{v} = \tau(\widetilde{\chi}_g)$, или, другими словами, умножению на -1 столбцов матрицы с номерами из некоторого набора индексов $J = \{j : v_j = -1\}$.

Тогда, предполагая, что для $\mathfrak{A}'$ нашелся вектор $\boldsymbol{\gamma}'$ из предложения 2.2, рассмотрим вектор $\boldsymbol{\gamma}$, $\gamma_i = v_i \cdot \gamma'_i$, у которого на -1 домножены компоненты с номерами из

J. Очевидно, что $A_{\mathfrak{A}} \cdot \boldsymbol{\gamma} = A_{\mathfrak{A}'} \cdot \boldsymbol{\gamma}' = \mathbf{0}$, т.е. система $\mathfrak{A}$ не полна. Противоречие доказывает утверждение. □

Предложение 3.11. *Транспозиция любой пары переменных в системе сохраняет ее полноту.*

Доказательство. Достаточно заметить, что операция эквивалентна некоторой перестановке σ столбцов матрицы системы. Далее доказательство дословно повторяет доказательство предложения 3.8. □

Из доказательств предложений данного раздела получаем два следующих утверждения.

Предложение 3.12. *Вышеперечисленные операции, а именно: замена функции на ее отрицание, замена переменной на ее отрицание, одновременное сложение функций системы с некоторой функцией, транспозиция переменных — сохраняют ранг матрицы системы, и, следовательно — тип полноты (сильная, слабая) для полных систем.*

Следствие 3.13. *Вышеперечисленные операции, а именно: замена функции на ее отрицание, замена переменной на ее отрицание, одновременное сложение функций системы с некоторой функцией, транспозиция переменных — сохраняют неполноту.*

Доказательство. Следует из утверждений 3.7, 3.8, 3.10, 3.11 и того, что все четыре операции обратимы. □

4. Структура множества полных систем функций в $P_2(2)$

В разделе будет определен набор классифицирующих операций и проведена классификация полных систем булевых функций от двух переменных.

Определение 4.1. Определим набор операций $\mathscr{F} = \{\mathrm{N_f}, \mathrm{N_v}, \mathrm{S}, \mathrm{T}\}$ над системой функций $\mathfrak{A} \subset P_2(n)$ следующим образом

1. Замена любой функции $f \in \mathfrak{A}$ на ее отрицание $\overline{f}$. Обозначение операции: $\mathrm{N_f}(f)$ (первые буквы от negation, function). Обозначение для преобразованной таким образом системы: $\mathrm{N_f}(\mathfrak{A}, f)$.

2. Замена всех вхождений произвольной переменной x_i в функции системы на ее $\overline{x}_i$. Обозначение для операции: $\mathrm{N_v}(x_i)$ (первые буквы от negation, variable). Обозначение для преобразованной таким образом системы: $\mathrm{N_v}(\mathfrak{A}, x_i)$.

3. Прибавление по модулю 2 одновременно ко всем функциям системы $\mathfrak{A}$ некоторой функцииf. Обозначение для операции: $\mathrm{S}(f)$ (первая буква sum). Обозначение для перобразованной таким образом системы: $\mathrm{S}(\mathfrak{A}, x_{i_1}x_{i_2}\dots x_{i_k})$ или $\mathfrak{A}\oplus x_{i_1}x_{i_2}\dots x_{i_k}$.

4. Транспозиция переменных x_i и x_j. Обозначение для операции: $\mathrm{T}(x_i, x_j)$ (первая буква transposition). Обозначение для преобразованной таким образом системы: $\mathrm{T}(\mathfrak{A}, x_i, x_j)$.

В разделе 3.3 были приведены утверждения, показывающие, что данные операции сохраняют сильную полноту (сильную неполноту) системы, следовательно, могут рассматриваться в качестве отношения эквивалентности на множестве всех сильно (слабо) полных систем, разбивая его на классы эквивалентности.

Системы $\mathfrak{A}$ и $\mathfrak{B}$ назовем *подобными*, или *эквивалентными*, если $\mathfrak{B}$ может быть получена из $\mathfrak{A}$ конечным количеством применений операций из $\mathscr{F}$. Класс систем, подобных $\mathfrak{A}$, обозначим $[\mathfrak{A}]_{\mathscr{F}}$.

Будем рассматривать сильно полные системы в $P_2(2)$. Такие системы имеют квадратные матрицы порядка $2^2 = 4$ (см стр. 9) и состоят из 4 функций. Для удобства в данном разделе переобозначим переменные: $x := x_1$, $y := x_2$.

4.1. Теорема о классификации сильно полных систем $P_2(2)$

Одним из основных результатов, полученных в данной работе, является следующая теорема.

Теорема 4.2. *Относительно набора операций $\mathscr{F} = \{\mathrm{N_f}, \mathrm{N_v}, \mathrm{S}, \mathrm{T}\}$ множество сильно полных систем в $P_2(2)$ разбивается на четыре попарно непересекающихся класса подобных систем B_1, B_2, B_3, B_4, где*

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

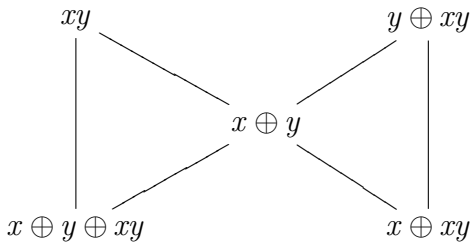
Лемма 4.3. *Пусть $\mathfrak{A}\subset P_2(2)$ — сильно полная система, $\mathfrak{A} = \{f_1, f_2, f_3, f_4\}$, где $f_1 = 0$ и $f_i \in T_0$, $i = 2, 3, 4$. Тогда найдется пара номеров $i \neq j$, $1 \leqslant i, j \leqslant 4$ такая, что либо $f_i = x \oplus f_j$, либо $f_i = y \oplus f_j$.*

Для удобства в данном разделе установим следующие обозначения для селекторных функций: $e_{x_1} = x$, $e_{x_2} = y$.

Доказательство. Если среди f_2, f_3, f_4 есть селекторные функции, то лемма очевидным образом выполняется в силу наличия тождественного нуля в системе $\mathfrak{A}$.

Пусть селекторных функций в системе нет. Если среди f_2, f_3, f_4 нашлась пара функций из утверждения доказываемой леммы, то лемма доказана.

Допустим, что таких пар нет. На графе для наглядности показаны пары функций от двух переменных, сохраняющих константу 0, не обладающих свойством $f_i = e_{x_k} \oplus f_j$:



Из графа видно, что тройками функций, среди которых нет искомых пар, являются $\{xy, x \oplus y, x \oplus y \oplus xy\}$ и $\{y \oplus xy, x \oplus xy, x \oplus y\}$. В первом случае матрица системы вырождена:

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

Во втором случае, аналогично:

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

Противоречие с сильной полнотой доказывает невозможность предположения о несуществовании искомых пар, и, следовательно, лемму. □

Справедливо следующее утверждение

Лемма 4.4. *Пусть $\mathfrak{A} \subset P_2(2)$ — сильно полная система. Тогда $\mathfrak{A}$ принадлежит одному из четырех множеств*

$$\begin{aligned} B_1 &= \Big[\{0, x, y, xy\}\Big]_{\mathscr{F}} & B_2 &= \Big[\{0, x, y, x \oplus y\}\Big]_{\mathscr{F}} \\ B_3 &= \Big[\{0, x, xy, y \oplus xy\}\Big]_{\mathscr{F}} & B_4 &= \Big[\{0, x, xy, x \oplus y \oplus xy\}\Big]_{\mathscr{F}} \end{aligned} \tag{4.1}$$

Доказательство. *Шаг 1.* Операциями 1 и 3 мы можем преобразовать систе-

му к системе $\mathfrak{A}_1$, в которой первая функция будет равна 0, а остальные три — сохранять 0. Системе $\mathfrak{A}_1$ соответствует метрица

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

Шаг 2. По лемме 4.3 среди оставшихся трех функций найдется пара функций либо вида $(x \oplus g, g)$, либо вида $(y \oplus g, g)$. Если имеет место второе, путем переименования переменных преобразуем к первому. Обозначим результат как $\mathfrak{A}_2$.

Шаг 3. Прибавив ко всем функциям из $\mathfrak{A}_2$ функцию g из предыдущего шага, получим систему $\mathfrak{A}_3 = \{0, x, *, *\}$ с матрицей

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

В силу невырожденности матрицы среди оставшихся двух функций обязательно содержится одна из функций, равных 1 на наборе $(x, y) = (0, 1)$ (что соответствует (-1) во втором столбце матрицы): y, $x \oplus y$, $y \oplus xy$, $x \oplus y \oplus xy$.

Рассмотрим подслучаи:

1) Есть функция y: матрица имеет вид

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

учитывая невырожденность, заключаем, что для последней строки возможны следующие случаи:

$\tau(\widetilde{\chi}_f)$	$f(x, y)$
$(1, 1, 1, -1)$	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) $(1, 1, 1, -1)$, функция xy: система $\{0, x, y, xy\}$ лежит в B_1.

1.2) $(1,-1,-1,1)$, функция $x \oplus y$: система $\{0, x, y, x \oplus y\}$ лежит в B_2.

1.3) $(1,1,-1,1)$, функция $x \oplus xy$, имеем цепочку замен

$$\{0, x, y, x \oplus xy\} \xrightarrow{\mathrm{N_v}(x)} \{0, \overline{x}, y, xy\} \xrightarrow{\mathrm{N_f}(x)} \{0, x, y, xy\}$$

исходная система лежит в B_1.

1.4) $(1,-1,1,1)$, функция $y \oplus xy$ — аналогично, исходная система лежит в B_1.

1.5) $(1,-1,-1,-1)$, функция $x \oplus y \oplus xy$:

$$\{0, x, y, x \oplus y \oplus xy\} \xrightarrow{\oplus y} \{0, x, y, x \oplus xy\}$$

и задача сведена к пункту 1.3), значит, исходная система лежит в B_1.

2) Есть функция $x \oplus y$: матрица имеет вид

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

Для последней строки возможны следующие случаи (при которых матрица невырождена):

$\tau(\widetilde{\chi}_f)$	$f(x,y)$
$(1,-1,1,-1)$	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) $(1,-1,1,-1)$, функция y — случай разобран в 1.2)

2.2) $(1,1,-1,1)$, функция $x \oplus xy$:

$$\{0, x, x \oplus y, x \oplus xy\} \xrightarrow{\oplus x} \{0, x, y, xy\}$$

тем самым попали в множество B_1.

2.3) $(1,-1,1,1)$, функция $y \oplus xy$:

$$\{0, x, x \oplus y, y \oplus xy\} \xrightarrow{\oplus x} \{0, x, y, x \oplus y \oplus xy\}$$

и задача сведена к 1.5), попали в B_1.

2.4) $(1,1,1,-1)$, функция xy:

$$\{0, x, x \oplus y, xy\} \xrightarrow{\oplus x} \{0, x, y, x \oplus xy\}$$

и задача сведена к 1.3), попали в B_1.

2.5) $(1,-1,-1,-1)$, функция $x \oplus y \oplus xy$:

$$\{0, x, x \oplus y, x \oplus y \oplus xy\} \xrightarrow{\oplus x} \{0, x, y, y \oplus xy\}$$

и задача сведена к 1.4), множество B_1.

3) В системе есть функция $x \oplus xy$. Матрица имеет вид

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

Аналогично, из условия невырожденности следует, что оставшаяся строка может прнимать следующие значения:

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

3.1) $(1,-1,1,-1)$, функция y — разобрано в случае 1.4), попали в множество B_1.

3.2) $(1,-1,-1,1)$, функция $x \oplus y$ — разобрано в случае 2.3), попали в множество B_1.

3.3) $(1,1,-1,1)$, функция $x \oplus xy$:

$$\{0, x, x \oplus xy, y \oplus xy\} \xrightarrow{\oplus x} \{0, x, xy, x \oplus y \oplus xy\}$$

попали в множество B_4.

3.4) $(1,1,1,-1)$, функция xy: система $\{0, x, y \oplus xy, xy\}$ лежит в множестве B_3.

4) В системе есть функция $x \oplus y \oplus xy$. Матрица имеет вид

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

В силу невырожденности матрицы последняя строка может принимать следующие значения:

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

4.1) $(1,-1,1,-1)$, функция y — случай разобран в 1.5), множество B_1.

4.2) $(1,-1,-1,1)$, функция $x \oplus y$ — случай разобран в 2.5), множество B_1.

4.3) $(1,1,-1,1)$, функция $x \oplus xy$:

$$\{0, x, x \oplus y \oplus xy, x \oplus xy\} \xrightarrow{\oplus x} \{0, x, xy, y \oplus xy\}$$

система лежит в B_3.

4.4) $(1,1,1,-1)$, функция xy: система $\{0, x, x \oplus y \oplus xy, xy\}$ лежит в B_4.

Разобраны все возможные случаи, лемма доказана. □

В доказанной лемме не утверждалось, что множества B_1, B_2, B_3, B_4 не пересекаются. Имеет место следующий факт.

Лемма 4.5. *Множества B_1, B_2 и $C = B_3 \cup B_4$ попарно не пересекаются.*

Доказательство. Пусть $\varkappa_1(\mathfrak{A}) := \min(s, 2^n - s)$, где s — суммарное количество конъюнкций степени n (максимально возможной) во всех полиномах Жегалкина функций из $\mathfrak{A} \subset P_2(n)$. Например, для системы $\mathfrak{A} = \{x, xy, x \oplus xy, y \oplus xy\} \subset P_2(2)$ имеем $\varkappa_1(\mathfrak{A}) = \min(3,1) = 1$.

Покажем, что $\varkappa_1(\mathfrak{A})$ является инвариантом множеств B_1, B_2, C относительно операций из $\mathscr{F}$.

Действительно:

а) $\mathrm{N_f}(f)$ есть прибавление единицы к некоторой функции из $\mathfrak{A}$, и, следовательно, числа рассматриваемых конъюнкций не изменяет, а $\varkappa_1(\mathfrak{A})$ тем более.

б) $\mathrm{N_v}(x_i)$ есть замена всех вхождений x_i на $(x_i \oplus 1)$. Очевидно, количества конъюнкций макисмальной степени в полиноме Жегалкина она не изменяет (пользу-

емся максимальностью степени), $\varkappa_1(\mathfrak{A})$ тем более.

в) $\mathrm{S}(g)$ может изменить число конъюнкций максимальной степени только в одном случае — если g содержит таковую в своем полиноме Жегалкина. Но тогда если в полиноме Жегалкина функций системы было s таких конъюнкций, то в новой системе их будет $(2^n - s)$, так что $\varkappa_1(\mathfrak{A}) = \varkappa_1(\mathfrak{A}')$.

г) $\mathrm{T}(x_i, x_j)$, очевидно, не изменяет числа конъюнкций максимальной степени, а $\varkappa_1(\mathfrak{A})$ — тем более.

Для случая $\mathfrak{A} \subset P_2(2)$ число $\varkappa_1(\mathfrak{A})$ может принимать значения $0, 1, 2$. Остается заметить, что

$$\varkappa_1(\mathfrak{A} \mid \mathfrak{A} \in B_1) = 1, \qquad \varkappa_1(\mathfrak{A} \mid \mathfrak{A} \in B_2) = 0, \qquad \varkappa_1(\mathfrak{A} \mid \mathfrak{A} \in C) = 2,$$

что доказывает лемму. □

Замечание 4.6. Из доказательства следует, что суммарное число конъюнкций xy в полиноме Жегалкина для систем из B_3 и B_4 всегда равно 2.

Лемма 4.7. $B_3 \cap B_4 = \varnothing$.

Доказательство. Рассмотрим $\mathfrak{A} \subset P_2(2)$ с функциями в виде полиномов Жегалкина. Пусть $\varkappa_2(\mathfrak{A})$ — четность суммарного числа p вхождений символов переменных в полиноме Жегалкина функций из $\mathfrak{A}$

$$\varkappa_2(\mathfrak{A}) = \begin{cases} 1, & \text{если } p \text{ нечетно} \\ 0, & \text{если } p \text{ четно} \end{cases}$$

Утверждается, что для множеств B_3 и B_4 эта величина инвариантна относительно операций из $\mathscr{F}$.

Действительно:

а) $\mathrm{N_f}(f)$ есть прибавление 1 к полиному Жегалкина функции f и, следовательно, количества символов переменных не изменяет.

б) $\mathscr{F}(x_i)$ есть замена вхождений x_i на $(x_i \oplus 1)$. Без ограничений общности пусть $x_i = x$. Число вхождений x в полиномах Жегалкина при такой операции не меняется. Число вхождений y меняется только за счет перехода конъюнкций xy в $(x \oplus 1)y = xy \oplus y$. По замечанию 4.6 число таких конъюнкций в полиномах Жегалкина системы четно, значит, число вхождений переменной y изменится на четное число, так что $\varkappa_2(\mathfrak{A}) = \varkappa_2(\mathfrak{A}')$.

в) $\mathrm{S}(g)$ изменяет количество вхождений всех переменных на четное число, т.к. в системе $\mathfrak{A} \subset P_2(2)$ 4 функции.

г) $\mathrm{T}(x, y)$ есть замена вхождений x на y и наоборот, очевидно, сохраняет $\varkappa_2(\mathfrak{A})$.

Для доказательства леммы осталось заметить, что

$$\varkappa_2(\mathfrak{A} \mid \mathfrak{A} \subset B_3) = 0, \qquad \varkappa_2(\mathfrak{A} \mid \mathfrak{A} \subset B_4) = 1 \qquad \square$$

Доказательство (Теоремы 4.2). Утверждения лемм 4.4, 4.5, 4.7 доказывают теорему 4.2. $\square$

4.2. Эквивалентность понятий полноты и сильной полноты в $P_2(2)$

Вопрос о соотношении понятий полноты и сильной полноты в пространстве $P_2(2)$ раскрывается следующей теоремой.

Теорема 4.8. *Пусть $\mathfrak{A} \subset P_2(2)$. Для того, чтобы система $\mathfrak{A}$ была полна, необходимо и достаточно, чтобы $\mathfrak{A}$ была сильно полна.*

Другими словами, это значит, что в пространстве $P_2(2)$ *отсутствуют слабо полные системы.* Забегая вперед, скажем, что этот факт весьма примечателен тем, что он в некотором смысле обособляет случай $P_2(n)$ для $n = 2$.

Доказательство. *Достаточность.* Очевидно.

Необходимость. Операциями из $\mathscr{F}$ без изменения типа полноты (как показано в разделе 3.3) можно привести систему $\mathfrak{A}$ к эквивалентной ей системе $\mathfrak{A}_1$ с матрицей

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

Необходимо проверить, что если матрица A вырождена, то система не слабо полна, т.е. существует вектор $\boldsymbol{\gamma}$ с компонентами из $\{\pm 1, 0\}$, такой что

$$A \cdot \boldsymbol{\gamma} = \mathbf{0} \tag{4.2}$$

Так как ранг вырожденной матрицы не превышает 3, возможны следующие случаи:

1) $\operatorname{rk} A = 1$: вектор $\boldsymbol{\gamma} = (1, 1, -1, -1)^T$, очевидно, удовлетворяет уравнению (4.2).

2) $\operatorname{rk} A = 2$: вычитанием первой строки из остальных (и, возможно, перестанов-

кой столбцов) матрица системы (4.2) сводится к виду

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

где $\alpha_i \in \{-2, 0\}$. Нетрудно видеть, что если оба α_i ненулевые, то вектор $\boldsymbol{\gamma} = (0, 0, 1, -1)^T$ удовлетворяет уравнению (4.2).

3) $\operatorname{rk} A = 3$: нетрудно видеть, вычитанием первой строки из последующих, затем вычитанием второй строки из последующих можно получить следующие матрицы (0 в последней строке имеет смысл, если в матрице больше трех строк).

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

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

В случае матрицы A'_1 в зависимости от значения α_1 либо $\boldsymbol{\gamma} = (0, 1, -1, 0)^T$, либо $\boldsymbol{\gamma} = (1, 0, -1, 0)^T$ удовлетворяют (4.2).

В случае матрицы A'_2: если только один из β_i равен нулю, то получаем случай, аналогичный предыдущему. Если оба β_i ненулевые и одного знака, то из построения матрицы (вычитанием строк) очевидно, что $\alpha_1 = \alpha_2$, тогда $\boldsymbol{\gamma} = (0, 0, 1, -1)^T$ удовлетворяет (4.2). Если же β_i разных знаков, то без ограничения общности из построения матрицы $\alpha_1 = 0$, $\alpha_2 = -2$ и $\boldsymbol{\gamma} = (1, 1, -1, -1)^T$ удовлетворяет (4.2).

В случае матрицы A'_3: $\boldsymbol{\gamma} = (1, -1, 0, 0)^T$ удовлетворяет (4.2).

Необходимость доказана. □

4.3. Теорема о классификации полных систем в $P_2(2)$

Следствием теоремы 4.2 и теоремы 4.8 является

Теорема 4.9. *Относительно набора операций $\mathscr{F} = \{\mathrm{N_f}, \mathrm{N_v}, \mathrm{S}, \mathrm{T}\}$ множество полных систем в $P_2(2)$ разбивается на четыре попарно непересекающихся класса подобных систем B_1, B_2, B_3, B_4, где*

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

5. О соотношении понятий полноты и сильной полноты

Теорема 4.8 дает ответ на вопрос, как связано понятие полноты и сильной полноты в $P_2(2)$. Для пространств более высоких размерностей ($n \geqslant 3$) ответ будет дан в этом разделе.

5.1. О неэквивалентности понятия полноты и сильной полноты в пространстве $P_2(3)$

Приведем пример, показывающий, что в пространстве $P_2(3)$ существуют слабо полные системы (или, что то же самое, что понятия полноты и сильной полноты не тождественны в $P_2(3)$).

Предложение 5.1. *В пространстве $P_2(3)$ существуют слабо полные системы функций.*

Доказательство. Рассмотрим систему $\mathfrak{A}$, состоящую из 7 функций и имеющую матрицу

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

Такая система, очевидно, не сильно полна. Докажем, что она полна.

Через A' обозначим подматрицу матрицы A, которая образована первыми семью столбцами, и докажем, что A' невырождена.

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

Вопрос о невырожденности A' сводится к аналогичному для главного минора 6-го порядка, который, очевидно, невырожден, таким образом, невырождена матрица A'.

Из только что доказанного следует, что $\operatorname{rk} A = 7$, причем вектор-столбцы, составляющие A', являются базисом в $\mathbb{R}^7$. Следовательно, вектор-столбец $(1,1,1,1,1,1,1)^T$, стоящий в последнем столбце матрицы A, выражается через первые семь однозначно.

Остается заметить, что

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

Таким образом, решениями однородной системы с матрицей A являются векторы

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

и только они, что исключает существование нетрививального вектора решений с компонентами из $\{1,-1,0\}$. Условие критерия полноты (предложение 2.2) выполняется, следовательно, система $\mathfrak{A}$ полна. □

В функциональном виде данный пример слабо полной системы будет представлен ниже (раздел 5.3), после рассмотрения общего случая.

5.2. О неэквивалентности понятия полноты и сильной полноты в пространстве $P_2(n)$, $n \geqslant 3$

Пример, представленный в предложении 5.1, является частным случаем более общей конструкции, которую мы приведем ниже. Предпошлем ей несколько вспомогательных утверждений.

Лемма 5.2. *Квадратная матрица $A = (a_{ij})_{i,j=1}^N$, такая, что*

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

где $\lambda \neq 0$, невырождена.

Доказательство. Не ограничивая общности положим $\lambda = 1$. Пусть матрица вырождена. Тогда одна из строк линейно выражается через остальные. Пусть, не ограничивая общности, первая строка линейно выражается через последующие с коэффициентами $k_2, k_3, \ldots, k_N$. Рассматривая поочередно компоненты этих строк, получим

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

Вычитая из первого уравнения поочередно последующие, получаем $k_i = -1$, $i = 2, \ldots, N$, что, очевидно, неверно. Значит, решений не существует, что доказывает утверждение. □

Лемма 5.3. *Пусть $N \geqslant 5$. Тогда существует матрица $A = (a_{ij})$ размера $(N-1) \times N$ такая, что задаваемая ей однородная линейная система не имеет среди решений векторов с компонентами из $\{1, -1, 0\}$.*

Доказательство. Зададим A размера $(N-1) \times N$ следующим образом:

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

Таким образом, матрица A выглядит так:

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

Обозначим через A' подматрицу размера $(N-1) \times (N-1)$, образованную первыми $(N-1)$ столбцами матрицы A.

Матрица A' невырождена. Действительно, после сложения с первой строкой каждой из последующих, получим матрицу вида

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

где подматрица A'' размера $(N-2)\times(N-2)$ удовлетворяет условиям утверждения 5.2 с $\lambda = 2$ и, следовательно, также невырождена. Невырожденность A' доказана.

Таким образом, столбцы матрицы A' образуют базис в $\mathbb{R}^{N-1}$, и, следовательно, последний столбец (единичный) матрицы A линейно выражается через первые $(N-1)$ столбцов единственным образом.

Осталось заметить, что коэффициенты такого представления одинаковы и равны $1/(N-3)$, откуда следует, что нетривиальной линейной комбинации столбцов матрицы A с коэффициентами из $\{1,-1,0\}$ не существует, так как все вектора коэффициентов такой линейной комбинации имеют вид

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

Искомая матрица построена. □

Замечание 5.4. Отметим, что условие $N\geqslant 5$ существенно — без него неверным становится самый последний шаг рассуждения.

Теорема 5.5. *Пусть $n\geqslant 3$. Тогда в пространстве $P_2(n)$ существуют слабо полные системы булевых функций.*

Доказательство. В условиях теоремы выполняется соотношение $2^n\geqslant 8$, следовательно, по лемме 5.3 (где $N=2^n$) можно построить матрицу с 2^n стобцами и ранга меньшего, чем 2^n, состоящую из ± 1, для которой выполняется критерий полноты (предложение 2.2).

Система булевых функций, которой соответствует построенная матрица, слабо полна по определению. Теорема доказана. □

Теоремы 4.8 и 5.5 дают ответ на вопрос, является ли достаточное условие полноты системы в $P_2(n)$

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

необходимым условием ее полноты. Для $n=2$, таким образом, ответ положительный, для $n\geqslant 3$ ответ отрицательный.

5.3. Примеры слабо полных систем

Приведем пример слабо полной системы булевых функций.

В пространстве $P_2(3)$ слабо полная система $\mathfrak{A}$, задаваемая матрицей из утверждения 5.1, имеет вид

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

Операциями из набора операций $\mathscr{F}$ над приведенной выше системой можно получить (см. предложение 3.12) целый класс подобных ей слабо полных систем.

В случае произвольного $n \geqslant 3$, как видно из примера, построенного при доказательстве теоремы 5.5, слабо полная система $\mathfrak{B}$ в пространстве $P_2(n)$ состоит из всех всех конъюнкций n переменных, кроме одной:

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

6. Связь с матрицами Адамара

В разделе рассматривается связь полных систем булевых функций с так называемыми *матрицами Адамара*.

Квадратная матрица $H = (h_{ij})_{i,j=1}^{k}$, $h_{ij} \in \{-1, 1\}$ называется *матрицей Адамара*, если ее столбцы (или, что эквивалентно, строки) ортогональны, т.е.

$$HH^T = kI$$

Подробнее о матрицах Адамара см. [4], [5].

Матрицы Адамара играют важную роль в теории кодирования (см., например, [4]), например, с их помощью строятся коды, лежащие на границе Плоткина ([4], теорема 2.0.5).

Необходимым условием того, что квадратная матрца — Адамарова, является кратность ее порядка четырем (см. [5]). Тем не менее, к настоящему моменту не найдено методов построения адамаровых матриц любого порядка, кратного четырем.

Ярковыраженная связь между матрицами некоторых сильно полных систем и матрицами Адамара делает возможным предположение о существовании методов построения новых матриц Адамара, использующих описание на языке сильно полных систем булевых функций.

Пусть $n \geqslant 1$. Приведем эквивалентное определение того, что матрица системы $\mathfrak{A}$, состоящей из 2^n булевых функций из $P_2(n)$ — адамарова.

Предложение 6.1. *Матрица $A_{\mathfrak{A}}$ размера $2^n \times 2^n$ — адамарова тогда и только тогда, когда $\rho(f_1, f_2) = 2^{n-1}$ для любой пары функций $f_1 \neq f_2$, $f_1, f_2 \in \mathfrak{A}$.*

Доказательство. Заметим, что для любой пары $\mathbf{v}_1, \mathbf{v}_2$ (в том числе совпадающих) строк матрицы $A_{\mathfrak{A}}$, соответствующих функциям f_1, f_2, справделиво выражение для их скалярного произведения

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

откуда, используя свойство адамаровых матриц ($(\mathbf{v}_1, \mathbf{v}_2) = 0$), получаем утверждение. □

В силу определения адамаровых матриц, имеет смысл рассматривать их связь только с сильно полными системами, так как любая система, имеющая адамарову матрицу, должна иметь полный ранг.

Предложение 6.2. *Пусть $\mathfrak{A}$ — система булевых функций с квадратной матрицейразмера $2^n \times 2^n$. Тогда операции из $\mathscr{F}$ (см. определение 4.1) не изменяют свойства адамаровости матрицы $A_{\mathfrak{A}}$.*

Доказательство. Операции $\mathrm{N_f}$, $\mathrm{N_v}$, S, T эквивалентны соответственно умножению некоторой строки $A_{\mathfrak{A}}$ на -1, некоторой перестановке столбцов $A_{\mathfrak{A}}$, умножению некоторого набора столбцов $A_{\mathfrak{A}}$ на -1, некоторой перестановке столбцов $A_{\mathfrak{A}}$.

Все упомянутые операции сохраняют свойство ортогональности строк. □

Следствие 6.3. *В любом замкнутом относительно $\mathscr{F}$ классе систем в $P_2(n)$, $n \geqslant 2$ все системы одновременно имеют либо адамаровы матрицы, либо не адамаровы.*

Напомним, что, согласно теореме 4.2 множество всех сильно полных систем в $P_2(2)$ разбивается на четыре класса эквивалентности относительно $\mathscr{F}$:

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

Так как этими классами описываются все сильно полные системы, то, в силу того, что адамарова матрица также описывает сильно полную систему, некотороые из этих классов обязаны иметь адамаровы матрицы. Нетрудно видеть, что это класс

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

Тензорным (*кронекеровым*) *произведением* (см. [4]) $A \otimes B$ матриц $A_{n\times m}$ и $B_{k\times l}$ называется блочная матрица

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

размера $nk \times ml$.

Следующее предложение доказано в [4].

Предложение 6.4. *Если A и B — матрицы Адамара, то $A \otimes B$ — тоже матрица Адамара.*

В работе [3] было дано довольно сложное доказательство того факта, что система $L^{(n)} \cap T_0^{(n)}$ — сильно полная. Дадим более простое доказательство.

Предложение 6.5. *Система $\mathfrak{A}_0(n) = L^{(n)} \cap T_0^{(n)} \subset P_2(n)$, $n \geqslant 2$ является сильно полной.*

Доказательство. Система $\mathfrak{A}_0(2)$, порождающая класс B_2, удовлетворяет утверждению. Как отмечалось выше, она имеет адамарову матрицу (обозначим ее A_2). В силу утверждения 6.4 операция тензорного произведения ее матрицы с матрицей

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

примененная $k \geqslant 0$ раз, порождает адамарову матрицу $C = X^{\otimes k} \otimes A_2$ размера 2^{k+2}, и, следовательно, задает некоторую сильно полную систему в $P_2(n)$, $n = k + 2$. Докажем, что это система есть $\mathfrak{A}_0(n)$.

Для этого остается заметить, что операция тензорного произведения матрицы X с матрицей Y_s любой системы $\mathfrak{B}(s)$ функций s переменных $x_1, x_2, \ldots, x_s$ дает матрицу, имеющую вид

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

которая соответствует системе функций $(s+1)$ переменных

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

где $\mathfrak{B}'(s+1) = \mathfrak{B}(s)$ (не зависит от новой переменной x_0) и $\mathfrak{B}''(s+1) = x_0 \oplus \mathfrak{B}(s)$.

Очевидно, что, строя таким образом новые системы и начиная с $\mathfrak{A}_0(2)$, будем на каждом шаге получать системы, состоящие из всех линейных функций, сохра-

няющих ноль. □

Возникает вопрос — только ли класс, порождаемый системой $\mathfrak{A}_0(n)$, обладает адамаровыми матрицами.

Напомним, что *нормализованной* матрицей Адамара называется матрица Адамара с единичными первой строкой и первым столбцом. В терминах матриц систем булевых функций — это матрицы систем, состоящих из функций, сохраняющих ноль, среди которых есть ноль.

Две адамаровы матрицы называются *эквивалентными*, если одна из них получена из другой путем применения преобразования из группы G, которую определим как группу, состоящую из преобразований матриц, порождающихся инверсиями (т.е. умножениями на -1) произвольной строки или столбца и перестановками пары строк или пары столбцов.

В книге [5] указано, что, вообще говоря, среди нормализованных матриц Адамара есть неэквивалентные (начиная с порядка 16, пример дан в Приложении). Например, попарно неэквивалентных матриц Адамара порядка 16 существует пять (см. [2]).

Имеет место следующее утверждение.

Предложение 6.6. *Пусть $n \geqslant 4$, $\mathfrak{A}_0 \subset P_2(n)$ — система из утверждения* 6.5. *Существует система $\mathfrak{B} \subset P_2(n)$, не подобная системе $\mathfrak{A}_0$ и имеющая адамарову матрицу.*

Доказательство. Заметим, что операции из $\mathscr{F}$, будучи рассмотренными как преобразования матриц систем, порождают некоторую подгруппу (обозначим ее F) группы G. Также отметим, что, согласно условию, рассматриваемые матрицы имеют порядок 2^n.

Докажем от противного. Пусть любая система $\mathfrak{B} \subset P_2(n)$, имеющая адамарову матрицу, подобна $\mathfrak{A}_0$. Тогда, по определению подобия, $A_{\mathfrak{B}} = f_k \circ \ldots \circ f_1 A_{\mathfrak{A}_0}$, где f_i, $1 \leqslant i \leqslant k$ — операции из множества $\mathscr{F}$, рассмотренные как операции над матрицами.

Но так как $f_k \circ \ldots \circ f_1 \in F \subset G$, то $f_k \circ \ldots \circ f_1 \in G$. Значит, любая адамарова матрица порядка 2^n, $n \geqslant 4$ эквивалентна матрице системы $\mathfrak{A}_0$, что неверно, согласно замечанию о количестве классов эквивалентности матриц Адамара, предваряющему доказываемое утверждение. □

Открыт вопрос о том, все ли матрицы Адамара порядка 2^3 порождаются системами из класса $\left[L^{(3)} \cap T_0^{(3)}\right]_{\mathscr{F}}$. Известно (см., например, [2]), что существует ровно один класс эквивалентности матриц Адамара порядка 8, однако пока неизвестно, равен ли этот класс классу подобия (в матричном виде) системы $\left[L^{(3)} \cap T_0^{(3)}\right]_{\mathscr{F}}$.

Таким образом, одна из задач на этом пути — определить, является ли группа F собственной подгруппой G (в этом случае эквивалентные матрицы Адамара могут соответствовать неподобным системам), или же $G = F$ (в этом случае эквивалентность в смысле матриц Адамара равносильна подобию в смысле систем).

7. Замечания о дальнейших путях исследований, постановки задач

7.1. О «проекциях» полных систем из $P_2(n+1)$ в $P_2(n)$

Предложение 7.1. *Пусть дана сильно полная система функций $\mathfrak{A}_{n+1}$ в пространстве $P_2(n+1)$. Тогда подстановка константы вместо некоторой переменной во все функции системы приведет к системе $\mathfrak{A}_n \subset P_2(n)$, которая является сильно полной.*

Доказательство. Без ограничения общности будем подставлять константу 0 (для константы 1 рассуждения аналогичные).

Надо доказать, что прямоугольная подматрица матрицы $A_{\mathfrak{A}_{n+1}}$, (имеющей по условию полный ранг 2^{n+1}), образованная первыми 2^n ее столбцами, будет иметь максимальный возможный ранг 2^n.

Представив строки матрицы $A_{\mathfrak{A}_{n+1}}$ как векторы в пространстве $\mathbb{R}^{2^{n+1}}$, образующие его базис, получим, что строки описанной выше подматрицы суть проекции этих векторов на некоторое подпространство $\mathbb{R}^{2^n}$.

Но очевидно, что проекции векторов базиса некоторого линейного пространства V на его подпространство W образуют систему векторов, линейная оболочка которых есть W. В нашем случае $V = \mathbb{R}^{2^{n+1}}$, $W = \mathbb{R}^{2^n}$. Значит, в спроектированной системе векторов можно выбрать 2^n линейно независимых, то есть ранг рассматриваемой подматрицы равен 2^n. □

7.2. Примеры получения полных систем более высоких порядков

Предложение 7.2. *Если система $\mathfrak{A} \subset P_2(n)$ сильно полна, то система $\mathfrak{A}' = \mathfrak{A} \cup (\mathfrak{A} \oplus x_{n+1}) \subset P_2(n+1)$ также сильно полна. Под $\mathfrak{A} \oplus x_{n+1}$ понимается система, состоящая из функций, к каждой из которых прибавлена функция x_{n+1}.*

Доказательство. Доказательство очевидно, если рассмотреть матрицу полученной системы. □

Таким образом, из порождающих систем классов B_1, B_2, B_3, B_4 получаем в $P_2(3)$ сильно полные системы следующего вида:

$$\begin{array}{llllllll}
\{0, & x, & y, & z, & xy, & x\oplus z, & y\oplus z, & xy\oplus z\}\\
\{0, & x, & y, & z, & x\oplus y, & x\oplus z, & y\oplus z, & x\oplus y\oplus z\}\\
\{0, & x, & z, & x\oplus z, & xy, & xy\oplus y, & xy\oplus z, & xy\oplus y\oplus z\}\\
\{0, & x, & z, & x\oplus z, & xy, & xy\oplus z, & xy\oplus x\oplus y, & xy\oplus x\oplus y\oplus z\}
\end{array}$$

Нетрудно видеть, что эти системы, будучи полученными из неподобных систем прибавлением новой переменной, порождают разные классы подобия в пространстве $P_2(3)$.

Указанный способ — общий для любой сильно полной системы и любого числа переменных n. Специальный же вид системы B_1 наводит на мысль о том, что ее можно распространить на более высокие размерности как $K_{(n)}$.

Действительно, система

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

сильно полна, как доказано в [3].

Для дальнейших замечаний введем определение которое уже использовалось при доказательстве некоторых утсверждений (см. стр. 20), а именно, обозначим $\varkappa_1(\mathfrak{A}) := \min(s, 2^n - s)$, где s — суммарное количество конъюнкций степени n (максимально возможной) во всех полиномах Жегалкина функций из $\mathfrak{A} \subset P_2(n)$. Например, для системы $\mathfrak{A} = \{x, xy, x\oplus xy, y\oplus xy\} \subset P_2(2)$ имеем $\varkappa_1(\mathfrak{A}) = \min(3,1) = 1$.

В доказательстве утверждения 4.5 показано, что для любой системы из $P_2(n)$ параметр $\varkappa_1$ является инвариантным относительно преобразований из $\mathscr{F}$.

Обратим внимание, что из пяти указанных систем первые четыре имеют параметр $\varkappa_1 = 0$, пятая имеет $\varkappa_1 = 1$.

Систему с $\varkappa_1 = 2$ находим, отталкиваясь от системы, порождающей класс B_3, с помощью домножения ее на z, присоединения селекторной функции z и объединения результата с исходной системой:

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

Другой пример сильно полной системы с $\varkappa_1 = 2$ получаем, отталкиваясь от системы, порождающей класс B_4:

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

Замечание 7.3. Аналогичным образом порожденная из B_2 система

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

также сильно полна.

Последние примеры наводят на гипотезу: если сильно полная система в $\mathfrak{A} \subset$ $\subset P_2(n)$ содержит нуль, сохраняет нуль, то система $\mathfrak{A}' = \mathfrak{A} \cup (\mathfrak{A} \,\&\, x_{n+1}) \cup \{x_{n+1}\} \subset$ $\subset P_2(n+1)$ также сильно полна.

Замечание 7.4. Можно заметить, что в классе подобных систем всегда содержится система, сохраняющая нуль. Таким образом, для любой системы булевых функций найдется подобная ей такая система, что к ней применимо предложение 7.5.

Назовем систему, содержащую нуль и сохраняющую нуль, *нормализованной*. У любой системы существует подобная ей нормализованная.

Предложение 7.5. *Пусть система $\mathfrak{A} \subset P_2(n)$ сильно полна и является нормализованной. Тогда система $\mathfrak{A}' = \mathfrak{A} \cup \{\mathfrak{A} \,\&\, x_{n+1}\} \cup \{x_{n+1}\} \subset P_2(n+1)$ также сильно полна.*

Доказательство. Проведем доказательство в матричном виде. Получим матрицу системы $\mathfrak{A}'$. Объединив матрицы для $\mathfrak{A}$, $\mathfrak{A} \,\&\, x_{n+1}$ и $\{x_{n+1}\}$ в $P_2(n+1)$, получим матрицу:

$$B = \left(\begin{array}{ccc|ccc} \multicolumn{3}{c|}{A} & \multicolumn{3}{c}{A} \\ \hline \multicolumn{3}{c|}{0} & \multicolumn{3}{c}{A} \\ \hline 1 & \dots & 1 & -1 & \dots & -1 \end{array}\right),$$

где невырожденная квадратная матрица A порядка 2^n есть матрица системы $\mathfrak{A}$, содержащая строку $(1, \dots, 1)$, так как система $\mathfrak{A}$ нормализована и содержит функцию 0.

Матрица B имеет 2^{n+1} столбцов и $2^{n+1}+1$ строк, две из которых равны $(1, \dots, 1)$ (они соответствуют двум функциям 0 в системе $\mathfrak{A}'$). Удалив одну из этих функций без ущерба системе, получим матрицу системы $\mathfrak{A}'$, равную

$$A' = \left(\begin{array}{ccc|ccc} 1 & \dots & 1 & -1 & \dots & -1 \\ \hline 1 & \dots & 1 & 1 & \dots & 1 \\ \hline \multicolumn{3}{c|}{\widetilde{A}} & \multicolumn{3}{c}{\widetilde{A}} \\ \hline \multicolumn{3}{c|}{1} & \multicolumn{3}{c}{\widetilde{A}} \end{array}\right),$$

где $\widetilde{A}$ — результат удаления из матрицы A строки $(1, \dots, 1)$. $\widetilde{A}$ имеет ранг $2^n - 1$.

Теперь докажем от противного, что A' невырождена. Пусть существует набор коэффициентов $\mu_1, \ldots, \mu_{2^{n+1}}$ такой, что линейная комбинация вектор-строк $\mathbf{a}_i$ матрицы A' с этими коэффициентами равна 0:

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

Разобъем множество номеров строк матрицы A' на три множества: $\Omega_1 = \{1, 2\}$, $\Omega_2 = \{3, \ldots, 3 + 2^n\}$ и $\Omega_3 = \{(3 + 2^n) + 1, \ldots, 2^{n+1}\}$. Обозначим за $\mathbf{x}_i$ и $\mathbf{y}_i$ подвекторы вектора $\mathbf{a}_i$, образованные, соответственно, первыми 2^n и последними 2^n его координатами. Тогда очевидны следующие факты:

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

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

Наконец, если среди μ_i, $i \in \Omega_3$ есть ненулевой коэффициент, то

$$\sum_{\Omega_1 \cup \Omega_3} \mu_i \mathbf{y}_i =: \mathbf{y} \neq (y, \ldots, y) \quad \text{ни для какого } y \in \mathbb{R}. \tag{7.3}$$

Последнее следует из того, что каждый из векторов $\mathbf{y}_1, \mathbf{y}_2$ имеет попарно равные компоненты, а никакая линейная комбинация строк матрицы $\widetilde{A}$ не может быть вектором с попарно одинаковыми компонентами, так как $\widetilde{A}$ — результат удаления из невырожденной матрицы A строки $(1, \ldots, 1)$.

Из выражений (7.1)–(7.3) следует, что если среди μ_i, $i \in \Omega_3$ есть ненулевой коэффициент, то

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

Из предположения следует, что $\mathbf{b} + \mathbf{x} = \mathbf{b} + \mathbf{y} = \mathbf{0}$, откуда $\mathbf{x} = \mathbf{y}$. В силу того, что в левой части стоит вектор с попарно одинаковыми координатами, а в правой — нет, получаем противоречие.

Значит, все коэффициенты μ_i, $i \in \Omega_3$ равны нулю. Тогда, как нетрудно видеть, предположение о равенстве линейной комбинации строк матрицы A' приводится к виду

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

тогда предположение сводится к равенству

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

что влечет $\mu_2 = 0$, $\mu_i = 0$, $i \in \mathfrak{Omega}_2$, так как в левой части последнего равенства стоит линейная комбинация строк матрицы A, которая невырождена.

Мы доказали, что все $\mu_i = 0$ и, таким образом, матрица A' невырождена, что означает сильную полноту системы $\mathfrak{A}'$. $\square$

Заключение

Теоремы 4.2, 4.8, 4.9, раскрывают в полной мере устройство полных систем в пространстве $P_2(2)$.

Сделаны попытки исследования структуры полных систем в пространстве функций $n \geqslant 3$ переменных.

Проведено исследование соотношения понятий сильной и слабой полноты, приведены примеры, доказывающие наличие слабо полных систем булевых функций в $P_2(n)$, $n \geqslant 3$ (теорема 5.5). Этот результат вводит некоторые трудности на пути дальнейшего описания полных систем, так как появляется необходимость отдельного описания сильно полных и слабо полных систем.

Направление поиска слабо полных систем представляется наиболее интересным направлением, так как оно позволяет сопоставлять булевой функции вектор расстояний длины, меньшей, чем 2^n.

Доказаны некоторые технические утверждения, касающиеся связи матриц Адамара и полных систем булевых функций.

С использованием инструментария, намеченного в данной работе, даны более простые доказательства некоторых утверждений, которые были доказаны в [3].

Найдены некоторые классы полных систем в пространстве $P_2(3)$. Способ их построения выводит некоторые гипотезы, которые в случае подтверждения приведут к методам обобщения имеющейся структуры полных систем (в $P_2(2)$) на случаи $n \geqslant 3$.

Намечен спектр вопросов, требующих исследования на этом пути (о равносильности понятий эквивалентности матриц Адамара и подобия систем функций, о возможности распространения полученных результатов на случай более высоких размерностей).

Приложение. Пример двух неэквивалентных матриц Адамара порядка 16

$$A_{16}^{1} = \left(\begin{array}{cccccccccccccccc}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
+ & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - \\
+ & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + \\
+ & + & + & + & - & - & - & - & + & + & + & + & - & - & - & - \\
+ & - & + & - & - & + & - & + & + & - & + & - & - & + & - & + \\
+ & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + \\
+ & - & - & + & - & + & + & - & + & - & - & + & - & + & + & - \\
+ & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - \\
+ & - & + & - & + & - & (+) & (-) & - & + & - & + & - & + & (-) & (+) \\
+ & + & - & - & + & + & - & - & - & - & + & + & - & - & + & + \\
+ & - & - & + & + & - & (-) & (+) & - & + & + & - & - & + & (+) & (-) \\
+ & + & + & + & - & - & - & - & - & - & - & - & + & + & + & + \\
+ & - & + & - & - & + & (-) & (+) & - & + & - & + & + & - & (+) & (-) \\
+ & + & - & - & - & - & + & + & - & - & + & + & + & + & - & - \\
+ & - & - & + & - & + & (+) & (-) & - & + & + & - & + & - & (-) & (+)
\end{array}\right)$$

$$A_{16}^2 = \left(\begin{array}{cccccccccccccccc}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
+ & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - \\
+ & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + \\
+ & + & + & + & - & - & - & - & + & + & + & + & - & - & - & - \\
+ & - & + & - & - & + & - & + & + & - & + & - & - & + & - & + \\
+ & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + \\
+ & - & - & + & - & + & + & - & + & - & - & + & - & + & + & - \\
+ & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - \\
+ & - & + & - & + & - & (-) & (+) & - & + & - & + & - & + & (+) & (-) \\
+ & + & - & - & + & + & - & - & - & - & + & + & - & - & + & + \\
+ & - & - & + & + & - & (+) & (-) & - & + & + & - & - & + & (-) & (+) \\
+ & + & + & + & - & - & - & - & - & - & - & - & + & + & + & + \\
+ & - & + & - & - & + & (+) & (-) & - & + & - & + & + & - & (-) & (+) \\
+ & + & - & - & - & - & + & + & - & - & + & + & + & + & - & - \\
+ & - & - & + & - & + & (-) & (+) & - & + & + & - & + & - & (+) & (-)
\end{array}\right)$$

Список литературы

[1] *Логачёв О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии // Москва, изд-во МЦНМО, 2004

[2] *Ф.Дж.Мак-Вильямс, Н.Дж.А.Слоэн* Теория кодов, исправляющих ошибки // Москва, изд-во «Связь», 1979

[3] *Малыхин В.В.* О некоторых метрических свойствах булевых функций. Дипломная работа. // Москва, МГУ им. М.В.Ломоносова, Механико-математический факультет, 2008

[4] *Сидельников В.М.* Теория кодирования // Москва, 2007

[5] *Холл М.* Комбинаторика // Москва, изд-во «Мир», 1970

[6] *Яблонский С.В.* Введение в дискретную математику // Москва, 1979