Федеральное государственное автономное образовательное учреждение
высшего образования
«Новосибирский национальный исследовательский государственный
университет»

На правах рукописи

Куценко Александр Владимирович

САМОДУАЛЬНЫЕ БЕНТ-ФУНКЦИИ И ИХ МЕТРИЧЕСКИЕ СВОЙСТВА

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
кандидат физико-математических наук, с.н.с.
Токарева Н.Н.

Новосибирск — 2020

Оглавление

Введение

Настоящая работа посвящена булевым функциям от чётного числа переменных, обладающим свойством максимальной нелинейности — бент-функциям. Данный класс функций имеет многочисленные приложения в таких областях как криптография, комбинаторика, теория кодирования. Исследуется отображение, которое каждой бент-функции ставит в соответствие дуальную к ней бент-функцию. Изучаются метрические, а также комбинаторные свойства неподвижных точек данного отображения — самодуальных бент-функций.

Приведём необходимые определения.

Пусть $\mathbb{F}_2^n$ — пространство двоичных векторов с n координатами. *Весом Хэмминга* вектора $x \in \mathbb{F}_2^n$ называется количество его координат, отличных от 0. *Расстоянием Хэмминга* $\mathrm{dist}\,(x,y)$ между двумя векторами $x,y \in \mathbb{F}_2^n$ называется количество координат, в которых эти векторы различаются. Легко видеть, что расстояние Хэмминга является метрикой на $\mathbb{F}_2^n$. *Булевой функцией* от n переменных называется произвольное отображение вида $\mathbb{F}_2^n \to \mathbb{F}_2$. Множество булевых функций от n переменных обозначается через $\mathcal{F}_n$. *Характеристическим вектором* (характеристической последовательностью) булевой функции $f \in \mathcal{F}_n$ называется вектор

$$F \equiv (-1)^f = \left((-1)^{f_0},(-1)^{f_1},\ldots,(-1)^{f_{2^n-1}}\right) \in \{\pm 1\}^{2^n},$$

где $(f_0,f_1,\ldots,f_{2^n-1}) \in \mathbb{F}_2^{2^n}$ — вектор значений (таблица истинности) функции f. *Весом Хэмминга* $\mathrm{wt}(f)$ булевой функции f называется вес Хэмминга её вектора значений. *Расстояние Хэмминга* $\mathrm{dist}\,(f,g)$ между двумя булевыми функциями $f,g \in \mathcal{F}_n$ определяется как число векторов пространства $\mathbb{F}_2^n$, на которых данные функции принимают различные значения. Символом $\oplus$ обозначим сложение по модулю 2. Для пары векторов $x,y \in \mathbb{F}_2^n$ через $\langle x,y\rangle$ обозначается значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Преобразованием Уолша—Адамара* булевой функции $f \in \mathcal{F}_n$ называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)\oplus\langle x,y\rangle}, \;\; y \in \mathbb{F}_2^n.$$

Нелинейностью булевой функции $f \in \mathcal{F}_n$ называется расстояние Хэмминга от функции f до множества всех аффинных булевых функций от n

переменных — мера удалённости функции от множества аффинных и, как следствие, линейных булевых функций. Соответственно, использование функций, обладающих высокой нелинейностью, в качестве компонент блочных и поточных шифров увеличивает стойкость к линейному криптоанализу [65] — одному из основных статистических видов криптоанализа блочных шифров. Например, функции, обладающие максимально возможной нелинейностью, были использованы в качестве составных элементов в поточном шифре Grain (2004) и блочном шифре CAST (1997).

Булева функция f от чётного числа переменных n называется **бент-функцией**, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$. В случае чётного n на бент-функциях, и только на них, достигается максимальное значение нелинейности $2^{n-1} - 2^{n/2-1}$. Множество бент-функций от n переменных обозначается через $\mathcal{B}_n$. Отметим, что для случая нечётного числа переменных нахождение максимального значения нелинейности является известной открытой проблемой теории кодирования, связанной с поиском радиуса покрытия кода Рида — Маллера первого порядка. Термин «бент-функция» предложил американский математик O. S. Rothaus, который исследовал данные функции в 60х годах прошлого века, при этом первая работа по данной теме была опубликована в 1976 году [75]. Тем не менее, известно [8], что булевы функции, обладающие аналогичными свойствами, в это же время также исследовались в Советском Союзе — математиками В. А. Елисеевым и О. П. Степченковым, которые использовали термин «минимальная функция».

Для более детального знакомства со свойством нелинейности, а также другими важными криптографическими свойствами можно порекомендовать книги О. А. Логачева, А. А. Сальникова, С. В. Смышляева, В. В. Ященко [10] и T. W, Cusick, P. Stănică [40], а также книгу C. Carlet [31] и другие его работы, посвящённые различным приложениям булевых функций [26] и векторных булевых функций [27]. Описанию известных результатов и открытых вопросов, связанных с бент-функциями и их обобщениями, посвящены монографии Н. Н. Токаревой [82] и S. Mesnager [69].

Всюду далее считается, что n — чётное натуральное число. Для каждой бент-функции $f \in \mathcal{B}_n$ соотношением

$$W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}, \ \ y \in \mathbb{F}_2^n$$

единственным образом определяется булева функция $\widetilde{f}$ от того же числа переменных. Функция $\widetilde{f}$ называется **дуальной** к бент-функции f. Булева функция $\widetilde{f}$ также является бент-функцией, кроме того, для неё справедливо соотношение $\widetilde{\widetilde{f}} = f$. Таким образом, множество бент-функций от n переменных, отличных от своих дуальных, разбивается на пары $(f, \widetilde{f})$, каждая из которых состоит из бент-функции и дуальной к ней. Функцию $\widetilde{f}$ впервые в своих работах отметили O. S. Rothaus и J. F. Dillon [44] в 70х годах прошлого века.

Матрицей Сильвестра — Адамара называется квадратная матрица порядка 2^n, обозначаемая H_n, определяемая следующими рекуррентными соотношениями:

$$H_0 = (1), \qquad H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, \; n \geqslant 2.$$

Нетрудно видеть, что данная матрица является симметричной, кроме того, она позволяет получить описание преобразование Уолша — Адамара в матрично-векторной форме [15]. В терминах характеристических векторов и матрицы Сильвестра — Адамара бент-функцию можно определить следующим образом: пусть n — чётное число, тогда $f \in \mathcal{F}_n$ — бент-функция, если $H_n(-1)^f \in \{\pm 2^{n/2}\}^{2^n}$. Характеристический вектор дуальной функции $\widetilde{f}$ однозначным образом находится из условия

$$H_n(-1)^f = 2^{n/2}(-1)^{\widetilde{f}}.$$

Отображение дуальности определяется на множестве бент-функций от n переменных и действует по правилу $f \to \widetilde{f}$. В терминах характеристических векторов оно имеет следующую эквивалентную форму: $(-1)^f \to (-1)^{\widetilde{f}}$. Известно, что оно сохраняет расстояние Хэмминга, то есть является изометричным отображением множества бент-функций [24]. Стоит отметить, что на данный момент отображение дуальности является единственным известным отображением, которое обладает таким свойством и при этом не расширяется до изометрии на множестве всех булевых функций от n переменных.

Исследованию того, как изменяются основные характеристики бент-функции под действием отображения дуальности, а также изучению его действия на конкретные классы бент-функций, посвящено большое количество работ. В частности, в работе [49] получено соотношение, связывающее алгебраические степени бент-функции и дуальной к ней. В статье [18] доказано, что бент-функция разложима в сумму двух бент-функций в том и только в том случае, когда

таким свойством обладает дуальная к ней. Связь между коэффициентами числовой нормальной формы (Numerical Normal Form) бент-функции и дуальной к ней изучалась в работах [29; 52]. Хорошо известно, что отображение дуальности сохраняет расширенную аффинную эквивалентность: дуальные расширенно аффинно эквивалентных бент-функций также расширенно аффинно эквивалентны. Действие отображения дуальности на некоторые классы бент-функций, например, класс Мэйорана — МакФарланда и класс Диллона $\mathcal{PS}_{ap}$, может быть описано относительно просто, в то время как во многих других случаях нахождение дуальной функции и исследование её свойств является нетривиальной задачей. Этим вопросам посвящены, например, работы [21; 32], в которых изучалось действие отображения дуальности на бент-функции из класса Нихо. Было показано, что дуальные к ним функции уже не принадлежат данному классу. Функции, являющиеся дуальными к бент-функциям из некоторых других мономиальных классов, изучались в работах [59—61]. В частности, было получено, что дуальные функции бент-функций Касами не являются мономиальными, тогда как дуальная функция (квадратичной) бент-функции с показателем Голда является квадратичной.

Важной метрической характеристикой отображения дуальности является расстояние Хэмминга между бент-функцией и дуальной к ней — количество позиций, в которых меняются вектор значений и характеристический вектор бент-функции под действием данного отображения. Величина $\mathrm{dist}(f,\widetilde{f})$ полностью характеризуется *отношением Рэлея булевой функции*. Для $f \in \mathcal{F}_n$ отношением Рэлея называется величина

$$S_f = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x,y \rangle}.$$

Описание всех бент-функций, находящихся на определённом расстоянии от своей дуальной функции или, другими словами, классификация бент-функций в терминах значений отношения Рэлея, является открытой проблемой. В работе L. E. Danielsen, M. G. Parker, P. Solé [41] можно найти характеризацию для бент-функций от малого числа переменных, а также ряд свойств отношения Рэлея и его вид для некоторых известных классов бент-функций.

Бент-функция f называется **самодуальной**, если она совпадает со своей дуальной, то есть $f = \widetilde{f}$. Таким образом, самодуальные бент-функции являются *неподвижными точками* отображения дуальности. Бент-функция f

называется **анти-самодуальной**, если она совпадает с отрицанием свой дуальной, то есть $f = \widetilde{f} \oplus 1$. Понятия *дуальной бент-* (dual bent) и *анти-дуальной бент-* (anti-dual bent) функций, по существу, аналоги определений самодуальной и анти-самодуальной бент-функций, соответственно, предложили B. Preneel и др. в работе [72]. Более общее понятие *самодуальной бент-функции на конечной абелевой группе* было введено О. А. Логачевым, А. А. Сальниковым, В. В. Ященко [9].

Из определения самодуальности следует, что характеристический вектор самодуальной бент-функции является собственным вектором матрицы H_n, соответствующим собственному числу $2^{n/2}$. В свою очередь, характеристический вектор анти-самодуальной бент-функции является собственным вектором, соответствующим собственному числу $\left(-2^{n/2}\right)$. Таким образом, вопрос характеризации самодуальных и анти-самодуальных бент-функций тесно связан с перечислением и исследованием свойств собственных векторов матрицы Сильвестра — Адамара, координаты которых суть числа ± 1.

Стоит отметить, что в случае чётного числа переменных на (анти-)самодуальных бент-функциях, и только на них, достигается максимальное (соответственно, минимальное) значение отношения Рэлея булевой функции. Для случая нечётного числа переменных поиск максимального значения отношения Рэлея булевой функции является открытым вопросом, что позволяет говорить о некоторой аналогии с известной проблемой поиска максимального значения нелинейности булевой функции для случая нечётного числа переменных.

Открытой проблемой является полная характеризация и описание классов эквивалентности самодуальных и анти-самодуальных бент-функций. Этому и другим вопросам, связанным с самодуальными и анти-самодуальными бент-функциями, посвящён ряд работ российских и зарубежных авторов. В частности, данные классы бент-функций были отражены в работах таких исследователей, как C. Carlet, X.-D. Hou, P. Solé, В. А. Зиновьев, J. Rifà, S. Mesnager, T. Helleseth, B. Preneel и др.

В частности, в работе C. Carlet, L. E. Danielsen, M. G. Parker, P. Solé [33] был получен ряд конструкций, а также описаны некоторые свойства самодуальных бент-функций. Представлена классификация самодуальных бент-функции от $2,4,6$ переменных и всех квадратичных самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность. По-

казано, что расстояние Хэмминга между самодуальной и анти-самодуальной бент-функциями от n переменных равно 2^{n-1}. Рассмотрены свойства характеристического вектора самодуальной бент-функции. В работе X.-D. Hou [50] приведена классификация всех квадратичных самодуальных бент-функций относительно действия ортогональной группы, основанная, в том числе, на классификации инволютивных симплектических матриц. Классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность, можно найти в статье [46]. Верхняя оценка количества самодуальных бент-функций, полученная на основе их взаимосвязи с формально самодуальными бент-функциями, представлена в работе [53]. В статьях S. Mesnager [68], а также J. Rifà и В. А. Зиновьева [74] предложены алгебраические и комбинаторные конструкции самодуальных бент-функций. Алгебраическим конструкцями бент-функций и самодуальных бент-функций, основанным на использовании инволюций, посвящены работы [39; 62].

Целью данной работы является исследование взаимосвязи между свойствами отображения дуальности и его неподвижных точек — самодуальных бент-функций, а также изучение метрических свойств самодуальных бент-функций. В работе доказано, что множества самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, которая определяет отображение дуальности в терминах характеристических векторов. Доказано, что изометричное отображение всех булевых функций от $n \geqslant 4$ переменных в себя сохраняет отношение Рэлея каждой булевой функции, если и только если оно является элементом группы автоморфизмов множества самодуальных бент-функций от n переменных. Данные результаты позволяют говорить о тесной связи свойств отображения дуальности и метрических свойств самодуальных бент-функций. Исследованы метрические свойства самодуальных бент-функций. Полностью описана группа автоморфизмов множества самодуальных бент-функций от $n \geqslant 4$ переменных. Доказано, что множество булевых функций, максимально удалённых от множества самодуальных (анти-самодуальных) бент-функций от $n \geqslant 4$ переменных, совпадает с множеством анти-самодуальных (самодуальных) бент-функций от n переменных. Доказано, что множество (анти-)самодуальных бент-функций от n переменных является метрически регулярным. Исследованы метрические свойства самодуальных бент-функций из класса Мэйорана — Мак-

Фарланда. Найдено минимальное расстояние Хэмминга между самодуальными бент-функциями от n переменных.

Основные положения, выносимые на защиту:

1. Доказано, что множества характеристических векторов самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным числам $2^{n/2}$ и $(-2^{n/2})$, соответственно.
2. Описаны группы автоморфизмов множеств самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных.
3. Установлено, что группа автоморфизмов множества самодуальных бент-функций совпадает с множеством изометричных отображений всех булевых функций от $n \geqslant 4$ переменных в себя, сохраняющих расстояние Хэмминга между каждой бент-функцией и дуальной к ней.
4. Доказано, что множество булевых функций, максимально удалённых от множества самодуальных (анти-самодуальных) бент-функций от $n \geqslant 4$ переменных, совпадает с множеством анти-самодуальных (самодуальных) бент-функций от n переменных. Таким образом, доказана метрическая регулярность множества (анти-)самодуальных бент-функций от n переменных.
5. Найден полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

Научная новизна и значимость: Работа носит теоретический характер. Все результаты диссертации являются новыми и снабжены полными доказательствами. Полученные результаты могут быть использованы для дальнейшего изучения свойств отображения дуальности, а также самодуальных и анти-самодуальных бент-функций. Например, для поиска спектра расстояний Хэмминга между самодуальными бент-функциями, классификации самодуальных бент-функций относительно изометричных отображений, сохраняющих самодуальность.

Методология и методы исследования. В диссертации используются комбинаторные методы и методы дискретного анализа, аппарат линейной алгебры. Для изучения метрических свойств самодуальных бент-функций используется соответствие между характеристическими векторами самодуальных и анти-

самодуальных бент-функций и собственными векторами матрицы Сильвестра — Адамара.

Апробация работы. Результаты работы докладывались на следующих конференциях и семинарах: Международная конференция «Sequences and Their Applications (SETA 2020)» (г. Санкт-Петербург, 2020 г.), Международная конференция «Boolean Functions and their Applications (BFA 2019, BFA 2020)» (Италия, г. Флоренция, 2019 г.; Норвегия, г. Лоен, 2020 г.), Симпозиум «Современные тенденции в криптографии (CTCrypt 2019, CTCrypt 2020)» (Калининградская область, г. Светлогорск, 2019 г.; Московская область, 2020 г.), Международный семинар «Дискретная математика и ее приложения» (Россия, г. Москва, 2016 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография (SIBECRYPT)» (г. Новосибирск, 2015 г.; г. Новосибирск, 2016 г.; г. Красноярск, 2017 г.; г. Абакан, 2018 г.; г. Томск, 2019 г.), семинар исследовательского центра Selmer Center in Secure Communication (Норвегия, г. Берген, февраль 2020 г.), семинары «Дискретный анализ», «Теория кодирования», «Криптография и криптоанализ» Института математики им. С. Л. Соболева СО РАН и кафедры теоретической кибернетики ММФ НГУ, семинар отдела теоретической кибернетики ИМ СО РАН.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель работы.

Первая глава является обзором известных результатов по свойствам отображения дуальности, отношения Рэлея, а также самодуальным и анти-самодуальным бент-функциям. Описаны известные свойства и характеристики отображения дуальности самодуальных бент-функций, включая метрические, а также алгоритмы перечисления всех самодуальных и анти-самодуальных бент-функций от n переменных, степень которых не превосходит заранее фиксированного числа. Приведены известные комбинаторные и алгебраические конструкции самодуальных и анти-самодуальных бент-функций. Рассмотрены известные результаты по классификации самодуальных бент-функций от $n \leqslant 8$

переменных. Описана классификация квадратичных самодуальных бент-функций. Перечислены верхние оценки количества самодуальных бент-функций, а также нижние оценки, полученные на основе известных конструкций.

Через $\mathrm{SB}^+(n)$ обозначим множество самодуальных бент-функций от n переменных, а через $\mathrm{SB}^-(n)$ — множество анти-самодуальных бент-функций от n переменных.

Обзор главы 1 опубликован в [89].

Во **второй главе** изучаются комбинаторные свойства бент-функций.

Пусть f_0,f_1,f_2,f_3 — бент-функции от n переменных. Рассмотрим булеву функцию f от $n+2$ переменных, определённую следующим образом:

$$f(00,x)=f_0(x),\ \ f(01,x)=f_1(x),\ \ f(10,x)=f_2(x),\ \ f(11,x)=f_3(x),\ \ x\in\mathbb{F}_2^n.$$

Теорема 1. *Бент-функция f от $n+2$ переменных, определённая указанным выше способом, является самодуальной тогда и только тогда, когда существует пара бент-функций $g_1,g_2\in\mathcal{B}_n$ и булева функция $h\in\mathcal{F}_n$ такие, что*

$$f_0=\widetilde{g}_2,\qquad f_1=\widetilde{g_1\oplus h},\qquad f_2=\widetilde{g}_1,\qquad f_3=\widetilde{g_2\oplus h}\oplus 1,$$

и функции g_1,g_2,h удовлетворяют следующей системе

$$\begin{cases} h=g_1\oplus g_2\oplus\widetilde{g}_1\oplus\widetilde{g}_2,\\ \widetilde{g_1\oplus h}=\widetilde{g}_1\oplus h,\\ \widetilde{g_2\oplus h}=\widetilde{g}_2\oplus h,\\ g_1\oplus\widetilde{g}_2=h\,(g_1\oplus g_2)\,. \end{cases}$$

Данный результат описывает самодуальные бент-функции от $n+2$ переменных, вектор значений которых является конкатенацией четырёх векторов значений бент-функций от n переменных.

Как было сказано ранее, действие отображения дуальности на бент-функцию $f\in\mathcal{B}_n$ может быть представлено в виде умножения характеристического вектора данной функции на матрицу Сильвестра — Адамара. С использованием итеративных конструкций самодуальных бент-функций, получаемых с помощью Теоремы 1, доказана следующая

Теорема 2. *Множества характеристических векторов самодуальных бент-функций и анти-самодуальных бент-функций от $n\geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным числам $2^{n/2}$ и $(-2^{n/2})$, соответственно.*

Таким образом, множества самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных полностью характеризуют собственные подпространства матрицы Сильвестра — Адамара. Пусть $f \in \mathcal{F}_n$ — произвольная бент-функция, и F^+, $F^- \in \mathbb{R}^{2^n}$ — проекции её характеристического вектора $(-1)^f$ на собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным значениям $2^{n/2}$ и $(-2^{n/2})$. Тогда действие отображения дуальности на функцию f описывается схемой

$$F^+ + F^- = (-1)^f \longrightarrow (-1)^{\widetilde{f}} = F^+ - F^-,$$

при этом в силу Теоремы 2 проекции F^+ и F^- есть линейные комбинации характеристических векторов самодуальных и анти-самодуальных бент-функций от n переменных.

Результаты главы 2 опубликованы в [87; 89; 90; 95; 98; 100].

В **третьей главе** изучаются группы автоморфизмов множеств самодуальных и анти-самодуальных бент-функций, а также изометричные отображения, меняющие местами данные множества функций. Исследуются метрические свойства отображения, которое каждой бент-функции от n переменных ставит в соответствие дуальную к ней бент-функцию.

Отображение, определённое на множестве булевых функций, называется *изометричным*, если оно сохраняет расстояние Хэмминга.

Как было отмечено ранее, отображение дуальности $f \to \widetilde{f}$ сохраняет расстояние Хэмминга между каждой бент-функцией и дуальной к ней.

Утверждение 5. *При $n \geqslant 4$ не существует изометричного отображения множества всех булевых функций от n переменных в себя, отличного от тождественного, обладающего тем свойством, что каждая самодуальная бент-функция от n переменных является его неподвижной точкой.*

Данный результат позволяет сделать вывод о том, что не существует изометричного отображения множества всех булевых функций от n переменных в себя, которое каждой бент-функции от n переменных ставит в соответствие дуальную к ней функцию. Таким образом, отображение дуальности не может быть доопределено до изометричного отображения всех булевых функций от n переменных в себя.

Группой автоморфизмов фиксированного множества булевых функций $M \subseteq \mathcal{F}_n$ называется группа изометричных отображений множества всех

булевых функций от n переменных в себя, оставляющих множество M на месте. Она обозначается через $\mathrm{Aut}\,(M)$.

Через $\mathrm{GL}\,(n,\mathbb{F}_2)$ обозначается *полная линейная группа* порядка n над полем $\mathbb{F}_2$. *Ортогональной группой* порядка n над полем $\mathbb{F}_2$ называется группа

$$\mathcal{O}_n = \left\{L \in \mathrm{GL}\,(n,\mathbb{F}_2) : LL^{\mathrm{T}} = I_n\right\},$$

где I_n — единичная матрица порядка n над полем $\mathbb{F}_2$. Группа преобразований, действующих на множестве всех булевых функций от n переменных по правилу

$$f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x\rangle \oplus d,$$

где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — чётное число, $d \in \mathbb{F}_2$, называется *расширенной ортогональной группой* и обозначается $\overline{\mathcal{O}}_n$.

Теорема 3. *Для $n \geqslant 4$ справедливо*

$$\mathrm{Aut}\left(\mathrm{SB}^+(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^-(n)\right) = \overline{\mathcal{O}}_n.$$

Таким образом, все изометричные отображения, сохраняющие (анти-)самодуальность, полностью характеризуются расширенной ортогональной группой. В частности, отсюда следует, что существующий подход к классификации самодуальных бент-функций является самым общим в рамках изометричных отображений множества всех булевых функций от n переменных, сохраняющих самодуальность.

Для случая $n \geqslant 4$ охарактеризованы изометричные отображения, меняющие местами множества самодуальных и анти-самодуальных бент-функций от n переменных. Доказано, что изометричное отображение всех булевых функций от n переменных в себя определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$, если и только если оно имеет вид $f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x\rangle \oplus d$, где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — нечётное число, $d \in \mathbb{F}_2$. Показано, что отображения данного вида, и только они, обладают следующим свойством: если расстояние Хэмминга между бент-функцией и дуальной к ней равно d, то такая бент-функция переходит в бент-функцию, находящуюся на расстоянии $2^n - d$ от своей дуальной.

Наличие данных изометричных соответствий во многих случаях позволяет тривиальным образом переносить утверждения, касающиеся метрических свойств самодуальных бент-функций, на анти-самодуальные бент-функции, и наоборот.

Изометричное отображение φ будем называть *перестановочным с отображением дуальности*, если оно переводит множество бент-функция от n переменных в себя, и для каждой бент-функции $f \in \mathcal{B}_n$ выполняется

$$\widetilde{\varphi(f)} = \varphi(\widetilde{f}).$$

С использованием отношения Рэлея булевой функции получено полное описание изометричных отображений, оставляющих класс бент-функций от $n \geqslant 4$ переменных на месте и сохраняющих расстояние Хэмминга между каждой бент-функцией и дуальной к ней, также охарактеризованы все отображения, перестановочные с отображением дуальности.

Теорема 4. *Пусть φ — изометричное отображение множества всех булевых функций от $n \geqslant 4$ переменных в себя. Тогда следующие условия эквивалентны:*

1) *φ перестановочно с отображением дуальности;*
2) *φ является элементом группы автоморфизмов множества бент-функций от n переменных и сохраняет расстояние Хэмминга между каждой бент-функцией и дуальной к ней;*
3) *φ является элементом группы автоморфизмов множества самодуальных бент-функций от n переменных.*

В силу того, что каждый элемент расширенной ортогональной группы оставляет множество бент-функций на месте, из Теорем 3 и 4 следует, что множество изометричных отображений, сохраняющих расстояние между бент-функцией и дуальной к ней, совпадает с группой автоморфизмов самодуальных бент-функций. Это позволяет говорить о наличии тесной связи между свойствами отображения дуальности и метрическими свойствами (анти-)самодуальных бент-функций.

Результаты главы 3 опубликованы в [87–89; 94; 96–99].

В **четвёртой главе** найдено минимальное расстояние между самодуальными бент-функциями и исследованы множества булевых функций, максимально удалённые от множеств (анти-)самодуальных бент-функций.

Утверждение 14. *Пусть $n \geqslant 4$, тогда минимальное расстояние Хэмминга между различными самодуальными бент-функциями от n переменных равно $2^{n/2}$.*

С использованием изометричных соответствий между множествами самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных, описываемых Утверждением 14, доказано, что минимальное расстояние Хэмминга между

различными анти-самодуальными бент-функциями от n переменных также равно $2^{n/2}$.

Для случая $n = 2$ имеем $\mathrm{SB}^+(2) = \{x_1x_2,\, x_1x_2 \oplus 1\}$ — данные функции являются отрицаниями друг друга и находятся на расстоянии 2^n. Но при $n \geqslant 4$ расстояние $2^{n/2}$, являющееся минимальным расстоянием между различными бент-функциями от n переменных, достижимо также и на (анти-)самодуальных бент-функциях.

Охарактеризованы множества булевых функций, находящиеся на максимальном удалении от множеств (анти-)самодуальных бент-функций.

Теорема 5. *Пусть $n \geqslant 4$, тогда*

- *Множество булевых функций, максимально удалённых от множества самодуальных бент-функций от n переменных, совпадает с множеством анти-самодуальных бент-функций от n переменных;*
- *Множество булевых функций, максимально удалённых от множества анти-самодуальных бент-функций от n переменных, совпадает с множеством самодуальных бент-функций от n переменных.*

Множество векторов, максимально удалённых от множества $A \subseteq \mathbb{F}_2^n$, обозначается через $\widehat{A}$. Множество A называется *метрически регулярным*, если $\widehat{\widehat{A}} = A$. Множество булевых функций называется *метрически регулярным*, если метрически регулярным является соответствующее ему множество векторов значений.

Теорема 6. *Множества самодуальных и анти-самодуальных бент-функций от n переменных являются метрически регулярными множествами.*

Используя двойственность между самодуальными и анти-самодуальными бент-функциями, вытекающую из приведённых выше результатов, можно определить данные функции в метрическом смысле: самодуальная бент-функция от $n \geqslant 4$ переменных — это булева функция от n переменных, максимально удалённая от множества анти-самодуальных бент-функций от n переменных. Аналогичное утверждение можно сформулировать для анти-самодуальных бент-функций.

Результаты главы 4 опубликованы в [87; 89; 95; 98; 99].

В **пятой главе** исследуются расстояния Хэмминга между самодуальными бент-функциями из одного известного класса.

Бент-функции от n переменных, представимые в виде

$$f(x,y) = \langle x,\pi(y)\rangle \oplus g(y),\ \ x,y \in \mathbb{F}_2^{n/2},$$

где π — перестановка на множестве $\mathbb{F}_2^{n/2}$, а g — булева функция от $n/2$ переменных, формируют хорошо известный *класс Мэйорана — МакФарланда* (1973). Данная конструкция является одной из первых конструкций бент-функций, её мощность даёт хорошую нижнюю оценку количества данных функций.

Через $\mathrm{SB}^+_{\mathcal{M}}(n)$ обозначим множество самодуальных бент-функций от n переменных из класса Мэйорана — МакФарланда, а через $\mathrm{SB}^-_{\mathcal{M}}(n)$ — множество анти-самодуальных бент-функций от n переменных из класса Мэйорана — МакФарланда.

Получен полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

Теорема 7. *Пусть* $f,g \in \mathrm{SB}^+_{\mathcal{M}}(n) \cup \mathrm{SB}^-_{\mathcal{M}}(n)$, *тогда если*

- $f \in \mathrm{SB}^+_{\mathcal{M}}(n)$, *а* $g \in \mathrm{SB}^-_{\mathcal{M}}(n)$, *то* $\mathrm{dist}(f,g) = 2^{n-1}$;
- $f,g \in \mathrm{SB}^+_{\mathcal{M}}(n)$ *или* $f,g \in \mathrm{SB}^-_{\mathcal{M}}(n)$, *то при* $n = 2$ *имеем* $\mathrm{dist}(f,g) = 2^n$, *а при* $n \geqslant 4$ *справедливо*

$$\mathrm{dist}(f,g) \in \left\{2^{n-1}, 2^{n-1} \pm 2^{n-r-1}\right\},\ r = 0,1,\ldots,n/2-1,$$

и все приведённые расстояния достижимы.

Из Теоремы 7 следует, что при $n \geqslant 4$ минимальное расстояние Хэмминга между рассматриваемыми функциями составляет 2^{n-2}.

Результаты главы 5 опубликованы в [86; 91; 92; 98; 99].

Благодарности. Я выражаю искреннюю благодарность своему научному руководителю Наталье Николаевне Токаревой за постановку интересных задач, положивших начало моим исследованиям, постоянную и всестороннюю поддержку, а также ценные советы и замечания, позволившие по-новому взглянуть на многие вопросы, рассматриваемые в работе. Приношу свою благодарность руководителю лаборатории дискретного анализа Института математики им. С. Л. Соболева СО РАН Александру Андреевичу Евдокимову и её сотрудникам, в частности, Николаю Александровичу Коломейцу и Владимиру Николаевичу Потапову, за внимание к работе, ценные советы и предложения. Хотелось бы выразить благодарность рецензентам моих статей и тезисов за

указание ценных замечаний и дополнений, позволивших улучшить качество работ. Выражаю признательность коллективу исследовательского центра Selmer Center in Secure Communication (Норвегия, г. Берген) за проявленный интерес к полученным результатам, а также полезные замечания. Выражаю благодарность Денису Станиславовичу Кротову, взявшему на себя труд прочитать текст рукописи. Отдельно хотелось бы поблагодарить своих коллег — Анастасию Александровну Городилову, Валерию Александровну Идрисову и Алексея Константиновича Облаухова за интересную и плодотворную совместную работу, а также дружескую атмосферу.

Публикации. Основные результаты по теме диссертации изложены в 15 печатных изданиях, 4 из которых изданы в журналах, рекомендованных ВАК, а также индексируемых Web of Science и Scopus, 11 — в тезисах докладов.

Объем и структура работы. Диссертация состоит из введения, 5 глав, заключения. Полный объём диссертации составляет 134 страницы, включая 9 таблиц. Список литературы содержит 100 наименований.

Глава 1. Дуальность и самодуальность бент-функции. Обзор известных результатов

1.1 Основные определения и обозначения

В данной главе приведены основные определения, используемые в тексте настоящей работы.

Пусть $\mathbb{F}_2^n$ — пространство двоичных векторов с n координатами. *Весом Хэмминга* вектора $x \in \mathbb{F}_2^n$ называется количество его координат, отличных от 0. *Расстоянием Хэмминга* $\mathrm{dist}\,(x,y)$ между двумя векторами $x,y \in \mathbb{F}_2^n$ называется количество координат, в которых эти векторы различаются. Легко видеть, что расстояние Хэмминга является метрикой на $\mathbb{F}_2^n$. *Булевой функцией* от n переменных называется произвольное отображение вида $\mathbb{F}_2^n \to \mathbb{F}_2$. Множество булевых функций от n переменных обозначается через $\mathcal{F}_n$. *Характеристическим вектором* (характеристической последовательностью) булевой функции $f \in \mathcal{F}_n$ называется вектор

$$F \equiv (-1)^f = \left((-1)^{f_0},(-1)^{f_1},\ldots,(-1)^{f_{2^n-1}}\right) \in \{\pm 1\}^{2^n},$$

где $(f_0,f_1,\ldots,f_{2^n-1}) \in \mathbb{F}_2^{2^n}$ — вектор значений (таблица истинности) функции f. *Весом Хэмминга* $\mathrm{wt}(f)$ булевой функции f называется вес Хэмминга её вектора значений. Булева функция $f \in \mathcal{F}_n$ называется *уравновешенной (сбалансированной)*, если $\mathrm{wt}(f) = 2^{n-1}$. *Расстояние Хэмминга* $\mathrm{dist}\,(f,g)$ между двумя булевыми функциями $f,g \in \mathcal{F}_n$ определяется как число векторов пространства $\mathbb{F}_2^n$, на которых данные функции принимают различные значения. Символом $\oplus$ обозначим сложение по модулю 2. Для пары векторов $x,y \in \mathbb{F}_2^n$ через $\langle x,y\rangle$ обозначается значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Преобразованием Уолша—Адамара* булевой функции $f \in \mathcal{F}_n$ называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x,y\rangle}, \;\; y \in \mathbb{F}_2^n.$$

Алгебраической нормальной формой (АНФ) или *полиномом Жегалкина* булевой функции $f \in \mathcal{F}_n$ называется представление

$$f\,(x_1,x_2,\ldots,x_n) = \bigoplus_{(i_1,i_2,\ldots,i_n) \in \mathbb{F}_2^n} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

где $a_z \in \mathbb{F}_2$ для каждого $z \in \mathbb{F}_2^n$ (с соглашением $0^0 = 1$). Для каждой булевой функции данное представление существует в единственном виде. *Алгебраической степенью* $\deg(f)$ булевой функции f называется максимальная из степеней мономов $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$ её АНФ, имеющих ненулевые коэффициенты $a_{i_1 i_2 \dots i_n}$.

Функция называется *аффинной*, если её степень не превышает единицу. Множество аффинных функций от n переменных обозначается через $\mathcal{A}_n$. Каждая аффинная функция $f \in \mathcal{A}_n$ единственным образом представима в виде $f(x) = \langle a,x\rangle \oplus a_0$, $x \in \mathbb{F}_2^n$, где $a \in \mathbb{F}_2^n$, $a_0 \in \mathbb{F}_2$. Если $\deg(f) = 2$, то булева функция f называется *квадратичной*.

Булевы функции $f,g \in \mathcal{F}_n$ называются *расширенно аффинно эквивалентными*, если существует элемент $A \in \mathrm{GL}\,(n,\mathbb{F}_2)$, вектор $b \in \mathbb{F}_2^n$ и аффинная функция $l \in \mathcal{A}_n$ такие, что

$$g(x) = f(Ax \oplus b) \oplus l(x), \;\; x \in \mathbb{F}_2^n.$$

Пусть $M_{k\times n}\,(\mathbb{F}_2)$ — множество матриц порядка $k \times n$ над полем $\mathbb{F}_2$. Для краткости будем обозначать $M_{n\times n} = M_n$. Через $\mathbf{0}_{k\times n} \in M_{k\times n}\,(\mathbb{F}_2)$ обозначается нулевая матрица порядка $k \times n$. Через $\mathrm{GL}\,(n,\mathbb{F}_2)$ обозначается *полная линейная группа* порядка n над полем $\mathbb{F}_2$. *Полная аффинная группа* порядка n над полем $\mathbb{F}_2$ состоит из преобразований вида $x \longrightarrow Ax \oplus b$, где $A \in \mathrm{GL}\,(n,\mathbb{F}_2)$ и $b \in \mathbb{F}_2^n$, обозначим её через $\mathrm{GA}\,(n,\mathbb{F}_2)$. Определим, согласно [55], *ортогональную группу* порядка n над полем $\mathbb{F}_2$, как

$$\mathcal{O}_n = \left\{L \in \mathrm{GL}\,(n,\mathbb{F}_2) : LL^{\mathrm{T}} = I_n\right\},$$

где L^{T} — транспонирование L, и I_n — единичная матрица порядка n над полем $\mathbb{F}_2$. Мощность ортогональной группы $\mathcal{O}_n$ равна (см. [64])

$$|\mathcal{O}_n| = \begin{cases} 2^{\frac{n^2}{4}} \prod\limits_{i=1}^{\frac{n}{2}-1} \left(2^{2i}-1\right), & \text{если } n \text{ — чётное,} \\ 2^{\frac{(n-1)^2}{4}} \prod\limits_{i=1}^{\frac{n-1}{2}} \left(2^{2i}-1\right), & \text{если } n \text{ — нечётное.} \end{cases}$$

Пусть A — квадратная $n \times n$ матрица над полем комплексных чисел. Ненулевой вектор $v \in \mathbb{C}^n$ называется *собственным вектором* матрицы A, соответствующим *собственному числу* $\lambda \in \mathbb{C}$, если $Av = \lambda v$. Линейная оболочка множества всех собственных векторов, соответствующих собственному числу λ, называется *собственным подпространством* для данного собственнного числа.

Рассмотрим линейное отображение $\psi : \mathbb{C}^n \to \mathbb{C}^n$. *Ядром* отображения ψ называется множество

$$\mathrm{Ker}\,(\psi) = \{x \in \mathbb{C}^n : \psi(x) = \mathbf{0} \in \mathbb{C}^n\}\,.$$

Как известно, ядро линейного оператора является подпространством. Действие линейного отображения в фиксированном базисе определяется квадратной матрицей порядка n. Если не оговорено особо, предполагается, что в качестве базиса используется стандартный базис $\{e_j\}_{j=1}^n$ пространства $\mathbb{C}^n$, где $e_i = \big(0,\ldots,0,\underbrace{1}_{i},0\ldots,0\big)$, $i = 1,2,\ldots,n$.

1.1.1 Коды Рида – Маллера

Двоичным кодом длины n называется произвольное подмножество $\mathbb{F}_2^n$. Элементы кода называются *кодовыми словами*. Минимальное расстояние Хэмминга между различными кодовыми словами кода C называется *кодовым расстоянием* данного кода. Если кодовые слова образуют линейное подпространство, код называется *линейным*. Двоичная матрица размера $k \times n$, строки которой образуют базис линейного кода длины n размерности k, называется его *порождающей матрицей*. *Проверочной матрицей* линейного кода C длины n и размерности k называется двоичная матрица H размера $(n-k) \times n$ такая, что $Hx = \mathbf{0}$ для каждого $x \in C$. В настоящей работе будут затронуты только двоичные линейные коды. Линейный код длины n и размерности k, имеющий кодовое расстояние d, будем называть $[n,k,d]$-кодом.

Кодом Рида – Маллера $\mathrm{RM}(r,m)$ порядка r и длины 2^m $(0 \leqslant r \leqslant m)$ называется множество всех векторов значений булевых функций от m переменных степени не выше r [70; 73]. Данный код, очевидно, является линейным.

Утверждение ([63]). *Код Рида – Маллера* $\mathrm{RM}(r,m)$ *является* $[n,k,d]$*-кодом с параметрами:* $n = 2^m$, $k = \sum\limits_{j=0}^{r} \binom{m}{j}$, $d = 2^{m-r}$.

Пусть $r = 2$, тогда типичное кодовое слово кода Рида – Маллера $\mathrm{RM}(2,m)$ имеет вид:

$$f(x) = \langle x,Qx\rangle \oplus l(x), \quad x \in \mathbb{F}_2^m, \tag{1.1}$$

где $Q \in M_m(\mathbb{F}_2)$ — верхняя треугольная матрица, $l \in \mathcal{A}_m$. В представлении (1.1) аффинная часть выделена в отдельную функцию, поэтому можно считать, что матрица Q имеет нулевую диагональ. В рамках другого представления:

$$f(x) = \langle x,Qx\rangle \oplus \varepsilon, \;\; x \in \mathbb{F}_2^m, \tag{1.2}$$

где $\varepsilon \in \mathbb{F}_2$, линейная часть квадратичной функции f определяется диагональными элементами матрицы Q.

Пусть *квадратичная форма* $\langle x,Qx\rangle$ зафиксирована, рассмотрим смежный класс кода Рида — Маллера второго порядка $\mathrm{RM}(2,m)$ по коду $\mathrm{RM}(1,m)$:

$$\{\langle x,Qx\rangle \oplus l(x) : l \in \mathcal{A}_m\}.$$

Данный смежный класс полностью характеризуется формой $\langle x,Qx\rangle$, другой его характеристикой является матрица $Q \oplus Q^{\mathrm{T}}$.

Двоичная симметричная матрица с нулевой диагональю называется *симплектической*. Известно, что ранг симплектической матрицы всегда есть чётное число, см. [63]. Симплектическая матрица $Q \oplus Q^{\mathrm{T}}$ называется *ассоциированной* с формой $\langle x,Qx\rangle$.

1.2 Отображение дуальности

В данном разделе приводится определение бент-функции и излагаются основные известные свойства отображения дуальности.

1.2.1 Бент-функция

Нелинейностью $Nl(f)$ булевой функции $f \in \mathcal{F}_n$ называется расстояние Хэмминга от функции f до множества всех аффинных булевых функций от n переменных, то есть

$$Nl(f) = \min_{g \in \mathcal{A}_n} \mathrm{dist}(f,g).$$

Пусть $g \in \mathcal{A}_n$ — аффинная функция, то есть $g(x) = \langle a,x \rangle \oplus a_0$, для некоторых $a \in \mathbb{F}_2^n, a_0 \in \mathbb{F}_2$. Нетрудно видеть, что

$$\mathrm{dist}(f,g) = 2^{n-1} - \frac{(-1)^{a_0} W_f(a)}{2}.$$

Тогда выражение для нелинейности можно представить в следующей форме

$$\begin{aligned} Nl(f) &= \min_{g \in \mathcal{A}_n} \mathrm{dist}(f,g) = \min_{a \in \mathbb{F}_2^n, a_0 \in \mathbb{F}_2} \left[2^{n-1} - \frac{(-1)^{a_0} W_f(a)}{2} \right] \\ &= 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)| . \end{aligned}$$

В силу известного *равенства Парсеваля*

$$\sum_{y \in \mathbb{F}_2^n} W_f^2(y) = 2^{2n}$$

заключаем, что

$$\max_{a \in \mathbb{F}_2^n} |W_f(a)| \geqslant 2^{n/2},$$

откуда немедленно следует верхняя оценка

$$Nl(f) \leqslant 2^{n-1} - 2^{n/2-1}.$$

Определение. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$.

Всюду далее в работе, если не оговорено особо, считается, что n — чётное натуральное число. Множество бент-функций от n переменных обозначается через $\mathcal{B}_n$. В случае чётного числа переменных, на бент-функциях, и только на них, достигается максимальное значение нелинейности $2^{n-1} - 2^{n/2-1}$. Для случая нечётного числа переменных нахождение максимального значения является открытой проблемой [47; 48], имеюшей отношение к теории кодирования.

Стоит отметить, бент-функции, в силу максимальной нелинейности, не обладают другим важным криптографическим свойством — *уравновешенностью*. Кроме того, алгебраическая степень бент-функции от n переменных ограничена сверху числом $n/2$, что влечёт потенциальную уязвимость к алгебраическим атакам. Поэтому часто бент-функции используются в качестве входных данных алгоритмов, целью работы которых является построение функций, обладающих

хорошими криптографическими характеристиками, такими как, например, высокие алгебраическая [67] и корреляционная [76] иммунность, а также высокой нелинейностью. Подробную информацию о других важных криптографических свойствах булевых функций можно найти в книгах О. А. Логачева, А. А. Сальникова, С. В. Смышляева, В. В. Ященко [10], T. W. Cusick, P. Stănică [40], в книге [31] и работах C. Carlet [26; 27], B. Preneel и др. [72], а также учебных пособиях Ю. В. Таранникова [16], И. А. Панкратовой [13], Г. П. Агибалова [2], В. М. Фомичёва [19].

Несмотря на то, что с момента первой публикации, посвящённой бент-функциям, прошло достаточно много времени, по-прежнему остаётся множество открытых вопросов, в частности, неизвестно точное число бент-функций и хорошие оценки для него, не описана расширенная аффинная классификация бент-функций от $n \geqslant 10$ переменных, актуален вопрос поиска новых конструкций. Один из первых обзоров по данной тематике представил J. Dillon в 1972 году [45]. Описанию известных результатов и открытых вопросов, связанных с бент-функциями и их обобщениями, посвящены монографии Н. Н. Токаревой [82] и S. Mesnager [69]. Открытые проблемы в области бент-функций также перечислены в работах C. Carlet [28; 31]. Обзор известных результатов можно найти в работах А. С. Кузьмина, А. А. Нечаева, В. А. Шишкина [7], C. Carlet, S. Mesnager [30] и A. Çeşmelioğlu, W. Meidl, A. Pott [36]. Более общая проблема приближения нелинейных функций линейными и связанные с ней вопросы рассматривались в статье М. М. Глухова [3].

1.2.2 Свойства отображения дуальности

Из определения бент-функции следует, что для каждой $f \in \mathcal{B}_n$ существует булева функция $\widetilde{f} \in \mathcal{F}_n$ такая, что

$$W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}, \ \ y \in \mathbb{F}_2^n. \tag{1.3}$$

Функция $\widetilde{f}$, определяемая из условия (1.3), называется *дуальной* к бент-функции f. Таким образом, для каждой бент-функции от n переменных однозначным образом определяется дуальная к ней булева функция от n переменных.

Перечислим базовые свойства дуальной функции:

– дуальная функция $\widetilde{f}$ является бент-функций от n переменных;
– если $\widetilde{f}$ — дуальная функция бент-функции f, а $\widetilde{\widetilde{f}}$ — дуальная функция для $\widetilde{f}$, то $\widetilde{\widetilde{f}} = f$;
– отображение $f \to \widetilde{f}$, определённое на множестве бент-функций от n переменных, сохраняет расстояние Хэмминга [24].

Матрицей Сильвестра — Адамара называется квадратная матрица порядка 2^n, обозначаемая H_n, определяемая следующими рекуррентными соотношениями:

$$H_0 = (1), \qquad H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, n \geqslant 2.$$

Нетрудно видеть, что данная матрица является симметричной, кроме того, она позволяет получить описание преобразование Уолша — Адамара в матрично-векторной форме [15]. В терминах характеристических векторов и матрицы Сильвестра — Адамара бент-функцию можно определить следующим образом: пусть n — чётное число, тогда $f \in \mathcal{F}_n$ — бент-функция, если $H_n(-1)^f \in \{\pm 2^{n/2}\}^{2^n}$. Характеристический вектор дуальной функции $\widetilde{f}$ однозначным образом находится из условия

$$H_n(-1)^f = 2^{n/2}(-1)^{\widetilde{f}}.$$

Отображение дуальности определяется на множестве бент-функций от n переменных и действует по правилу $f \to \widetilde{f}$. В терминах характеристических векторов оно имеет следующую эквивалентную форму: $(-1)^f \to (-1)^{\widetilde{f}}$. Отметим, что на данный момент отображение дуальности является единственным известным изометричным отображением множества бент-функций, которое не расширяется до изометрии на множестве всех булевых функций от n переменных.

Рассмотрим известные результаты по изменению свойств бент-функции под действием отображения дуальности. X.-D. Hou в работе [49] было доказано следующее неравенство, связывающее алгебраические степени бент-функции и дуальной к ней.

Теорема ([49]). *Пусть $f \in \mathcal{B}_n$, тогда*

$$n/2 - \deg(f) \geqslant \frac{n/2 - \deg(\widetilde{f})}{\deg(\widetilde{f}) - 1}.$$

Из данного неравенства, следует, в частности, что если $\deg(f) = 2$, то справедливо $\deg(\widetilde{f}) = 2$. Аналогично, при $\deg(f) = n/2$ имеем $\deg(\widetilde{f}) = n/2$. Отметим, что последнее было отмечено ещё в работе J. F. Dillon [44].

Связь между значениями бент-функции и дуальной к ней на подпространствах булева куба описывает следующая

Теорема ([44]). *Пусть $f \in \mathcal{B}_n$, тогда для любого подпространства $V \subseteq \mathbb{F}_2^n$ справедливо*

$$\sum_{x \in V} f(x) = 2^{\dim V - 1} - 2^{n/2-1} + 2^{\dim V - n/2} \sum_{x \in V^\perp} \widetilde{f}(x),$$

где через $V^\perp$ обозначается подпространство, ортогональное подпространству V.

Данный результат позволяет получать соотношения между коэффициентами АНФ бент-функции и дуальной к ней.

Следствие. *Пусть $f \in \mathcal{B}_n$, тогда*

$$\sum_{x \preccurlyeq y} f(x) = 2^{\mathrm{wt}(y)-1} - 2^{n/2-1} + 2^{\mathrm{wt}(y)-n/2} \sum_{x \preccurlyeq y \oplus \mathbf{1}} \widetilde{f}(x),$$

где символ $u \preccurlyeq v$ означает покоординатное предшествование вектора $u \in \mathbb{F}_2^n$ вектору $v \in \mathbb{F}_2^n$.

Таким образом, некоторые результаты, полученные для дуальной функции, представляется возможным использовать для исследования свойств бент-функции.

Одной из открытых проблем в области бент-функций, тесно связанной с вопросом мощности данного множества функций, является *проблема декомпозиции*, впервые рассмотренная Н. Н. Токаревой в работе [80]. В виде гипотезы она формулируется следующим образом: пусть $n \geqslant 2$ — чётное число, тогда каждая булева функция от n переменных степени не выше $n/2$ может быть представлена в виде суммы двух бент-функций от n переменных. Обзор частных результатов по данной проблеме можно найти в статье [83]. Применительно к дуальным функциям интересен следующий результат Н. Н. Токаревой из работы [18].

Теорема ([18]). *Бент-функция от $n \geqslant 4$ переменных разложима в сумму двух бент-функций от n переменных тогда и только тогда, когда таким свойством обладает дуальная к ней бент-функция.*

Таким образом, упомянутая выше гипотеза не может рассматриваться отдельно для бент-функции и дуальной к ней, и свойство разложимости сохраняется под действием отображения дуальности.

Производной булевой функции $f \in \mathcal{F}_n$ *по направлению* $a \in \mathbb{F}_2^n$ называется булева функция $D_a f(x) = f(x) \oplus f(x \oplus a)$ от n переменных. Понятие производной булевой функции имеет тесную связь с характеризацией бент-функций. Известно [75], что булева функция $f \in \mathcal{F}_n$ является бент-функцией, если и только если её производная по любому ненулевому направлению уравновешенна. Как показано C. Carlet в работе [25] (см. также [22]), производные бент-функции и дуальной к ней связывает следующее соотношение.

Утверждение ([25]). *Пусть* $f \in \mathcal{B}_n$ *и* $a,b \in \mathbb{F}_2^n$, *обозначим*

$$d = \sum_{x \in \mathbb{F}_2^n} (-1)^{D_b f(x) \oplus \langle a,x \rangle}, \quad \widetilde{d} = \sum_{y \in \mathbb{F}_2^n} (-1)^{D_a \widetilde{f}(y) \oplus \langle b,y \rangle},$$

тогда

$$\begin{cases} \widetilde{d} = d, \\ d = (-1)^{\langle a,b \rangle} d. \end{cases}$$

Следствие. *Пусть* $a,b \in \mathbb{F}_2^n$ — *такие векторы, что* $\langle a,b \rangle = 1$, *тогда*

$$\sum_{y \in \mathbb{F}_2^n} (-1)^{D_a \widetilde{f}(y) \oplus \langle b,y \rangle} = \sum_{x \in \mathbb{F}_2^n} (-1)^{D_b f(x) \oplus \langle a,x \rangle} = 0.$$

Термин «дуальность» также встречается в других областях дискретной математики, в частности, в теории кодирования, где имеет иной смысл. *Дуальным* или *ортогональным* к линейному коду $C \in \mathbb{F}_2^n$ называется код

$$C^{\perp} = \{x \in \mathbb{F}_2^n : \langle x,y \rangle = 0 \text{ для каждого } y \in C\},$$

то есть такой код, кодовые слова которого ортогональны всем словам кода C. Очевидно, что $C^{\perp}$ также является линейным кодом. Код, совпадающий со своим дуальным, называется *самодуальным*. Отметим, что известные *соотношения Мак-Вильямс* [63], устанавливающие взаимосвязь между весовыми спектрами кода и дуального к нему, в англоязычной литературе часто именуются как «MacWilliams duality». Изучению булевых функций в контексте соотношений Мак-Вильямс и связанному с этим понятием дуальности посвящена статья J. Y. Hyun, H. Lee, Y. Lee [54]. Соответствующие самодуальные бент-функции, в том числе от малого числа переменных, изучались в работах [53; 78].

1.3 Самодуальные бент-функции

Бент-функция f называется *самодуальной*, если она совпадает со своей дуальной бент-функций, то есть $f = \widetilde{f}$.

Бент-функция f называется *анти-самодуальной*, если она совпадает с отрицанием своей дуальной бент-функции, то есть $f = \widetilde{f} \oplus 1$.

Множество самодуальных бент-функций от n переменных, согласно [50], обозначается через $\mathrm{SB}^+(n)$, а множество анти-самодуальных бент-функций от n переменных — через $\mathrm{SB}^-(n)$.

1.3.1 Характеристические векторы

Из определения самодуальности следует, что характеристический вектор самодуальной бент-функции является собственным вектором матрицы H_n, соответствующим собственному числу $2^{n/2}$. В свою очередь, характеристический вектор анти-самодуальной бент-функции является собственным вектором, соответствующим собственному числу $\left(-2^{n/2}\right)$. Данное наблюдение непосредственым образом использовалось в работах [9; 33; 41; 46] при определении (анти-)самодуальности и исследовании данных классов бент-функций. Таким образом, одним из известных подходов к работе с самодуальными бент-функциями является использование прямой связи с собственными векторами матрицы Сильвестра — Адамара, координаты которых суть числа ± 1. В этом случае изучение самодуальности включает характеризацию и исследование свойств данных векторов. Более подробную информацию о собственных векторах матриц Адамара порядка 2^n можно найти, например, в работе [85].

Как известно, собственные векторы вещественной симметричной матрицы, соответствующие различным собственным числам, ортогональны. Следовательно, можно охарактеризовать расстояние Хэмминга между самодуальной и анти-самодуальной бент-функциями.

Утверждение ([33]). *Расстояние Хэмминга между самодуальной и анти-самодуальной бент-функциями от n переменных равно 2^{n-1}.*

Также, с использованием отмеченного выше соответствия в работе [33] получен следующий результат.

Теорема ([33]). *Пусть* $Z \in \{\pm 1\}^{2^{n-1}}$, *тогда если справедливо*

$$Y = Z + \frac{2H_{n-1}}{2^{n/2}} Z \in \{\pm 1\}^{2^{n-1}},$$

то вектор (Y,Z) *является характеристическим вектором самодуальной бент-функции от* n *переменных, а вектор* $(Z,-Y)$ *— характеристическим вектором анти-самодуальной бент-функции от* n *переменных.*

Более того, характеристические векторы всех самодуальных и анти-самодуальных бент-функций удовлетворяют данному разложениию.

Из существования данного разложения следует взаимно-однозначное соответствие

$$\underbrace{(-1)^f = (Y,Z)}_{f\ -\ \text{самодуальная бент-функция}} \quad \Longleftrightarrow \quad \underbrace{(-1)^g = (Z,-Y)}_{g\ -\ \text{анти-самодуальная бент-функция}}$$

между самодуальными и анти-самодуальными бент-функциями от n переменных.

Следствие. $\left|\mathrm{SB}^+(n)\right| = \left|\mathrm{SB}^-(n)\right|$.

В силу того, что первая половина координат характеристического вектора (Y,Z), где $Y,Z \in \{\pm 1\}^{2^{n-1}}$, каждой самодуальной бент-функции от n переменных однозначно определяется второй половиной — вектором Z — по правилу

$$Y = Z + \frac{2H_{n-1}}{2^{n/2}} Z,$$

можно сделать следующий вывод:

Следствие. $\left|\mathrm{SB}^+(n)\right| \leqslant 2^{2^{n-1}}$.

Анализ характеристических векторов $Y,Z \in \{\pm 1\}^{2^{n-1}}$ показывает, что данную оценку можно усилить. Булева функция $f \in \mathcal{F}_n$ называется *платовидной порядка* r, где $0 \leqslant r \leqslant n$, если $W_f(y) \in \left\{0, \pm 2^{n-r/2}\right\}$ для каждого $y \in \mathbb{F}_2^n$. Заметим, что аффинные функции и бент-функции образуют крайние случаи, так как аффинная функция является платовидной порядка 0, а бент-функция от n переменных — порядка n.

Утверждение ([33]). *Пусть* $Z \in \{\pm 1\}^{2^{n-1}}$, *тогда если справедливо*

$$Y = Z + \frac{2H_{n-1}}{2^{n/2}} Z \in \{\pm 1\}^{2^{n-1}},$$

то векторы Y,Z *являются характеристическими векторами платовидных булевых функций порядка* $n-2$ *от* $n-1$ *переменной.*

Таким образом, число (анти-)самодуальных бент-функций от n переменных не превосходит числа платовидных булевых функций порядка $n-2$ от $n-1$ переменной.

1.3.2 Классы эквивалентности для малого числа переменных

Вопрос классификации самодуальных бент-функций на основе вычислительных экспериментов тесно связан с возможными способами перебора данных функций. В работе [33] представлен алгоритм перечисления всех самодуальных бент-функций от n переменных степени не выше r, явным образом использующий соответствие между характеристическими векторами самодуальных бент-функций и собственными векторами матрицы Сильвестра — Адамара, все координаты которых суть числа ± 1. Данный алгоритм основан на существовании разложения характеристического вектора самодуальной бент-функции от n переменных.

Алгоритм $\mathrm{SDB}(n,r)$:

1. Сгенерировать Z — характеристический вектор кодового слова кода $\mathrm{RM}(r,n-1)$;
2. Вычислить $Y = Z + \frac{2H_{n-1}}{2^{n/2}} Z$;
3. Если $Y \in \{\pm 1\}^{2^{n-1}}$, то вывести (Y,Z), иначе перейти к другому Z (вернуться на Шаг 1).

Используя взаимно-однозначное соответствие между самодуальными и анти-самодуальными бент-функциями, можно получить алгоритм перечисление всех анти-самодуальных бент-функций от n переменных степени не выше r [33].

Алгоритм $\mathrm{NSDB}(n,r)$:

1. Сгенерировать Z — характеристический вектор кодового слова кода $\mathrm{RM}(r,n-1)$;

2. Вычислить $Y = Z - \frac{2H_{m-1}}{2^{n/2}} Z$;
3. Если $Y \in \{\pm 1\}^{2^{m-1}}$, то вывести (Y,Z), иначе перейти к другому Z (вернуться на Шаг 1).

Время работы данных алгоритмов определяет мощность кода $\mathrm{RM}(r,n-1)$, равная 2^k, где

$$k = \sum_{j=0}^{r} \binom{n-1}{j},$$

что позволяет говорить о существенно меньшей временной сложности в сравнении с полным перебором.

Суть алгоритма $\mathrm{SDB}(n,r)$ заключается в нахождении всех решений $Y,Z \in \{\pm 1\}^{2^{n-1}}$ уравнения

$$\left(2^{n/2} I_{2^m-1} + 2H_{n-1}\right) Z - 2^{m/2} Y = \mathbf{0}$$

при условии, что Z — характеристический булевой функции от n переменных степени не выше r. Пусть G — порождающая матрица кода $\mathrm{RM}(r,n-1)$, тогда общая система целочисленного программирования имеет следующий вид:

$$\begin{pmatrix} \mathbf{0}_{2^{n-1}\times 2^{n-1}} & -I_{2^{n-1}} & G^{\mathrm{T}} & -2I_{2^{n-1}} \\ -2^{n/2+1} I_{2^{n-1}} & 2^{n/2+1} I_{2^{n-1}} + 4H_{n-1} & \mathbf{0}_{k\times k} & \mathbf{0}_{2^{n-1}\times 2^{n-1}} \end{pmatrix} \begin{pmatrix} y \\ z \\ w \\ s \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ v \end{pmatrix},$$

где $w \in \{0,1\}^k$, $y,z \in \{0,1\}^{2^{n-1}}$, $s \in \mathbb{Z}_+^{2^{n-1}}$ — неизвестные, и $v = 2H_{n-1}(1,1,\ldots,1)^{\mathrm{T}}$.

В статье [46] авторами предложен способ уменьшения времени работы с помощью введения дополнительных ограничений. Алгоритм $\mathrm{SDB}(m,r)$, а также его дальнейшее развитие с помощью введения данных ограничений, были использованы в работах [33; 46] для поиска класов эквивалентности самодуальных бент-функций от малого числа переменных.

В работах [33; 46] исследовались отображения множества булевых функций от n переменных в себя, сохраняющие самодуальность. В статье [33] показано, что отображение вида

$$f(x) \longrightarrow f(Lx) \oplus d,$$

где $L \in \mathcal{O}_n$, $d \in \mathbb{F}_2$, сохраняет самодуальность бент-функции. Более общий вид отображений, обладающих данным свойством, представлен в [46]:

Теорема ([46]). *Отображения множества булевых функций, имеющие вид*

$$f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x \rangle \oplus d, \tag{1.4}$$

где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — *чётное число,* $d \in \mathbb{F}_2$, *сохраняют самодуальность бент-функции.*

Группа преобразований, действующих на множестве всех булевых функций от n переменных по правилу (1.4), называется *расширенной ортогональной группой* и обозначается $\overline{\mathcal{O}}_n$ [41; 46]. Отметим, что каждое такое отображение является частным случаем расширенного аффинного преобразования и, следовательно, не меняет степень функции. Известно, что группа $\overline{\mathcal{O}}_n$ является подгруппой группы $\mathrm{GL}\,(n+2,\mathbb{F}_2)$ [46]. Расширенная ортогональная группа использовалась для классификации самодуальных бент-функций, представленной в статьях [33; 46].

Далее будем говорить, что самодуальные бент-функции f,g от n переменных являются *эквивалентными*, если существует преобразование, являющееся элементом расширенной ортогональной группы $\overline{\mathcal{O}}_n$, которое отображает функцию f в g.

С помощью алгоритма $\mathrm{SDB}(n,r)$ получена следующая

Теорема ([33]). *Существует* 1, 2 *и* 8 *классов эквивалентности самодуальных бент-функций от* 2, 4 *и* 6 *переменных, соответственно, и* 4 *класса эквивалентности квадратичных самодуальных бент-функций от* 8 *переменных.*

К примеру, для случая двух переменных самодуальными являются всего две бент-функции: x_1x_2 и $x_1x_2 \oplus 1$. Они, очевидно, принадлежат одному классу эквивалентности. Для четырёх переменных есть два класса эквивалентности: первый содержит 12 самодуальных бент-функций, его представителем является функция $x_1x_2 \oplus x_3x_4$, а второй — 8 функций, его представитель — функция $x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_3 \oplus x_1$.

Дальнейшее исследование классов эквивалентности самодуальных бент-функций от 8 переменных было продолжено в работе [46]. Для проведения вычислительных экспериментов была разработана усовершенствованная версия алгоритма $\mathrm{SDB}(m,r)$, в рамках которой с помощью введения дополнительных ограничений удалось уменьшить пространство перебора.

Теорема ([46]). *Существует* 4 *и* 45 *классов эквивалентности самодуальных бент-функций от* 8 *переменных степени два и три, соответственно. Общее число самодуальных бент-функций от* 8 *переменных степени два и три равно* 104 960 *и* 1 162 420 992*, соответственно.*

В статье [46] отмечено, что при отсутствии ограничений на степень искомой функции вычислительные эксперименты показали существование не менее 36 732 классов эквивалентности самодуальных бент-функций от 8 переменных. Эти классы содержат не менее $1\ 665\ 560\ 535\ 367\ 680 \simeq 2^{50.56}$ различных самодуальных бент-функций.

В таблице 1.1 собраны известные (см. [33; 46]) количественные характеристики по классификации самодуальных бент-функций от $n \leqslant 8$ переменных.

	Степень	Число классов	Число функций	Общее число функций
$n = 2$	2	1	2	2
$n = 4$	2	2	20	20
$n = 6$	2	3	752	42 896
	3	5	42 144	
$n = 8$	2	4	104 960	$\geqslant 1\ 665\ 560\ 535\ 367\ 680 \simeq 2^{50.56}$
	3	45	1 162 420 992	
	4	$\geqslant 36\ 683$	...	

Таблица 1.1 — Количественные характеристики по классификации самодуальных бент-функций от n переменных

1.3.3 Квадратичные функции

В данном разделе будут изложены основные результаты работы X.-D. Hou [50], в которой представлена классификация квадратичных самодуальных и анти-самодуальных бент-функций относительно действия ортогональной группы.

Хорошо известно (см., например, [44]), что для квадратичных бент-функций от n переменных существует всего один класс расширенной аффинной

эквивалентности, его представитель — бент-функция

$$f(x) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-1}x_n, \;\; x \in \mathbb{F}_2^n.$$

Мощность данного класса, согласно [58] (см. также [63]), равна

$$2^{\frac{1}{4}\left(n^2+2n+4\right)} \prod_{i=0}^{n/2-1} \left(2^{2i+1}-1\right). \tag{1.5}$$

Известно [4; 5], что на квадратичных бент-функциях, и только на них, достигаются некоторые экстремальные значения метрических характеристик, связанных с минимальным расстоянием между бент-функциями.

Приведём некоторые обозначения. Через $A \boxplus B$ обозначим блочное сложение матриц: пусть $A \in M_k(\mathbb{F}_2)$ и $B \in M_r(\mathbb{F}_2)$, тогда

$$A \boxplus B = \begin{pmatrix} A & \mathbf{0}_{k\times r} \\ \mathbf{0}_{r\times k} & B \end{pmatrix} \in M_{k+r}(\mathbb{F}_2).$$

Пусть $U_n \in M_n(\mathbb{F}_2)$ — верхняя треугольная матрица с нулевой диагональю, все остальные элементы которой равны 1. Через $\operatorname{diag}(d_1,d_2,\ldots,d_n)$ обозначим диагональную матрицу размера $n \times n$, диагональные элементы которой равны $d_1,d_2,\ldots,d_n$, соответственно. Пусть $J_n \in M_n(\mathbb{F}_2)$ — матрица, все элементы которой равны 1.

Теорема ([50])**.** *Квадратичная функция от n переменных*

$$f(x) = \langle x, Qx \rangle \oplus d$$

является (анти-)самодуальной бент-функций тогда и только тогда, когда справедливо

$$\left(Q \oplus Q^{\mathrm{T}}\right)^2 = I_n,$$

и матрица

$$\left(Q \oplus Q^{\mathrm{T}}\right) Q \left(Q \oplus Q^{\mathrm{T}}\right) \oplus Q^{\mathrm{T}}$$

является симплектической.

Будем называть квадратные матрицы A и B *ортогонально подобными*, если существует квадратная ортогональная матрица P такая, что $A = PBP^{\mathrm{T}}$. В силу того, что ассоциированные симплектические матрицы (анти-)самодуальных

бент-функций являются инволютивными, классификация данных функций влечёт знание классификации инволютивных симплектических матриц относительно действия ортогональной группы. Данная классификация описывается в следующей

Теорема ([50]). *Каждая инволютивная симплектическая матрица ортогонально подобна одной из следующих канонических форм*

$$C_{s,t} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \cdots \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{s} \boxplus (I_t \oplus J_t)\,,$$

где $0 \leqslant s \leqslant n/2 - 1$ *и* $2s + t = n$.

В настоящем разделе определим действие элемента $L \in \mathcal{O}_n$ на $f \in \mathrm{SB}^+(n)$, как функцию $f(L^{\mathrm{T}}x) \in \mathrm{SB}^+(n)$. Две самодуальных бент-функции от n переменных f,g будем называть *ортогонально эквивалентными*, если существует элемент $L \in \mathcal{O}_n$ такой, что $f\,(Lx) = g(x)$ для всех $x \in \mathbb{F}_2^n$, то есть эти функции принадлежат одной орбите относительно действия группы $\mathcal{O}_n$. Далее будем представлена классификация квадратичных (анти-)самодуальных бент-функций относительно действия ортогональной группы.

Теорема ([50]). *Пусть* f *— квадратичная самодуальная или анти-самодуальная бент-функция от* n *переменных такая, что* $f(\mathbf{0}) = 0$. *Пусть ассоциированная симплектическая матрица функции* f *ортогонально подобна матрице* $C_{s,t}$, *где* $0 \leqslant s \leqslant n/2 - 1$ *и* $2s + t = n$. *Тогда при*

1) $s > 0$ *функция* f *ортогонально эквивалентна одной из следующих канонических форм:*

$$g^0_{s,t}(x) = \langle x, Q^{(0)}x\rangle,$$
$$g^1_{s,t}(x) = \langle x, Q^{(1)}x\rangle,$$

где

$$Q^{(0)} = \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \boxplus \cdots \boxplus \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{s} \boxplus \left(U_t \oplus \operatorname{diag}\left(c_1,c_2,\ldots,c_t\right)\right),$$

$$Q^{(1)} = \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \boxplus \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \boxplus \cdots \boxplus \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{s} \boxplus \left(U_t \oplus \operatorname{diag}\left(c_1,c_2,\ldots,c_t\right)\right),$$

где $c = (c_1,c_2,\ldots,c_t) \in \mathbb{F}_2^t$ *— такой вектор, что* $\operatorname{wt}(c) = n/2 - s + 1$*;*

2) $s = 0$ *есть два случая. Для нечётного* $n/2$ *функция* f *ортогонально эквивалентна одной из следующих канонических форм:*

$$h_n^0(x) = \langle x,U_n x\rangle,$$
$$h_n^2(x) = \langle x, \left(U_n \oplus \operatorname{diag}\left(1,1,0,0,\ldots,0\right)\right) x\rangle.$$

При чётном $n/2$ *функция* f *ортогонально эквивалентна одной из следующих канонических форм:*

$$h_n^1(x) = \langle x, \left(U_n \oplus \operatorname{diag}\left(1,0,0,\ldots,0\right)\right) x\rangle,$$
$$h_n^3(x) = \langle x, \left(U_n \oplus \operatorname{diag}\left(1,1,1,0,0,\ldots,0\right)\right) x\rangle.$$

Более того, справедливо

$$g^0_{s,t} \in \begin{cases} \mathrm{SB}^+(n), & \textit{при } n/2 - s \equiv 1{,}2 \pmod 4, \\ \mathrm{SB}^-(n), & \textit{при } n/2 - s \equiv 0{,}3 \pmod 4, \end{cases}$$

$$g^1_{s,t} \in \begin{cases} \mathrm{SB}^-(n), & \textit{при } n/2 - s \equiv 1{,}2 \pmod 4, \\ \mathrm{SB}^+(n), & \textit{при } n/2 - s \equiv 0{,}3 \pmod 4, \end{cases}$$

$$h^0_n \in \begin{cases} \mathrm{SB}^+(n), & \textit{при } n/2 \equiv 1 \pmod 4, \\ \mathrm{SB}^-(n), & \textit{при } n/2 \equiv 3 \pmod 4, \end{cases}$$

$$h^2_n \in \begin{cases} \mathrm{SB}^-(n), & \textit{при } n/2 \equiv 1 \pmod 4, \\ \mathrm{SB}^+(n), & \textit{при } n/2 \equiv 3 \pmod 4, \end{cases}$$

$$h^1_n \in \begin{cases} \mathrm{SB}^-(n), & \textit{при } n/2 \equiv 0 \pmod 4, \\ \mathrm{SB}^+(n), & \textit{при } n/2 \equiv 2 \pmod 4, \end{cases}$$

$$h^3_n \in \begin{cases} \mathrm{SB}^+(n), & \textit{при } n/2 \equiv 0 \pmod 4, \\ \mathrm{SB}^-(n), & \textit{при } n/2 \equiv 2 \pmod 4. \end{cases}$$

Мощность каждой из орбит определяет мощность соответствующего класса эквивалентности.

Теорема ([50]). *Для канонических форм из предыдущей теоремы справедливо*

$$\left|\left[g^0_{s,t}\right]\right| = \left|\left[g^1_{s,t}\right]\right| = \begin{cases} 2^{n+\frac{1}{4}\left(s^2-4s-9\right)} \dfrac{\prod\limits_{i=\frac{s+1}{2}}^{n/2-1}\left(2^{2i}-1\right)}{\prod\limits_{i=1}^{n/2-s-1}\left(2^{2i}-1\right)}, & \textit{если } s \textit{ — нечётное}, \\ 2^{n+\frac{1}{4}\left(s^2-2s-8\right)} \dfrac{\prod\limits_{i=s/2+1}^{n/2-1}\left(2^{2i}-1\right)}{\prod\limits_{i=1}^{n/2-s-1}\left(2^{2i}-1\right)}, & \textit{если } s \textit{ — чётное}, \end{cases}$$

$$\begin{aligned} \left|\left[h^0_n\right]\right| = \left|\left[h^2_n\right]\right| &= 2^{n-2}, \qquad \textit{если } n/2 \textit{ — нечётное}, \\ \left|\left[h^1_n\right]\right| = \left|\left[h^3_n\right]\right| &= 2^{n-2}, \qquad \textit{если } n/2 \textit{ — чётное}. \end{aligned}$$

Для $n \leqslant 12$ в таблице 1.2 приведены численные данные по количеству квадратичных бент-функций от n переменных, полученные с помощью формулы (1.5), а также численные данные по количеству самодуальных бент-функций от n переменных.

	$n=2$	$n=4$	$n=6$	$n=8$	$n=10$	$n=12$
$\left\lvert \mathrm{SB}^{+}(n) \right\rvert$, $\deg=2$	2	20	752	$\simeq 2^{16.68}$	$\simeq 2^{25.75}$	$\simeq 2^{36.78}$
$\lvert \mathcal{B}_n \rvert$, $\deg=2$	8	896	1 777 664	$\simeq 2^{35.75}$	$\simeq 2^{54.75}$	$\simeq 2^{77.75}$
$\frac{\log_2 \lvert \mathcal{B}_n \rvert}{\log_2 \left\lvert \mathrm{SB}^{+}(n) \right\rvert}$, $\deg=2$	3	≈ 2.269	≈ 2.173	≈ 2.143	≈ 2.126	≈ 2.113

Таблица 1.2 — Сравнение числа квадратичных функций от n переменных

Таким образом, задача классификации самодуальных бент-функций минимально возможной степени — квадратичных функций — имеет достаточно нетривиальное решение, требующее, в частности, наличия классификации инволютивных симплектических матриц. Отметим, что глава 5 настоящей диссертации посвящена исследованию метрических свойств одного известного подкласса квадратичных самодуальных бент-функций.

1.3.4 Конструкции

Рассмотрим прямые конструкции самодуальных бент-функций. Бент-функции от n переменных, представимые в виде

$$f(x,y) = \langle x,\pi(y)\rangle \oplus g(y), \;\; x,y \in \mathbb{F}_2^{n/2},$$

где π — перестановка на множестве $\mathbb{F}_2^{n/2}$, а g — булева функция от $n/2$ переменных, формируют хорошо известный *класс Мэйорана — МакФарланда* [66]. Данный класс имеет мощность, равную $\left(2^{n/2}!\right) \cdot 2^{2^{n/2}}$. Обозначим данный класс через $\mathcal{M}_n$. Дуальная функция бент-функции Мэйорана — МакФарланда $f(x,y)$ имеет вид

$$\widetilde{f}(x,y) = \left\langle \pi^{-1}(x),y\right\rangle \oplus g\left(\pi^{-1}(x)\right), \;\; x,y \in \mathbb{F}_2^{n/2},$$

Через $\mathrm{SB}^{+}_{\mathcal{M}}(n)$ обозначим множество самодуальных бент-функций от n переменных из класса Мэйорана — МакФарланда, а через $\mathrm{SB}^{-}_{\mathcal{M}}(n)$ — множество анти-самодуальных бент-функций от n переменных из класса Мэйорана — МакФарланда. В работе [33] найдены необходимые и достаточные условия (анти-)самодуальности таких бент-функций.

Теорема ([33]). *Бент-функция Мэйорана — МакФарланда $f(x,y)$ является самодуальной (анти-самодуальной) тогда и только тогда, когда*

$$\pi(y) = L(y \oplus c),\ \ g(y) = \langle c,y\rangle \oplus d,\ \ y \in \mathbb{F}_2^{n/2},$$

где $L \in \mathcal{O}_{n/2}$, $c \in \mathbb{F}_2^{n/2}$, $\mathrm{wt}(c)$ — чётное (нечётное) число, $d \in \mathbb{F}_2^n$.

Следствие. $\left|\mathrm{SB}^+_{\mathcal{M}}(n)\right| = \left|\mathrm{SB}^-_{\mathcal{M}}(n)\right| = 2^{n/2} \cdot \left|\mathcal{O}_{n/2}\right|$.

Отметим, что все самодуальные бент-функции из класса Мэйорана — МакФарланда являются квадратичными. Также отметим связь данных функций с самодуальными кодами.

Утверждение. *В условиях предыдущей теоремы, линейный код с проверочной матрицей $\left(I_{n/2},L\right)$ является самодуальным, а вектор (Lc,c) — его кодовым словом. Обратно, каждой упорядоченной паре (H,v), состоящей из проверочной матрицы H самодуального кода C длины n и кодового слова $v \in C$, можно поставить в соответствие самодуальную бент-функцию из класса $\mathrm{SB}^+_{\mathcal{M}}(n)$.*

Вопрос существования квадратичных самодуальных бент-функций за пределами класса Мэйорана — МакФарланда в работе [33] был обозначен в качестве открытого. J. Rifà и В. А. Зиновьев в статье [74] предложили конструкцию квадратичных самодуальных бент-функций, не являющихся бент-функциями из класса Мэйорана — МакФарланда, но расширенно аффинно эквивалентных им.

Класс *бент-функций Диллона*, также обозначаемый $\mathcal{PS}_{ap}$, состоит из функций вида $f(x,y) = g(x/y)$, $x,y \in \mathbb{F}_{2^{n/2}}$ (с соглашением $x/0 = 0$ для всех $x \in \mathbb{F}_{2^{n/2}}$), где булева функция $g : \mathbb{F}_{2^{n/2}} \to \mathbb{F}_2$ является уравновешенной и $g(0) = 0$. Дуальная функция бент-функции Диллона $f(x,y)$ имеет вид $\widetilde{f}(x,y) = g(y/x)$, $x,y \in \mathbb{F}_{2^{n/2}}$. Справедлива следующая

Теорема ([33]). *Бент-функция Диллона является самодуальной, если $g(1) = 0$ и $g(u) = g(1/u)$ для каждого $u \in \mathbb{F}_{2^{n/2}}$, отличного от $0,1$.*

Следствие. *Число самодуальных бент-функций Диллона равно* $\binom{2^{n/2-1}-1}{2^{n/2-2}}$.

Выходя за рамки класса $\mathcal{PS}_{ap}$ и рассматривая отрицания данных функций, можно получить следующее

Следствие. *Пусть* $g : \mathbb{F}_{2^{n/2}} \to \mathbb{F}_2$ *— булева функция такая, что* $g(1) = g(0)$ *и* $g(u) = g(1/u)$ *для каждого ненулевого* $u \in \mathbb{F}_{2^{n/2}}$*. Если* g *— уравновешенная функция, то булева функция* $f(x,y) = g(x/y)$*,* $x,y \in \mathbb{F}_{2^{n/2}}$ *(с соглашением* $1/0 = 0$*), будет самодуальной бент-функцией от* n *переменных.*

Приведём следующую простую конструкцию самодуальных бент-функций, основанную на так называемой *прямой сумме* бент-функций. Предполагается, что n,m — чётные натуральные числа. Пусть $f \in \mathrm{SB}^+(n) \cup \mathrm{SB}^-(n)$. В соответствии с обозначениями из работы [33] будем говорить, что *дуальность* функции f равна 0, если $f \in \mathrm{SB}^+(n)$, и 1 — иначе. Тогда

Утверждение ([33])**.** *Пусть* $f \in \mathrm{SB}^+(n) \cup \mathrm{SB}^-(n)$*,* $g \in \mathrm{SB}^+(m) \cup \mathrm{SB}^-(m)$*, и дуальности данных функций равны* ε_f *и* ε_g*, соответственно. Тогда для булевой функции* $h(x,y) = f(x) \oplus g(y)$*,* $x \in \mathbb{F}_2^n$*,* $y \in \mathbb{F}_2^m$*, от* $n+m$ *переменных справедливо*

$$h \in \begin{cases} \mathrm{SB}^+(n+m), & \text{если } \varepsilon_f \oplus \varepsilon_g = 0, \\ \mathrm{SB}^-(n+m), & \text{если } \varepsilon_f \oplus \varepsilon_g = 1, \end{cases}$$

Следующая итеративная конструкция позволяет по каждой бент-функции от n переменных построить самодуальную бент-функцию от $n+2$ переменных.

Утверждение ([33])**.** *Пусть* F *— характеристический вектор бент-функции от* n *переменных. Тогда вектор* $\left(F,\widetilde{F},\widetilde{F},-F\right)$ *будет являться характеристическим вектором самодуальной бент-функции от* $n+2$ *переменных.*

Следствие. *Справедливо* $|\mathcal{B}_n| \leqslant \left|\mathrm{SB}^+(n+2)\right|$.

Следующая конструкция, основанная на использовании трёх самодуальных бент-функций, предложена в работе [68].

Утверждение ([68])**.** *Пусть* f_1,f_2,f_3 *— самодуальные бент-функции от* n *переменных такие, что функция* $f_1 \oplus f_2 \oplus f_3$ *является самодуальной бент-функцией от* n *переменных. Тогда функция*

$$f(x) = f_1(x)f_2(x) \oplus f_1(x)f_3(x) \oplus f_2(x)f_3(x), \;\; x \in \mathbb{F}_2^n,$$

также будет являться самодуальной бент-функцией от n *переменных.*

Вопрос существования набора из трёх различных анти-самодуальных бент-функций от n переменных таких, что их сумма снова будет анти-самодуальной бент-функцией от n переменных, был отмечен S. Mesnager в качестве открытой проблемы [68]. В работе [37] с использованием алгебраической конструкции построено семейство анти-самодуальных бент-функций от n переменных, обладающее следующим свойством: сумма любых трёх функций из данного семейства снова является анти-самодуальной бент-функцией от n переменных. Данное семейство функций позволило получить решение указанной выше проблемы.

Представим некоторые известные алгебраические конструкции самодуальных бент-функций. Пусть $\mathbb{F}_{2^k}$ — подполе $\mathbb{F}_{2^n}$. Тогда *функция следа* $\mathrm{Tr}_k^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ определяется как

$$\mathrm{Tr}_k^n(x) = x + x^{2^k} + x^{2^{2k}} + x^{2^{3k}} + \ldots + x^{2^{n-k}}, \ \ x \in \mathbb{F}_{2^n}.$$

Утверждение ([39]). *Пусть $\varphi_1,\varphi_2,\varphi_3$ — инволюции, определённые на $\mathbb{F}_{2^n}$. Тогда функция*

$$\begin{aligned} g(x,y) = {} & \mathrm{Tr}_1^m\left(x\varphi_1(y)\right)\mathrm{Tr}_1^m\left(x\varphi_2(y)\right) \\ & + \mathrm{Tr}_1^m\left(x\varphi_1(y)\right)\mathrm{Tr}_1^m\left(x\varphi_3(y)\right) \\ & + \mathrm{Tr}_1^m\left(x\varphi_2(y)\right)\mathrm{Tr}_1^m\left(x\varphi_3(y)\right), \ \ x,y \in \mathbb{F}_{2^m}, \end{aligned}$$

будет являться бент-функцией от $2m$ переменных, если и только если $\varphi_1 + \varphi_2 + \varphi_3$ — также инволюция. Более того, бент-функция g будет самодуальной бент-функцией.

Пусть t,m — натуральные числа, при этом t является делителем m. Пусть f — отображение вида $\mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$. Элемент $\alpha \in \mathbb{F}_{2^m}$ называется a-линейным транслятором функции f, если

$$f(x + \alpha u) - f(x) = au, \ \ x \in \mathbb{F}_{2^n}, u \in \mathbb{F}_{2^t}.$$

Теорема ([62]). *Пусть t,m — натуральные числа, при этом t является делителем m. Пусть $f_1,f_2,\ldots,f_k$ — отображения вида $\mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$. Положим γ_{rj} ($1 \leqslant r \leqslant 3$, $1 \leqslant j \leqslant k$) — 0-линейный транслятор для каждой f_i, где $i = 1,2,\ldots,k$. Тогда для k произвольных отображений $h_1,h_2,\ldots,h_k$ вида $\mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$*

булева функция

$$g(x,y) = \mathrm{Tr}_1^m(xy) + \mathrm{Tr}_1^m\left(x\sum_{i=1}^{k}\gamma_{1i}h_i(f_i(y))\right)\mathrm{Tr}_1^m\left(x\sum_{i=1}^{k}\gamma_{2i}h_i(f_i(y))\right) + \mathrm{Tr}_1^m\left(x\sum_{i=1}^{k}\gamma_{1i}h_i(f_i(y))\right)\mathrm{Tr}_1^m\left(x\sum_{i=1}^{k}\gamma_{3i}h_i(f_i(y))\right) + \mathrm{Tr}_1^m\left(x\sum_{i=1}^{k}\gamma_{2i}h_i(f_i(y))\right)\mathrm{Tr}_1^m\left(x\sum_{i=1}^{k}\gamma_{3i}h_i(f_i(y))\right), \quad x,y \in \mathbb{F}_{2^m}$$

будет являться самодуальной бент-функцией от $2m$ *переменных.*

Другие алгебраические конструкции самодуальных бент-функций, в том числе основанные на использовании инволюций, представлены в работах [39; 62; 68].

Таким образом, существует ряд прямых конструкций самодуальных бент-функций. Также известны конструкции, предполагающие наличие самодуальных бент-функций, в некоторых случаях зависящих от меньшего числа переменных. Тем не менее, в ряде случаев сложный вид конструкций затрудняет исследование мощности порождаемых ими множеств самодуальных бент-функций, а также сравнение с другими полученными конструкциями на предмет возможных пересечений. Также стоит отметить, что известные оценки числа самодуальных бент-функций далеки от их точного числа, что говорит об актуальности вопроса поиска новых конструкций и исследовании мощностей, порождаемых ими множеств функций.

1.3.5 Оценки числа самодуальных бент-функций

Пусть $f \in \mathcal{F}_n$, через C_f обозначим *носитель* функции f, то есть множество значений аргумента, на которых функция f принимает значение 1:

$$C_f = \{x \in \mathbb{F}_2^n : f(x) = 1\}.$$

Согласно [53] (см. также [63]), код $C \subseteq \mathbb{F}_2^n$ называется *формально самодуальным* относительно однородного многочлена $F_C(x,y)$ степени n, ассоциированного с C, если

$$F_C(x,y) = F_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

Если C — формально самодуальный код, то функция $f \in \mathcal{F}_n$, такая, что $C_f = C$, называется *формально самодуальной* булевой функцией.

Пусть $C \subseteq \mathbb{F}_2^n$, обозначим через $A_i(C)$ — количество кодовых слов кода C, вес Хэмминга которых равен i, $i = 0,1,\ldots,n$. Положим

$$W_C^+(x,y) = W_C(x,y) + 2^{n/2-1}x^n,$$

где

$$W_C(x,y) = \sum_{i=0}^{n} A_i(C)\, x^{n-i}y^i$$

— *весовая функция* кода C. Более подробную информацию о весовых спектрах кодов можно найти в монографии [63].

В работе [53] исследовались формально самодуальные булевы функции, носитель которых формально самодуален относительно многочлена $W_C^+(x,y)$. Доказано, что каждая самодуальная бент-функция является формально самодуальной, и для каждой самодуальной бент-функции f от n переменных справедливо

$$W_{C_f}(x,y) = -2^{n/2-1}x^n + \sum_{j=0}^{n/2} a_j \left(x^2+y^2\right)^{n/2-j} \left(xy-y^2\right)^j,$$

где $a_0,a_1,\ldots,a_{n/2} \in \mathbb{Z}$ — некоторый набор коэффициентов. Ясно, что каждый набор $\left(a_0,a_1,\ldots,a_{n/2}\right) \in \mathbb{Z}^{n/2+1}$ соотношением

$$-2^{n/2-1}x^n + \sum_{j=0}^{n/2} a_j \left(x^2+y^2\right)^{n/2-j} \left(xy-y^2\right)^j = \sum_{i=0}^{n} k_i x^{n-i}y^i$$

определяет некоторый набор чисел $k_0,k_1,\ldots,k_n \in \mathbb{Z}$. Обозначим через

$$\mathcal{T} = \left\{ \left(a_0,a_1,\ldots,a_{n/2}\right) \in \mathbb{Z}^{n/2+1} : 0 \leqslant k_i \leqslant \binom{n}{i},\ i = 0,1,2,\ldots,n \right\},$$

множество всех наборов коэффициентов, определяющих наборы чисел, которые задают весовую функцию некоторого двоичного кода длины n. Каждый такой код C имеет ровно k_i кодовых слов веса i. Условием $C_f = C$ можно определить булеву функцию f, при этом имеем $A_i(C_f) = A_i(C_f,\boldsymbol{a}) = k_i$. Для фиксированного набора $\boldsymbol{a} = \left(a_0,a_1,\ldots,a_{n/2}\right) \in \mathcal{T}$ обозначим множество всех булевых

функций, соответствующих всем таким кодам, через

$$\mathcal{F}_n^{\boldsymbol{a}} = \left\{ f \in \mathcal{F}_n : \sum_{i=0}^{n} A_i\left(C_f\right) x^{n-i} y^i = \right.$$
$$\left. -2^{n/2-1} x^n + \sum_{j=0}^{n/2} a_j \left(x^2+y^2\right)^{n/2-j} \left(xy-y^2\right)^j \right\}.$$

Имеем включение $\mathrm{SB}^+(n) \subseteq \bigcup\limits_{\boldsymbol{a}\in\mathcal{T}} \mathcal{F}_n^{\boldsymbol{a}}$. Таким образом, справедлива следующая

Теорема ([53]). *Количество самодуальных бент-функций от n переменных не превосходит числа*

$$\sum_{\boldsymbol{a}\in\mathcal{T}} \prod_{i=0}^{n} \binom{\binom{n}{i}}{A_i\left(C_f, \boldsymbol{a}\right)}.$$

В таблице 1.3 представлены численные значения для данной верхней оценки и нижних оценок, полученных на основе конструкций, представленных в разделе 1.3.4. В силу существования взаимно-однозначного соответствия между самодуальными и анти-самодуальными бент-функциями (см. раздел 1.3.1), данные оценки справедливы также для количества анти-самодуальных бент-функций.

	$n = 2$	$n = 4$	$n = 6$	$n = 8$
Известные нижние оценки				
Класс Диллона $\mathcal{PS}_{ap}$ (с отрицанием функций)	2	2	6	70
Класс Мэйорана — МакФарланда	2	8	48	768
Квадратичные функции	2	20	752	$\simeq 2^{16.68}$
Прямая сумма двух (анти-)самодуальных бент-функций	–	8	80	$\simeq 2^{17.39}$
Итеративная конструкция (Carlet и др., 2010)	–	8	896	$\simeq 2^{32.34}$
Известные верхние оценки				
Характеристические векторы[a]	4	112	$\simeq 2^{23.74}$	2^{128}
Формально самодуальные функции	6	3 220	$\cdots$	$\cdots$
Число самодуальных бент-функций от n переменных				
	2	**20**	$\mathbf{42\,896 \simeq 2^{15.39}}$	$\mathbf{\geqslant 2^{50.56}}$
Число бент-функций от n переменных				
	8	896	$\simeq 2^{32.34}$	$\simeq 2^{106.29}$
$\frac{\log_2 \log_2 \lvert \mathrm{SB}^+(n) \rvert}{\log_2 \log_2 \lvert \mathcal{B}_n \rvert}$	–	≈ 0.641	≈ 0.786	$\geqslant 0.840$

Таблица 1.3 — Известные оценки числа самодуальных бент-функций от n переменных

[a] Для $n \leqslant 6$ используется число платовидных функций порядка $n-2$ от $n-1$ переменной

1.4 Отношение Рэлея бент-функции

Настоящий раздел посвящён изложению известных результатов касательно отношения Рэлея и расстояния между бент-функцией и дуальной к ней.

1.4.1 Определение и основные свойства

Согласно [33; 41] *отношением Рэлея* (the Rayleigh quotient) S_f булевой функции f от n переменных называется величина

$$S_f = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x,y \rangle} = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} W_f(y).$$

Для $f \in \mathcal{B}_n$ определяется *нормализованное отношение Рэлея* N_f

$$N_f = \frac{1}{2^{n/2}} S_f = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \widetilde{f}(x)}.$$

Значение данной величины для бент-функций обусловлено следующим наблюдением. Из равенства

$$\frac{1}{2^{n/2}} S_f = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \widetilde{f}(x)} = 2^n - 2 \cdot \mathrm{dist}(f, \widetilde{f})$$

следует, что

$$\mathrm{dist}(f, \widetilde{f}) = 2^{n-1} - \frac{1}{2^{n/2+1}} S_f,$$

то есть отношение Рэлея полностью характеризует расстояние Хэмминга между бент-функцией $f \in \mathcal{B}_n$ и дуальной к ней функцией $\widetilde{f}$.

В работах [33; 41] исследовалось отношение Рэлея бент-функций. Доказана следующая оценка

Теорема ([33]). *Абсолютное значение отношения Рэлея булевой функции от чётного числа переменных n не превосходит числа $2^{3n/2}$, при этом данная оценка достигается на самодуальных $\left(+2^{3n/2}\right)$ и анти-самодуальных бент-функциях $\left(-2^{3n/2}\right)$, и только на них.*

В терминах характеристических векторов отношение Рэлея булевой функции $f \in \mathcal{F}_n$ с характеристическим вектором F, выглядит следующим образом

$$S_f = \langle F, H_n F \rangle .$$

Используя известные утверждения касательно экстремальных значений отношения Рэлея эрмитовой матрицы и его связи с собственными числами и соответствующими им собственными векторами, можно получить утверждение, аналогичное приведённой выше оценке для абсолютного значения S_f.

Поиск максимального значения отношения Рэлея булевой функции от нечётного числа переменных является открытой проблемой [33; 41]. Сложность по сравнению со случаем чётного n обусловлена тем, что собственные векторы матрицы Сильвестра — Адамара H_n при нечётном n уже не могут являться элементами множества $\{\pm 1\}^{2^n}$. Известна следующая оценка

Теорема ([33]). *Пусть $m \geqslant 3$ — нечётное число, тогда*

$$\max_{f \in \mathcal{F}_m} |S_f| \geqslant 2^{(3m-1)/2}.$$

Данная оценка была получена с помощью конкатенации векторов значений двух самодуальных бент-функций от $m-1$ переменных.

В работе [41] изучались отображения, оставляющие класс бент-функций от n переменных на месте и сохраняющие отношение Рэлея каждой бент-функции от n переменных.

Теорема ([41]). *Пусть $f \in \mathcal{B}_n$, тогда для бент-функций $g, h \in \mathcal{B}_n$, определённых как*

$$g(x) = f(Lx) \oplus d, \;\; x \in \mathbb{F}_2^n,$$
$$h(x) = f(x \oplus c) \oplus \langle c, x \rangle , \;\; x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$, справедливо

$$N_g = N_f,$$
$$N_h = (-1)^{\langle c, c \rangle} N_f.$$

Отсюда следует, что действие расширенной ортогональной группы $\overline{\mathcal{O}}_n$ не меняет отношение Рэлея каждой бент-функции от n переменных и, следовательно, сохраняет расстояние Хэмминга между каждой бент-функций от n переменных и дуальной к ней.

1.4.2 Расстояние Хэмминга между бент-функций и дуальной к ней

Приведём вид расстояния между бент-функцией и дуальной к ней для некоторых известных классов и конструкций.

Пусть n,m — чётные натуральные числа. Для прямой суммы бент-функций известно следующее

Утверждение ([41]). *Пусть $f \in \mathcal{B}_n$ и $g \in \mathcal{B}_m$ — бент-функции от n и m переменных, соответственно. Тогда для бент функции*

$$h(x,y) = f(x) \oplus g(y), \;\; x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m,$$

справедливо

$$N_h = N_f N_g.$$

Следствие ([41]). *В обозначениях предыдущего утверждения справедливо*

$$\mathrm{dist}(h,\widetilde{h}) = 2^{m+1}\mathrm{dist}(f,\widetilde{f}) + 2^{n+1}\mathrm{dist}(g,\widetilde{g}) - 2 \cdot \mathrm{dist}(f,\widetilde{f})\mathrm{dist}(g,\widetilde{g}).$$

Для бент-функций Мэйорана — МакФарланда, построенных с помощью аффинной подстановки специального вида, справедлива следующая

Теорема ([41]). *Пусть $f(x,y)$ — бент-функция от n переменных из класса Мэйорана — МакФарланда, имеющая вид*

$$f(x,y) = \langle x, Ly \oplus a \rangle \oplus g(y), \;\; x,y \in \mathbb{F}_2^{n/2},$$

где $L \in \mathcal{O}_{n/2}$, $a \in \mathbb{F}_2^{n/2}$, и $g \in \mathcal{F}_{n/2}$. Тогда

$$N_f = (-1)^{\langle a,a \rangle} \left(\sum_{x \in \mathbb{F}_2^{n/2}} (-1^{\langle a,Lx \rangle \oplus g(x)} \right)^2.$$

Следствие. *В обозначениях предыдущей теоремы справедливо*

$$\mathrm{dist}(f,\widetilde{f}) = 2^{n-1} - \frac{1}{2}(-1)^{\langle a,a \rangle} \left(\sum_{x \in \mathbb{F}_2^{n/2}} (-1^{\langle a,Lx \rangle \oplus g(x)} \right)^2.$$

Напомним, что класс *бент-функций Диллона* $\mathcal{PS}_{ap}$, состоит из функций вида $f(x,y) = g(x/y)$, $x,y \in \mathbb{F}_{2^{n/2}}$ (с соглашением $1/0 = 0$), где булева функция $g : \mathbb{F}_{2^{n/2}} \to \mathbb{F}_2$ является уравновешенной и $g(0) = 0$. Обозначим

$$K_g = \sum_{u \in \mathbb{F}_{2^{n/2}}} (-1)^{g(u)+g(1/u)}.$$

В частности, если $g = \mathrm{Tr}_1^{n/2}$, величина K_g называется *суммой Клостермана*.

Теорема ([41]). *Для бент-функции f, построенной с помощью указанной выше конструкции, справедливо*

$$N_f = 2^{n/2} + \left(2^{n/2} - 1\right) K_g.$$

Следствие. *В обозначениях предыдущей теоремы справедливо*

$$\mathrm{dist}(f,\widetilde{f}) = 2^{n-1} - 2^{n/2-1} - \frac{1}{2}\left(2^{n/2} - 1\right) K_g.$$

Дуальные функции бент-функций из классов Мэйорана — МакФарланда и Диллона достаточно просто находятся по виду бент-функции. Тем не менее, полная характеризация достижимых расстояний между бент-функцией и дуальной к ней в рамках данных классов, даже в частных случаях является нетривиальной задачей.

1.5 Обобщения дуальности

Отметим ряд работ, посвящённых исследованию понятий дуальности и самодуальности для различных обобщений бент-функций, а также исследованию данного вопроса применительно к векторным бент-функциям.

В статье L. Sok, M. Shi, P. Solé [77] приведены свойства, конструкции, а также классификация самодуальных кватернарных бент-функций, то есть функций вида $\mathbb{F}_2^n \to \mathbb{Z}_4$. С использованием связи с самодуальными булевыми бент-функциями показано, что не существует самодуальных кватернарных бент-функций от нечётного числа переменных.

Классификация квадратичных самодуальных бент-функций вида $\mathbb{F}_p^n \to \mathbb{F}_p$ (p — нечётное простое число) получена в работе X.-D. Hou [51]. Самодуальные бент-функции из этого же обобщения изучались в статье A. Çeşmelioğlu, W. Meidl, A. Pott [34].

Понятие самодуальной бент-функции на конечной абелевой группе введено в работе О. А. Логачева, А. А. Сальникова, В. В. Ященко [9]. В статье B. Xu [84] рассматривались дуальные бент-функции на конечных группах.

Обобщению понятия дуальности бент-функции для векторных бент-функций посвящена работа A. Çeşmelioğlu, W. Meidl, A. Pott [35], в которой предложены понятия самодуальности, а также *слабой самодуальности* (weak self-duality) векторной бент-функции.

Глава 2. Комбинаторные свойства самодуальных бент-функций

В данной главе получены необходимые и достаточные условия самодуальности бент-функции, построенной с помощью конкатенации векторов значений четырёх бент-функций от n переменных, а также исследованы свойства множества характеристических векторов самодуальных бент-функций.

2.1 Конструкция самодуальных бент-функций от $n+2$ переменных

В данном разделе будут найдены необходимые и достаточные условия самодуальности бент-функции от $n+2$ переменных, вектор значений которой является конкатенацией четырёх векторов значений бент-функций от n переменных.

2.1.1 Бент итеративные функции

Пусть f_0,f_1,f_2,f_3 — булевы функции от n переменных. Рассмотрим булеву функцию f от $n+2$ переменных, определённую следующим образом:

$$f(00,x) = f_0(x),\ \ f(01,x) = f_1(x),\ \ \ f(10,x) = f_2(x),\ \ f(11,x) = f_3(x),\ \ x \in \mathbb{F}_2^n.$$

A. Canteaut и P. Charpin в работе [22] исследовали ограничения бент-функций на подпространства коразмерности 1 и 2. Из представленных результатов следует, что если функция f является бент-функций, то либо все функции f_0,f_1,f_2,f_3 являются бент-функциями, либо ни одна из них не является.

Для случая, когда все функции f_0,f_1,f_2,f_3 являются бент-функциями, B. Preneel и др. в работе [72] нашли необходимые и достаточные условия, при которых функция f будет бент-функцией.

Теорема ([72]). *Пусть f_0,f_1,f_2,f_3 — бент-функции, тогда булева функция f является бент-функцией в том и только в том случае, когда для любого $y \in \mathbb{F}_2^n$*

справедливо

$$W_{f_0}(y)W_{f_1}(y)W_{f_2}(y)W_{f_3}(y) = -2^{2n}. \tag{2.1}$$

Учитывая, что для каждого $y \in \mathbb{F}_2^n$ справедливо $W_{f_i}(y) = 2^{n/2}(-1)^{\widetilde{f}_i(y)}$, $i = 0,1,2,3$, можно легко получить эквивалентную форму условия (2.1) в терминах дуальных функций:

$$\widetilde{f}_0 \oplus \widetilde{f}_1 \oplus \widetilde{f}_2 \oplus \widetilde{f}_3 = 1.$$

Содержательно, теорема предлагает итеративную конструкцию бент-функций от $n+2$ переменных на основе конкатенации векторов значений четырёх бент-функций от n переменных, на которые накладывается условие (2.1). Также отметим простое

Следствие. *Пусть f_0, f_1, f_2, f_3 — бент-функции от n переменных, для которых справедливо (2.1), тогда вектор значений, полученный произвольной перестановкой векторов значений функций f_0, f_1, f_2, f_3 также будет вектором значений бент-функции от $n+2$ переменных. Всего существует $4! = 24$ таких перестановок.*

Согласно [80], бент-функции, полученные с помощью отмеченной выше конструкции, называются *бент итеративными функциями* (bent iterative, $\mathcal{BI}$), множество таких функций от $n+2$ переменных обозначается через $\mathcal{BI}_{n+2}$. В той же работе были получены нижние оценки на количество бент итеративных функций от $n+2$ переменных. В статье [38] был представлен сравнительный анализ различных итеративных конструкций бент-функций от $n \leqslant 10$ переменных. Из приведённых численных данных следует, что класс $\mathcal{BI}$ имеет наибольшую мощность среди рассмотренных в данной работе конструкций.

Известно [22], что существуют бент-функции из классов Мэйорана — МакФарланда и $\mathcal{PS}$ (Partial Spreads) [44], которые не являются бент итеративными функциями. В свою очередь, из результатов, представленных в работе [23], посвящённой ненормальным бент-функциям, следует, что в классе $\mathcal{BI}_n$ есть функции, неэквивалентные бент-функциям из класса Мэйорана — МакФарланда.

2.1.2 Условия самодуальности

В данном разделе получены необходимые и достаточные условия того, что бент итеративная функция является самодуальной. Множество (анти-)самодуальных бент-функций из класса $\mathcal{BI}_{n+2}$ обозначается через $\mathrm{SB}^{+}_{\mathcal{BI}}(n+2)$ $\left(\mathrm{SB}^{-}_{\mathcal{BI}}(n+2)\right)$. Нам понадобится следующая

Лемма 1. *Бент-функция $f \in \mathcal{BI}_{n+2}$ является самодуальной если и только если*

$$\begin{cases} 2\widetilde{f}_0 = f_0 + f_1 + f_2 + f_3 - 1, \\ 2\widetilde{f}_1 = f_0 - f_1 + f_2 - f_3 + 1, \\ 2\widetilde{f}_2 = f_0 + f_1 - f_2 - f_3 + 1, \\ 2\widetilde{f}_3 = f_0 - f_1 - f_2 + f_3 + 1. \end{cases}$$

Доказательство. Пусть F_i — характеристичекий вектор булевой функции f_i, $i = 0,1,2,3$. Имеем $(-1)^f = (F_0,F_1,F_2,F_3) \in \{\pm 1\}^{2^{n+2}}$. Вектор $(-1)^f$ будет характеристическим вектором самодуальной бент-функции тогда и только тогда, когда

$$\begin{aligned} \widetilde{F} = \mathcal{H}_{n+2}G &= \frac{1}{2^{(n+2)/2}} \begin{pmatrix} H_n & H_n & H_n & H_n \\ H_n & -H_n & H_n & -H_n \\ H_n & H_n & -H_n & -H_n \\ H_n & -H_n & -H_n & H_n \end{pmatrix} \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \end{pmatrix} \\ &= \frac{2^{n/2}}{2^{(n+2)/2}} \begin{pmatrix} \widetilde{F}_0 + \widetilde{F}_1 + \widetilde{F}_2 + \widetilde{F}_3 \\ \widetilde{F}_0 - \widetilde{F}_1 + \widetilde{F}_2 - \widetilde{F}_3 \\ \widetilde{F}_0 + \widetilde{F}_1 - \widetilde{F}_2 - \widetilde{F}_3 \\ \widetilde{F}_0 - \widetilde{F}_1 - \widetilde{F}_2 + \widetilde{F}_3 \end{pmatrix} = \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \end{pmatrix}. \end{aligned}$$

Перепишем предпоследнее равенство, используя тот факт, что для каждой $f \in \mathcal{F}_n$ и любого $x \in \mathbb{F}_2^n$ справедливо $(-1)^{f(x)} = 1 - 2f(x)$. Аналогичное верно для характеристических векторов $\widetilde{F}_i$. Таким образом, для дальнейшего анализа полученной системы уравнений переходим к её представлению с

использованием булевых функций.

$$\begin{pmatrix} 1-2f_0 \\ 1-2f_1 \\ 1-2f_2 \\ 1-2f_3 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1-2\widetilde{f}_0+1-2\widetilde{f}_1+1-2\widetilde{f}_2+1-2\widetilde{f}_3 \\ 1-2\widetilde{f}_0-1+2\widetilde{f}_1+1-2\widetilde{f}_2-1+2\widetilde{f}_3 \\ 1-2\widetilde{f}_0+1-2\widetilde{f}_1-1+2\widetilde{f}_2-1+2\widetilde{f}_3 \\ 1-2\widetilde{f}_0-1+2\widetilde{f}_1-1+2\widetilde{f}_2+1-2\widetilde{f}_3 \end{pmatrix}$$
$$= \frac{1}{2}\begin{pmatrix} 4-2\widetilde{f}_0-2\widetilde{f}_1-2\widetilde{f}_2-2\widetilde{f}_3 \\ -2\widetilde{f}_0+2\widetilde{f}_1-2\widetilde{f}_2+2\widetilde{f}_3 \\ -2\widetilde{f}_0-2\widetilde{f}_1+2\widetilde{f}_2+2\widetilde{f}_3 \\ -2\widetilde{f}_0+2\widetilde{f}_1+2\widetilde{f}_2-2\widetilde{f}_3 \end{pmatrix} = \begin{pmatrix} 2-\widetilde{f}_0-\widetilde{f}_1-\widetilde{f}_2-\widetilde{f}_3 \\ -\widetilde{f}_0+\widetilde{f}_1-\widetilde{f}_2+\widetilde{f}_3 \\ -\widetilde{f}_0-\widetilde{f}_1+\widetilde{f}_2+\widetilde{f}_3 \\ -\widetilde{f}_0+\widetilde{f}_1+\widetilde{f}_2-\widetilde{f}_3 \end{pmatrix}.$$

Тогда имеем

$$2\begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} \widetilde{f}_0+\widetilde{f}_1+\widetilde{f}_2+\widetilde{f}_3-2 \\ \widetilde{f}_0-\widetilde{f}_1+\widetilde{f}_2-\widetilde{f}_3 \\ \widetilde{f}_0+\widetilde{f}_1-\widetilde{f}_2-\widetilde{f}_3 \\ \widetilde{f}_0-\widetilde{f}_1-\widetilde{f}_2+\widetilde{f}_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = H_2\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix},$$

следовательно,

$$2H_2\begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{pmatrix} = H_2H_2\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} + H_2\begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 4\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} + \begin{pmatrix} 2 \\ -2 \\ -2 \\ -2 \end{pmatrix},$$

что эквивалентно условию

$$2\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} = \begin{pmatrix} f_0+f_1+f_2+f_3 \\ f_0-f_1+f_2-f_3 \\ f_0+f_1-f_2-f_3 \\ f_0-f_1-f_2+f_3 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

□

Из вида разложения характеристического вектора самодуальной бент-функции (см. раздел 1.3.1) следует, что для характеристических векторов F_0,F_1,F_2,F_3 должно выполняться

$$\begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} F_2 \\ F_3 \end{pmatrix} + \frac{2}{2^{n/2}}H_{n-1}\begin{pmatrix} F_2 \\ F_3 \end{pmatrix} = \begin{pmatrix} F_2 \\ F_3 \end{pmatrix} + \frac{2}{2^{n/2}}\begin{pmatrix} H_{n-2} & H_{n-2} \\ H_{n-2} & -H_{n-2} \end{pmatrix}\begin{pmatrix} F_2 \\ F_3 \end{pmatrix}$$
$$= \begin{pmatrix} F_2 \\ F_3 \end{pmatrix} + \begin{pmatrix} \mathcal{H}_{n-2} & \mathcal{H}_{n-2} \\ \mathcal{H}_{n-2} & -\mathcal{H}_{n-2} \end{pmatrix}\begin{pmatrix} F_2 \\ F_3 \end{pmatrix} = \begin{pmatrix} F_2+\widetilde{F}_2+\widetilde{F}_3 \\ F_3+\widetilde{F}_2-\widetilde{F}_3 \end{pmatrix}.$$

Тогда

$$\begin{pmatrix}\mathcal{H}_{n-2}F_0\\ \mathcal{H}_{n-2}F_1\end{pmatrix}=\begin{pmatrix}\widetilde{F}_0\\ \widetilde{F}_1\end{pmatrix}=\begin{pmatrix}\widetilde{F}_2+F_2+F_3\\ \widetilde{F}_3+F_2-F_3\end{pmatrix},$$

получаем два уравнения, которые следуют из системы

$$2\begin{pmatrix}F_0\\ F_1\\ F_2\\ F_3\end{pmatrix}=\begin{pmatrix}\widetilde{F}_0+\widetilde{F}_1+\widetilde{F}_2+\widetilde{F}_3\\ \widetilde{F}_0-\widetilde{F}_1+\widetilde{F}_2-\widetilde{F}_3\\ \widetilde{F}_0+\widetilde{F}_1-\widetilde{F}_2-\widetilde{F}_3\\ \widetilde{F}_0-\widetilde{F}_1-\widetilde{F}_2+\widetilde{F}_3\end{pmatrix}$$

которая фигурирует в доказательстве леммы 1.

Таким образом, упомянутая модель разложения характеристического вектора самодуальной бент-функции уже присутствует в утверждении леммы 1.

Перейдём к основному результату данного раздела. Пусть f_0,f_1,f_2,f_3 — бент-функции от n переменных. Рассмотрим булеву функцию f от $n+2$ переменных, определённую следующим образом:

$$f(00,x)=f_0(x),\quad f(01,x)=f_1(x),\quad f(10,x)=f_2(x),\quad f(11,x)=f_3(x),\quad x\in\mathbb{F}_2^n.$$

Теорема 1. *Бент-функция f от $n+2$ переменных, определённая указанным выше способом, является самодуальной тогда и только тогда, когда существует пара бент-функций $g_1,g_2\in\mathcal{B}_n$ и булева функция $h\in\mathcal{F}_n$ такие, что*

$$f_0=\widetilde{g}_2,\qquad f_1=\widetilde{g_1\oplus h},\qquad f_2=\widetilde{g}_1,\qquad f_3=\widetilde{g_2\oplus h\oplus 1},$$

и функции g_1,g_2,h удовлетворяют следующей системе

$$\begin{cases}h=g_1\oplus g_2\oplus\widetilde{g}_1\oplus\widetilde{g}_2,\\ \widetilde{g_1\oplus h}=\widetilde{g}_1\oplus h,\\ \widetilde{g_2\oplus h}=\widetilde{g}_2\oplus h,\\ g_1\oplus\widetilde{g}_2=h\,(g_1\oplus g_2)\,.\end{cases}$$

Доказательство. Из леммы 1 следует, что

$$\begin{cases}2\widetilde{f}_0=f_0+f_1+f_2+f_3-1,\\ 2\widetilde{f}_1=f_0-f_1+f_2-f_3+1,\\ 2\widetilde{f}_2=f_0+f_1-f_2-f_3+1,\\ 2\widetilde{f}_3=f_0-f_1-f_2+f_3+1.\end{cases}$$

Обозначим $h = f_1 \oplus f_2$, то есть $f_1 = f_2 + h - 2f_2h$, тогда

$$\begin{cases} 2\widetilde{f}_0 = f_0 + f_2 + h - 2f_2h + f_2 + f_3 - 1, \\ 2\widetilde{f}_1 = f_0 - f_2 - h + 2f_2h + f_2 - f_3 + 1, \\ 2\widetilde{f}_2 = f_0 + f_2 + h - 2f_2h - f_2 - f_3 + 1, \\ 2\widetilde{f}_3 = f_0 - f_2 - h + 2f_2h - f_2 + f_3 + 1. \end{cases}$$

следовательно,

$$\begin{cases} 2\widetilde{f}_0 = f_0 + 2f_2 + h - 2f_2h + f_3 - 1, \\ 2\widetilde{f}_1 = f_0 - h + 2f_2h - f_3 + 1, \\ 2\widetilde{f}_2 = f_0 + h - 2f_2h - f_3 + 1, \\ 2\widetilde{f}_3 = f_0 - 2f_2 - h + 2f_2h + f_3 + 1. \end{cases}$$

Рассмотрим эту систему, варьируя значения, которые может принимать функция h:

1) для каждого $x \in \mathbb{F}_2^n$ такого, что $h(x) = 0$, имеем

$$\begin{cases} 2\widetilde{f}_0 = f_0 + 2f_2 + f_3 - 1, \\ 2\widetilde{f}_1 = f_0 - f_3 + 1, \\ 2\widetilde{f}_2 = f_0 - f_3 + 1, \\ 2\widetilde{f}_3 = f_0 - 2f_2 + f_3 + 1, \end{cases}$$

то есть в этом случае должно выполняться

$$f_0 = f_3 \oplus 1, \quad f_2 = \widetilde{f}_0, \quad \widetilde{f}_3 = \widetilde{f}_0 \oplus 1,$$

2) для каждого $x \in \mathbb{F}_2^n$ такого, что $h(x) = 1$, имеем

$$\begin{cases} 2\widetilde{f}_0 = f_0 + f_3, \\ 2\widetilde{f}_1 = f_0 + 2f_2 - f_3, \\ 2\widetilde{f}_2 = f_0 - 2f_2 - f_3 + 2, \\ 2\widetilde{f}_3 = f_0 + f_3. \end{cases}$$

то есть в этом случае должно выполняться

$$f_0 = f_3, \quad f_2 = \widetilde{f}_1, \quad \widetilde{f}_2 = f_2 \oplus 1.$$

Анализ полученных ограничений из обоих случаев даёт условия

$$
\begin{aligned}
&f_3 = hf_0 \oplus (h \oplus 1)(f_0 \oplus 1) = f_0 \oplus h \oplus 1,\\
&f_2 = h\left(\widetilde{f_2} \oplus 1\right) \oplus (h \oplus 1)\widetilde{f_0} = h\left(\widetilde{f_2} \oplus \widetilde{f_0}\right) \oplus \widetilde{f_0} \oplus h,\\
&f_1 = f_2 \oplus h = h\left(\widetilde{f_2} \oplus \widetilde{f_0}\right) \oplus \widetilde{f_0},
\end{aligned}
$$

то есть

$$
\begin{cases}
f_1 = h\left(\widetilde{f_2} \oplus \widetilde{f_0}\right) \oplus \widetilde{f_0},\\
f_2 = h\left(\widetilde{f_2} \oplus \widetilde{f_0}\right) \oplus \widetilde{f_0} \oplus h,\\
f_3 = f_0 \oplus h \oplus 1.
\end{cases} \tag{2.2}
$$

Перепишем данные уравнения над полем $\mathbb{R}$

$$
\begin{cases}
f_3 = 1 - f_0 - h + 2hf_0,\\
f_2 = \widetilde{f_0} - h\widetilde{f_0} - h\widetilde{f_2} + h,\\
f_1 = \widetilde{f_0} - h\widetilde{f_0} + h\widetilde{f_2},
\end{cases}
$$

и подставим в исходную систему

$$
\begin{cases}
2\widetilde{f_0} = f_0 + \left(\widetilde{f_0} - h\widetilde{f_0} + h\widetilde{f_2}\right) + \left(\widetilde{f_0} - h\widetilde{f_0} - h\widetilde{f_2} + h\right) + (1 - f_0 - h + 2hf_0) - 1,\\
2\widetilde{f_1} = f_0 - \left(\widetilde{f_0} - h\widetilde{f_0} + h\widetilde{f_2}\right) + \left(\widetilde{f_0} - h\widetilde{f_0} - h\widetilde{f_2} + h\right) - (1 - f_0 - h + 2hf_0) + 1,\\
2\widetilde{f_2} = f_0 + \left(\widetilde{f_0} - h\widetilde{f_0} + h\widetilde{f_2}\right) - \left(\widetilde{f_0} - h\widetilde{f_0} - h\widetilde{f_2} + h\right) - (1 - f_0 - h + 2hf_0) + 1,\\
2\widetilde{f_3} = f_0 - \left(\widetilde{f_0} - h\widetilde{f_0} + h\widetilde{f_2}\right) - \left(\widetilde{f_0} - h\widetilde{f_0} - h\widetilde{f_2} + h\right) + (1 - f_0 - h + 2hf_0) + 1.
\end{cases}
$$

Получаем

$$
\begin{cases}
h\widetilde{f_0} = hf_0,\\
\widetilde{f_1} = f_0 + h - h\widetilde{f_2} - hf_0,\\
\widetilde{f_2} = f_0 - hf_0 + h\widetilde{f_2},\\
\widetilde{f_3} = 1 - \widetilde{f_0} - h + 2h\widetilde{f_0}.
\end{cases}
$$

следовательно,

$$
\begin{cases}
h\widetilde{f_0} = hf_0,\\
\widetilde{f_1} = h\left(\widetilde{f_2} \oplus 1\right) \oplus (h \oplus 1)f_0,\\
\widetilde{f_2}(h \oplus 1) = f_0(h \oplus 1),\\
\widetilde{f_3} = \widetilde{f_0} \oplus h \oplus 1.
\end{cases}
$$

Перепишем третье уравнение в следующей форме

$$f_0 = hf_0 \oplus \widetilde{f_2}(h \oplus 1) = h\widetilde{f_2} \oplus \widetilde{f_2} \oplus h\widetilde{f_0},$$

тогда второе уравнение примет вид

$$\begin{aligned}\widetilde{f_1} &= h\left(\widetilde{f_2} \oplus 1\right) \oplus (h \oplus 1)f_0 = h\left(\widetilde{f_2} \oplus 1\right) \oplus (h \oplus 1)\left(h\widetilde{f_2} \oplus \widetilde{f_2} \oplus h\widetilde{f_0}\right) \\ &= h\widetilde{f_2} \oplus h \oplus h\widetilde{f_2} \oplus h\widetilde{f_2} \oplus h\widetilde{f_0} \oplus h\widetilde{f_2} \oplus \widetilde{f_2} \oplus h\widetilde{f_0} = \widetilde{f_2} \oplus h.\end{aligned}$$

Обозначим $g_1 = \widetilde{f_2}$ и $g_2 = \widetilde{f_0}$ и запишем полученную систему уравнений:

$$\begin{cases} f_0 = \widetilde{g_2}, \\ f_2 = \widetilde{g_1}, \\ f_0 = h\,(g_1 \oplus g_2) \oplus g_1, \\ \widetilde{f_1} = g_1 \oplus h, \\ \widetilde{f_3} = g_2 \oplus h \oplus 1. \end{cases}$$

Теперь запишем итоговую систему, образованную указанными выше уравнениями, а также системой (2.2):

$$\begin{cases} f_0 = \widetilde{g_2}, \\ f_1 = \widetilde{g_1 \oplus h}, \\ f_2 = \widetilde{g_1}, \\ f_3 = \widetilde{g_2 \oplus h} \oplus 1, \\ h = g_1 \oplus g_2 \oplus \widetilde{g_1} \oplus \widetilde{g_2}, \\ \widetilde{g_2} = h\,(g_1 \oplus g_2) \oplus g_1, \\ \widetilde{g_1 \oplus h} = \widetilde{g_1} \oplus h, \\ \widetilde{g_2 \oplus h} = \widetilde{g_2} \oplus h. \end{cases}$$

□

Рассмотрим два крайних случая: $h = 0$ и $h = 1$. В первом случае получаем характеристический вектор

$$\left(F, \widetilde{F}, \widetilde{F}, -F\right) \in \{\pm 1\}^{2^{n+2}}$$

самодуальной бент-функции от $n + 2$ переменных, где F — характеристический вектор произвольной бент-функции от n переменных. Данная конструкция ранее

была предложена в работе [33] (см. раздел 1.3.4). Для случая $h \equiv 1$ получаем следующую конструкцию

Утверждение 1. *Пусть* $F_1, F_2 \in \{\pm 1\}^{2^n}$ *— характеристические векторы самодуальной и анти-самодуальной бент-функций от* n *переменных, соответственно. Тогда вектор*

$$(G_2, -G_1, G_1, G_2) \in \{\pm 1\}^{2^{n+2}}$$

будет характеристическим вектором самодуальной бент-функции от $n+2$ *переменных.*

Доказательство. При $h = 1$ характеристический вектор функции f имеет вид $(G_2, -G_1, G_1, G_2)$. Также должны выполняться условия $\widetilde{g}_2 = g_2 \oplus 1$ и $\widetilde{g}_1 = g_1$. □

Утверждение 2. *Справедливо*

$$|\mathcal{B}_n| + \left|\mathrm{SB}^+(n)\right|^2 \leqslant \left|\mathrm{SB}^+_{\mathcal{BI}}(n+2)\right| \leqslant |\mathcal{B}_n|^2 .$$

Доказательство. Итеративная конструкция из работы [33], а также конструкция, приведённая в утверждении 1, образуют непересекающиеся множества функций, следовательно,

$$\left|\mathrm{SB}^+_{\mathcal{BI}}(n+2)\right| \geqslant |\mathcal{B}_n| + \left|\mathrm{SB}^+(n)\right| \cdot \left|\mathrm{SB}^-(n)\right| .$$

В силу существования взаимно-однозначного соответствия (см. раздел 1.3.1) между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$, получаем требуемую нижнюю оценку. Верхняя оценка обусловлена требованием существования пары бент-функций g_1, g_2 от n переменных. □

Таким образом, оценку, полученную с помощью итеративной конструкции (Carlet и др., 2010), представленной в разделе 1.3.4, можно усилить:

	$n=2$	$n=4$	$n=6$	$n=8$
Известные нижние оценки				
Класс Диллона $\mathcal{PS}_{ap}$ (с отрицанием функций)	2	2	6	70
Класс Мэйорана – МакФарланда	2	8	48	768
Квадратичные функции	2	20	752	$\simeq 2^{16.68}$
Прямая сумма двух (анти-)самодуальных бент-функций	–	8	80	$\simeq 2^{17.39}$
Итеративная конструкция (Carlet и др., 2010)	–	8	896	$\simeq 2^{32.34}$
Итеративные конструкции (Carlet и др., 2010; утверждение 1)	–	12	1296	$\simeq 2^{32.76}$
Точное число самодуальных бент-функций от n переменных				
	2	**20**	**42 896**	$\geqslant \mathbf{2^{50.56}}$

Таблица 2.1 — Известные нижние оценки числа самодуальных бент-функций от n переменных (с учётом утверждения 2)

2.2 Множество характеристических векторов

В данном разделе будет установлена прямая связь между линейной оболочкой множества характеристических векторов (анти-)самодуальных бент-функций от n переменных и собственными подпространствами матрицы Сильвестра – Адамара H_n. Данная связь позволит получить представление действия отображения дуальности в терминах характеристических векторов самодуальных бент-функций.

Обозначим $\mathcal{H}_n = 2^{-n/2} H_n$, данная матрица является симметричной и ортогональной. Из симметричности матрицы $\mathcal{H}_n$ следует, что

$$\left(\operatorname{Ker}\left(\mathcal{H}_n + I_{2^n}\right)\right)^{\perp} = \operatorname{Ker}\left(\mathcal{H}_n - I_{2^n}\right),$$
$$\left(\operatorname{Ker}\left(\mathcal{H}_n - I_{2^n}\right)\right)^{\perp} = \operatorname{Ker}\left(\mathcal{H}_n + I_{2^n}\right).$$

В работах [33; 41] была доказана следующая

Лемма 2. ([33; 41]) *Спектр матрицы $\mathcal{H}_n$ состоит из собственных значений $(+1)$ и (-1), имеющих кратность 2^{n-1}. Базис собственного подпространства, соответствующего собственному числу $(+1)$, может быть образован строками матрицы $\left(H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1}\right)$. Ортогональное разложение пространства $\mathbb{R}^{2^n}$ в прямую сумму собственных подпространств матрицы $\mathcal{H}_n$*

имеет вид

$$\mathbb{R}^{2^n} = \mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}) \oplus \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})\,.$$

Здесь символ $\oplus$ используется для обозначения прямой суммы подпространств.

Таким образом,

$$\dim\left(\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})\right) = \dim\left(\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})\right) = 2^{n-1}.$$

Множество самодуальных бент-функций от $n = 2$ переменных состоит из функций x_1x_2 и $x_1x_2 \oplus 1$, характеристические векторы которых равны $(1,1,1,-1)$ и $(-1,-1,-1,1)$, соответственно. Эти характеристические векторы образуют линейно зависимое множество в пространстве $\mathbb{R}^4$. В свою очередь, множество $\mathrm{SB}^-(2)$ состоит из функций $x_1x_2 \oplus x_1 \oplus x_2$ и $x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ с характеристическими векторами $(1,-1,-1,-1)$ и $(-1,1,1,1)$, соответственно. Эта пара векторов также линейно зависима.

Следующий результат показывает, что при $n \geqslant 4$ среди характеристических векторов (анти-)самодуальных бент-функций от n переменных существует набор из 2^{n-1} линейно независимых векторов.

Теорема 2. *Множества характеристических векторов самодуальных бент-функций и анти-самодуальных бент-функций от $n \geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным числам $2^{n/2}$ и $(-2^{n/2})$, соответственно.*

Доказательство. Заметим, что справедливость утверждения для множества характеристических векторов самодуальных бент-функций в силу существования взаимно-однозначного соответствия между самодуальными и анти-самодуальными бент-функциями (см. раздел 1.3.1) влечёт его справедливость для множества характеристических векторов анти-самодуальных бент-функций.

Далее будет построено множество, состоящее из 2^{n-1} самодуальных бент-функций, характеристические векторы которых линейно независимы. Доказательство будет вестись по индукции.

База индукции: Для $n = 4$ существует 10 различных самодуальных бент-функций, принимающих значение 0 на векторе $\mathbf{0} \in \mathbb{F}_2^4$. Оставшиеся 10 самодуальных бент-функций от 4 переменных являются их отрицаниями. Характеристические векторы первых 8 (относительно лексикографического порядка

векторов значений) самодуальных бент-функций, записанные в виде строк, образуют матрицу, ранг которой равен $8 = 2^{n-1}$.

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

Индукционный шаг: Предположим, что утверждение справедливо для всех положительных чётных $n = 4,6,\ldots,n_0$, где $n_0 \geqslant 4$. Положим $n = n_0 + 2$. Тогда по индукционному предположению существует набор из $2^{(n-2)-1} = 2^{n-3}$ самодуальных бент-функций $f_1^{n-2},f_2^{n-2},\ldots,f_{2^{n-3}}^{n-2}$ от $n-2$ переменных, характеристические векторы $F_1^{n-2},F_2^{n-2},\ldots,F_{2^{n-3}}^{n-2}$ которых линейно независимы. Используя взаимно однозначное соответствие между множествами самодуальных и анти-самодуальных бент-функций, получаем 2^{n-3} анти-самодуальных бент-функции $g_1^{n-2},g_2^{n-2},\ldots,g_{2^{n-3}}^{n-2}$ от $n-2$ переменных с линейно-независимыми характеристическими векторами $G_1^{n-2},G_2^{n-2},\ldots,G_{2^{n-3}}^{n-2}$, соответственно.

Используем итеративные конструкции самодуальных бент-функций, представленные в разделе 1.3.4 и утверждении 1. Пусть F и G — характеристические векторы самодуальной и анти-самодульной бент-функций от $n-2$ переменных соответственно, тогда векторы

$$\begin{aligned}
\mathbf{F} &= (F,F,F,-F), \\
\mathbf{G} &= (G,-G,-G,-G), \\
\mathbf{FG} &= (F,-G,G,F),
\end{aligned}$$

будут характеристическими векторами самодуальных бент-функций от n переменных. Подставив в первые два шаблона упомянутые выше множества характеристических векторов, получим 2^{n-3} векторов вида

$$\mathbf{F}_i^n = \left(F_i^{n-2},F_i^{n-2},F_i^{n-2},-F_i^{n-2}\right),\ \ i = 1,2,\ldots,2^{n-3},$$

и 2^{n-3} векторов вида

$$\mathbf{G}_j^n = \left(G_j^{n-2},-G_j^{n-2},-G_j^{n-2},-G_j^{n-2}\right),\ \ j = 1,2,\ldots,2^{n-3}.$$

Заметим, что множества $S_{\mathbf{F}} = \{\mathbf{F}_i^n\}_{i=1}^{2^{n-3}}$ и $S_{\mathbf{G}} = \{\mathbf{G}_i^n\}_{i=1}^{2^{n-3}}$ по индукционному предположению состоят из линейно независимых векторов, более того, для каждой пары векторов $\mathbf{F} \in \{\mathbf{F}_i^n\}_{i=1}^{2^{n-3}}$, $\mathbf{G} \in \{\mathbf{G}_i^n\}_{i=1}^{2^{n-3}}$ справедливо

$$\langle \mathbf{F},\mathbf{G} \rangle = \langle F,G \rangle - \langle F,G \rangle - \langle F,G \rangle + \langle F,G \rangle = 0,$$

следовательно, линейные оболочки множеств $S_{\mathbf{F}}$ и $S_{\mathbf{G}}$ пересекаются только по нулевому элементу пространства $\mathbb{R}^{2^n}$, значит множество $S_{\mathbf{F}} \cup S_{\mathbf{G}}$ состоит из $2^{n-3} + 2^{n-3} = 2^{n-2}$ линейно независимых векторов.

Используем третий шаблон и рассмотрим 2^{n-2} самодуальных бент-функции от n переменных, определяемых характеристическими векторами

$$\begin{aligned}
(\mathbf{FG})_1^n &= \left(F_1^{n-2}, -G_1^{n-2}, G_1^{n-2}, F_1^{n-2}\right), \\
(\mathbf{FG})_2^n &= \left(F_2^{n-2}, -G_1^{n-2}, G_1^{n-2}, F_2^{n-2}\right), \\
&\cdots \\
(\mathbf{FG})_{2^{n-3}}^n &= \left(F_{2^{n-3}}^{n-2}, -G_1^{n-2}, G_1^{n-2}, F_{2^{n-3}}^{n-2}\right), \\
(\mathbf{FG})_{2^{n-3}+1}^n &= \left(F, -G_1^{n-2}, G_1^{n-2}, F\right), \\
(\mathbf{FG})_{2^{n-3}+2}^n &= \left(F_{2^{n-3}}^{n-2}, -G_2^{n-2}, G_2^{n-2}, F_{2^{n-3}}^{n-2}\right), \\
(\mathbf{FG})_{2^{n-3}+3}^n &= \left(F_{2^{n-3}}^{n-2}, -G_3^{n-2}, G_3^{n-2}, F_{2^{n-3}}^{n-2}\right), \\
&\cdots \\
(\mathbf{FG})_{2^{n-2}}^n &= \left(F_{2^{n-3}}^{n-2}, -G_{2^{n-3}}^{n-2}, G_{2^{n-3}}^{n-2}, F_{2^{n-3}}^{n-2}\right),
\end{aligned}$$

где

$$F = \beta_1 F_1^{n-2} + \beta_2 F_2^{n-2} + \cdots + \beta_{2^{n-3}} F_{2^{n-3}}^{n-2}$$

для некоторого вектора $\beta = (\beta_1,\beta_2,\ldots,\beta_{2^{n-3}}) \in \mathbb{R}^{2^{n-3}}$ такого, что $\sum\limits_{i=1}^{2^{n-3}} \beta_i \neq 1$, например, $\beta_1 = -1$ и $\beta_2 = \beta_3 = \cdots = \beta_{2^{n-3}} = 0$.

Докажем, что векторы $\{(\mathbf{FG})_i^n\}_{i=1}^{2^{n-2}}$ линейно независимы. Предположим, что существует ненулевой вектор коэффициентов $\lambda = (\lambda_1,\lambda_2,\ldots,\lambda_{2^{n-3}}) \in \mathbb{R}^{2^{n-2}}$ такой, что

$$\sum_{i=1}^{2^{n-2}} \lambda_i \, (\mathbf{FG})_i^n = \mathbf{0} \in \mathbb{R}^{2^n}.$$

Нетрудно видеть, что коэффициенты $\lambda_{2^{n-3}+2},\lambda_{2^{n-3}+3},\ldots,\lambda_{2^{n-2}}$ в силу линейной независимости элементов множества $S_{\mathbf{G}}$ должны быть равны нулю. При $\lambda_{2^{n-3}+1} = 0$ в силу линейной независимости элементов множества $S_{\mathbf{F}}$

оставшиеся коэффициенты также равны нулю — получаем противоречие с нетривиальностью вектора $\lambda \in \mathbb{R}^{2^{n-2}}$. Поэтому имеем $\lambda_{2^{n-3}+1} \neq 0$ и

$$\sum_{i=1}^{2^{n-3}} \lambda_i F_i^{n-2} + \lambda_{2^{n-3}+1} F = \sum_{i=1}^{2^{n-3}} \lambda_i F_i^{n-2} + \lambda_{2^{n-3}+1} \left(\sum_{i=1}^{2^{n-3}} \beta_i F_i^{n-2} \right) = \mathbf{0} \in \mathbb{R}^{2^{n-2}},$$

следовательно,

$$\lambda_i = -\lambda_{2^{n-3}+1} \beta_i, \;\; i = 1,2,\ldots,2^{n-3}.$$

Но тогда

$$\begin{aligned} \sum_{i=1}^{2^{n-3}} \lambda_i G_1^{n-2} + \lambda_{2^{n-3}+1} G_1^{n-2} &= -\sum_{i=1}^{2^{n-3}} \lambda_{2^{n-3}+1} \beta_i G_1^{n-2} + \lambda_{2^{n-3}+1} G_1^{n-2} \\ &= \lambda_{2^{n-3}+1} \left(1 - \sum_{i=1}^{2^{n-3}} \beta_i \right) G_1^{n-2} = \mathbf{0} \in \mathbb{R}^{2^{n-2}}, \end{aligned}$$

что невозможно при $\sum\limits_{i=1}^{2^{n-3}} \beta_i \neq 1$, так как $\lambda_{2^{n-3}+1} \neq 0$ и $\left\| G_1^{n-2} \right\| > 0$.

Таким образом, множество $S_{\mathbf{FG}} = \{(\mathbf{FG})_i^n\}_{i=1}^{2^{n-2}}$ состоит из 2^{n-2} линейно независимых векторов. Осталось заметить, что для любых $\mathbf{F} \in \{\mathbf{F}_i^n\}_{i=1}^{2^{n-3}}$, $\mathbf{G} \in \{\mathbf{G}_i^n\}_{i=1}^{2^{n-3}}$ и $\mathbf{AB} = (A, -B, B, A)$, где $A,B \in \{\pm 1\}^{2^{n-2}}$, справедливо

$$\begin{aligned} \langle \mathbf{AB}, \mathbf{F} \rangle &= \langle A,F \rangle - \langle B,F \rangle + \langle B,F \rangle - \langle A,F \rangle = 0, \\ \langle \mathbf{AB}, \mathbf{G} \rangle &= \langle A,G \rangle + \langle B,G \rangle - \langle B,G \rangle - \langle A,G \rangle = 0, \end{aligned}$$

то есть линейные оболочки множеств $S_{\mathbf{F}}$, $S_{\mathbf{G}}$ и $S_{\mathbf{FG}}$ пересекаются только по нулевому элементу пространства $\mathbb{R}^{2^n}$, следовательно, множество $S_{\mathbf{G}} \cup S_{\mathbf{G}} \cup S_{\mathbf{FG}}$, по построению образованное характеристическими векторами самодуальных бент-функций, состоит из $2^{n-3} + 2^{n-3} + 2^{n-2} = 2^{n-1}$ линейно независимых векторов.

В силу того, что размерности пространств $\mathrm{Ker}\left(H_n \pm 2^{n/2} I_{2^n}\right)$ равны 2^{n-1}, найденный набор векторов является базисом собственного подпространства $\mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right)$ и, после соответствующего преобразования, базисом подпространства $\mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$, соответственно. □

Докажем, что для характеристических векторов самодуальных бент-функций справедливы соотношения определённого вида, связывающие между собой скалярные произведения четырёх его подвекторов.

Утверждение 3. *Пусть* $n \geqslant 4$ *и* $f \in \mathrm{SB}^+(n) \cup \mathrm{SB}^-(n)$. *Для характеристического вектора* $(-1)^f = \left(F^{00},F^{01},F^{10},F^{11}\right)$, *где* $F^{00},F^{01},F^{10},F^{11} \in \{\pm 1\}^{2^{n-2}}$, *справедливо*

$$\left\langle F^{00},F^{01}\right\rangle + \left\langle F^{10},F^{11}\right\rangle = 0,$$
$$\left\langle F^{00},F^{10}\right\rangle + \left\langle F^{01},F^{11}\right\rangle = 0.$$

Доказательство. В силу существования взаимно однозначного соответствия между множествами самодуальных и анти-самодуальных бент-функций, достаточно доказать справедливость утверждения для самодуального случая. Пусть $f \in \mathrm{SB}^+(n)$, согласно теореме 2 существуют векторы

$$\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_{2^{n-3}}) \in \mathbb{R}^{2^{n-3}},$$
$$\beta = (\beta_1,\beta_2,\ldots,\beta_{2^{n-3}}) \in \mathbb{R}^{2^{n-3}},$$
$$\gamma = (\gamma_1,\gamma_2,\ldots,\gamma_{2^{n-2}}) \in \mathbb{R}^{2^{n-2}},$$

такие, что

$$(-1)^f = \sum_{i=1}^{2^{n-3}} \alpha_i \mathbf{F}_i^n + \sum_{j=1}^{2^{n-3}} \beta_j \mathbf{G}_j^n + \sum_{k=1}^{2^{n-2}} \gamma_k \left(\mathbf{FG}\right)_k^n,$$

где множества $S_{\mathbf{F}} = \{\mathbf{F}_i^n\}_{i=1}^{2^{n-3}}$, $S_{\mathbf{G}} = \left\{\mathbf{G}_j^n\right\}_{j=1}^{2^{n-3}}$ и $S_{\mathbf{FG}} = \{(\mathbf{FG})_k^n\}_{k=1}^{2^{n-2}}$ определены так же как и в доказательстве теоремы 2. Используя вид функций из множеств $S_{\mathbf{F}}$, $S_{\mathbf{G}}$, $S_{\mathbf{FG}}$, для удобства обозначим

$$\mathbf{F}_i^n = \left(F_i,F_i,F_i,-F_i\right),$$
$$\mathbf{G}_j^n = \left(G_j,-G_j,-G_j,-G_j\right),$$
$$\left(\mathbf{FG}\right)_k^n = \left(A_k,-B_k,B_k,A_k\right),$$

где $F_i,A_k \in \mathrm{Ker}\left(\mathcal{H}_{n-2} - I_{2^{n-2}}\right)$, $G_j,B_k \in \mathrm{Ker}\left(\mathcal{H}_{n-2} + I_{2^{n-2}}\right)$, $i,j = 1,2,\ldots,2^{n-3}$, $k = 1,2,\ldots,2^{n-2}$, и определим следующие векторы

$$\mathbf{F} = \sum_{i=1}^{2^{n-3}} \alpha_i F_i, \qquad \mathbf{G} = \sum_{j=1}^{2^{n-3}} \beta_j G_j, \qquad \mathbf{A} = \sum_{k=1}^{2^{n-2}} \gamma_k A_k, \qquad \mathbf{B} = \sum_{k=1}^{2^{n-2}} \gamma_k B_k.$$

В данных обозначениях характеристичекий вектор $(-1)^f$ имеет вид

$$(-1)^f = \begin{pmatrix} F^{00} \\ F^{01} \\ F^{10} \\ F^{11} \end{pmatrix} = \begin{pmatrix} \mathbf{F}+\mathbf{G}+\mathbf{A} \\ \mathbf{F}-\mathbf{G}-\mathbf{B} \\ \mathbf{F}-\mathbf{G}+\mathbf{B} \\ -\mathbf{F}-\mathbf{G}+\mathbf{A} \end{pmatrix} \in \{\pm 1\}^{2^n}.$$

Нетрудно видеть, что $\mathbf{F},\mathbf{G} \in \{0,\pm 1/2,\pm 1\}^{2^{n-2}}$, $\mathbf{A},\mathbf{B} \in \{0,\pm 1\}^{2^{n-2}}$. Выпишем все возможные наборы значений, которые могут принимать координаты $\mathbf{F}_l,\mathbf{G}_l,\mathbf{A}_l,\mathbf{B}_l$, $l = 1,2,\ldots,2^{n-2}$.

$\mathbf{F}_l$	$\mathbf{G}_l$	$\mathbf{A}_l$	$\mathbf{B}_l$	Число наборов
$1/2$	$1/2$	0	± 1	$a_1^{\pm}$
$1/2$	$-1/2$	± 1	0	$a_2^{\pm}$
$-1/2$	$1/2$	± 1	0	$a_3^{\pm}$
$-1/2$	$-1/2$	0	± 1	$a_4^{\pm}$
± 1	0	0	0	$a_5^{\pm}$
0	± 1	0	0	$a_6^{\pm}$
0	0	± 1	± 1	$a_7^{\pm,\pm}$
0	0	± 1	∓ 1	$a_7^{\pm,\mp}$

Таблица 2.2 — Возможные комбинации значений

Из таблицы 2.2 видно, что

$$\begin{aligned}
\langle \mathbf{F},\mathbf{A} \rangle &= \frac{1}{2}\left(a_2^+ - a_2^-\right) + \frac{1}{2}\left(-a_3^+ + a_3^-\right), \\
\langle \mathbf{G},\mathbf{A} \rangle &= \frac{1}{2}\left(-a_2^+ + a_2^-\right) + \frac{1}{2}\left(a_3^+ - a_3^-\right), \\
\langle \mathbf{F},\mathbf{B} \rangle &= \frac{1}{2}\left(a_1^+ - a_1^-\right) + \frac{1}{2}\left(-a_4^+ - a_4^-\right), \\
\langle \mathbf{G},\mathbf{B} \rangle &= \frac{1}{2}\left(a_1^+ - a_1^-\right) + \frac{1}{2}\left(-a_4^+ - a_4^-\right),
\end{aligned}$$

то есть, имеем

$$\begin{aligned}
\langle \mathbf{F},\mathbf{A} \rangle &= -\langle \mathbf{G},\mathbf{A} \rangle, \\
\langle \mathbf{F},\mathbf{B} \rangle &= \langle \mathbf{G},\mathbf{B} \rangle.
\end{aligned}$$

Также заметим, что числа $\langle \mathbf{G},\mathbf{A} \rangle$, $\langle \mathbf{F},\mathbf{B} \rangle$ равны нулю, следовательно,

$$\langle \mathbf{F},\mathbf{A} \rangle = \langle \mathbf{G},\mathbf{A} \rangle = \langle \mathbf{F},\mathbf{B} \rangle = \langle \mathbf{G},\mathbf{B} \rangle = 0.$$

Распишем первое скалярное произведение

$$\begin{aligned}\left\langle F^{00},F^{01}\right\rangle + \left\langle F^{10},F^{11}\right\rangle &= \langle \mathbf{F}+\mathbf{G}+\mathbf{A},\mathbf{F}-\mathbf{G}-\mathbf{B}\rangle \\ &+ \langle \mathbf{F}-\mathbf{G}+\mathbf{B},-\mathbf{F}-\mathbf{G}+\mathbf{A}\rangle \\ &= \langle \mathbf{F},\mathbf{F}\rangle - \langle \mathbf{F},\mathbf{G}\rangle - \langle \mathbf{F},\mathbf{B}\rangle \\ &+ \langle \mathbf{G},\mathbf{F}\rangle - \langle \mathbf{G},\mathbf{G}\rangle - \langle \mathbf{G},\mathbf{B}\rangle \\ &+ \langle \mathbf{A},\mathbf{F}\rangle - \langle \mathbf{A},\mathbf{G}\rangle - \langle \mathbf{A},\mathbf{B}\rangle \\ &- \langle \mathbf{F},\mathbf{F}\rangle - \langle \mathbf{F},\mathbf{G}\rangle + \langle \mathbf{F},\mathbf{A}\rangle \\ &+ \langle \mathbf{G},\mathbf{F}\rangle + \langle \mathbf{G},\mathbf{G}\rangle - \langle \mathbf{G},\mathbf{A}\rangle \\ &- \langle \mathbf{B},\mathbf{F}\rangle - \langle \mathbf{B},\mathbf{G}\rangle + \langle \mathbf{B},\mathbf{A}\rangle \\ &= 2\langle \mathbf{F},\mathbf{A}\rangle - 2\langle \mathbf{G},\mathbf{A}\rangle - 2\langle \mathbf{F},\mathbf{B}\rangle - 2\langle \mathbf{G},\mathbf{B}\rangle = 0.\end{aligned}$$

Второе скалярное произведение имеет вид

$$\begin{aligned}\left\langle F^{00},F^{10}\right\rangle + \left\langle F^{01},F^{11}\right\rangle &= \langle \mathbf{F}+\mathbf{G}+\mathbf{A},\mathbf{F}-\mathbf{G}+\mathbf{B}\rangle \\ &+ \langle \mathbf{F}-\mathbf{G}-\mathbf{B},-\mathbf{F}-\mathbf{G}+\mathbf{A}\rangle \\ &= \langle \mathbf{F},\mathbf{F}\rangle - \langle \mathbf{F},\mathbf{G}\rangle + \langle \mathbf{F},\mathbf{B}\rangle \\ &+ \langle \mathbf{G},\mathbf{F}\rangle - \langle \mathbf{G},\mathbf{G}\rangle + \langle \mathbf{G},\mathbf{B}\rangle \\ &+ \langle \mathbf{A},\mathbf{F}\rangle - \langle \mathbf{A},\mathbf{G}\rangle + \langle \mathbf{A},\mathbf{B}\rangle \\ &- \langle \mathbf{F},\mathbf{F}\rangle - \langle \mathbf{F},\mathbf{G}\rangle + \langle \mathbf{F},\mathbf{A}\rangle \\ &+ \langle \mathbf{G},\mathbf{F}\rangle + \langle \mathbf{G},\mathbf{G}\rangle - \langle \mathbf{G},\mathbf{A}\rangle \\ &+ \langle \mathbf{B},\mathbf{F}\rangle + \langle \mathbf{B},\mathbf{G}\rangle - \langle \mathbf{B},\mathbf{A}\rangle \\ &= 2\langle \mathbf{F},\mathbf{A}\rangle - 2\langle \mathbf{G},\mathbf{A}\rangle + 2\langle \mathbf{F},\mathbf{B}\rangle + 2\langle \mathbf{G},\mathbf{B}\rangle = 0.\end{aligned}$$

□

Таким образом, множества самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных характеризуют собственные подпространства матрицы Сильвестра — Адамара H_n. Содержательно, это выражается в следующем. Пусть $f \in \mathcal{B}_n$ — произвольная бент-функция, и $F^+,F^- \in \mathbb{R}^{2^n}$ — ортогональные проекции её характеристического вектора $(-1)^f$ на собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным значениям $2^{n/2}$ и $(-2^{n/2})$. В силу теоремы 2 проекции F^+ и F^- есть

линейные комбинации характеристических векторов самодуальных и анти-самодуальных бент-функций от n переменных:

$$F^+ = \sum_{i=1}^{2^{n-1}} \alpha_i F_i^+, \qquad\qquad F^- = \sum_{j=1}^{2^{n-1}} \beta_j F_j^-,$$

где $\alpha_k,\beta_l \in \mathbb{R}$, $k,l = 1,2,\ldots,2^{n-1}$, а наборы векторов $\left\{F_i^+\right\}_{i=1}^{2^{n-1}}$ и $\left\{F_j^-\right\}_{j=1}^{2^{n-1}}$ — базисы собственных подпространств $\mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right)$ и $\mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$, состоящие из характеристических векторов самодуальных и анти-самодуальных бент-функций от n переменных, соответственно. Тогда действие отображения дуальности на функцию f можно описать схемой

$$H_n(-1)^f = H_n\left(F^+ + F^-\right) = 2^{n/2}F^+ - 2^{n/2}F^- = 2^{n/2}(-1)^{\widetilde{f}},$$

то есть в терминах характеристических векторов справедливо

$$F^+ + F^- = (-1)^f \xrightarrow{\sim} (-1)^{\widetilde{f}} = F^+ - F^-,$$

то есть коэффициенты в разложении по базису изменяются согласно правилу

$$(\alpha_1,\alpha_2,\ldots,\alpha_{2^{n-1}},\beta_1,\beta_2,\ldots,\beta_{2^{n-1}}) \xrightarrow{\sim} (\alpha_1,\alpha_2,\ldots,\alpha_{2^{n-1}},-\beta_1,-\beta_2,\ldots,-\beta_{2^{n-1}}).$$

Глава 3. Изометричные отображения и отображение дуальности

В данной главе исследуется группа автоморфизмов множества самодуальных бент-функций, а также изометричные отображения, сохраняющие некоторые метрические свойства отображения дуальности. Отмечается тесная связь между данными объектами.

3.1 Определения и обозначения

Отображение φ множества всех булевых функций от n переменных в себя называется *изометричным*, если оно сохраняет расстояние Хэмминга между функциями, то есть

$$\mathrm{dist}(\varphi(f),\varphi(g)) = \mathrm{dist}(f,g),$$

для любых $f,g \in \mathcal{F}_n$. Группа изометричных отображений множества всех булевых функций от n переменных в себя обозначается через $\mathcal{I}_n$.

Пример 1. Композиция афинной замены координат и сдвига на аффинную функцию, то есть отображение вида

$$f(x) \longrightarrow f\left(Ax \oplus b\right) \oplus \langle c,x\rangle \oplus d, \tag{3.1}$$

где $A \in \mathrm{GL}\,(n,\mathbb{F}_2)$, $b,c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$, является элементом $\mathcal{I}_n$.

Общая форма изометричных отображений множества всех булевых функций от n переменных в себя имеет следующий вид (А. А. Марков, 1956)

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

где π — подстановка на множестве $\mathbb{F}_2^n$, и $g \in \mathcal{F}_n$ [11]. Каждое отображение такого вида обозначается через $\varphi_{\pi,g} \in \mathcal{I}_n$.

Квадратная матрица называется *мономиальной* (*обобщённой перестановочной*), если в каждой её строке и в каждом столбце ровно один ненулевой элемент. Между группой $\mathcal{I}_n$ и множеством всех мономиальных матриц порядка 2^n

с ненулевыми элементами из множества $\{\pm 1\}$ существует взаимно-однозначное соответствие. Пусть $\mathbf{v}_0,\mathbf{v}_1,\ldots,\mathbf{v}_{2^n-1}$ — все элементы пространства $\mathbb{F}_2^n$, упорядоченные лексикографически. Зафиксируем произвольное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$, тогда для любой $f \in \mathcal{F}_n$ и её характеристического вектора

$$(-1)^f = \left((-1)^{f(\mathbf{v}_0)},(-1)^{f(\mathbf{v}_1)},\ldots,(-1)^{f(\mathbf{v}_{2^n-1})}\right)$$

характеристический вектор

$$(-1)^{f'} = \left((-1)^{f'(\mathbf{v}_0)},(-1)^{f'(\mathbf{v}_1)},\ldots,(-1)^{f'(\mathbf{v}_{2^n-1})}\right)$$

булевой функции $f' = \varphi_{\pi,g}(f) \in \mathcal{F}_n$ может быть представлен как

$$(-1)^{f'} = A(-1)^f,$$

где A — мономиальная матрица порядка 2^n, которая строится на основе подстановки π и функции g. Рассмотрим её построение более подробно. Для каждого $i = 1,2,\ldots,2^n$ ненулевой элемент строки i расположен на позиции с номером j — данный номер определяется из условия, что двоичным представлением числа $(j-1)$ является вектор $\pi(\mathbf{v}_{i-1})$. Произведение характеристического вектора $(-1)^f$ на матрицу A имеет вид

$$i\begin{pmatrix} & & j & & \\ & & 0 & & \\ & & \vdots & & \\ 0 & \cdots & (-1)^{g(\mathbf{v}_{i-1})} & \cdots & 0 \\ & & \vdots & & \\ & & 0 & & \end{pmatrix} \cdot \begin{pmatrix} (-1)^{f(\mathbf{v}_0)} \\ (-1)^{f(\mathbf{v}_1)} \\ \vdots \\ (-1)^{f(\mathbf{v}_{2^n-1})} \end{pmatrix} = \begin{pmatrix} \vdots \\ \vdots \\ (-1)^{f(\pi(\mathbf{v}_{i-1}))\oplus g(\mathbf{v}_{i-1})} \\ \vdots \\ \vdots \end{pmatrix}.$$

Таким образом, i-я компонента вектора $A(-1)^f$ равна

$$(-1)^{f'(\mathbf{v}_{i-1})} = (-1)^{f(\pi(\mathbf{v}_{i-1}))} \cdot (-1)^{g(\mathbf{v}_{i-1})} = (-1)^{f(\pi(\mathbf{v}_{i-1}))\oplus g(\mathbf{v}_{i-1})},$$

из чего следует, что

$$f'(x) = f(\pi(x)) \oplus g(x), \;\; x \in \mathbb{F}_2^n.$$

3.2 Отображение дуальности

В настоящем разделе изучается связь между отображением дуальности и изометричными отображениями множества всех булевых функций от n переменных в себя.

3.2.1 Аффинная эквивалентность бент-функции от малого числа переменных и дуальной к ней

Известно, что задача проверки аффинной эквивалентности бент-функции и дуальной к ней в общем случае является нетривиальной [59]. Отметим, что она связана с более общей постановкой проблемы, которая заключается в проверке эквивалентности двух фиксированных булевых функций, её, в частности, в своей работе [44] отмечал J. F. Dillon. Эквивалентность бент-функции своей дуальной означает, что на данной функции действие отображения дуальности может быть представлено в виде композиции обратимой аффинной замены координат и сдвига на аффинную функцию. Задача описания и классификации всех бент-функций от n переменных, обладающих таким свойством, представляется нетривиальной.

Предположим, что в некотором классе аффинной эквивалентности бент-функций от n переменных, скажем C, существует бент-функция f', эквивалентная своей дуальной. Каждая другая бент-функция f из этого класса эквивалентна функции f', следовательно, функции $\widetilde{f}$ и $\widetilde{f'}$ также расширенно аффинно эквиваленты, так как эквивалентность двух бент-функций влечёт эквивалентность их дуальных. В этом случае функция $\widetilde{f}$ лежит в классе C, а значит и любая другая бент-функция из класса C эквивалентна своей дуальной бент-функции. В частности, наличие в некотором классе расширенной аффинной эквивалентности (анти-)самодуальной бент-функций влечёт эквивалентность каждой бент-функции из этого класса своей дуальной. Так, например, каждая квадратичная бент-функция всегда эквивалента своей дуальной.

В настоящем разделе данный вопрос расширенной аффинной эквивалентности бент-функции и дуальной к ней будет изучен для бент-функций от малого числа переменных.

Утверждение 4. *Каждая бент-функция от $n \leqslant 6$ переменных расширенно аффинно эквивалентна своей дуальной.*

Доказательство. В каждом из случаев $n = 2$, $n = 4$ существует по одному классу расширенной аффинной эквивалентности с представителями x_1x_2 и $x_1x_2 \oplus x_3x_4$, соответственно, то есть каждая бент-функция от 2 и 4 переменных эквивалентна своей дуальной.

Для случая $n = 6$ существует 4 класса $C_i, i = 1,2,3,4$, расширенной аффинной эквивалентности [75]. Их представителями являются:

$$\begin{aligned}
f_1(x) &= x_1x_2 \oplus x_3x_4 \oplus x_5x_6,\\
f_2(x) &= x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6,\\
f_3(x) &= x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5,\\
f_4(x) &= x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5\\
&\quad \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6,
\end{aligned}$$

где $x \in \mathbb{F}_2^6$.

Исходя из рассуждений, приведённых выше, для доказательства утверждения достаточно показать, что в каждом из представленных классов аффинной эквивалентности бент-функций от 6 переменных найдётся бент-функция, эквивалентная своей дуальной.

Класс C_1: Функция $f_1(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ является самодуальной [33];

Класс C_2: Рассмотрим обратимую матрицу

$$A = \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 1\\
1 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0
\end{pmatrix}$$

и бент-функцию

$$\begin{aligned}
f(x) = f_2(Ax) &= \langle (x_1,x_2,x_3), (x_4,x_5,x_6)\rangle \oplus x_4x_5x_6\\
&= \langle (x_1,x_2,x_3), \pi(x_4,x_5,x_6)\rangle \oplus g(x_4,x_5,x_6) \in \mathcal{M}_n,
\end{aligned}$$

где $\pi : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ — тождественная подстановка, и $g(y) = y_1y_2y_3$ для любого $y \in \mathbb{F}_2^3$. Можно показать, что

$$\begin{aligned}\widetilde{f}(x) &= \left\langle \pi^{-1}(x_1,x_2,x_3), (x_4,x_5,x_6) \right\rangle \oplus g\left(\pi^{-1}(x_1,x_2,x_3)\right) \\ &= x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_1x_2x_3 = f_2(x);\end{aligned}$$

Класс C_3: Рассмотрим обратимую матрицу

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix},$$

вектор $c = (0,1,0,0,0,0) \in \mathbb{F}_2^6$ и функцию

$$\begin{aligned}f(x) &= f_3(Ax) \oplus \langle c,x \rangle = x_4(x_1 \oplus x_2)x_3 \oplus (x_1 \oplus x_2)x_6x_5 \oplus x_4(x_1 \oplus x_2) \\ &\oplus x_4x_6 \oplus (x_1 \oplus x_2)(x_2 \oplus x_4) \oplus x_3x_5 \oplus x_6x_5 \oplus x_2 \\ &= (x_1 \oplus x_2)x_3x_4 \oplus (x_1 \oplus x_2)x_5x_6 \oplus x_1x_4 \oplus x_2x_4 \oplus x_4x_6 \oplus x_1x_2 \\ &\oplus x_1x_4 \oplus x_2x_2 \oplus x_2x_4 \oplus x_3x_5 \oplus x_6x_5 \oplus x_2 \\ &= (x_1 \oplus x_2)x_3x_4 \oplus (x_1 \oplus x_2)x_5x_6 \oplus x_1x_2 \oplus x_3x_5 \oplus x_4x_6 \oplus x_5x_6.\end{aligned}$$

Эта бент-функция является самодуальной [33].

Класс C_4: Предположим, что в классе C_4 существует бент-функция f, которая не является расширенно аффинно эквивалентной функции $\widetilde{f}$. Этот значит, что $\widetilde{f} \in C_1 \cup C_2 \cup C_3$. Но в этом случае, в силу предыдущих рассуждений имеем

$$\widetilde{\widetilde{f}} = f \in C_1 \cup C_2 \cup C_3$$

С другой стороны, $C_4 \cap (C_1 \cup C_2 \cup C_3) = \emptyset$, таким образом, получаем противоречие. Следовательно, каждая бент-функция из класса C_4 эквивалентна своей дуальной.

□

Рассмотрим граф, вершинам которого соответствуют классы расширенной аффинной эквиалентности бент-функций от n переменных. Будем считать, что две его вершины, соответствующие некоторым классам C и C', связаны ребром, если для каждой бент-функции из класса C дуальная к ней лежит в классе C'.

Ясно, что данный граф обладает следующими свойствами:

— В нём существуют изолированные вершины, например, соответствующие классам, в которых есть самодуальные или анти-самодуальные бент-функции;

— Все оставшиеся вершины имеют степень 1, формируя, таким образом, паросочетание.

3.2.2 Неподвижные точки отображения дуальности и изометричные отображения

Неподвижными точками отображения дуальности являются самодуальные бент-функции. В настоящем разделе будет изучен вопрос, существует ли изометричное отображение множества всех булевых функций от n переменных в себя, неподвижные точки которого включали бы множество самодуальных бент-функций от n переменных. Из полученных результатов следует несуществование изометричного отображения, которое каждой бент-функции ставит в соответствие дуальную к ней.

Нам понадобится следующая

Лемма 3. *Пусть $n \geqslant 4$, тогда для любых различных $x,y \in \mathbb{F}_2^n$ найдётся пара самодуальных бент-функций f,g от n переменных такая, что*

$$f(x) \oplus f(y) \oplus g(x) \oplus g(y) = 1.$$

Доказательство. Доказательство будет вестись по индукции.

База индукции: Для $n = 4$ достаточно 7 векторов значений самодуальных бент-функций от 4 переменных. Они указаны в таблице 3.1:

$\mathbf{f}_1$	0	0	0	0	0	0	1	1	0	1	0	1	0	1	1	0
$\mathbf{f}_2$	0	0	0	0	0	1	0	1	0	0	1	1	0	1	1	0
$\mathbf{f}_3$	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0
$\mathbf{f}_4$	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	1
$\mathbf{f}_5$	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	1
$\mathbf{f}_6$	0	0	1	0	0	1	0	0	0	1	0	0	1	1	0	1
$\mathbf{f}_7$	0	1	0	0	0	0	1	0	0	0	1	0	1	0	1	1

Таблица 3.1 — Требуемые векторы значений самодуальных бент-функций от 4 переменных

В таблицах 3.2 и 3.3 на пересечении строки i и столбца j расположена пара чисел (k,l) таких, что

$$\mathbf{f}_k(\mathbf{i}) \oplus \mathbf{f}_k(\mathbf{j}) \oplus \mathbf{f}_l(\mathbf{i}) \oplus \mathbf{f}_l(\mathbf{j}) = 1,$$

где $\mathbf{i},\mathbf{j} \in \mathbb{F}_2^4$ — двоичные представления целых чисел $(i-1),(j-1) \in \{0,1,\ldots,15\}$.

	0	1	2	3	4	5	6	7
0	—	(1,7)	(1,6)	(1,3)	(1,5)	(1,2)	(1,2)	(1,5)
1	(1,7)	—	(1,6)	(1,3)	(1,5)	(1,2)	(1,2)	(1,5)
2	(1,6)	(1,6)	—	(1,3)	(1,5)	(1,2)	(1,2)	(1,5)
3	(1,3)	(1,3)	(1,3)	—	(1,3)	(1,2)	(1,2)	(1,3)
4	(1,5)	(1,5)	(1,5)	(1,3)	—	(1,2)	(1,2)	(1,6)
5	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)	—	(1,3)	(1,2)
6	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)	(1,3)	—	(1,2)
7	(1,5)	(1,5)	(1,5)	(1,3)	(1,6)	(1,2)	(1,2)	—
8	(1,4)	(1,4)	(1,4)	(1,3)	(1,4)	(1,2)	(1,2)	(1,4)
9	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)	(1,3)	(1,4)	(1,2)
10	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)	(1,4)	(1,3)	(1,2)
11	(1,4)	(1,4)	(1,4)	(1,3)	(1,4)	(1,2)	(1,2)	(1,4)
12	(1,3)	(1,3)	(1,3)	(1,4)	(1,3)	(1,2)	(1,2)	(1,3)
13	(1,4)	(1,4)	(1,4)	(1,3)	(1,4)	(1,2)	(1,2)	(1,4)
14	(1,4)	(1,4)	(1,4)	(1,3)	(1,4)	(1,2)	(1,2)	(1,4)
15	(1,4)	(1,4)	(1,4)	(1,3)	(1,4)	(1,2)	(1,2)	(1,4)

Таблица 3.2 — Пары самодуальных бент-функций от 4 переменных

	8	9	10	11	12	13	14	15
0	(1,4)	(1,2)	(1,2)	(1,4)	(1,3)	(1,4)	(1,4)	(1,4)
1	(1,4)	(1,2)	(1,2)	(1,4)	(1,3)	(1,4)	(1,4)	(1,4)
2	(1,4)	(1,2)	(1,2)	(1,4)	(1,3)	(1,4)	(1,4)	(1,4)
3	(1,3)	(1,2)	(1,2)	(1,3)	(1,4)	(1,3)	(1,3)	(1,3)
4	(1,4)	(1,2)	(1,2)	(1,4)	(1,3)	(1,4)	(1,4)	(1,4)
5	(1,2)	(1,3)	(1,4)	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)
6	(1,2)	(1,4)	(1,3)	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)
7	(1,4)	(1,2)	(1,2)	(1,4)	(1,3)	(1,4)	(1,4)	(1,4)
8	—	(1,2)	(1,2)	(1,6)	(1,3)	(1,5)	(1,5)	(1,5)
9	(1,2)	—	(1,3)	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)
10	(1,2)	(1,3)	—	(1,2)	(1,2)	(1,2)	(1,2)	(1,2)
11	(1,6)	(1,2)	(1,2)	—	(1,3)	(1,5)	(1,5)	(1,5)
12	(1,3)	(1,2)	(1,2)	(1,3)	—	(1,3)	(1,3)	(1,3)
13	(1,5)	(1,2)	(1,2)	(1,5)	(1,3)	—	(1,6)	(1,6)
14	(1,5)	(1,2)	(1,2)	(1,5)	(1,3)	(1,6)	—	(1,7)
15	(1,5)	(1,2)	(1,2)	(1,5)	(1,3)	(1,6)	(1,7)	—

Таблица 3.3 — Пары самодуальных бент-функций от 4 переменных (продолжение)

Индукционный шаг: Предположим, что утверждение справедливо для всех положительных чётных $n = 4,6,\ldots,n_0$, где $n_0 \geqslant 4$. Положим $n = n_0 + 2$.

Рассмотрим два произвольных вектора $u,v \in \mathbb{F}_2^{n+2}$ и представим их в форме $u = (a_1,a_2,y)$ и $v = (b_1,b_2,z)$, где $a_1,a_2,b_1,b_2 \in \mathbb{F}_2$, $y,z \in \mathbb{F}_2^n$.

Случай 1: $y \neq z$. По индукционному предположению для векторов y,z существует пара функций $f_n,g_n \in \mathrm{SB}^+(n)$ такая, что

$$f_n(y) \oplus f_n(z) \oplus g_n(y) \oplus g_n(z) = 1.$$

Рассмотрим самодуальные бент-функции $f_{n+2},g_{n+2} \in \mathrm{SB}^+(n+2)$, полученные с помощью итеративной конструкции из работы [33], см. раздел 1.3.4:

$$\begin{aligned}
f_{n+2}(0,0,x) &= f_n(x), & g_{n+2}(0,0,x) &= g_n(x),\\
f_{n+2}(0,1,x) &= f_n(x), & g_{n+2}(0,1,x) &= g_n(x),\\
f_{n+2}(1,0,x) &= f_n(x), & g_{n+2}(1,0,x) &= g_n(x),\\
f_{n+2}(1,1,x) &= f_n(x) \oplus 1, & g_{n+2}(1,1,x) &= g_n(x) \oplus 1,
\end{aligned}$$

где $x \in \mathbb{F}_2^n$. Рассмотрим сумму

$$\begin{aligned}\Delta &= f_{n+2}(u) \oplus f_{n+2}(v) \oplus G(u) \oplus G(v) \\ &= f_{n+2}\left(a_1,a_2,y\right) \oplus f_{n+2}\left(b_1,b_2,z\right) \oplus G\left(a_1,a_2,y\right) \oplus G\left(b_1,b_2,z\right)\end{aligned}$$

и все возможные варианты означиваний для $a_1,a_2,b_1,b_2 \in \mathbb{F}_2$:

– при $(a_1,a_2) \in \{(0,0),(0,1),(1,0)\}$, $(b_1,b_2) \in \{(0,0),(0,1),(1,0)\}$:
$\Delta = f_n(y) \oplus f_n(z) \oplus g_n(y) \oplus g_n(z) = 1$;

– при $(a_1,a_2) \in \{(0,0),(0,1),(1,0)\}$, $(b_1,b_2) = (1,1)$:
$\Delta = f(y) \oplus (f(z) \oplus 1) \oplus g(y) \oplus (g(z) \oplus 1) = 1$;

– при $(a_1,a_2) = (1,1)$, $(b_1,b_2) \in \{(0,0),(0,1),(1,0)\}$:
$\Delta = (f(y) \oplus 1) \oplus f(z) \oplus (g(y) \oplus 1) \oplus g(z) = 1$;

– при $(a_1,a_2) = (1,1)$, $(b_1,b_2) = (1,1)$:
$\Delta = (f(y) \oplus 1) \oplus (f(z) \oplus 1) \oplus (g(y) \oplus 1) \oplus (g(z) \oplus 1) = 1$.

Таким образом, справедливо

$$f_{n+2}(u) \oplus f_{n+2}(v) \oplus g_{n+2}(u) \oplus g_{n+2}(v) = 1.$$

Случай 2: $y = z$. Тогда $(a_1,a_2) \neq (b_1,b_2)$ то есть, либо $a_1 \neq b_1$, либо $a_2 \neq b_2$, либо обе пары соответствующих элементов различны. Без ограничения общности предположим, что $a_2 \neq b_2$. В этом случае векторы $y^a = (a_2,y_1,y_2,y_3,\ldots,y_{n-1}) \in \mathbb{F}_2^n$ и $y^b = (b_2,y_1,y_2,y_3,\ldots,y_{n-1}) \in \mathbb{F}_2^n$ различны. По индукционному предположению существует пара функций $f'_n,g'_n \in \mathrm{SB}^+(n)$ таких, что

$$f'_n\left(y^a\right) \oplus f'_n\left(y^b\right) \oplus g'_n\left(y^a\right) \oplus g'_n\left(y^b\right) = 1.$$

Определим самодуальные бент-функции $f''_{n+2},g''_{n+2} \in \mathrm{SB}^+(n+2)$:

$$\begin{aligned}
f''_{n+2}(0,0,x) &= f'_n(x), & g''_{n+2}(0,0,x) &= g'_n(x),\\
f''_{n+2}(0,1,x) &= f'_n(x), & g''_{n+2}(0,1,x) &= g'_n(x),\\
f''_{n+2}(1,0,x) &= f'_n(x), & g''_{n+2}(1,0,x) &= g'_n(x),\\
f''_{n+2}(1,1,x) &= f'_n(x) \oplus 1, & g''_{n+2}(1,1,x) &= g'_n(x) \oplus 1,
\end{aligned}$$

где $x \in \mathbb{F}_2^n$. Пусть L — перестановочная матрица порядка $(n+2)$, имеющая следующий вид:

$$L = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & I_n & \\ 0 & 0 & & & \\ \hline 0 & 1 & 0 & \dots & 0 \end{array}\right),$$

тогда булевы функции

$$f'_{n+2}(a,x,b) = f''_{n+2}(L(a,x,b)) = f''_{n+2}(a,b,x),$$
$$g'_{n+2}(a,x,b) = g''_{n+2}(L(a,x,b)) = g''_{n+2}(a,b,x),$$

где $a,b \in \mathbb{F}_2$, $x \in \mathbb{F}_2^n$, будут самодуальными бент-функциями (см. раздел 3.3).

По построению векторы

$$u = (a_1,a_2,y) = (a_1,y^a,y_n),$$
$$v = (b_1,b_2,z) = \left(b_1,y^b,y_n\right),$$

где $a_1,a_2,b_1,b_2 \in \mathbb{F}_2$, $y,z \in \mathbb{F}_2^n$, различны. Рассмотрим сумму

$$\begin{aligned}\Delta' &= f'_{n+2}(u) \oplus f'_{n+2}(v) \oplus g'_{n+2}(u) \oplus g'_{n+2}(v) \\ &= f'_{n+2}\left(a_1,y^a,y_n\right) \oplus f'_{n+2}\left(b_1,y^b,y_n\right) \oplus g'_{n+2}\left(a_1,y^a,y_n\right) \oplus g'_{n+2}\left(b_1,y^b,y_n\right)\end{aligned}$$

и все возможные варианты означиваний для $a_1,b_1,y_n \in \mathbb{F}_2$:

— при $y_n = 0$:
$\Delta' = f'_n\left(y^a\right) \oplus f'_n\left(y^b\right) \oplus g'_n\left(y^a\right) \oplus g'_n\left(y^b\right) = 1$;

— при $y_n = 1$, $(a_1,b_1) = (0,0)$:
$\Delta' = f'_n\left(y^a\right) \oplus f'_n\left(y^b\right) \oplus g'_n\left(y^a\right) \oplus g'_n\left(y^b\right) = 1$;

— при $y_n = 1$, $(a_1,b_1) = (0,1)$:
$\Delta' = f'_n\left(y^a\right) \oplus f'_n\left(y^b\right) \oplus \left(g'_n\left(y^a\right) \oplus 1\right) \oplus \left(g'_n\left(y^b\right) \oplus 1\right) = 1$;

— при $y_n = 1$, $(a_1,b_1) = (1,0)$:
$\Delta' = \left(f'_n\left(y^a\right) \oplus 1\right) \oplus \left(f'_n\left(y^b\right) \oplus 1\right) \oplus g'_n\left(y^a\right) \oplus g'_n\left(y^b\right) = 1$;

— при $y_n = 1$, $(a_1,b_1) = (1,1)$:
$\Delta' = \left(f'_n\left(y^a\right) \oplus 1\right) \oplus \left(f'_n\left(y^b\right) \oplus 1\right) \oplus \left(g'_n\left(y^a\right) \oplus 1\right) \oplus \left(g'_n\left(y^b\right) \oplus 1\right) = 1$.

Таким образом, для функций f'_{n+2},g'_{n+2} справедливо

$$f'_{n+2}(u) \oplus f'_{n+2}(v) \oplus g'_{n+2}(u) \oplus g'_{n+2}(v) = 1.$$

□

Утверждение 5. *При $n \geqslant 4$ не существует изометричного отображения множества всех булевых функций от n переменных в себя, отличного от тождественного, обладающего тем свойством, что каждая самодуальная бент-функция от n переменных является его неподвижной точкой.*

Доказательство. Пусть $n \geqslant 4$. Предположим, что такое изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ существует. Пусть перестановке π соответствует перестановочная матрица $S = (s_{ij})$ порядка 2^n такая, что для каждой самодуальной бент-функции $f \in \mathrm{SB}^+(n)$ справедливо

$$\varphi_{\pi,g}(f) = S\mathbf{f} \oplus \mathbf{g} = \mathbf{f},$$

то есть

$$(S \oplus I_{2^n})\,\mathbf{f} = \mathbf{g},$$

где $\mathbf{g}$ — вектор значений функции g, а $\mathbf{f} \in \mathbb{F}_2^{2^n}$ — вектор значений функции f. Заметим, что матрица S не может быть единичной, следовательно, в матрице $(S \oplus I_{2^n})$ есть по крайней мере две строки, в каждой из которых не менее двух ненулевых элементов. Другими словами, существуют такие индексы $i,j,k \in \{1,2,\ldots,2^n\}$, $(i \neq j)$, что для вектора значений $\mathbf{f}$ каждой самодуальной бент-функции $f \in \mathrm{SB}^+(n)$ справедливо

$$\mathbf{f}_i \oplus \mathbf{f}_j = \mathbf{g}_k.$$

Из леммы 3 следует, что существует пара функций $f',f'' \in \mathrm{SB}^+(n)$ с векторами значений $\mathbf{f}'$,$\mathbf{f}''$, соответственно, таких, что

$$\left(\mathbf{f}'_i \oplus \mathbf{f}'_j\right) \oplus \left(\mathbf{f}''_i \oplus \mathbf{f}''_j\right) = 1.$$

Последнее выражение влечёт $\mathbf{g}_k \oplus \mathbf{g}_k = 1$ для некоторого $k \in \{1,2,\ldots,2^n\}$. Таким образом, приходим к противоречию. □

Из данного утверждения следует, что при $n \geqslant 4$ не существует изометричного отображения множества всех булевых функций от n переменных в себя, которое каждой бент-функции от n переменных ставит в соответствие дуальную к ней функцию. Предположим, что при $n = 2$ такое отображение, скажем $\varphi_{\pi,g} \in \mathcal{I}_2$, существует. Пусть оно описывается перестановочной матрицей S порядка 4 и вектором значений $\mathbf{g}$ булевой функции $g \in \mathcal{F}_2$, то есть для каждой $f \in \mathcal{B}_2$ имеем

$$\varphi_{\pi,g}(f) = S\mathbf{f} \oplus \mathbf{g} = \widetilde{\mathbf{f}},$$

где $\mathbf{f} \in \mathbb{F}_2^4$ — вектор значений функции f, а $\widetilde{\mathbf{f}} \in \mathbb{F}_2^4$ — вектор значений дуальной к ней функции. Из таблицы 3.4 следует, что первая строка матрицы S должна

Бент-функция, f	Вектор $\mathbf{f}$	Дуальная функция, $\widetilde{f}$	Вектор $\widetilde{\mathbf{f}}$
x_1x_2	$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$	x_1x_2	$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$
$x_1x_2 \oplus x_1$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$	$x_1x_2 \oplus x_2$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$
$x_1x_2 \oplus x_2$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$x_1x_2 \oplus x_1$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$
$x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$	$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$	$x_1x_2 \oplus x_1 \oplus x_2$	$\begin{pmatrix}0\\1\\1\\1\end{pmatrix}$

Таблица 3.4 — Пример действия отображения дуальности на некоторые бент-функции от 2 переменных

быть либо нулевой, либо состоять только из ненулевых элементов: противоречие с тем, что по выбору матрица является перестановочной.

Получаем следующее

Утверждение 6. *Не существует изометричного отображения множества всех булевых функций от n переменных в себя, которое каждой бент-функции от n переменных ставит в соответствие дуальную к ней функцию.*

Таким образом, не существует изометричного отображения, отличного от тождественного, которое каждую самодуальную бент-функцию переводит в себя. В следующем разделе для $n \geqslant 4$ будут охарактеризованы все изометричные отображения, оставляющие множество всех самодуальных бент-функций от n переменных на месте.

3.3 Группа автоморфизмов множества самодуальных бент-функций

Группой автоморфизмов фиксированного множества булевых функций $M \subseteq \mathcal{F}_n$ называется группа изометричных отображений множества всех булевых функций от n переменных в себя, оставляющих множество M на месте. Она обозначается через $\mathrm{Aut}\,(M)$. Важность нахождения данной группы обусловлена тем, что структура математического объекта и, в особенности, его метрические свойства, тесно связаны с группой автоморфизмов данного объекта [1]. Также знание группы автоморфизмов имеет значение применительно к вопросу классификации соответствующих функций на основе изометричных отображений, которые сохраняют характеризующие свойства и отличительные признаки данных функций. Более подробную информацию о методах классификации булевых функций можно найти в работе А. В. Черёмушкина [20].

Вопрос описания группы автоморфизмов конкретной бент-функции изучал U. Dempwolff в 2006 году [42]. Ещё в первых работых, посвящённых бент-функциям, было сделано наблюдение, что преобразования вида (3.1) переводят множество бент-функций от n переменных в себя [44; 75]. Группа автоморфизмов множества всех бент-функций от n переменных была полностью охарактеризована Н. Н. Токаревой в 2010 году в работе [17]: было доказано, что каждое изометричное отображение множества всех булевых функций от n переменных в себя, оставляющее множество бент-функций от n переменных на месте, является композицией аффинной замены координат и сдвига на аффинную функцию, другими словами, описывается (3.1) и в терминах групп представляет собой полупрямое произведение аффинной группы $\mathrm{GA}(n)$ и группы векторов пространства $\mathbb{F}_2^{n+1}$.

С учётом этого факта из утверждения 6 можно сделать следующий вывод.

Следствие 1. *Отображение дуальности, определённое на множестве бент-функций от n переменных, не может быть представлено в виде композиции аффинной замены координат и сдвига на аффинную функцию.*

Задача определения взаимосвязи между группами автоморфизмов двух математических объектов, один из которых является вложением в другой, как правило нетривиальна [1]. Далее рассматривается задача поиска взаимосвязи между группами автоморфизмов бент-функций и самодуальных бент-функций

от n переменных. В теминах теории кодирования данная задача есть поиск групп автоморфизмов двух нелинейных кодов, образованных множествами векторов значений бент-функций и самодуальных бент-функций.

Как было отмечено в разделе 1.3.2, отображения вида

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c,x \rangle \oplus d,$$

где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — чётное число, $d \in \mathbb{F}_2$, сохраняют самодуальность бент-функции [33; 46]. Очевидно, что каждое такое отображение является элементом группы $\mathcal{I}_n$ с

$$\pi(x) = L\left(x \oplus c\right),\ g(x) = \langle c,x \rangle \oplus d,\ x \in \mathbb{F}_2^n,$$

Напомним, что группа отображений данного вида называется *расширенной ортогональной группой* и обозначается $\overline{\mathcal{O}}_n$ [41; 46].

Далее положим $n \geqslant 4$ — чётное натуральное число. В настоящем разделе приведённый выше результат будет обобщён в рамках группы $\mathcal{I}_n$.

Был исследован вопрос, как связаны между собой множества отображений, сохраняющих самодуальность и анти-самодуальность, или, другими словами, группы автоморфизмов множеств $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$.

Утверждение 7. *Для изометричного отображения $\varphi_{\pi,g} \in \mathcal{I}_n$ с матрицей A следующие условия эквивалентны:*

1) $\varphi_{\pi,g}$ сохраняет самодуальность;

2) $\varphi_{\pi,g}$ сохраняет анти-самодуальность;

3) $AH_n = H_nA$.

Доказательство. По теореме 2 при $n \geqslant 4$ существует подмножество функций $\{f_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^+(n)$, характеристические векторы которых $\{F_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$ образуют линейно независимое множество. Также существует подмножество функций $\{g_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^-(n)$, характеристические векторы которых $\{G_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$ образуют линейно независимое множество.

Докажем, что из первого пункта утверждения следует второй. Предположим, что $\varphi_{\pi,g}$ сохраняет самодуальность. В силу обратимости матрицы A векторы $\{AF_i\}_{i=1}^{2^{n-1}}$ также образуют линейно независимый набор характеристических векторов булевых функций $\{\varphi_{\pi,g}\left(f_i\right)\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^+(n)$. Тогда для каждого характеристического вектора $F' \in \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$ булевой функции $f' \in \mathrm{SB}^-(n)$ имеем

$$\langle AF',AF_i \rangle = \left\langle A^{\mathrm{T}}AF',F_i \right\rangle = \langle F',F_i \rangle = 0$$

для $i = 1,2,\ldots,2^{n-1}$, следовательно, справедливо $AF' \in \mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$, что влечёт $\varphi_{\pi,g}(f') \in \mathrm{SB}^-(n)$. Таким образом, для каждой анти-самодуальной бент-функции f' её образ $\varphi_{\pi,g}(f')$ также является анти-самодуальной бент-функцией.

Аналогично, можно показать, что из второго пункта утверждения следует первый. Таким образом, заключаем, что первые два пункта эквиваленты.

Теперь докажем эквивалентность первого и третьего пунктов. Если выполняется $A\mathcal{H}_n = \mathcal{H}_n A$, то для характеристического вектора F произвольной булевой функции $f \in \mathrm{SB}^+(n)$ справедливо

$$\mathcal{H}_n(AF) = A(\mathcal{H}_n F) = AF,$$

следовательно, отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ с матрицей A сохраняет самодульность.

Обозначим $B = \mathcal{H}_n A - A\mathcal{H}_n$ и предположим, что отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ с матрицей A сохраняет самодуальность и, как показано выше, анти-самодуальность. В частности, для $i = 1,2,\ldots,2^{n-1}$ имеем

$$\mathcal{H}_n(AF_i) = AF_i,$$
$$\mathcal{H}_n(AG_i) = -AG_i.$$

Для $i = 1,2,\ldots,2^{n-1}$ справедливо

$$(\mathcal{H}_n A - A\mathcal{H}_n)F_i = \mathcal{H}_n(AF_i) - A(\mathcal{H}_n F_i) = \mathcal{H}_n(AF_i) - AF_i = BF_i.$$

Тогда $BF_i = \mathbf{0} \in \mathbb{R}^{2^n}$ для каждого $i = 1,2,\ldots,2^{n-1}$. Отсюда, а также из того факта, что множество $\{F_i\}_{i=1}^{2^{n-1}}$ образует базис собственного подпространства $\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$, следует, что все строки матрицы B являются элементами собственного подпространства $(\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n}))^\perp = \mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$.

Для $i = 1,2,\ldots,2^{n-1}$ также имеем

$$(\mathcal{H}_n A - A\mathcal{H}_n)G_i = \mathcal{H}_n(AG_i) - A(\mathcal{H}_n G_i) = \mathcal{H}_n(AG_i) + AG_i = BG_i.$$

В этом случае $BG_i = \mathbf{0} \in \mathbb{R}^{2^n}$ для каждого $i = 1,2,\ldots,2^{n-1}$. В силу того, что множество $\{G_i\}_{i=1}^{2^{n-1}}$ образует базис собственного подпространства $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$ заключаем, что все строки матрицы B являются элементами собственного подпространства $(\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}))^\perp = \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$.

Таким образом, доказано, что все строки матрицы B лежат в пересечении подпространств

$$\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}) \cap \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n}),$$

но в силу ортогональности собственных подпространств матрицы $\mathcal{H}_n$, соответствующим различным собственным числам, данное пересечение состоит только из нулевого элемента пространства $\mathbb{R}^n$. Следовательно, матрица B — нулевая матрица. □

Следствие 2. *При* $n \geqslant 4$ *справедливо*

$$\mathrm{Aut}\left(\mathrm{SB}^+(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^-(n)\right).$$

Критерий самодуальности (условие $A\mathcal{H}_n = \mathcal{H}_n A$) может быть сформулироан следующим образом: если $n \geqslant 4$, то изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ принадлежет $\mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$ тогда и только тогда, когда для любых $x,y \in \mathbb{F}_2^n$ справедливо

$$\langle \pi(x),y\rangle \oplus g(x) = \left\langle x,\pi^{-1}(y)\right\rangle \oplus g\left(\pi^{-1}(y)\right).$$

Случай $n = 2$ является исключением, потому что, в частности, теорема 2 и утверждение 7 не выполняются. Действительно, рассмотрим изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_2$ с матрицей:

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Оно отображает самодуальную бент-функцию $f(x_1,x_2) = x_1x_2$ с характеристическим вектором $(1,1,1,-1)$ в её отрицание $(-1,-1,-1,1)$, а анти-самодуальную бент-функцию $f(x_1,x_2) = x_1x_2 \oplus x_1 \oplus x_2$ с характеристическим вектором $(1,-1,-1,-1)$ оно отображает в себя. Таким образом, данное изометричное отображение сохраняет и самодуальность, и анти-самодуальность. Но в то же время

$$A\mathcal{H}_n = \begin{pmatrix} -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}, \quad \mathcal{H}_n A = \begin{pmatrix} -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1. \end{pmatrix},$$

следовательно, $A\mathcal{H}_n \neq \mathcal{H}_n A$.

Теперь рассмотрим изометричное отображение $\varphi_{\pi',g'} \in \mathcal{I}_2$, которому соответствует матрица

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

Оно отображает самодуальную бент-функцию $f(x_1,x_2) = x_1x_2$ с характеристическим $(1,1,1,-1)$ в себя, но анти-самодуальную бент-функцию $f(x_1,x_2) = x_1x_2 \oplus x_1 \oplus x_2$ с характеристическим вектором $(1,-1,-1,-1)$ оно отображает в бент-функцию $f(x_1,x_2) = x_1x_2 \oplus x_2 \oplus 1$ с характеристическим вектором $(-1,1,-1,-1)$. Данная бент-функция не является ни самодуальной, ни анти-самодуальной, значит рассматриваемое изометричное отображение сохраняет самодуальность, но не сохраняет анти-самодуальность.

Из утверждения 7 следует, что при $n \geqslant 4$ проблема характеризации изометричных отображений с указанными свойствами непосредственно связана с задачей перечисления всех мономиальных матриц порядка $2^n \times 2^n$ с ненулевыми элементами из множества $\{\pm 1\}$, перестановочных с матрицей $\mathcal{H}_n$. Её решение описывает следующая

Теорема 3. *Для $n \geqslant 4$ справедливо*

$$\mathrm{Aut}\left(\mathrm{SB}^+(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^-(n)\right) = \overline{\mathcal{O}}_n.$$

Доказательство. В силу следствия 2 достаточно найти группу автоморфизмов множества самодуальных бент-функций от n переменных. Как было упомянуто ранее, группа $\overline{\mathcal{O}}_n$ сохраняет самодуальность.

Теперь, пусть $\varphi_{\pi,g} \in \mathcal{I}_n$ произвольное отображение, сохраняющее самодуальность, и A — его матрица. Обозначим через $T_{a,r}$ характеристический вектор аффинной функции от n переменных $l(x) = \langle a,x \rangle \oplus r$, где $a,x \in \mathbb{F}_2^n, r \in \mathbb{F}_2$. Другими словами, вектор $T_{a,r}$ равен некоторой строке или столбцу матрицы H_n при $r = 0$ и совпадает с некоторой строкой матрицы $(-H_n)$ в случае $r = 1$. Согласно утверждению 7 имеем $A\mathcal{H}_n = \mathcal{H}_n A$, следовательно

$$\mathcal{H}_n(AT_{a,r}) = A(\mathcal{H}_n T_{a,r}) = 2^{n/2}\sigma \cdot Ae_k = 2^{n/2}\sigma' \cdot e_{k'},$$

где $k,k' \in \{1,2,\ldots,2^n\}$, $\sigma,\sigma' \in \{\pm 1\}$. Тогда

$$AT_{a,r} = 2^{n/2}\sigma' \cdot \mathcal{H}_n e_{k'} = T_{a',r'}$$

для некоторых $a' \in \mathbb{F}_2^n$, $r' \in \mathbb{F}_2$.

Таким образом, отображение $\varphi_{\pi,g}$ отображает множество аффинных функций от n переменных в себя, значит имеет вид

$$f(x) \longrightarrow f\left(Lx \oplus b\right) \oplus \langle c,x \rangle \oplus d, \tag{3.2}$$

где $L \in \mathrm{GL}\left(n,\mathbb{F}_2\right)$, $b,c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$, (см., к примеру, [63]).

Рассмотрим условие $AH_n = H_nA$. Строки матрицы Сильвестра — Адамара соответствуют характеристическим векторам линейных функций от n переменных [15; 40], следовательно,

$$H_n = \begin{pmatrix} (-1)^{\langle \mathbf{v}_0,\mathbf{v}_0 \rangle} & (-1)^{\langle \mathbf{v}_0,\mathbf{v}_1 \rangle} & \cdots & (-1)^{\langle \mathbf{v}_0,\mathbf{v}_{2^n-1} \rangle} \\ (-1)^{\langle \mathbf{v}_1,\mathbf{v}_0 \rangle} & (-1)^{\langle \mathbf{v}_1,\mathbf{v}_1 \rangle} & \cdots & (-1)^{\langle \mathbf{v}_1,\mathbf{v}_{2^n-1} \rangle} \\ \vdots & \vdots & \ddots & \vdots \\ (-1)^{\langle \mathbf{v}_{2^n-1},\mathbf{v}_0 \rangle} & (-1)^{\langle \mathbf{v}_{2^n-1},\mathbf{v}_1 \rangle} & \cdots & (-1)^{\langle \mathbf{v}_{2^n-1},\mathbf{v}_{2^n-1} \rangle} \end{pmatrix}.$$

Выпишем в явном виде строку i и столбец j матрицы A аффинного преобразования (3.2). Для $i = 1,2,\ldots,2^n$ строка i матрицы A есть вектор с единственной ненулевым элементом, равным $(-1)^{\langle c,\mathbf{v}_{i-1} \rangle \oplus d}$. Он расположен на позиции j, где $(j-1)$ — целое число с двоичным представлением $(L\mathbf{v}_{i-1} \oplus b)$.

$$\begin{matrix} & & & & j & & & \\ \Big(& 0 & \cdots & 0 & (-1)^{\langle c,\mathbf{v}_{i-1} \rangle \oplus d} & 0 & \cdots & 0 \Big). \end{matrix}$$

Для $j = 1,2,\ldots,2^n$ столбец j матрицы A есть вектор с единственным ненулевым элементом, равным $(-1)^{\left\langle c,L^{-1}(\mathbf{v}_{j-1} \oplus b) \right\rangle \oplus d}$. Он расположен на позиции i, где $(i-1)$ — целое число с двоичным представлением $L^{-1}\left(\mathbf{v}_{j-1} \oplus b\right)$.

$$i \begin{pmatrix} 0 \\ \vdots \\ 0 \\ (-1)^{\left\langle c,L^{-1}(\mathbf{v}_{j-1} \oplus b) \right\rangle \oplus d} \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

Фиксируем произвольные $i,j \in \{0,1,\ldots,2^n-1\}$, используя представление матрицы Сильвестра — Адамара и вид строки матрицы A, выпишем в явном виде

элементы произведение матрицы A и H_n, а также матриц H_n и A:

$$(AH_n)_{i+1,j+1} = (-1)^{\langle c,\mathbf{v}_i\rangle \oplus \langle L\mathbf{v}_i \oplus b,\mathbf{v}_j\rangle \oplus d},$$
$$(H_nA)_{i+1,j+1} = (-1)^{\left\langle \mathbf{v}_i,L^{-1}(\mathbf{v}_j\oplus b)\right\rangle \oplus \left\langle c,L^{-1}(\mathbf{v}_j\oplus b)\right\rangle \oplus d}.$$

Условие $AH_n = H_nA$ влечёт равенство $(AH_n)_{i+1,j+1} = (H_nA)_{i+1,j+1}$ для всех $i,j = 0,1,\ldots,2^n-1$. Соответственно, должно выполняться

$$(-1)^{\langle c,\mathbf{v}_i\rangle \oplus \langle L\mathbf{v}_i \oplus b,\mathbf{v}_j\rangle \oplus d} = (-1)^{\left\langle \mathbf{v}_i,L^{-1}(\mathbf{v}_j\oplus b)\right\rangle \oplus \left\langle c,L^{-1}(\mathbf{v}_j\oplus b)\right\rangle \oplus d},$$

или, эквивалентно,

$$\langle c,x\rangle \oplus \langle Lx \oplus b,y\rangle \oplus d = \left\langle x,L^{-1}\left(y\oplus b\right)\right\rangle \oplus \left\langle c,L^{-1}\left(y\oplus b\right)\right\rangle \oplus d,\ \ x,y \in \mathbb{F}_2^n. \quad (3.3)$$

Подставим нулевой вектор $y = \mathbf{0} \in \mathbb{F}_2^n$ в (3.3). Получим

$$\langle c,x\rangle = \left\langle x,L^{-1}b\right\rangle \oplus \left\langle c,L^{-1}b\right\rangle,$$

$$\left\langle x,L^{-1}b\oplus c\right\rangle = \left\langle c,L^{-1}b\right\rangle$$

для каждого $x \in \mathbb{F}_2^n$. Тогда

$$\begin{cases} L^{-1}b \oplus c = 0, \\ \left\langle c,L^{-1}b\right\rangle = 0, \end{cases}$$

$$\begin{cases} b = Lc, \\ \mathrm{wt}\,(c)\ \text{— чётное число}. \end{cases} \quad (3.4)$$

Вернёмся к условию (3.3) и учтём (3.4):

$$\langle c,x\rangle \oplus \langle Lx \oplus Lc,y\rangle = \left\langle x,L^{-1}\left(y\oplus Lc\right)\right\rangle \oplus \left\langle c,L^{-1}\left(y\oplus Lc\right)\right\rangle,$$
$$\langle c,x\rangle \oplus \langle Lx,y\rangle \oplus \langle Lc,y\rangle = \left\langle x,L^{-1}y\right\rangle \oplus \langle x,c\rangle \oplus \left\langle c,L^{-1}y\right\rangle \oplus \langle c,c\rangle,$$
$$\langle Lx,y\rangle \oplus \langle Lc,y\rangle = \left\langle x,L^{-1}y\right\rangle \oplus \left\langle c,L^{-1}y\right\rangle,$$
$$\langle L\left(x\oplus c\right),y\rangle = \left\langle \left(L^{-1}\right)^{\mathrm{T}}\left(x\oplus c\right),y\right\rangle$$

для всех $x,y \in \mathbb{F}_2^n$. В этом случае

$$L\left(x\oplus c\right) = \left(L^{-1}\right)^{\mathrm{T}}\left(x\oplus c\right),\ \ x \in \mathbb{F}_2^n,$$

то есть

$$Lz = \left(L^{-1}\right)^{\mathrm{T}} z,\ \ z \in \mathbb{F}_2^n.$$

Данное условие эквивалентно тому, что

$$L = \left(L^{-1}\right)^{\mathrm{T}}. \tag{3.5}$$

Таким образом, принимая во внимание условия (3.4) и (3.5), получаем следующие условия на параметры отображения (3.2):

$$\begin{cases} L^{-1} = L^{\mathrm{T}}, \\ b = Lc, \\ \mathrm{wt}\,(c) \ \text{— чётное число.} \end{cases}$$

□

Следствие 3. *Пусть $n \geqslant 4$, тогда изометричное отображение всех булевых функций от n переменных в себя сохраняет (анти-)самодуальность, если и только если оно имеет вид $f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x \rangle \oplus d$, где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — чётное число, $d \in \mathbb{F}_2$.*

Таким образом, подход к классификации самодуальных бент-функций, предложенный в работах [33; 46], является самым общим в рамках изометричных отображений множества всех булевых функций от n переменных, сохраняющих самодуальность.

3.4 Метрические свойства отображения дуальности

Отображение дуальности порождает разбиение множества бент-функций от n переменных на классы такое, что в рамках каждого класса все бент-функции находятся на одинаковом расстоянии от своей дуальной. В данном разделе будет получена характеризация всех изометричных отображений, сохраняющих структуру данных классов. Ключевым моментом в решении данной задачи является обнаружение тесной связи между рассматриваемыми отображениями, а также группой автоморфизмов множества самодуальных бент-функций от n переменных.

В разделе 1.4 было отмечено, что действие расширенной ортогональной группы сохраняет отношение Рэлея каждой бент-функции. В данном разделе будут приведена полная характеризация изометричных отображений из группы $\mathcal{I}_n$, сохраняющих отношение Рэлея каждой булевой функции.

Утверждение 8. *Изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ сохраняет отношение Рэлея каждой булевой функции от n переменных тогда и только тогда, когда оно сохраняет самодуальность бент-функции от n переменных.*

Доказательство. Необходимость следут из того факта, что $S_f = +2^{3n/2}$ в том и только в том случае, когда $f \in \mathrm{SB}^+(n)$ [33]) (см. раздел 1.4).

Докажем достаточность. Пусть отображение $\varphi_{\pi,g}$ с матрицей A сохраняет самодуальность. Зафиксируем произвольную булеву функцию $f \in \mathcal{F}_n$ и запишем её отношение Рэлея в следующем виде

$$S_f = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x,y \rangle} = \langle F, H_n F \rangle ,$$

где F — характеристический вектор булевой функции f. Отображение сохраняет отношение Рэлея функции f, если $S_{\varphi_{\pi,g}(f)} = S_f$. Действие отображения $\varphi_{\pi,g}$ описывается матрицей A, то есть

$$S_{\varphi_{\pi,g}(f)} = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{\varphi_{\pi,g}(f)(x) \oplus \varphi_{\pi,g}(f)(y) \oplus \langle x,y \rangle} = \langle AF, H_n (AF) \rangle .$$

Из утверждения 7 следует, что $AH_n = H_n A$, следовательно, справедлива цепочка равенств

$$\langle AF, H_n (AF) \rangle = \langle AF, A (H_n F) \rangle = \left\langle A^{\mathrm{T}} AF, H_n F \right\rangle = \langle F, H_n F \rangle .$$

Таким образом, отображение $\varphi_{\pi,g}$ сохраняет отношение Рэлея функции f. В силу произвольности выбора f заключаем, что рассматриваемое отображение сохраняет отношение Рэлея каждой булевой функции от n переменных. □

Ниже будет приведён пример изометричного отображения, сохраняющего расстояние Хэмминга между каждой бент-функцией и дуальной к ней.

Пусть φ — изометричное отображение множества всех булевых функций от n переменных в себя, являющееся элементом группы автоморфизмов множества бент-функций от n переменных. Зафиксируем бент-функцию от n переменных, скажем f, и пусть она под действием отображения φ переходит в бент-функцию $g \in \mathcal{B}_n$. Имеем следующую схему

$$\begin{array}{ccc} f & \xrightarrow{\sim} & \widetilde{f} \\ {\scriptstyle \varphi}\downarrow & & \\ g & \xrightarrow{\sim} & \widetilde{g} \end{array}$$

Интересен вопрос, при каких условиях отображение φ переводит дуальную функцию $\widetilde{f}$ в $\widetilde{g}$, то есть

$$\begin{array}{ccc} f & \xrightarrow{\sim} & \widetilde{f} \\ \varphi \downarrow & & \downarrow \varphi \\ g & \xrightarrow{\sim} & \widetilde{g} \end{array}$$

или, другими словами, справедливо

$$\widetilde{\varphi(f)} = \varphi(\widetilde{f}). \tag{3.6}$$

В этом случае

$$\mathrm{dist}(\varphi(f),\widetilde{\varphi(f)}) = \mathrm{dist}(\varphi(f),\varphi(\widetilde{f})) = \mathrm{dist}(f,\widetilde{f}).$$

Таким образом, если условие (3.6) справедливо для *каждой* бент-функции от n переменных, изометричное отображение сохраняет расстояние между каждой бент-функцией и дуальной к ней. Изометричное отображение, являющееся элементом группы автоморфизмов множества бент-функций, такое, что условие (3.6) справедливо для каждой бент-функции, будем называть *перестановочным с отображением дуальности*.

Следующий результат устанавливает взаимосвязь между группой автоморфизмов самодуальных бент-функций от n переменных и изометричными отображениями, сохраняющими расстояние Хэмминга между каждой бент-функцией от n переменных и дуальной к ней.

Теорема 4. *Пусть φ — изометричное отображение множества всех булевых функций от $n \geqslant 4$ переменных в себя. Тогда следующие условия эквивалентны:*

1) *φ перестановочно с отображением дуальности;*
2) *φ является элементом группы автоморфизмов множества бент-функций от n переменных и сохраняет расстояние Хэмминга между каждой бент-функцией и дуальной к ней;*
3) *φ является элементом группы автоморфизмов множества самодуальных бент-функций от n переменных.*

Доказательство. Пусть $\varphi \in \mathcal{I}_n$.

Докажем эквивалентность первого и третьего пунктов.

Предположим, что отображение φ перестановочно с отображением дуальности. Тогда, если $f \in \mathrm{SB}^+(n)$, имеем

$$\widetilde{\varphi(f)} = \varphi(\widetilde{f}) = \varphi(f),$$

то есть бент-функция $\varphi(f)$ также является самодуальной. Следовательно, в силу произвольности выбора f, заключаем, что отображение φ сохраняет самодуальность.

Теперь, пусть A — матрица отображения φ. Если отображение φ сохраняет самодуальность, то по утверждению 7 для каждой функции $f \in \mathcal{B}_n$ в терминах характеристических векторов имеем

$$(-1)^{\widetilde{\varphi(f)}} = \mathcal{H}_n(-1)^{\varphi(f)} = \mathcal{H}_n A(-1)^f = A\mathcal{H}_n(-1)^f = A(-1)^{\widetilde{f}} = (-1)^{\varphi(\widetilde{f})},$$

то есть для φ справедливо (3.6). Кроме того, из теоремы 3 следует, что оно является элементом группы $\varphi \in \mathrm{Aut}\,(\mathcal{B}_n)$. Заключаем, что изометричные отображения всех булевых функций от n переменных в себя, обладающие свойством (3.6), в точности описываются группой автоморфизмов множества самодуальных бент-функций от n переменных.

Докажем эквивалентность второго и третьего пунктов.

Если φ сохраняет расстояние Хэмминга между каждой бент-функцией от n переменных и дуальной к ней, то оно сохраняет (анти-)самодуальность, следовательно, $\varphi \in \mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$.

Если отображение φ сохраняет (анти-)самодуальность, то по утверждению 8 оно сохраняет отношение Рэлея, в то же время из вида отображений, описываемых теоремой 3, следует, что оно оставляет множество бент-функций от n переменных на месте. Осталось заметить, что расстояние Хэмминга между бент-функций $f \in \mathcal{B}_n$ и дуальной к ней функцией $\widetilde{f}$ может быть выражено через значение S_f:

$$\mathrm{dist}(f,\widetilde{f}) = 2^{n-1} - \frac{1}{2^{n/2+1}} S_f.$$

□

Следствие 4. *Изометричное отображение множества всех булевых функций от $n \geqslant 4$ переменных в себя оставляет множество бент-функций от n переменных на месте и сохраняет расстояние Хэмминга между каждой бент-функцией от n переменных и дуальной к ней в том и только в том случае, когда оно имеет вид $f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x\rangle \oplus d$, где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — чётное число, $d \in \mathbb{F}_2$.*

Таким образом, при $n \geqslant 4$ группа автоморфизмов множества самодуальных бент-функций характеризует изометричные отображения, сохраняющие разбиение множества бент-функций от n переменных на классы относительно расстояний Хэмминга между бент-функцией и дуальной к ней, а также являющиеся перестановочными с отображением дуальности.

На основании теоремы 4 и приведённых выше рассуждений можно сделать вывод о наличии тесной связи свойств отображения дуальности и метрических свойств самодуальных бент-функций. Исследованию свойств множества самодуальных бент-функций, а также их подклассов посвящены главы 4 и 5.

3.5 Изометричные отображения между множествами самодуальных и анти-самодуальных бент-функций

В данном разделе будут описаны изометричные оображения, определяющие взаимно-однозначные соответствия между множествами самодуальных и анти-самодуальных бент-функций. Отмечается их связь с отображениями, меняющими знак отношения Рэлея каждой булевой функции.

3.5.1 Общий вид соответствий

В данном разделе будут описаны все взаимно однозначные соответствия между самодуальными и анти-самодуальными бент-функциями от $n \geqslant 4$ переменных, определяемые на основе изометричных отображений множества всех булевых функций от n переменных в себя. Наличие данных соответствий позволяет во многих случаях тривиальным образом переносить утверждения, касающиеся метрических свойств самодуальных бент-функций, на анти-самодуальныые бент-функции, и наоборот.

Ранее отмеченное взаимно однозначное соответствие между множествами самодуальных и анти-самодуальных бент-функций от n переменных (см. раздел 1.3.1) в терминах отображений имеет вид

$$f(x) \longrightarrow f\left(x \oplus c\right) \oplus \langle c,x \rangle \,, \tag{3.7}$$

где $c = (1,0,0,\ldots,0) \in \mathbb{F}_2^n$. В статье [50] была приведена более общая форма соответствий между множествами $\left|\mathrm{SB}^+(n)\right|$ и $\left|\mathrm{SB}^-(n)\right|$, основанная на отображении (3.7), с уточнением, что в качестве вектора $c \in \mathbb{F}_2^n$ может быть взят любой другой двоичный вектор длины n, имеющий нечётный вес Хэмминга. Заметим, что отображения такого вида являются элементами группы $\mathcal{I}_n$.

Далее положим $n \geqslant 4$ — чётное натуральное число. В настоящем разделе приведённый выше результат будет обобщён в рамках группы $\mathcal{I}_n$.

Утверждение 9. *Изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ с матрицей A определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ тогда и только тогда, когда $AH_n = -H_nA$.*

Доказательство. Если $\mathcal{H}_nA = -A\mathcal{H}_n$, то для любой пары характеристических векторов F,F' булевых функций $f \in \mathrm{SB}^+(n)$ и $f' \in \mathrm{SB}^-(n)$, соответственно, справедливо

$$\mathcal{H}_n\left(AF\right) = -A\left(\mathcal{H}_nF\right) = -AF,$$
$$\mathcal{H}_n\left(AF'\right) = -A\left(\mathcal{H}_nF'\right) = AF',$$

следовательно, отображение $\varphi_{\pi,g}$ меняет местами множества $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$.

Как и в доказательстве утверждения 7, зафиксируем наборы функций $\{f_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^+(n)$ и $\{g_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^-(n)$ с линейно независимыми характеристическими векторами $\{F_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$ и $\{G_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\left(H_n + I_{2^n}\right)$, соответственно. Предположим, что отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ с матрицей A определяет взаимно-однознчное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$, обозначим $B = \mathcal{H}_nA + A\mathcal{H}_n$. В частности, для $i = 1,2,\ldots,2^{n-1}$ справедливо

$$\mathcal{H}_n\left(AF_i\right) = -AF_i,$$
$$\mathcal{H}_n\left(AG_i\right) = AG_i.$$

Для $i = 1,2,\ldots,2^{n-1}$ имеем

$$\left(\mathcal{H}_nA + A\mathcal{H}_n\right)F_i = \mathcal{H}_n\left(AF_i\right) + A\left(\mathcal{H}_nF_i\right) = \mathcal{H}_n\left(AF_i\right) + AF_i = BF_i.$$

Тогда $BF_i = \mathbf{0} \in \mathbb{R}^{2^n}$ для каждого $i = 1,2,\ldots,2^{n-1}$. В силу того, что множество $\{F_i\}_{i=1}^{2^{n-1}}$ образует базис собственного подпространства $\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$, заключаем, что все строки матрицы B принадлежат собственному подпространству $\left(\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)\right)^{\perp} = \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$.

Для $i = 1,2,\ldots,2^{n-1}$ также имеем

$$(\mathcal{H}_n A + A\mathcal{H}_n)\, G_i = \mathcal{H}_n\,(AF_i) + A\,(\mathcal{H}_n G_i) = \mathcal{H}_n\,(AG_i) - AG_i = BG_i.$$

В этом случае $BG_i = \mathbf{0} \in \mathbb{R}^{2^n}$ для каждого $i = 1,2,\ldots,2^{n-1}$. В силу того, что множество $\{G_i\}_{i=1}^{2^{n-1}}$ образует базис собственного подпространства $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$, заключаем, что все строки матрицы B принадлежат собственному подпространству $(\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}))^{\perp} = \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$.

Таким образом, все строки матрицы B принадлежат пересечению собственных подпространств

$$\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}) \cap \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})\,,$$

но, как ранее было отмечено в доказательстве утверждения 7, в силу ортогональности собственных подпространств матрицы $\mathcal{H}_n$, соответствующим различным собственным числам, данное пересечение состоит только из нулевого элемента пространства $\mathbb{R}^n$. Следовательно, матрица B — нулевая матрица. □

Данный критерий (условие $A\mathcal{H}_n = -\mathcal{H}_n A$) может быть сформулирован следующим образом: при $n \geqslant 4$ изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ тогда и только тогда, когда для любых $x,y \in \mathbb{F}_2^n$ справедливо

$$\langle \pi(x),y\rangle \oplus g(x) = \left\langle x,\pi^{-1}(y)\right\rangle \oplus g\left(\pi^{-1}(y)\right) \oplus 1.$$

Утверждение 10. *Пусть $n \geqslant 4$, тогда изометричное отображение всех булевых функций от n переменных в себя определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$, если и только если оно имеет вид $f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x\rangle \oplus d$, где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — нечётное число, $d \in \mathbb{F}_2$.*

Доказательство. Пусть $f \in \mathrm{SB}^+(n) \cup \mathrm{SB}^-(n)$, то есть $\widetilde{f} = f \oplus \varepsilon$ для некоторого $\varepsilon \in \mathbb{F}_2$. Рассмотрим булеву функцию

$$g(x) = f\,(L\,(x \oplus c)) \oplus \langle c,x\rangle \oplus d,$$

где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — нечётное число, $d \in \mathbb{F}_2$. Преобразование Уолша — Адамара данной функции имеет вид

$$\begin{aligned} W_g(y) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y\rangle \oplus g(x)} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y\rangle \oplus f(L(x \oplus c)) \oplus \langle c,x\rangle \oplus d} \\ &= (-1)^d \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y \oplus c\rangle \oplus f(L(x \oplus c))} = (-1)^d \sum_{z \in \mathbb{F}_2^n} (-1)^{\left\langle L^{-1}z \oplus c, y \oplus c\right\rangle \oplus f(z)} \\ &= (-1)^{d \oplus \langle c,y\rangle \oplus \langle c,c\rangle} \sum_{z \in \mathbb{F}_2^n} (-1)^{\langle z, L(y \oplus c)\rangle \oplus f(z)} \\ &= (-1)^{d \oplus \langle c,y\rangle \oplus 1} 2^{n/2} (-1)^{\widetilde{f}(L(y \oplus c))} = 2^{n/2} (-1)^{f(L(y \oplus c)) \oplus \langle c,y\rangle \oplus d \oplus \varepsilon \oplus 1} \\ &= 2^{n/2} (-1)^{g(y) \oplus \varepsilon \oplus 1} = 2^{n/2} (-1)^{\widetilde{g}(y)}, \end{aligned}$$

следовательно, $\widetilde{g}(y) = g(y) \oplus \varepsilon \oplus 1$ для каждого $y \in \mathbb{F}_2^n$, получаем доказательство достаточности.

Докажем необходимость. Пусть $\varphi_{\pi,g} \in \mathcal{I}_n$ — изометричное отображение, определяющее взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$. Используя рассуждения, аналогичные тем, что были приведены в ходе доказательства теоремы 3, можно показать, что $\varphi_{\pi,g}$ может быть представлено в виде

$$f(x) \longrightarrow f\left(Lx \oplus b\right) \oplus \langle c,x\rangle \oplus d, \tag{3.8}$$

где $L \in \mathrm{GL}\left(n,\mathbb{F}_2\right)$, $b,c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$.

Согласно утверждению 9 имеем $AH_n = -H_nA$. В ходе доказательства теоремы 3 было показано, что

$$\begin{aligned} \left(AH_n\right)_{i+1,j+1} &= (-1)^{\langle c,\mathbf{v}_i\rangle \oplus \langle L\mathbf{v}_i \oplus b,\mathbf{v}_j\rangle \oplus d}, \\ \left(H_nA\right)_{i+1,j+1} &= (-1)^{\left\langle \mathbf{v}_i, L^{-1}(\mathbf{v}_j \oplus b)\right\rangle \oplus \left\langle c, L^{-1}(\mathbf{v}_j \oplus b)\right\rangle \oplus d} \end{aligned}$$

для всех $i,j \in \{0,1,\ldots,2^n-1\}$.

Условие $AH_n = -H_nA$ влечёт $\left(AH_n\right)_{i+1,j+1} = -\left(H_nA\right)_{i+1,j+1}$ для любых $i,j = 0,1,\ldots,2^n-1$, следовательно, должно выполняться условие

$$(-1)^{\langle c,\mathbf{v}_i\rangle \oplus \langle L\mathbf{v}_i \oplus b,\mathbf{v}_j\rangle \oplus d} = (-1)^{\left\langle \mathbf{v}_i, L^{-1}(\mathbf{v}_j \oplus b)\right\rangle \oplus \left\langle c, L^{-1}(\mathbf{v}_j \oplus b)\right\rangle \oplus d \oplus 1},$$

или, эквивалентное ему,

$$\langle c,x\rangle \oplus \langle Lx \oplus b,y\rangle \oplus d = \left\langle x, L^{-1}\left(y \oplus b\right)\right\rangle \oplus \left\langle c, L^{-1}\left(y \oplus b\right)\right\rangle \oplus d \oplus 1, \;\; x,y \in \mathbb{F}_2^n. \tag{3.9}$$

Подставим в (3.9) нулевой вектор $y = \mathbf{0} \in \mathbb{F}_2^n$. Тогда

$$\langle c,x\rangle = \left\langle x, L^{-1}b\right\rangle \oplus \left\langle c, L^{-1}b\right\rangle \oplus 1,$$

$$\langle x,L^{-1}b \oplus c\rangle = \langle c,L^{-1}b\rangle \oplus 1$$

для каждого $x \in \mathbb{F}_2^n$. Тогда

$$\begin{cases} L^{-1}b \oplus c = 0, \\ \langle c,L^{-1}b\rangle = 1, \end{cases}$$

$$\begin{cases} b = Lc, \\ \mathrm{wt}\,(c) \ \text{— нечётное число.} \end{cases} \tag{3.10}$$

Вернёмся к (3.9) и учтём условия (3.10):

$$\begin{aligned} \langle c,x\rangle \oplus \langle Lx \oplus Lc,y\rangle &= \left\langle x,L^{-1}\left(y \oplus Lc\right)\right\rangle \oplus \left\langle c,L^{-1}\left(y \oplus Lc\right)\right\rangle \oplus 1, \\ \langle c,x\rangle \oplus \langle Lx,y\rangle \oplus \langle Lc,y\rangle &= \left\langle x,L^{-1}y\right\rangle \oplus \langle x,c\rangle \oplus \left\langle c,L^{-1}y\right\rangle \oplus \langle c,c\rangle \oplus 1, \\ \langle Lx,y\rangle \oplus \langle Lc,y\rangle &= \left\langle x,L^{-1}y\right\rangle \oplus \left\langle c,L^{-1}y\right\rangle, \\ \langle L\left(x \oplus c\right),y\rangle &= \left\langle \left(L^{-1}\right)^T\left(x \oplus c\right),y\right\rangle \end{aligned}$$

для всех $x,y \in \mathbb{F}_2^n$. Можно показать, что последнее равенство влечёт

$$L = \left(L^{-1}\right)^{\mathrm{T}}. \tag{3.11}$$

Таким образом, объединяя условия (3.10) и (3.11), получаем следующие условия на параметры отображения (3.8):

$$\begin{cases} L^{-1} = L^{\mathrm{T}}, \\ b = Lc, \\ \mathrm{wt}\,(c) \ \text{— нечётное число.} \end{cases}$$

□

Таким образом, чётность веса Хэмминга вектора $c \in \mathbb{F}_2^n$ из определения расширенной ортогональной группы регулирует действие изометричного отображения между сохранением (анти-)самодуальности и взаимно-однозначным соответствием между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$.

3.5.2 Отображения, меняющие знак отношения Рэлея

В данном разделе будут приведена характеризация изометричных отображений из группы $\mathcal{I}_n$, меняющих знак отношения Рэлея.

Утверждение 11. *Изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ меняет знак отношения Рэлея каждой булевой функции от n переменных тогда и только тогда, когда оно определяет взаимно-однозначное соответствие между множествами* $\mathrm{SB}^+(n)$ *и* $\mathrm{SB}^-(n)$.

Доказательство. Необходимость, как и в доказательстве утверждения 8, следует из того факта, что $S_f = +2^{3n/2}$ в том и только в том случае, когда $f \in \mathrm{SB}^+(n)$ и $S_f = (-2^{3n/2})$ тогда и только тогда, когда $f \in \mathrm{SB}^-(n)$ [33]) (см. раздел 1.4).

Докажем достаточность. Пусть отображение $\varphi_{\pi,g}$ с матрицей A определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$. Из утверждения 9 следует, что $AH_n = -H_nA$.

Зафиксируем произвольную булеву функцию $f \in \mathcal{F}_n$ и запишем её отношение Рэлея в следующем виде

$$S_f = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x,y \rangle} = \langle F, H_n F \rangle ,$$

где F — характеристический вектор булевой функции f. Отображение меняет знак отношения Рэлея функции f, если $S_{\varphi_{\pi,g}(f)} = -S_f$. Действие отображения $\varphi_{\pi,g}$ описывается матрицей A, то есть

$$S_{\varphi_{\pi,g}(f)} = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{\varphi_{\pi,g}(f)(x) \oplus \varphi_{\pi,g}(f)(y) \oplus \langle x,y \rangle} = \langle AF, H_n (AF) \rangle .$$

Из утверждения 9 следует, что $AH_n = -H_nA$, следовательно, справедлива цепочка равенств

$$\langle AF, H_n (AF) \rangle = \langle AF, -A (H_n F) \rangle = - \left\langle A^{\mathrm{T}} AF, H_n F \right\rangle = - \langle F, H_n F \rangle ,$$

следовательно, отображение $\varphi_{\pi,g}$ меняет знак отношения Рэлея функции f. В силу произвольности выбора f заключаем, что рассматриваемое отображение меняет знак отношение Рэлея каждой булевой функции от n переменных. □

Следствие 5. *Пусть $n \geqslant 4$, тогда изометричное отображение всех булевых функций от n переменных в себя меняет знак отношения Рэлея каждой булевой функции от n переменных, если и только если оно имеет вид $f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x \rangle \oplus d$, где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — нечётное число, $d \in \mathbb{F}_2$.*

Таким образом, отображения, описанные в Утверждении 10, и только они, обладают следующим свойством: если расстояние Хэмминга между бент-функцией и дуальной к ней равно d, то такая бент-функция переходит в бент-функцию, находящуюся на расстоянии $2^n - d$ от своей дуальной.

Из утверждений 8 и 11 следует

Утверждение 12. *Изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$, меняющее знак или сохраняющее отношение Рэлея каждой булевой функции, оставляет множество бент-функций от n переменных на месте.*

3.6 Обзор основных результатов главы

Подытожим основные результаты, полученные в данной главе.

Пусть $n \geqslant 4$ — чётное натуральное число, $\varphi_{\pi,g}$ — изометричное отображение множества всех булевых функций от n переменных в себя с матрицей A, а именно

$$\varphi_{\pi,g} : f(x) \longrightarrow f\left(\pi(x)\right) \oplus g(x),$$

где $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — подстановка на множестве $\mathbb{F}_2^n$, и $g \in \mathcal{F}_n$. Матрица A имеет вид

$$i \begin{pmatrix} & & & & j & & & \\ & & & & \vdots & & & \\ & & & & 0 & & & \\ & & & & \vdots & & & \\ \dots & 0 & \dots & & (-1)^{g(\mathbf{v}_{i-1})} & \dots & 0 & \dots \\ & & & & \vdots & & & \\ & & & & 0 & & & \\ & & & & \vdots & & & \end{pmatrix},$$

где в строке i ненулевой элемент $(-1)^{g(\mathbf{v}_{i-1})}$ расположен на позиции j, где $(j-1)$ — целое число, двоичное представление которого есть вектор $\pi\left(\mathbf{v}_{i-1}\right)$.

Таким образом, если условие (3.6) справедливо для *каждой* бент-функции от n переменных, изометричное отображение сохраняет расстояние между каждой бент-функцией и дуальной к ней. Изометричное отображение, являющееся элементом группы автоморфизмов множества бент-функций, такое, что условие

$$\widetilde{\varphi(f)} = \varphi(\widetilde{f})$$

справедливо для каждой бент-функции $f \in \mathcal{B}_n$, будем называть *перестановочным с отображением дуальности*.

Следующие условия **эквивалентны**:

1) $\varphi_{\pi,g}$ сохраняет самодуальность;
2) $\varphi_{\pi,g}$ сохраняет анти-самодуальность;
3) $\varphi_{\pi,g}$ сохраняет отношение Рэлея каждой булевой функции;
4) $\varphi_{\pi,g}$ перестановочно с отображением дуальности;
5) $\varphi_{\pi,g}$ является элементом группы автоморфизмов множества бент-функций от n переменных и сохраняет расстояние Хэмминга между каждой бент-функцией и дуальной к ней;
6) $\varphi_{\pi,g}$ оставляет множество бент-функций на месте и сохраняют расстояние Хэмминга между каждой бент-функцией и дуальной к ней;
7) $\pi(x) = L\,(x \oplus c)$, $g(x) = \langle c,x\rangle \oplus d$, где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — чётное число, $d \in \mathbb{F}_2$;
8) $AH_n = H_nA$.

Следующие условия **эквивалентны**:

1) $\varphi_{\pi,g}$ определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$;
2) $\varphi_{\pi,g}$ меняет знак отношения Рэлея каждой булевой функции от n переменных;
3) $\pi(x) = L\,(x \oplus c)$, $g(x) = \langle c,x\rangle \oplus d$, где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — нечётное число, $d \in \mathbb{F}_2$;
4) $AH_n = -H_nA$.

Глава 4. Метрические характеристики множества самодуальных бент-функций

В данной главе найдено минимальное расстояние Хэмминга между самодуальными бент-функциями, а также описаны множества булевых функций, максимально-удалённых от множества (анти-)самодуальных бент-функций. Доказана метрическая регулярность множества (анти-)самодуальных бент-функций.

Задачу нахождения минимального расстояния на некотором подмножестве булевых функций от n переменных можно рассматривать как поиск кодового расстояния в общем случае нелинейного кода длины n, образованного векторами значений функций из этого множества. В частности, векторы значений бент-функций, а также самодуальных и анти-самодуальных бент-функций, образуют нелинейные коды.

Хорошо известно, что степень бент-функции от n переменных не превосходит числа $n/2$ [75]. Следовательно, множество векторов значений бент-функций от n переменных образует подмножество в коде $\mathrm{RM}(n/2,n)$. Тогда, учитывая значение кодового расстояния для кодов Рида — Маллера, можно сделать вывод о том, что минимальное расстояние Хэмминга на множестве бент-функций ограничено снизу числом $2^{n/2}$. При этом нетрудно видеть, что минимальное расстояние Хэмминга в точности равно данной нижней границе: достаточно рассмотреть следующую пару бент-функций из класса Мэйорана — МакФарланда

$$f(x,y) = \langle x,y\rangle\,,\ \ x,y \in \mathbb{F}_2^{n/2}$$
$$g(x,y) = f(x,y) \oplus y_1y_2\ldots y_{n/2}.$$

Свойства бент-функций, находящихся на минимальном расстоянии друг от друга, широко исследовались в работах Н. А. Коломейца [4—6; 56; 57]. Был найден критерий того, что две бент-функции находятся на минимальном расстоянии друг от друга; получена точная верхняя оценка на число бент-функций на минимальном расстоянии от фиксированной бент-функции; введено понятие графа минимальных расстояний и описаны его свойства для некоторых известных классов бент-функций.

Несуществование самодуальных бент-функций от n переменных степени выше k, где $k < n/2$, повлекло бы за собой оценку

$$\min_{f,g \in \mathrm{SB}^+(n)} \mathrm{dist}\,(f,g) \geqslant 2^{n-k} > 2^{n/2}.$$

Значения, которые может принимать степень самодуальной бент-функции, изучены в следующем разделе.

4.1 Алгебраическая степень самодуальной бент-функции

Нетрудно показать, что при $n \geqslant 4$ степень бент-функции от n переменных может принимать любое значение из множества $\{2,3,\ldots,n/2\}$. Для доказательства данного утверждения достаточно рассмотреть частный случай конструкции Мэйорана — МакФарланда

$$f(x,y) = \langle x,y \rangle \oplus g(y), \;\; x,y \in \mathbb{F}_2^{n/2},$$

в рамках которого, в силу наличия свободы в выборе булевой функции g, всегда можно построить бент-функцию от n переменных, имеющую требуемую степень. Заметим, что все бент-функции от 2 переменных являются квадратичными.

В работе [37] была представлена конструкция анти-самодуальных бент-функций от n переменных, позволяющая получать функции любой степени от 2 до $n/2 - 1$.

Далее будут охарактеризованы все значения, которые может принимать степень самодуальной бент-функции. Заметим, что отображение $f(x) \longrightarrow f(x \oplus c) \oplus \langle c,x \rangle$, где $c \in \mathbb{F}_2^n$ и $\mathrm{wt}\,(c)$ — нечётное число, которое является примером отображения, отпределяющего взаимно однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ (см. раздел 3.5.1), не меняет степень функции f. Следовательно, существование самодуальной бент-функции степени d влечёт существования анти-самодуальной бент-функции, имеющей такую же степень.

Утверждение 13. *Пусть $n \geqslant 4$, тогда для любого числа $d \in \{2,3,\ldots,n/2\}$ существует самодуальная бент-функция от n переменных, степень которой равна d.*

Доказательство. Очевидно, что утверждение справедливо для $d = 2$, так как функция

$$f(x) = \bigoplus_{i=1}^{n/2} x_{2i-1}x_{2i}, \;\; x \in \mathbb{F}_2^n,$$

является квадратичной самодуальной бент-функцией для любого натурального чётного n.

Пусть $d \geqslant 3$, соответственно, имеем $n \geqslant 4$. Обозначим $k = (n-2)/2$ и рассмотрим функцию Мэйорана – МакФарланда $f \in \mathcal{M}_{2k}$:

$$f(x,y) = \langle x, \pi(y) \rangle, \;\; x,y \in \mathbb{F}_2^k.$$

где отображение $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$, $\pi(y) = (\pi_1(y), \pi_2(y), \ldots, \pi_k(y))$, $y \in \mathbb{F}_2^k$, задаётся следующими координатными функциями

$$\pi_i(y) = \begin{cases} \pi_i(y) = y_i, & \text{если } i \in \{1,2,\ldots,k\} \setminus \{d-1\}, \\ \pi_{d-1}(y) = y_{d-1} \oplus \prod\limits_{j=1}^{d-2} y_j, & \text{если } i = d-1. \end{cases}$$

Очевидно, что данная векторная функция является взаимно-однозначной, кроме того, справедливо $\pi = \pi^{-1}$.

Имеем

$$f(x,y) = \bigoplus_{i=1}^{k} x_i y_i \oplus x_{d-1} \prod_{j=1}^{d-2} y_j, \;\; x,y \in \mathbb{F}_2^k,$$

$$\widetilde{f}(x,y) = \bigoplus_{i=1}^{k} x_i y_i \oplus y_{d-1} \prod_{j=1}^{d-2} x_j, \;\; x,y \in \mathbb{F}_2^k,$$

тогда

$$f(x,y) \oplus \widetilde{f}(x,y) = x_{d-1} \prod_{i=1}^{d-2} y_i \oplus y_{d-1} \prod_{j=1}^{d-2} x_j, \;\; x,y \in \mathbb{F}_2^k.$$

Рассмотрим булеву функцию g от $2k+2$ переменных:

$$g(u,v,x,y) = (u \oplus v)\left(f(x,y) \oplus \widetilde{f}(x,y)\right) \oplus f(x,y) \oplus uv,$$

где $u,v \in \mathbb{F}_2$, $x,y \in \mathbb{F}_2^k$. Эта функция имеет характеристический вектор

$$\left(F, \widetilde{F}, \widetilde{F}, -F\right)$$

где F — характеристический вектор бент-функции f, и, следовательно, является самодуальной бент-функцией от $2k+2$ переменных (см. раздел 1.3.4). По построению её степень равна d. □

4.2 Минимальное расстояние Хэмминга

Далее будет показано, что минимальное расстояние Хэмминга между бент-функциями от $n \geqslant 4$ переменных также достижимо на множестве самодуальных и анти-самодуальных бент-функций.

Утверждение 14. *Пусть $n \geqslant 4$, тогда минимальное расстояние Хэмминга между различными самодуальными бент-функциями от n переменных равно $2^{n/2}$.*

Доказательство. Для $n = 4$ рассмотрим две самодуальные бент-функции:

$$f_4(x) = x_1x_2 \oplus x_3x_4, \;\; x \in \mathbb{F}_2^4,$$
$$g_4(x) = f_4(Lx) = x_1x_4 \oplus x_2x_3, \;\; x \in \mathbb{F}_2^4,$$

где L — перестановочная матрица следующего вида

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Ясно, что

$$f_4(x) \oplus g_4(x) = (x_1 \oplus x_3)(x_2 \oplus x_4),$$

следовательно, $\mathrm{dist}(f_4,g_4) = 2^{n/2}$.

Для каждого чётного $n \geqslant 6$ рассмотрим пару самодуальных бент-функций $f_n,g_n \in \mathrm{SB}^+(n)$ с характеристическими векторами

$$F_n = (F_{n-2}, -R_{n-2},R_{n-2},F_{n-2}),$$
$$G_n = (G_{n-2}, -R_{n-2},R_{n-2},G_{n-2}),$$

соответственно, где F_{n-2} и G_{n-2} — характеристические векторы самодуальных бент-функций $f_{n-2} \in \mathrm{SB}^+(n-2)$ и $g_{n-2} \in \mathrm{SB}^+(n-2)$, и для каждого чётного m вектор R_{2m} — характеристический вектор анти-самодуальной бент-функции $r_{2m} \in \mathrm{SB}^-(2m)$, имеющей вид

$$r_{2m}(x) = \bigoplus_{i=1}^{m} x_{2i-1}x_{2i} \oplus x_{2m-1} \oplus x_{2m}, \;\; x \in \mathbb{F}_2^{2m}.$$

Таким образом, получаем

$$\begin{aligned}\operatorname{dist}(f_n,g_n) &= 2\cdot\operatorname{dist}(f_{n-2},g_{n-2})\\ &= 2^2\cdot\operatorname{dist}(f_{n-4},g_{n-4})\\ &= \cdots\\ &= 2^k\cdot\operatorname{dist}(f_{n-2k},g_{n-2k})\\ &= \cdots\\ &= 2^{(n-4)/2}\cdot\operatorname{dist}(f_4,g_4)\\ &= 2^{n/2}.\end{aligned}$$

□

Используя изометричные взаимно однозначные соответствия между множествами самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных, описываемые Утверждением 10, получаем

Следствие 6. *Пусть $n \geqslant 4$, тогда минимальное расстояние Хэмминга между различными анти-самодуальными бент-функциями от n переменных равно $2^{n/2}$.*

При $n = 2$ существуют две самодуальных бент-функции от n переменных: x_1x_2 и $x_1x_2 \oplus 1$, одна из которых является отрицанием другой. Следовательно, расстояние Хэмминга между ними равно 2^n. Аналогично можно показать, что пара анти-самодуальных бент-функций от двух переменных находится на расстоянии 2^n.

4.3 Метрическая регулярность

В данном разделе будут охарактризованы множества булевых функций, максимально удалённых от множеств самодуальных и анти-самодуальных бент-функций от n переменных.

4.3.1 Определения и обозначения

Пусть $A \subseteq \mathbb{F}_2^n$ и $y \in \mathbb{F}_2^n$. Определим *расстояние* между вектором y и множеством A как

$$\mathrm{dist}(y,A) = \min_{x \in A} \mathrm{dist}(y,x).$$

Радиусом покрытия множества A называется число

$$\rho(A) = \max_{z \in \mathbb{F}_2^n} \mathrm{dist}(z,A).$$

Вектор $z \in \mathbb{F}_2^n$ такой, что $\mathrm{dist}(z,A) = \rho(A)$, будем называть *максимально удалённым* от множества A. Множество векторов, максимально удалённых от множества $A \subseteq \mathbb{F}_2^n$, обозначется через $\widehat{A}$ [12]. Множество A называется *метрически регулярным*, если $\widehat{\widehat{A}} = A$. Множество булевых функций называется *метрически регулярным*, если метрически регулярным является множество соответствующих им векторов значений [82].

Пример 2. В работе [81] было показано, что аффинную функций от чётного числа n переменных можно определить как функцию, максимально удалённую от множества всех бент-функций от n переменных, то есть

$$\widehat{\mathcal{B}}_n = \mathcal{A}_n.$$

С другой стороны, в силу того, что бент-функции — это в точности те булевы функции, которые максимально удалёны от множества всех аффинных функций, справедливо

$$\widehat{\mathcal{A}}_n = \mathcal{B}_n.$$

Следовательно, множества аффинных функций и бент-функций от n переменных являются метрически регулярными множествами.

Множества функций, находящиеся на максимальном расстоянии от функций, ассоциированных с разбиениями пространства $\mathbb{F}_2^n$ (partition set functions), изучались в работе [79]. Было показано, что существуют разбиения, которым соответствуют метрически регулярные множества функций.

4.3.2 Основной результат

В силу того, что для каждой функции $f \in \mathrm{SB}^+(n)$ её отрицание $f \oplus 1$ также является самодуальной бент-функцией от n переменных, радиус покрытия множества $\mathrm{SB}^+(n)$ не превосходит числа 2^{n-1}. Как было отмечено в разделе 1.3.1 расстояние Хэмминга между каждой самодуальной и анти-самодуальной бент-функциями от n переменных равно 2^{n-1}, из чего следует, что радиус покрытия множества $\mathrm{SB}^+(n)$ в точности равен данной верхней границе.

Следующий результат характеризует множества булевых функций, находящиеся на максимальном расстоянии от множеств самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных.

Теорема 5. *Пусть $n \geqslant 4$, тогда*

- *Множество булевых функций, максимально удалённых от множества самодуальных бент-функций от n переменных, совпадает с множеством анти-самодуальных бент-функций от n переменных;*
- *Множество булевых функций, максимально удалённых от множества анти-самодуальных бент-функций от n переменных, совпадает с множеством самодуальных бент-функций от n переменных.*

Доказательство. В силу того, что расстояние Хэмминга между самодуальной и анти-самодуальной бент-функциями от n переменных равно 2^{n-1}, справедливо включение

$$\mathrm{SB}^-(n) \subseteq \widehat{\mathrm{SB}^+(n)}. \tag{4.1}$$

Положим $n \geqslant 4$. Согласно теореме 2 среди характеристических векторов самодуальных бент-функций от n переменных существует набор из 2^{n-1} линейно независимых векторов. Обозначим эти векторы через $F_1^+, F_2^+, \ldots, F_{2^{n-1}}^+$, а соответствующие им самодуальные бент-функции от n переменных через $f_1^+, f_2^+, \ldots, f_{2^{n-1}}^+$.

Пусть $f \in \mathcal{F}_n$ произвольная булева функция из множества $\widehat{\mathrm{SB}^+(n)}$, то есть такая, что $\mathrm{dist}\left(f, \mathrm{SB}^+(n)\right) = 2^{n-1}$, из чего следует, что $\mathrm{dist}(f,g) = 2^{n-1}$ для любой $g \in \mathrm{SB}^+(n)$. Обозначим характеристический вектор самодуальной бент-функции f через F, и, используя лемму 2, рассмотрим её разложение $F =$

$F^+ + F^-$, где $F^\pm \in \operatorname{Ker}(\mathcal{H}_n \mp I_{2^n})$, см. также [41]. Заметим, что из равенства $\operatorname{dist}\left(f,f_i^+\right) = 2^{n-1}$ и выражения

$$\operatorname{dist}\left(f,f_i^+\right) = 2^{n-1} - \frac{1}{2}\left\langle F,F_i^+\right\rangle$$

следует, что $\left\langle F,F_i^+\right\rangle = 0$. Векторы F^+ и F^- ортогональны друг другу, так как они являются собственными векторами симметричной вещественной матрицы $\mathcal{H}_n$, соответствующими различным собственным значениям. Тогда справедливо

$$\langle F,F\rangle = \left\langle F^+,F^+\right\rangle + \left\langle F^-,F^-\right\rangle. \tag{4.2}$$

В силу того, что $F^+ \in \operatorname{Ker}(\mathcal{H}_n - I_{2^n})$, для некоторого вектора $\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_{2^{n-1}}) \in \mathbb{R}^{2^{n-1}}$ имеем $F^+ = \sum\limits_{i=1}^{2^{n-1}} \alpha_i F_i^+$. Подставив данную линейную комбинацию в (4.2), получим

$$\begin{aligned}\langle F,F\rangle &= \Big\langle F, \sum_{i=1}^{2^{n-1}} \alpha_i F_i^+\Big\rangle + \left\langle F,F^-\right\rangle = \sum_{i=1}^{2^{n-1}} \alpha_i \underbrace{\left\langle F,F_i^+\right\rangle}_{=0} + \left\langle F,F^-\right\rangle \\ &= \left\langle F,F^-\right\rangle = \left\langle F^+ + F^-,F^-\right\rangle = \left\langle F^-,F^-\right\rangle,\end{aligned}$$

следовательно, $\left\langle F^+,F^+\right\rangle = 0$, то есть $F^+ = \mathbf{0}$. Тогда $F = F^- \in \operatorname{Ker}(\mathcal{H}_n + I_{2^n})$, из чего немедленно следует $f \in \mathrm{SB}^-(n)$.

Таким образом, справедливо включение

$$\widehat{\mathrm{SB}^+(n)} \subseteq \mathrm{SB}^-(n). \tag{4.3}$$

Из включений (4.1) и (4.3) следует равенство

$$\widehat{\mathrm{SB}^+(n)} = \mathrm{SB}^-(n).$$

Доказательство для анти-самодуальных бент-функций аналогично, с учётом существования изометричных взаимно-однозначных соответствий между самодуальными и анти-самодуальными бент-функциями (см. раздел 1.3.1 и утверждение 10). □

Следствие 7. *Пусть $n \geqslant 4$, тогда булева функция от n переменных является:*

— *самодуальной, если и только если она находится на расстоянии 2^{n-1} от множества всех анти-самодуальных бент-функций от n переменных, то есть принадлежит множеству $\widehat{\mathrm{SB}^-(n)}$;*

— *анти-самодуальной, если и только если она находится на расстоянии* 2^{n-1} *от множества всех самодуальных бент-функций от* n *переменных, то есть принадлежит множеству* $\widehat{\mathrm{SB}^+(n)}$.

Данный факт позволяет установить связь между самодуальными и анти-самодуальными бент-функциями в метрическом смысле: самодуальная бент-функция от $n \geqslant 4$ переменных — это булева функция от n переменных, максимально удалённая от множества анти-самодуальных бент-функций от n переменных. Аналогичное утверждение можно сформулировать для анти-самодуальных бент-функций.

Отдельно рассмотрим случай $n = 2$. Булева функция $x_1x_2 \oplus x_1$ от двух переменных находится на расстоянии 2^{n-1} от множества $\mathrm{SB}^+(2)$, но она не является анти-самодуальной, следовательно, имеем строгое включение $\mathrm{SB}^-(2) \subset \widehat{\mathrm{SB}^+(2)}$, то есть $\widehat{\mathrm{SB}^+(2)} \neq \mathrm{SB}^-(2)$. Ясно, что $\widehat{\mathrm{SB}^-(2)} \neq \mathrm{SB}^+(2)$. Таким образом, множества $\mathrm{SB}^+(2)$ и $\mathrm{SB}^-(2)$ не являются метрическими дополнениями друг друга.

Теорема 6. *Множества самодуальных и анти-самодуальных бент-функций от* n *переменных являются метрически регулярными множествами.*

Доказательство. Пусть $n = 2$, обозначим

$$\mathcal{S} = \{x_1x_2 \oplus x_1,\, x_1x_2 \oplus x_2,\, x_1x_2 \oplus x_1 \oplus 1,\, x_1x_2 \oplus x_2 \oplus 1\} \subset \mathcal{F}_2.$$

Вспомним, что

$$\mathrm{SB}^+(2) = \{x_1x_2,\, x_1x_2 \oplus 1\},$$
$$\mathrm{SB}^-(2) = \{x_1x_2 \oplus x_1 \oplus x_2,\, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\}.$$

Очевидно, что для любой функции $f \in \mathcal{S}$ выполняется

$$\mathrm{dist}\left(f, \mathrm{SB}^+(2)\right) = \mathrm{dist}\left(f, \mathrm{SB}^-(2)\right) = 2^{n-1},$$

$$\widehat{\mathcal{S}} = \mathrm{SB}^+(2) \cup \mathrm{SB}^-(2).$$

Справедливо

$$\widehat{\mathrm{SB}^+(2)} = \mathcal{S} \cup \mathrm{SB}^-(2),$$

Метрическое дополнение множества $\mathcal{S} \cup \mathrm{SB}^-(2)$ совпадает с $\mathrm{SB}^+(2)$, следовательно, $\mathrm{SB}^+(2)$ — метрически регулярное множество.

Более того, имеем

$$\widehat{\mathrm{SB}^-(2)} = \mathcal{S} \cup \mathrm{SB}^+(2).$$

Метрическое дополнение множества $\mathcal{S} \cup \mathrm{SB}^+(2)$ совпадает с $\mathrm{SB}^-(2)$, следовательно, множество $\mathrm{SB}^-(2)$ также является метрически регулярным множеством.

Случай $n \geqslant 4$ следует из теоремы 5. □

Пусть $X \subseteq \mathbb{F}_2^n$ — метрически регулярное множество с радиусом покрытия ρ. В соответствии с [71] множества $X,\widehat{X}$ называются *строго метрически регулярными*, если для каждого $y \in \mathbb{F}_2^n$ справедливо

$$\mathrm{dist}\,(y,X) + \mathrm{dist}(y,\widehat{X}) = \rho.$$

Множество булевых функций называется *строго метрически регулярным*, если соответствующее ему множество векторов значений является строго метрически регулярным.

Утверждение 15. *Для $n \geqslant 4$ множества $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ не являются строго метрически регулярными.*

Доказательство. Рассмотрим линейную функцию $f \equiv 0$. Для неё справедливо

$$\mathrm{dist}\left(f,\mathrm{SB}^+(n)\right) = \mathrm{dist}\left(f,\mathrm{SB}^-(n)\right) = 2^{n-1} - 2^{n/2-1},$$

следовательно,

$$\mathrm{dist}\left(f,\mathrm{SB}^+(n)\right) + \mathrm{dist}\left(f,\mathrm{SB}^-(n)\right) = 2^n - 2^{n/2} > 2^{n-1}$$

для $n \geqslant 4$. □

Глава 5. Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана – МакФарланда

Полное описание всех достижимых расстояний Хэмминга между бент-функциями от n переменных является открытым вопросом. Известны некоторые частные результаты, например, в работе В. Н. Потапова [14] было доказано, что между двумя различными бент-функциями от n переменных достижимы расстояния вида $2^{n/2+1} - 2^p$, где $1 \leqslant p \leqslant n/2$. Минимальное расстояние между бент-функциями упоминалось в разделе 4.2.

В данной главе будет описан спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана – МакФарланда.

5.1 Вспомогательные утверждения

При изучении многих свойств квадратичных булевых функций ключевое значение имеет широко известная

Теорема Диксона ([43] (см. также [63])).

1) *Для каждой симплектической матрицы B ранга $2r$ существует такая обратимая двоичная матрица A, что у матрицы ABA^{T} все элементы равны нулю, за исключением двух диагоналей, лежащих непосредственно над и под главной диагональю, и эти диагонали имеют вид $1010\ldots100\ldots0$, где число единиц равно r;*
2) *Любую булеву функцию, степень которой не превосходит 2,*

$$f(x) = \langle x,Qx\rangle \oplus \langle l,x\rangle \oplus \varepsilon, \;\; x \in \mathbb{F}_2^n,$$

где Q — верхняя треугольная матрица, $l \in \mathbb{F}_2^n$ и $\varepsilon \in \mathbb{F}_2$, заменой переменных $x = A^{\mathrm{T}}y$, где A — матрица, определяемая п. 1) теоремы при $B = Q \oplus Q^{\mathrm{T}}$, можно привести к виду

$$f'(y) = \bigoplus_{i=1}^{r} y_{2i-1}y_{2i} \oplus \langle l',x\rangle \oplus \varepsilon, \;\; y \in \mathbb{F}_2^n,$$

где $l' \in \mathbb{F}_2^n$;

3) Если выражение $\langle l',y\rangle$ *линейно зависит только от* $y_1,y_2,\ldots,y_{2r}$*, то существует аффинное преобразование, которое приводит* $f'(y)$ *к виду*

$$f''(z)=\bigoplus_{i=1}^{r} z_{2i-1}z_{2i}\oplus\varepsilon_1,\ \ z\in\mathbb{F}_2^n,$$

где $\varepsilon_1\in\mathbb{F}_2$.

Нам понадобится следующая

Лемма 4. *Пусть* $A,B,C\in M_n(\mathbb{F}_2)$ *— матрицы такие, что* $C=A\oplus B$*. Если выполняется* $AA^{\mathrm{T}}=BB^{\mathrm{T}}=I_n$*, то столбцы матрицы* C *образуют линейно зависимое подмножество векторов из* $\mathbb{F}_2^n$.

Доказательство. Сначала докажем, что в каждой строке матриц A и B нечётное число единиц. Обозначим через $A_i\in\mathbb{F}_2^n$ и $\left(A^{\mathrm{T}}\right)^j\in\mathbb{F}_2^k$ строку i матрицы A и столбец j матрицы A^{T} соответственно, $i,j=1,2,\ldots,n$.

Имеем

$$\langle A_i,A_j\rangle=\left\langle A_i,\left(A^{\mathrm{T}}\right)^j\right\rangle=\bigoplus_{r=1}^{n}a_{ir}a_{jr}=(I_n)_{ij}.$$

Тогда

$$\bigoplus_{l=1}^{n}a_{il}=\bigoplus_{l=1}^{n}a_{il}a_{il}=\left\langle A_i,A_i\right\rangle=1.$$

Таким образом, в каждой строке матрицы A число единиц нечётно. Аналогичным образом можно показать, что в каждой строке матрицы B число единиц также нечётно.

Так как каждая строка матрицы C получается сложением по модулю 2 соответствующих строк матриц A и B, заключаем, что все строки матрицы C содержат чётное число единиц. Отсюда получаем, что $C^1\oplus C^2\oplus\ldots\oplus C^n=\mathbf{0}$, где $C^j\in\mathbb{F}_2^n$ — столбец j матрицы C, $j=1,2,\ldots,n$. Другими словами, столбцы матрицы C образуют линейно зависимое множество в $\mathbb{F}_2^n$. □

Пусть $k\geqslant 2$. Через $e_i\in\mathbb{F}_2^{2k}$, $i=1,2,\ldots,2k$, обозначим вектор, у которого координата i равна единице, а все остальные — 0. Через $Q^{(2k)}\in M_{2k}(\mathbb{F}_2)$ обозначим симплектическую матрицу

$$\left(Q^{(2k)}\right)_i=\begin{cases}e_{k+i}\oplus e_{k+i+1}, & \text{при } i\in\{1,2,\ldots,k-1\},\\ e_{k+1}\oplus e_{2k}, & \text{при } i=k,\\ \mathbf{0}_{2k}, & \text{при } i\in\{k+1,k+2,\ldots,2k\},\end{cases}$$

где $i = 1,2,\ldots,k$. Справедлива

Лемма 5. *Булева функция*

$$f(x) = \left\langle x, Q^{(2k)}x \right\rangle \oplus x_1 \oplus x_2, \;\; x \in \mathbb{F}_2^{2k}$$

линейным преобразованием переменных может быть приведена к виду

$$\bigoplus_{i=1}^{k-1} y_{2i-1}y_{2i} \oplus \bigoplus_{j=1}^{2(k-1)} a_j y_j, \;\; y \in \mathbb{F}_2^{2k},$$

где $(a_1,a_2,\ldots,a_{2k-2}) \in \mathbb{F}_2^{2k-2}$.

Доказательство. Далее матрицу $Q^{(2k)} \in M_{2k}(\mathbb{F}_2)$, построенную с помощью указанной выше конструкции, будем обозначать через $Q_0^{(2k)}$. Через $H^{(2k)}$ обозначим симплектическую матрицу порядка $2k \times 2k$, у которой все элементы равны нулю, за исключением двух диагоналей, лежащих непосредственно над и под главной диагональю, и эти диагонали имеют вид $1010\ldots100\ldots0$, где число единиц равно $k-1$. Матрицу, соответствующую искомому линейному преобразованию, будем обозначать через $A^{(2k)} = \left(a_{ij}^{(2k)}\right) \in M_{2k}(\mathbb{F}_2)$. Доказательство проведём индукцией по k.

База индукции: $k = 2$. В этом случае имеем

$$B^{(4)} = Q_0^{(4)} \oplus \left(Q_0^{(4)}\right)^{\mathrm{T}} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Заметим, что ранг матрицы $B^{(4)}$ равен 2. Рассмотрим обратимую матрицу

$$A^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Непосредственная проверка показывает, что

$$A^{(4)}B^{(4)}\left(A^{(4)}\right)^{\mathrm{T}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = H^{(4)},$$

сдедовательно (см. теорему Диксона), замена переменных $x = \left(A^{(4)}\right)^{\mathrm{T}} y$ преобразует функцию f к виду

$$y_1 y_2 \oplus \left\langle (1,1,0,0), \left(A^{(4)}\right)^{\mathrm{T}} y \right\rangle = y_1 y_2 \oplus y_1, \;\; y \in \mathbb{F}_2^4.$$

Индукционный шаг: предположим, что для всех $k < k_0$, где $k_0 \geqslant 3$, утверждение верно. Пусть $k = k_0$. В этом случае симплектическая матрица

$$B^{(2k)} = Q_0^{(2k)} \oplus \left(Q_0^{(2k)}\right)^{\mathrm{T}} = \left(\begin{array}{cc|cc} & & 1 & 1 \\ & & & 1 \\ & \mathbf{0}_{k\times k} & & \\ & & & \\ & & 1 & \\ \hline 1 & & & \\ 1 & 1 & & \\ & 1 & & \\ & & & \mathbf{0}_{k\times k} \\ & & & \\ & & & \end{array}\right.$$

имеет ранг $2(k-1)$. Рассмотрим три обратимых матрицы $A_1^{(2k)}$,$A_2^{(2k}$,$A_3^{(2k)} \in M_{2k}(\mathbb{F}_2)$:

$$\left(A_1^{(2k)}\right)_i = \begin{cases} e_i & \text{при } i \in \{1,2,\ldots,k-2\}, \\ e_{k-1} \oplus e_k & \text{при } i = k-1, \\ e_{k+1} \oplus e_{2k} & \text{при } i = k, \\ e_{i+1} & \text{при } i \in \{k+1,k+2,\ldots,2k-2\}, \\ e_k & \text{при } i = 2k-1, \\ e_{2k} & \text{при } i = 2k, \end{cases}$$

$$A_2^{(2k)} = \left(\begin{array}{c|cc} A^{(2k-2)} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0}^{\mathrm{T}} & 1 & 0 \\ \mathbf{0}^{\mathrm{T}} & 0 & 1 \end{array}\right),$$

$$\left(A_3^{(2k)}\right)_i = \begin{cases} e_i & \text{при } i \in \{1,2,\ldots,2k-4\}, \\ e_{2k-1} & \text{при } i = 2k-3, \\ e_{2k} & \text{при } i = 2k-2, \\ e_{2k-3} & \text{при } i = 2k-1, \\ e_{2k-2} & \text{при } i = 2k, \end{cases}$$

где $i = 1,2,\ldots,2k$.

$$A_1^{(2k)} = \begin{array}{c} \\ k \\ \\ \\ \\ \\ \\ 2k \end{array} \begin{array}{c} \begin{array}{cccc|c|cccc} & & & & k & & & & & 2k \end{array} \\ \left(\begin{array}{cccc|c|cccc} 1 & 0 & \ldots & 0 & 0 & & & & & \\ 0 & \ddots & & \vdots & \vdots & & & & & \\ \vdots & & \ddots & 0 & 0 & & \mathbf{0}_{(k-1)\times k} & & & \\ 0 & \ldots & 0 & 1 & 1 & & & & & \\ \hline 0 & \ldots & \ldots & 0 & 0 & 1 & 0 & \ldots & 0 & 1 \\ \hline & & & & \vdots & 0 & \ddots & & \vdots & 0 \\ & & & & \vdots & \vdots & & \ddots & 0 & \vdots \\ & & \mathbf{0}_{k\times(k-1)} & & 0 & 0 & \ldots & 0 & 1 & \vdots \\ & & & & 1 & 0 & \ldots & \ldots & 0 & 0 \\ & & & & 0 & 0 & \ldots & \ldots & 0 & 1 \end{array}\right) \end{array}.$$

Обозначим $Q_j^{(2k)} = A_j^{(2k)} Q_{j-1}^{(2k)} \left(A_j^{(2k)}\right)^{\mathrm{T}} \in M_{2k}(\mathbb{F}_2)$, $j = 1,2,3$. Для данных матриц верно следующее:

$$Q_1^{(2k)} = A_1^{(2k)} Q_0^{(2k)} \left(A_1^{(2k)}\right)^{\mathrm{T}} = \left(\begin{array}{c|cc} Q_0^{(2k-2)} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0}^{\mathrm{T}} & 0 & 1 \\ \mathbf{0}^{\mathrm{T}} & 1 & 0 \end{array}\right),$$

$$Q_2^{(2k)} = A_2^{(2k)} Q_1^{(2k)} \left(A_2^{(2k)}\right)^{\mathrm{T}} = \left(\begin{array}{c|cc} H^{(2k-2)} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0}^{\mathrm{T}} & 0 & 1 \\ \mathbf{0}^{\mathrm{T}} & 1 & 0 \end{array}\right),$$

$$Q_3^{(2k)} = A_3^{(2k)} Q_2^{(2k)} \left(A_3^{(2k)}\right)^{\mathrm{T}} = H^{(2k)}.$$

Таким образом,

$$A_3^{(2k)} A_2^{(2k)} A_1^{(2k)} Q_0^{(2k)} \left(A_3^{(2k)} A_2^{(2k)} A_1^{(2k)}\right)^{\mathrm{T}} = H^{(2k)}.$$

По индукционному предположению выражение

$$\left\langle (1,1,0,0,\ldots,0), \left(A^{(2k-2)}\right)^{\mathrm{T}} y \right\rangle, \;\; y \in \mathbb{F}_2^{2k-2},$$

не зависит от y_{2k-3} и y_{2k-2}. Это эквивалентно тому, что

$$\begin{cases} a_{2k-3,1}^{(2k-2)} = a_{2k-3,2}^{(2k-2)}, \\ a_{2k-2,1}^{(2k-2)} = a_{2k-2,2}^{(2k-2)}. \end{cases}$$

В то же время

$$\left(A_3^{(2k)} A_2^{(2k)}\right) \cdot A_1^{(2k)} = \left(\begin{array}{cc|c} * & * & * \\ \hline a_{2k-3,1}^{(2k-2)} & a_{2k-3,2}^{(2k-2)} & * \\ a_{2k-2,1}^{(2k-2)} & a_{2k-2,2}^{(2k-2)} & * \end{array}\right) \cdot \left(\begin{array}{cc|c} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & * \\ \vdots & \vdots & * \\ 0 & 0 & * \end{array}\right)$$

$$= \left(\begin{array}{cc|c} ** & ** & ** \\ \hline a_{2k-3,1}^{(2k-2)} & a_{2k-3,2}^{(2k-2)} & ** \\ a_{2k-2,1}^{(2k-2)} & a_{2k-2,2}^{(2k-2)} & ** \end{array}\right),$$

следовательно, выражение

$$\left\langle (1,1,0,0,\ldots,0), \left(A_3^{(2k)} A_2^{(2k)} A_1^{(2k)}\right)^{\mathrm{T}} y \right\rangle, \;\; y \in \mathbb{F}_2^{2k},$$

в свою очередь, не зависит от y_{2k-1} и y_{2k}.

Таким образом, на основании теоремы Диксона можно заключить, что искомое преобразование переменных $x = \left(A^{(2k)}\right)^{\mathrm{T}} y$, $x,y \in \mathbb{F}_2^{2k}$, определяется матрицей $\left(A^{(2k)}\right)^{\mathrm{T}}$, где $A^{(2k)} = A_3^{(2k)} A_2^{(2k)} A_1^{(2k)}$. $\square$

5.1.1 Весовой спектр кода Рида – Маллера порядка 2

В этом разделе приведены утверждения, которые будут использоваться для получения основного результата.

Лемма 6. *Пусть булева функция $f \in \mathcal{F}_{2k}$ имеет вид*

$$f(x) = \bigoplus_{i=1}^{r} x_{2i-1}x_{2i} \oplus \varepsilon, \;\; x \in \mathbb{F}_2^{2k},$$

где $\varepsilon \in \mathbb{F}_2$ и $1 \leqslant r \leqslant k$, тогда

$$\mathrm{wt}(f) = \begin{cases} 2^{2k-1} - 2^{2k-r-1}, & \textit{при } \varepsilon = 0, \\ 2^{2k-1} + 2^{2k-r-1}, & \textit{при } \varepsilon = 1. \end{cases}$$

Доказательство. Положим $\varepsilon = 0$. Обозначим через S подмножество векторов $(x_1,x_2,\ldots,x_{2r}) \in \mathbb{F}_2^{2r}$, на которых квадратичная часть функции f равна единице. Ясно, что $\mathrm{wt}(f) = 2^{2k-2r} \cdot |S|$. Пусть через $\lceil a \rceil$ обозначается верхняя целая часть числа $a \in \mathbb{R}$. Запишем выражение для $|S|$:

$$\begin{aligned} |S| &= \sum_{m=1}^{\lceil r/2 \rceil} \binom{r}{2m-1} \sum_{j=0}^{r-m} \binom{r-m}{j} 2^j \\ &= \sum_{m=1}^{\lceil r/2 \rceil} \binom{r}{2m-1} 3^{r-m} \\ &= 3^r \sum_{i=0}^{r} \binom{r}{i} \frac{1-(-1)^i}{2} \left(\frac{1}{3}\right)^i \\ &= \frac{3^r}{2} \left\{ \sum_{t=0}^{r} \binom{r}{t} \left(\frac{1}{3}\right)^t - \sum_{l=0}^{r} \binom{r}{l} \left(-\frac{1}{3}\right)^l \right\} \\ &= \frac{3^r}{2} \left\{ \left(\frac{4}{3}\right)^r - \left(\frac{2}{3}\right)^r \right\} = 2^{2r-1} - 2^{r-1}. \end{aligned}$$

Тогда $\mathrm{wt}(f) = 2^{2k-2r}\,|S| = 2^{2k-2r}\left(2^{2r-1} - 2^{r-1}\right) = 2^{2k-1}\left(1 - 2^{-r}\right)$.

При $\varepsilon = 1$ выражение для веса Хэмминга примет вид:

$$\mathrm{wt}(f) = 2^{2k} - 2^{2k-2r}\,|S| = 2^{2k} - 2^{2k-1}\left(1 - 2^{-r}\right) = 2^{2k-1}\left(1 + 2^{-r}\right).$$

□

Пусть $Q \in M_n(\mathbb{F}_2)$ — верхняя треугольная матрица. Спектр весов смежного класса

$$\{\langle x,Qx\rangle \oplus l(x) : l \in \mathcal{A}_n\}, \tag{5.1}$$

где квадратичная форма $\langle x,Qx\rangle$ фиксирована, описывает следующая

Теорема (о весовом спектре смежного класса кода Рида — Маллера второго порядка) ([63], глава 15)**.** *Если ранг симплектической матрицы $B = Q \oplus Q^{\mathrm{T}}$ равен $2r$, то спектр весов смежного класса (5.1) кода $\mathrm{RM}(2,n)$ по коду $\mathrm{RM}(1,n)$ равен*

$$\left\{2^{n-1},\, 2^{n-1} - 2^{n-r-1},\, 2^{n-1} + 2^{n-r-1}\right\}.$$

5.2 Спектр расстояний Хэмминга

В этом разделе будет найден полный спектр расстояний Хэмминга между самодуальными и анти-самодуальными, а также анти-самодуальными бент-функциями из класса Мэйорана — МакФарланда. Всюду далее полагается, что n — чётное натуральное число.

5.2.1 Самодуальные бент-функции

Утверждение 16. *Пусть $f,g \in \mathrm{SB}^{+}_{\mathcal{M}}(n)$, где $n \geqslant 4$, тогда*

$$\mathrm{dist}(f,g) \in \left\{2^{n-1}, 2^{n-1} \pm 2^{n-r-1}\right\},\ r = 0,1,\ldots,n/2-1,$$

и все приведённые расстояния достижимы.

Доказательство. Положим $n = 2k$, где $k \geqslant 2$ — натуральное число. Рассмотрим произвольную пару самодуальных бент-функций $f,g \in \mathrm{SB}^{+}_{\mathcal{M}}(n)$ (см. раздел 1.3.4):

$$f(x,y) = \langle x, L_f(y) \oplus L_f(b_f)\rangle \oplus \langle b_f, y\rangle \oplus \varepsilon_f,$$
$$g(x,y) = \langle x, L_g(y) \oplus L_g(b_g)\rangle \oplus \langle b_g, y\rangle \oplus \varepsilon_g,$$

где $L_f,L_g \in \mathcal{O}_n$, $b_f,b_g \in \mathbb{F}_2^k$, $\varepsilon_f,\varepsilon_g \in \mathbb{F}_2$, и векторы $L_f b_f$ и $L_g b_g$ имеют чётный вес Хэмминга.

Далее будет рассмотрена булева функция G, равная сумме функций f и g по модулю 2. Очевидно, $\mathrm{wt}(G) = \mathrm{dist}(f,g)$. На первом этапе доказательства будет получено представление данной функции в виде

$$G(x,y) = G(v) = \langle Qv,v\rangle \oplus \langle L,v\rangle \oplus \varepsilon,\ \ v \in \mathbb{F}_2^{2k}$$

для последующего применения теоремы о спектре весов кода Рида — Маллера второго порядка. На втором этапе для доказательства достижимости соответствующих весов Хэмминга будут приведены конкретные конструкции Q, l и ε.

ЭТАП I.

Рассмотрим следующую булеву функцию от $2k$ переменных:

$$\begin{aligned} G(x,y) &= f(x,y) \oplus g(x,y) \\ &= \langle x,L_f(y) \oplus L_f(b_f)\rangle \oplus \langle b_f,y\rangle \oplus \varepsilon_f \oplus \langle x,L_g(y) \oplus L_g(b_g)\rangle \oplus \langle b_g,y\rangle \oplus \varepsilon_g. \end{aligned}$$

Имеем

$$\mathrm{dist}(f,g) = \mathrm{wt}(f \oplus g) = \mathrm{wt}(G). \tag{5.2}$$

Для удобства будем использовать следующие обозначения:

$$\begin{aligned} v &= (x,y), \\ A &= L_f \oplus L_g, \\ c &= L_f b_f \oplus L_g b_g, \\ b &= b_f \oplus b_g, \\ l &= (c,b), \\ \varepsilon &= \varepsilon_f \oplus \varepsilon_g, \end{aligned}$$

тогда

$$G(x,y) = \langle x,Ay\rangle \oplus \langle c,x\rangle \oplus \langle b,y\rangle \oplus \varepsilon = \langle Qv,v\rangle \oplus \langle l,v\rangle \oplus \varepsilon = G(v),$$

где верхняя треугольная матрица Q имеет вид

$$Q = \begin{pmatrix} \mathbf{0}_{k\times k} & A \\ \mathbf{0}_{k\times k} & \mathbf{0}_{k\times k} \end{pmatrix}.$$

Пусть ранг матрицы A, совпадающий с рангом матрицы Q, равен r, тогда, очевидно, ранг матрицы $B = Q \oplus Q^{\mathrm{T}}$, имеющей вид

$$B = \begin{pmatrix} \mathbf{0}_{k\times k} & A \\ A^{\mathrm{T}} & \mathbf{0}_{k\times k} \end{pmatrix},$$

будет равен $2r$. В этом случае, согласно теореме о весовом спектре смежного класса кода Рида — Маллера второго порядка, справедливо

$$\mathrm{wt}(G) \in \left\{2^{2k-1},\, 2^{2k-1} - 2^{2k-r-1},\, 2^{2k-1} + 2^{2k-r-1}\right\}. \tag{5.3}$$

ЭТАП II.

Рассматривая различные значения ранга r матрицы A, изучим вопрос достижимости весов, фигурирующих в (5.3). Данный ранг в силу леммы 4 ограничен сверху числом $k-1$.

Рассмотрим наименьшее значение ранга: $\underline{r = 0}$.

Вес 2^{2k}. Пусть $L_f = L_g = I_k$, $b_f = b_g = (1,1,0,0,\ldots,0) \in \mathbb{F}_2^k$, $\varepsilon_f = 0$, $\varepsilon_g = 1$. Тогда $L = \mathbf{0}$ и справедливо: $G \equiv 1$, то есть $\mathrm{wt}(G) = 2^{2k}$;

Вес 2^{2k-1}. Пусть $b_f \neq b_g$, например, $b_f = (1,1,0,0,\ldots,0) \in \mathbb{F}_2^k$, $b_g = \mathbf{0}$, $L_f = L_g = I_k$, $\varepsilon = 0$, тогда $G(v) = \langle l,v\rangle$ — линейная функция, причём $l \neq \mathbf{0}$. Вес Хэмминга такой линейной функции равен 2^{2k-1};

Вес 0. Данный вес достигается при $L_f = L_g$, $b_f = b_g$, $\varepsilon_f = \varepsilon_g$.

Для значений ранга $\underline{r = 1,2,\ldots,k-2}$, имеем:

Пусть $b_f = b_g = \mathbf{0}$, тогда $l = \mathbf{0}$, то есть у булевой функции G нулевая линейная часть, а матрица A имеет ненулевой ранг. Согласно теореме Диксона квадратичная часть булевой функции G может быть приведена к виду

$$q(z) = \bigoplus_{i=1}^{r} z_{2i-1}z_{2i} \oplus \varepsilon, \quad z \in \mathbb{F}_2^{2k},$$

где r — ранг матрицы Q, совпадающий с рангом матрицы A. Используя лемму 6, заключаем, что вес Хэмминга функции G равен $2^{2k-1} - (-1)^{\varepsilon}2^{2k-r-1}$. Надлежащим образом подберём ε, положим $L_f = I_k$, и пусть строки матрицы L_g имеют следующий вид:

$$(L_g)_i = \begin{cases} e_{i+1}, & \text{при } i \in \{1,2,\ldots,r\}, \\ e_1, & \text{при } i = r+1, \\ e_i, & \text{при } i \in \{r+2,r+3,\ldots,k\}, \end{cases}$$

где $i = 1,2,\ldots,k$;

Вес $2^{2k-1} - 2^{2k-r-1}$. Возьмём L_f,L_g,b_f,b_g, указанные выше, $\varepsilon = 0$;

Вес $2^{2k-1} + 2^{2k-r-1}$. Возьмём L_f,L_g,b_f,b_g, указанные выше, $\varepsilon = 1$.

Рассмотрим наибольшее значение ранга: $\underline{r = k-1}$.

Повторяя рассуждения из предыдущего пункта, взяв те же самые L_f,b_f,b_g и выбрав в качестве L_g матрицу, строка i которой есть

$$(L_g)_i = \begin{cases} e_{i+1}, & \text{при } i \in \{1,2,\ldots,k-1\}, \\ e_1, & \text{при } i = k, \end{cases}$$

где $i = 1,2,\ldots,k$, получим функцию G, для которой справедливо: $\mathrm{wt}(G) = 2^{2k-1} - (-1)^{\varepsilon}2^{2k-1-(k-1)}$;

Вес $2^{2k-1} - 2^{2k-1-(k-1)}$. Возьмём L_f,L_g,b_f,b_g, указанные выше, $\varepsilon = 0$;

Вес $2^{2k-1} + 2^{2k-(k-1)-1}$. Возьмём L_f,L_g,b_f,b_g, указанные выше, $\varepsilon = 1$.

Таким образом, все возможные при $r = 0,1,\ldots,k-1$ значения веса $\mathrm{wt}(G)$ достижимы. С учётом (5.2) имеем:

$$\mathrm{dist}(f,g) \in \left\{2^{n-1},2^{n-1} \pm 2^{n-r-1}\right\},\ r = 0,1,\ldots,n/2-1,$$

В силу того, что $k = n/2$, получаем требуемое. □

5.2.2 Анти-самодуальные бент-функции

Утверждение 17. *Пусть $f,g \in \mathrm{SB}^{-}_{\mathcal{M}}(n)$, где $n \geqslant 4$, тогда*

$$\mathrm{dist}(f,g) \in \left\{2^{n-1},2^{n-1} \pm 2^{n-r-1}\right\},\ r = 0,1,\ldots,n/2-1,$$

и все приведённые расстояния достижимы.

Доказательство. Положим $n = 2k$, где $k \geqslant 2$ — натуральное число. Рассмотрим произвольную пару анти-самодуальных бент-функций $f,g \in \mathrm{SB}^{-}_{\mathcal{M}}(n)$ (см. раздел 1.3.4):

$$f(x,y) = \langle x,L_f(y) \oplus L_f(b_f)\rangle \oplus \langle b_f,y\rangle \oplus \varepsilon_f,$$
$$g(x,y) = \langle x,L_g(y) \oplus L_g(b_g)\rangle \oplus \langle b_g,y\rangle \oplus \varepsilon_g,$$

где $L_f,L_g \in \mathcal{O}_n$, $b_f,b_g \in \mathbb{F}_2^k$, $\varepsilon_f,\varepsilon_g \in \mathbb{F}_2$, и векторы $L_f b_f$ и $L_g b_g$ имеют нечётный вес Хэмминга.

Дальнейшее доказательство будет проводится по той же схеме, что и доказательство утверждения 16.

ЭТАП I.

Повторяя рассуждения, приведённые на первом этапе доказательства утверждения 16, можно показать, что

$$G(x,y) = f(x,y) \oplus g(x,y) = \langle Qv,v\rangle \oplus \langle L,v\rangle \oplus \varepsilon = G(v),$$

где все обозначения имеют тот же смысл, В частности, $A = L_f \oplus L_g$, а матрицы Q,B имеют вид

$$Q = \begin{pmatrix} \mathbf{0}_{k\times k} & A \\ \mathbf{0}_{k\times k} & \mathbf{0}_{k\times k} \end{pmatrix}, \qquad B = \begin{pmatrix} \mathbf{0}_{k\times k} & A \\ A^{\mathrm{T}} & \mathbf{0}_{k\times k} \end{pmatrix}.$$

Пусть, как и прежде, ранг матрицы A, совпадающий с рангом матрицы Q, равен r, тогда ранг матрицы B будет равен $2r$. В этом случае, согласно теореме о весовом спектре смежного класса кода Рида — Маллера второго порядка, справедливо

$$\mathrm{wt}(G) \in \left\{2^{2k-1},\, 2^{2k-1} - 2^{2k-r-1},\, 2^{2k-1} + 2^{2k-r-1}\right\}. \tag{5.4}$$

ЭТАП II.

Как это было сделано ранее — при доказательстве утверждения 16 — рассмотрим различные значения ранга r матрицы A и изучим вопрос достижимости весов, фигурирующих в (5.4). Данный ранг в силу леммы 4 ограничен сверху числом $k-1$.

Рассмотрим наименьшее значение ранга: $\underline{r = 0}$.

Вес 2^{2k}. Пусть $L_f = L_g = I_k$, $b_f = b_g = (1,0,0,\ldots,0) \in \mathbb{F}_2^k$, $\varepsilon_f = 0$, $\varepsilon_g = 1$. Тогда $l = \mathbf{0}$ и справедливо: $G \equiv 1$, то есть $\mathrm{wt}(G) = 2^{2k}$;

Вес 2^{2k-1}. Пусть $b_f \neq b_g$, например, $b_f = (1,0,0,\ldots,0) \in \mathbb{F}_2^k$, $b_g = \mathbf{0}$, $L_f = L_g = I_k$, $\varepsilon = 0$, тогда $G(v) = \langle l,v\rangle$ — линейная функция, причём $l \neq \mathbf{0}$. Вес Хэмминга данной линейной функции равен 2^{2k-1};

Вес 0. Данный вес достигается при $L_f = L_g$, $b_f = b_g$, $\varepsilon_f = \varepsilon_g$.

Для значений ранга $\underline{r = 1,2,\ldots,k-2}$, получаем следующее.

Пусть $b_f = b_g = e_k$, тогда $L = \mathbf{0}$, то есть у булевой функции G нулевая линейная часть, а матрица A имеет ненулевой ранг. Ранее было показано, что в

этом случае $\mathrm{wt}(G) = 2^{2k-1} - (-1)^{\varepsilon}2^{2k-r-1}$. Положим $L_f = I_k$ и L_g — матрица, строки которой имеют следующий вид:

$$(L_g)_i = \begin{cases} e_{i+1}, & \text{при } i \in \{1,2,\ldots,r\}, \\ e_1, & \text{при } i = r+1, \\ e_i, & \text{при } i \in \{r+2, r+3, \ldots, k\}, \end{cases}$$

где $i = 1,2,\ldots,k$;

Вес $2^{2k-1} - 2^{2k-r-1}$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 0$;

Вес $2^{2k-1} + 2^{2k-r-1}$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 1$.

Рассмотрим наибольшее значение ранга: $\underline{r = k-1}$.

Пусть $L_f = I_k$, и выберем в качестве L_g матрицу:

$$(L_g)_i = \begin{cases} e_{i+1}, & \text{при } i \in \{1,2,\ldots,k-1\}, \\ e_1, & \text{при } i = k, \end{cases}$$

где $i = 1,2,\ldots,k$. Положим $b_f = b_g = e_2$, тогда $l = (1,1,0,0,\ldots,0) \in \mathbb{F}_2^{2k}$. Используя лемму 5 и теорему Диксона, заключаем, что вес Хэмминга функции G равен $\mathrm{wt}(G) = 2^{2k-1} - (-1)^{\varepsilon_1}2^{2k-1-(k-1)}$, где (см. [63], глава 15):

$$\varepsilon_1 = \varepsilon \oplus \bigoplus_{i=1}^{k-1} l_{2i-1}l_{2i} = \varepsilon \oplus 1;$$

Вес $2^{2k-1} - 2^{2k-1-(k-1)}$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 1$;

Вес $2^{2k-1} + 2^{2k-1-(k-1)}$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 0$;

Отметим, что в случае нечётного k можно обойтись без использования леммы 5, взяв $b_f = b_g = (1,1,\ldots,1) \in \mathbb{F}_2^k$, для которых $L = \mathbf{0}$;

Таким образом, все возможные при $r = 0,1,\ldots,k-1$ значения веса $\mathrm{wt}(G)$ достижимы. С учётом (5.2) имеем:

$$\mathrm{dist}(f,g) \in \left\{2^{n-1}, 2^{n-1} \pm 2^{n-r-1}\right\},\ r = 0,1,\ldots,n/2-1,$$

В силу того, что $k = n/2$, получаем требуемое. □

5.2.3 Основной результат

Объединим полученные ранее результаты касательно спектров расстояний между функциями из множеств самодуальных и анти-самодуальных бент-функций из класса Мэйорана — МакФарланда.

Теорема 7. *Пусть* $f,g \in \mathrm{SB}^{+}_{\mathcal{M}}(n) \cup \mathrm{SB}^{-}_{\mathcal{M}}(n)$, *тогда если*

- $f \in \mathrm{SB}^{+}_{\mathcal{M}}(n)$, *а* $g \in \mathrm{SB}^{-}_{\mathcal{M}}(n)$, *то* $\mathrm{dist}(f,g) = 2^{n-1}$;
- $f,g \in \mathrm{SB}^{+}_{\mathcal{M}}(n)$ *или* $f,g \in \mathrm{SB}^{-}_{\mathcal{M}}(n)$, *то при* $n = 2$ *имеем* $\mathrm{dist}(f,g) = 2^n$, *а при* $n \geqslant 4$ *справедливо*

$$\mathrm{dist}(f,g) \in \left\{2^{n-1}, 2^{n-1} \pm 2^{n-r-1}\right\}, \; r = 0,1,\ldots,n/2-1,$$

и все приведённые расстояния достижимы.

Доказательство. Случай, когда функции f,g являются самодуальными (анти-самодуальными), следует из утверждения 16 (17). Значение расстояния для случай, когда функции f,g принадлежат разным множествам, следует из того факта, что расстояние Хэмминга между самодуальной и анти-самодуальной бент-функциями от n переменных равно 2^{n-1}, см. раздел 1.3.1. При $n = 2$ только две бент-функции из класса Мэйорана — МакФарланда являются самодуальными: $f_1(x_1,x_2) = x_1x_2$ и $g_1(x_1,x_2) = x_1x_2 \oplus 1$, а функции $f_2(x_1,x_2) = x_1x_2 \oplus x_1 \oplus x_2$ и $g_2(x_1,x_2) = x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ — анти-самодуальными. Очевидно, что

$$\begin{aligned}\mathrm{dist}\,(f_1,g_1) &= \mathrm{dist}\,(f_2,g_2) = 2^n,\\ \mathrm{dist}\,(f_1,g_2) &= \mathrm{dist}\,(f_2,g_1) = 2^{n-1}.\end{aligned}$$

□

Следствие 8. *Пусть* $n \geqslant 4$, *и* $f,g \in \mathrm{SB}^{+}_{\mathcal{M}}(n)$ — *различные самодуальные бент-функции. Справедливо*

$$\mathrm{dist}(f,g) \geqslant 2^{n-2},$$

и данная нижняя оценка является точной.

Доказательство. Из теоремы 7 следует, что минимальное из достижимых расстояний есть $2^{n-1} - 2^{n-1-1} = 2^{n-2}$. □

Стоит отметить, что данная оценка также следует из того факта, что кодовое расстояние кода Рида — Маллера $\mathrm{RM}(2,m)$ равно 2^{m-2}. В силу этого факта следствие 8 можно доказать, заметив лишь, что для различных (анти-)самодуальных бент-функций f и g из класса Мэйорана — МакФарланда выполняется $\deg(f \oplus g) \leqslant 2$, а также непосредственно указав соответствующую пару (анти-)самодуальных бент-функций, которые находятся на расстоянии 2^{n-2} друг от друга.

Таким образом, в настоящий главе получены все расстояния Хэмминга, достижимые между функциями из известного класса квадратичных самодуальных бент-функций — самодуальными бент-функциям, построенными с помощью конструкции Мэйорана — МакФарланда. Решение общей задачи, связанной с нахождением спектра расстояний Хэмминга в рамках всего множества квадратичных самодуальных бент-функций, может использовать известную классификацию данных функций, приведённую в разделе 1.3.3.

Заключение

Приведем список основных результатов данной работы.

1. Доказано, что множества характеристических векторов самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным числам $2^{n/2}$ и $(-2^{n/2})$, соответственно.
2. Описаны группы автоморфизмов множеств самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных.
3. Установлено, что группа автоморфизмов множества самодуальных бент-функций совпадает с множеством изометричных отображений всех булевых функций от $n \geqslant 4$ переменных в себя, сохраняющих расстояние Хэмминга между каждой бент-функцией и дуальной к ней.
4. Доказано, что множество булевых функций, максимально удалённых от множества самодуальных (анти-самодуальных) бент-функций от $n \geqslant 4$ переменных, совпадает с множеством анти-самодуальных (самодуальных) бент-функций от n переменных. Таким образом, доказана метрическая регулярность множества (анти-)самодуальных бент-функций от n переменных.
5. Найден полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

Список литературы

1. С. В. Августинович, Е. В. Горкунов. Об автоморфизмах линейных кодов над простым полем // Сиб. электрон. матем. изв. — 2017. — Т. 14. — С. 210–217.
2. Г. П. Агибалов. Избранные теоремы начального курса криптографии. — Томск : НТЛ, 2005. — 116 с.
3. М. М. Глухов. О приближении дискретных функций линейными функциями // Матем. вопр. криптогр. — 2016. — Т. 7, № 4. — С. 29–50.
4. Н. А. Коломеец. Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. опер. — 2012. — Т. 19, № 1. — С. 41–58.
5. Н. А. Коломеец. Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикл. дискрет. матем. — 2014. — 3(25). — С. 28–39.
6. Н. А. Коломеец, А. В. Павлов. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикл. дискрет. матем. — 2009. — 4(6). — С. 5–20.
7. А. С. Кузьмин, А. А. Нечаев, В. А. Шишкин. Бент- и гипербент-функции над конечным полем // Тр. по дискр. матем. — 2007. — Т. 10. — С. 97–122.
8. А. С. Кузьмин, В. Т. Марков, А. А. Нечаев, В. Шишкин, А. Б. Шишков. Бент-функции и гипербент-функции над полем из 2^l элементов // Пробл. передачи информации. — 2008. — Т. 44, № 1. — С. 15–37.
9. О. А. Логачев, А. А. Сальников, В. В. Ященко. Бент-функции на конечной абелевой группе // Дискрет. матем. — 1997. — Т. 9, № 4. — С. 3–20.
10. О. А. Логачев, А. А. Сальников, С. В. Смышляев, В. В. Ященко. Булевы функции в теории кодирования и криптологии. — ЛЕНАНД, 2015. — 576 с.
11. А. А. Марков О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. — МЦНМО, 2003. — С. 70–93.

12. А. К. Облаухов. О метрическом дополнении подпространств булева куба // Дискретн. анализ и исслед. опер. — 2016. — Т. 23, № 3. — С. 93—106.

13. И. А. Панкратова. Булевы функции в криптографии: Учебное пособие. — ТГУ, 2014. — 88 с.

14. В. Н. Потапов. Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информ. — 2012. — Т. 48, № 1. — С. 54—63.

15. В. Н. Сачков. Введение в комбинаторные методы дискретной математики. — 2-е изд. — М. : МЦНМО, 2004. — 424 с.

16. Ю. В. Таранников. Комбинаторные свойства дискретных структур и приложения к криптологии. — МЦНМО, 2011. — 152 с.

17. Н. Н. Токарева. Группа автоморфизмов множества бент-функций // Дискрет. матем. — 2010. — Т. 22, № 4. — С. 34—42.

18. Н. Н. Токарева. О разложении дуальной бент-функции в сумму двух бент-функций // Прикл. дискрет. матем. — 2014. — 4(26). — С. 59—61.

19. В. М. Фомичёв. Дискретная математика и криптология. Курс лекций. — М. : ДИАЛОГ-МИФИ, 2003. — 400 с.

20. А. В. Черёмушкин. Методы аффинной и линейной классификации двоичных функций // Тр. по дискр. матем. — 2001. — Т. 4. — С. 273—314.

21. L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, S. Mesnager. Further Results on Niho Bent Functions // IEEE Trans. Inform. Theory. — 2012. — Vol. 58, no. 11. — P. 6979—6985.

22. A. Canteaut, P. Charpin. Decomposing bent functions // IEEE Trans. Inform. Theory. — 2003. — Vol. 49, no. 8. — P. 2004—2019.

23. A. Canteaut, M. Daum, H. Dobertin, G. Leander. Finding nonnormal bent functions // Discrete Appl. Math. — 2006. — Vol. 154, no. 2. — P. 202—218.

24. C. Carlet. Two New Classes of Bent Functions // Advances in Cryptology — EUROCRYPT '93. — 1994. — P. 77—101. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 765).

25. C. Carlet. On Cryptographic Propagation Criteria for Boolean Functions // Information and Computation. — 1999. — Vol. 151, no. 1/2. — P. 32—56.

26. C. Carlet Boolean functions for cryptography and error correcting codes // Boolean Methods and Models in Mathematics, Computer Science, and Engineering / ed. by Y. Crama, P. L. Hammer. — Cambridge Univ. Press, 2010. — P. 257—397.

27. C. Carlet Vectorial Boolean functions for cryptography // Boolean Methods and Models in Mathematics, Computer Science, and Engineering / ed. by Y. Crama, P. L. Hammer. — Cambridge Univ. Press, 2010. — P. 398—472.

28. C. Carlet. Open Questions on Nonlinearity and on APN Functions // Arithmetic of Finite Fields. — 2015. — P. 83—107. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 9061).

29. C. Carlet, P. Guillot. A new representation of Boolean functions // Proceedings of AAECC'13. — 1999. — P. 94—103. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 1719).

30. C. Carlet, S. Mesnager. Four decades of research on bent functions // Des. Codes Cryptogr. — 2016. — Vol. 78, no. 1. — P. 5—50.

31. C. Carlet. Boolean Functions for Cryptography and Coding Theory. — Cambridge University Press, 2020. — 620 p.

32. C. Carlet, T. Helleseth, A. Kholosha, S. Mesnager. On the dual of bent functions with 2^r Niho exponents // 2011 IEEE International Symposium on Information Theory (ISIT). — 2011. — P. 703—707.

33. C. Carlet, L. E. Danielsen, M. G. Parker, P. Solé. Self-dual bent functions // Int. J. Inform. Coding Theory. — 2010. — Vol. 1. — P. 384—399.

34. A. Çeşmelioğlu, W. Meidl, A. Pott. On the dual of (non)-weakly regular bent functions and self-dual bent functions // Adv. Math. Commun. — 2013. — Vol. 7, no. 4. — P. 425—440.

35. A. Çeşmelioğlu, W. Meidl, A. Pott. Vectorial bent functions and their duals // Linear Algebra and its Appl. — 2018. — Vol. 548. — P. 305—320.

36. A. Çeşmelioğlu, W. Meidl, A. Pott A survey on bent functions and their duals // Combinatorics and Finite Fields. Difference Sets, Polynomials, Pseudorandomness and Applications. — De Gruyter, 2019. — Chap. 3. P. 39—56.

37. T. Chunming, Z. Zhou, Y. Qi, X. Zhang, C. Fan, T. Helleseth. Generic Construction of Bent Functions and Bent Idempotents With Any Possible Algebraic Degrees // J. Pure Appl. Algebra. — 2017. — Vol. 63, no. 10. — P. 6149—6157.

38. J.-J. Climent, F. J. Garcia, V. Requena. A construction of bent functions of $n + 2$ variables from a bent function of n variables and its cyclic shifts // Algebra. — 2014. — Vol. 2014. — Article ID 701298.

39. R. S. Coulter, S. Mesnager. Bent Functions From Involutions Over $\mathbb{F}_{2^n}$ // IEEE Trans. Inform. Theory. — 2018. — Vol. 64, no. 4. — P. 2979—2986.

40. T. W. Cusick, P. Stănică. Cryptographic Boolean Functions and Applications. — 2nd ed. — Acad. Press, 2017. — 288 p.

41. L. E. Danielsen, M. G. Parker, P. Solé. The Rayleigh quotient of bent functions // Cryptography and Coding. — 2009. — P. 418—432. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 5921).

42. U. Dempwolff. Automorphisms and equivalence of bent functions and of difference sets in elementary Abelian 2-groups // Commun. Algebra. — 2006. — Vol. 34, no. 3. — P. 1077—1131.

43. L. E. Dickson. Linear groups with an exposition of the Galois field theory. — B.G. Teubner, 1901.

44. J. F. Dillon. Elementary Hadamard difference sets : PhD thesis. — College Park : University of Maryland, 1974.

45. J. Dillon A survey of bent functions // NSA Technical Journal. — 1972. — P. 191—215.

46. T. Feulner, L. Sok, P. Solé, A. Wassermann. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. — 2013. — Vol. 68, no. 1. — P. 395—406.

47. R. L. Graham, N. J. A. Sloane. On the Covering Radius of Codes // IEEE Trans. Inform. Theory. — 1985. — Vol. IT—31, no. 3. — P. 385—401.

48. X.-D. Hou. On the norm and covering radius of the first-order Reed — Muller codes // IEEE Trans. Inform. Theory. — 1997. — Vol. 43, no. 3. — P. 1025—1027.

49. X.-D. Hou. New constructions of bent functions // J. Combin. Inform. System Sci. — 2000. — Vol. 25. — P. 173—189.

50. X.-D. Hou. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. — 2012. — Vol. 63, no. 2. — P. 183—198.

51. X.-D. Hou. Classification of p-ary self dual quadratic bent functions, p odd // J. Algebra. — 2013. — Vol. 391. — P. 62—81.

52. X.-D. Hou, P. Langevin. Results on bent functions // J. Comb. Theory Ser. A. — 1997. — Vol. 80. — P. 232—246.

53. J. Y. Hyun, H. Lee, Y. Lee. MacWilliams duality and Gleason-type theorem on self-dual bent functions // Des. Codes Cryptogr. — 2012. — Vol. 63, no. 3. — P. 295—304.

54. J. Y. Hyun, H. Lee, Y. Lee. Boolean functions with MacWilliams duality // Des. Codes Cryptogr. — 2014. — Vol. 72, no. 2. — P. 273—287.

55. G. J. Janusz. Parametrization of self-dual codes by orthogonal matrices // Finite Fields Appl. — 2007. — Vol. 13, no. 3. — P. 450—491.

56. N. Kolomeec. The graph of minimal distances of bent functions and its properties // Des. Codes Cryptogr. — 2017. — Vol. 85, no. 3. — P. 1—16.

57. N. A. Kolomeec. On a property of quadratic Boolean functions // Матем. вопр. криптогр. — 2014. — Т. 5, № 2. — С. 79—85.

58. P. Langevin, G. Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880 // Des. Codes Cryptogr. — 2011. — Vol. 59, no. 1—3. — P. 193—205.

59. P. Langevin, G. Leander, G. McGuire. Kasami bent function are not equivalent to their duals // Finite Fields and Applications: Eighth International Conference on Finite Fields and Applications. Contemp. Math. Vol. 461. — 2008. — P. 187—197.

60. P. Langevin, G. Leander. Monomial bent functions and Stickelberger's theorem // Finite Fields Appl. — 2008. — Vol. 14, no. 3. — P. 727—742.

61. N. G. Leander. Monomial bent functions // IEEE Trans. Inform. Theory. — 2006. — Vol. 52, no. 2. — P. 738—743.

62. G. Luo, X. Cao, S. Mesnager. Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. — 2019. — Vol. 11, no. 6. — P. 1261—1273.

63. F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correctiong Codes. — North-Holland Publishing Company, 1977. — 782 p.

64. J. MacWilliams. Orthogonal matrices over finite fields // The American Mathematical Monthly. — 1969. — Vol. 76, no. 2. — P. 152—164.

65. M. Matsui. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology — EUROCRYPT '93. — 1994. — P. 386—397. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 765).

66. R. L. McFarland. A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. — 1973. — Vol. 15, no. 1. — P. 1—10.

67. W. Meier, E. Pasalic, C. Carlet. Algebraic Attacks and Decomposition of Boolean Functions // Advances in Cryptology — EUROCRYPT 2004. — 2004. — P. 474—491. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 3027).

68. S. Mesnager. Several New Infinite Families of Bent Functions and Their Duals // IEEE Trans. Inform. Theory. — 2014. — Vol. 60, no. 7. — P. 4397—4407.

69. S. Mesnager. Bent functions: Fundamentals and results. — Springer International Publishing, 2016. — 544 p.

70. D. E. Muller. Application of Boolean algebra to switching circuit design and to error detection // IRE Transactions on Electronic Computation. — 1954. — Vol. EC—3. — P. 6—12.

71. A. Oblaukhov. A lower bound on the size of the largest metrically regular subset of the Boolean cube // Cryptogr. Commun. — 2019. — Vol. 11, no. 4. — P. 777—791.

72. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle. Propagation characteristics of Boolean functions // Advances in Cryptology — EUROCRYPT '90. — 1991. — P. 161—173. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 473).

73. I. S. Reed. A class of multiple-error-correcting codes and their decoding scheme // IRE Trans. Inform. Theory. — 1954. — Vol. IT—4, no. 3. — P. 38—49.

74. J. Rifà, V. A. Zinoviev. On binary quadratic symmetric bent and almost bent functions. — arXiv:1211.5257v3.

75. O. S. Rothaus. On “bent” functions // J. Combin. Theory, Ser. A. — 1976. — Vol. 20, no. 3. — P. 300—305.

76. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. — 1984. — No. 5. — P. 776—780.

77. L. Sok, M. Shi, P. Solé. Classification and Construction of quaternary self--dual bent functions // Cryptogr. Commun. — 2018. — Vol. 10, no. 2. — P. 277—289.

78. L. Sok, P. Solé. On Formally Self-dual Boolean Functions in 2,4 and 6 Variables // Arithmetic of Finite Fields. — 2012. — P. 81—91. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 7369).

79. P. Stănică, T. Sasao, J. T. Butler. Distance duality on some classes of Boolean functions // J. Comb. Math. Comb. Comput. — 2018. — Vol. 107. — P. 181—198.

80. N. Tokareva. On the number of bent functions from iterative constructions: lower bounds // Adv. Math. Commun. — 2011. — Vol. 5, no. 4. — P. 609—621.

81. N. Tokareva. Duality between bent functions and affine functions // Discrete Math. — 2012. — Vol. 312, no. 3. — P. 666—670.

82. N. Tokareva. Bent Functions: Results and Applications to Cryptography. — Acad. Press, 2015. — 220 p.

83. N. N. Tokareva. On decomposition of a Boolean function into sum of bent functions // Сиб. электрон. матем. изв. — 2014. — Т. 11. — С. 745—751.

84. B. Xu. Dual bent functions on finite groups and C-algebras // J. Pure Appl. Algebra. — 2016. — Vol. 220, no. 3. — P. 1055—1073.

85. R. Yarlagadda, J. Hershey. A note on the eigenvectors of Hadamard matrices of order 2^n // Linear Algebra Appl. — 1982. — Vol. 45. — P. 43—53.

Публикации автора по теме диссертации

86. А. В. Куценко. Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана-МакФарланда // Дискретный анализ и исследование операций. — 2018. — Т. 25, № 1. — С. 98—119. — Перевод: *Kutsenko, A. V.* The Hamming distance spectrum between self-dual Maiorana–McFarland bent functions / A. V. Kutsenko // Journal of Applied and Industrial Mathematics. 2018. Vol. 12, no. 1. P. 112–125.

87. A. Kutsenko. Metrical properties of self-dual bent functions // Designs, Codes and Cryptography. — 2020. — Vol. 88, no. 1. — P. 201—222.

88. A. Kutsenko. The group of automorphisms of the set of self-dual bent functions // Cryptography and Communications. — 2020. — Vol. 12, no. 5. — P. 881—898.

89. A. Kutsenko, N. Tokareva. Metrical properties of the set of bent functions in view of duality // Прикладная дискретная математика. — 2020. — № 49. — С. 18—34.

90. А. В. Куценко. О самодуальных булевых бент-функциях // Прикладная дискретная математика. Приложение. — 2015. — № 8. — С. 34—35.

91. А. В. Куценко. О расстоянии Хэмминга между самодуальными булевыми бент-функциями // Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова. — 2016. — С. 386—388.

92. А. В. Куценко. О множестве расстояний Хэмминга между самодуальными бент-функциями // Прикладная дискретная математика. Приложение. — 2016. — № 9. — С. 29—30.

93. А. В. Куценко. О свойствах изометричных отображений множества бент-функций // Тезисы докладов Международной конференции «Математика в современном мире», посвящённой 60-летию Института математики им. С. Л. Соболева. — 2017. — С. 439.

94. А. В. Куценко. О некоторых свойствах известных изометричных отображений множества бент-функций // Прикладная дискретная математика. Приложение. — 2017. — № 10. — С. 43—44.

95. А. В. Куценко. О некоторых свойствах самодуальных бент-функций // Прикладная дискретная математика. Приложение. — 2018. — № 11. — С. 44—46.

96. А. В. Куценко. Изометричные отображения множества всех булевых функций в себя, сохраняющие самодуальность и отношение Рэлея // Прикладная дискретная математика. Приложение. — 2019. — № 12. — С. 55—58.

97. A. Kutsenko. Isometric Mappings of the Set of all Boolean Functions into Itself which Preserve Self-duality and the Rayleigh Quotient // Proceedings of the 4th workshop Boolean Functions and their Applications (BFA 2019), Florence, Italy, June 16-21, 2019. — 2019.

98. А. В. Куценко. О метрических свойствах множества самодуальных бент-функций // Прикладная дискретная математика. Приложение. — 2020. — № 13. — С. 21—27.

99. A. Kutsenko. On metrical properties of self-dual generalized bent functions // Proceedings of the 5th workshop Boolean Functions and their Applications (BFA 2020), Loen, Norway, September 15-17, 2020. — 2020.

100. A. Kutsenko. On constructions and properties of self-dual generalized bent functions // Proceedings of the 11th International Conference on Sequences and Their Applications (SETA 2020), Saint-Petersburg, September 22-25, 2020. — 2020.