

УДК 519.7

DOI 10.17223/20710410/69/2

**ОПИСАНИЕ НЕКОТОРЫХ КЛАССОВ ИЗОМЕТРИЧНЫХ
ОТОБРАЖЕНИЙ, СОХРАНЯЮЩИХ САМОДУАЛЬНОСТЬ
ОБОБЩЁННОЙ БЕНТ-ФУНКЦИИ¹**

А. В. Куценко

*Новосибирский государственный университет, г. Новосибирск, Россия***E-mail:** alexandrkutsenko@bk.ru

Обобщённая булева функция, обладающая равномерным спектром Уолша — Адамара, называется обобщённой бент-функцией. Обобщённая бент-функция, совпадающая со своей дуальной бент-функцией, называется самодуальной. В работе исследуются изометричные отображения множества всех обобщённых булевых функций в себя, оставляющие класс самодуальных обобщённых бент-функций от n переменных на месте. Предложено новое отображение, сохраняющее самодуальность обобщённой бент-функции. Вводится понятие действия унитарного оператора на множестве обобщённых булевых функций от n переменных, представленных своими характеристическими векторами. В рамках рассматриваемого класса унитарных операторов описаны все отображения, сохраняющие самодуальность. Исследуется обобщённый вид изометричного отображения, соответствующего комплексному сопряжению характеристического вектора.

Ключевые слова: *обобщённая бент-функция, самодуальная бент-функция, изометричное отображение.*

**CHARACTERIZATION OF SOME CLASSES
OF ISOMETRIC MAPPINGS THAT PRESERVE SELF-DUALITY
OF GENERALIZED BENT FUNCTION**

A. V. Kutsenko

Novosibirsk State University, Novosibirsk, Russia

A generalized Boolean function with flat Walsh — Hadamard spectrum is called generalized bent (gbent) function. Gbent function that coincides with its dual bent function is called self-dual. In this paper, we study isometric mappings of the set of all generalized Boolean functions into itself that preserve self-duality. A new mapping that preserves the self-duality of a gbent function is proposed. We introduce the concept of the action of an unitary operator on the set of generalized Boolean functions in n variables, represented by their characteristic vectors. Within the considered class of unitary operators, all mappings that preserve self-duality are described. A generalized form of isometric mapping corresponding to the complex conjugation of the characteristic vector is investigated.

Keywords: *generalized Boolean function, self-dual bent function, isometric mapping.*

¹Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2025-349.

Введение

Бент-функции образуют один из самых известных классов булевых функций, он нашёл широкое применение в различных областях алгебры и дискретной математики. Согласно определению, бент-функцией называется булева функция от чётного числа переменных, обладающая равномерным спектром Уолша — Адамара. Равномерность спектра Уолша — Адамара открывает ряд приложений в криптографии, обработке сигналов, а также теории кодирования. Термин «бент-функция» был предложен О. Ротхаусом в 70-х годах XX в. [1], но, несмотря на долгую историю изучения данного класса функций и наличие большого количества работ, связанных с ними, по-прежнему существует много открытых проблем, в ряде случаев имеющих пересечение с другими комбинаторными объектами. Известен ряд обобщений булевых бент-функций, рассматриваемых как с теоретической, так и с практической точек зрения. Более подробную информацию о бент-функциях, их свойствах, конструкциях и связанных открытых проблемах можно найти в [2].

В настоящей работе рассматриваются функции вида $\mathbb{F}_2^n \rightarrow \mathbb{Z}_q$, где $\mathbb{F}_2^n$ — пространство двоичных векторов с n координатами; q — натуральное число. Данное обобщение булевых функций нашло приложение в теории обработки сигналов и теории кодирования [3]. В рамках данного обобщения бент-функции — это обобщённые булевы функции от n переменных с равномерным спектром Уолша — Адамара, то есть функции, обладающие тем свойством, что абсолютное значение каждого коэффициента Уолша — Адамара равно $2^{n/2}$. Такие функции называются *обобщёнными бент-функциями* [3]. Свойства и конструкции обобщённых бент-функций исследуются во многих работах, например в [4–6]. Стоит отметить, что обобщённая бент-функция не обязательно зависит от чётного числа переменных. Для класса обобщённых бент-функций вводится понятие регулярной обобщённой бент-функции, то есть такой функции, для которой определена дуальная к ней обобщённая бент-функция. Известно, что при $q = 2^k$, $k \geq 2$, все обобщённые бент-функции являются регулярными как для чётного, так и для нечётного n , за исключением единственного случая, когда $k = 2$, а n — нечётное число [7]. Регулярная обобщённая бент-функция, совпадающая со своей дуальной, называется самодуальной. Класс самодуальных булевых бент-функций получил большое внимание, ему посвящено много работ, в частности [8–13]. Один из открытых вопросов о самодуальных обобщённых бент-функциях — описание изометричных отображений, сохраняющих самодуальность. Данный вопрос тесно связан с задачей исследования группы автоморфизмов этого класса функций, что подразумевает изучение его структурных и метрических свойств. Дополнительно ставятся вопросы выбора метрики и исследования группы автоморфизмов в различных метриках. Подробную информацию о других известных обобщениях бент-функций, а также их свойствах и приложениях можно найти в [2, 14].

Настоящая работа посвящена изучению изометричных отображений множества всех обобщённых булевых функций от n переменных в себя, сохраняющих самодуальность. Рассматриваются отображения вида

$$f(x) \rightarrow \gamma \cdot f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n,$$

где $\gamma \in \{1, q-1\}$; π — подстановка на множестве $\mathbb{F}_2^n$; g — обобщённая булева функция от n переменных. Работа имеет следующую структуру. В п. 1 даются необходимые определения и обозначения. В п. 2 приводится обобщение некоторых свойств множества характеристических векторов самодуальных бент-функций. В п. 3 вводится понятие действия линейного оператора $\mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ на множестве обобщённых булевых

функций от n переменных, описываются все унитарные операторы, отображающие множество всех обобщённых булевых функций от n переменных в себя. Каждый такой оператор определяет некоторое изометричное отображение в метрике Хэмминга и метрике Ли. В п. 4 предложено новое отображение, сохраняющее самодуальность обобщённой бент-функции. В рамках рассматриваемого класса унитарных операторов (то есть при $\gamma = 1$) описаны все операторы, сохраняющие самодуальность обобщённой бент-функции. В п. 5 исследуется изометричное отображение, основанное на комплексном сопряжении характеристического вектора, а также его обобщение ($\gamma = q - 1$).

1. Используемые определения и обозначения

Весом Хэмминга $\text{wt}_H(x)$ вектора $x \in \mathbb{F}_2^n$ называется число координат x , отличных от нуля. Для $x, y \in \mathbb{F}_2^n$ через $\langle x, y \rangle$ обозначим выражение $\bigoplus_{i=1}^n x_i y_i$, где $\oplus$ — сложение по модулю 2. *Обобщённой булевой функцией* от n переменных называется произвольное отображение из пространства $\mathbb{F}_2^n$ в кольцо $\mathbb{Z}_q$ [15]. В случае $q = 2$ функция называется *булевой функцией*. *Расстоянием Хэмминга* $\text{dist}_H(f, g)$ между обобщёнными булевыми функциями f, g от n переменных называется число векторов из пространства $\mathbb{F}_2^n$, на которых функции принимают разные значения. *Весом Ли* элемента $x \in \mathbb{Z}_q$ называется число $\text{wt}_L(x) = \min\{x, q - x\}$. *Весом Ли* обобщённой булевой функции от n переменных называется сумма весов Ли всех её значений:

$$\text{wt}_L(f) = \sum_{x \in \mathbb{F}_2^n} \text{wt}_L(f(x)).$$

Расстояние Ли $\text{dist}_L(f, g)$ между обобщёнными булевыми функциями f, g от n переменных есть число $\text{wt}_L(f - g)$. В булевом случае $q = 2$ веса, а также расстояния Хэмминга и Ли совпадают.

Пусть $\omega = e^{2\pi i/q}$ — примитивный корень степени q из 1. *Характеристическим вектором* обобщённой булевой функции f от n переменных называется вектор

$$F = \omega^f = (\omega^{f_0}, \omega^{f_1}, \dots, \omega^{f_{2^n-1}})$$

с 2^n координатами, где $(f_0, f_1, \dots, f_{2^n-1})$ — вектор значений функции f . *Преобразованием Уолша — Адамара* обобщённой булевой функции f от n переменных называется комплекснозначная функция

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

Обобщённая булева функция f от n переменных называется *обобщённой бент-функцией*, если

$$|H_f(y)| = 2^{n/2}$$

для всех $y \in \mathbb{F}_2^n$ [3] (см. также препринт 2006 г.). Если существует обобщённая булева функция $\tilde{f}$ от n переменных, такая, что $H_f(y) = \omega^{\tilde{f}(y)} 2^{n/2}$ для всех $y \in \mathbb{F}_2^n$, то f называется *регулярной*, а $\tilde{f}$ — её *дуальной*. Отметим, что дуальная функция $\tilde{f}$ также является обобщённой бент-функцией; в булевом случае $q = 2$ все бент-функции регулярны.

Регулярная обобщённая бент-функция f называется *самодуальной*, если $f = \tilde{f}$, и *антисамодуальной*, если $f = \tilde{f} + q/2$. Таким образом, в настоящей работе при рассмотрении антисамодуальных обобщённых бент-функций считается, что q — чётное число. Соответствующие множества функций будем обозначать через $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

2. Характеристические векторы самодуальных обобщённых бент-функций

Приведём обобщение некоторых известных фактов о характеристических векторах самодуальных булевых бент-функций [8, 11, 12].

Ненулевой вектор $v \in \mathbb{C}^n$ называется *собственным вектором* $(n \times n)$ -матрицы A , соответствующим *собственному числу* $\lambda \in \mathbb{C}$, если $Av = \lambda v$. Линейная оболочка собственных векторов, соответствующих собственному числу λ , называется *собственным подпространством*, соответствующим собственному числу λ . *Ядром* линейного оператора $\varphi : \mathbb{C}^n \rightarrow \mathbb{C}^n$ называется множество

$$\text{Ker}(\varphi) = \{x \in \mathbb{C}^n : \varphi(x) = \mathbf{0} \in \mathbb{C}^n\},$$

где $\mathbf{0}$ — нулевой элемент пространства $\mathbb{C}^n$.

Принимая во внимание тот факт, что в фиксированном базисе каждый линейный оператор $\mathbb{C}^n \rightarrow \mathbb{C}^n$ характеризуется некоторой $(n \times n)$ -матрицей, приведённые понятия можно рассматривать как по отношению к линейным операторам, так и по отношению к квадратным матрицам соответствующего порядка, что далее используется в зависимости от контекста.

Матрицей Сильвестра — Адамара (матрицей Адамара типа Сильвестра) порядка n называется $(2^n \times 2^n)$ -матрица

$$H_n = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n},$$

где $\otimes$ — операция кронекерова произведения. Как матрица Адамара, данная матрица обладает следующим свойством:

$$H_n H_n^T = 2^n I_{2^n},$$

где I_{2^n} — единичная матрица порядка 2^n .

Обозначим $\mathcal{H}_n = 2^{-n/2} H_n$, данная матрица является симметричной и ортогональной. В силу того, что строки матрицы H_n соответствуют характеристическим векторам всех линейных булевых функций от n переменных, взятых в лексикографическом порядке, регулярную обобщённую бент-функцию от n переменных можно определить как функцию, чей характеристический вектор F удовлетворяет условию $\mathcal{H}_n F \in \{\pm 1\}^{2^n}$. Таким образом, характеристический вектор самодуальной обобщённой бент-функции является собственным вектором матрицы $\mathcal{H}_n$, соответствующим собственному числу $+1$. Аналогично характеристический вектор антисамодуальной обобщённой бент-функции является собственным вектором матрицы $\mathcal{H}_n$, соответствующим собственному числу -1 .

В работе [8] рассматривается ортогональное разложение пространства $\mathbb{R}^{2^n}$ по собственным подпространствам матрицы $\mathcal{H}_n$:

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

Здесь символом $\oplus$ обозначается прямая сумма подпространств. Нетрудно видеть, что аналогичное разложение можно получить и для комплекснозначного пространства:

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

Известно, что

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

где $\dim(V)$ есть размерность подпространства $V \subseteq \mathbb{R}^{2^n}$. Как отмечено ранее, матрица $\mathcal{H}_n$ является симметричной, следовательно, подпространства $\text{Ker}(\mathcal{H}_n + I_{2^n})$ и $\text{Ker}(\mathcal{H}_n - I_{2^n})$ являются взаимно ортогональными.

В работе [11] доказано, что при $n \geq 4$ множества характеристических векторов (анти)самодуальных булевых бент-функций от n переменных порождают собственные подпространства матрицы $\mathcal{H}_n$, то есть имеют размерность 2^{n-1} . Данный результат можно обобщить следующим образом:

Утверждение 1. Пусть $n \geq 4$, тогда множества характеристических векторов (анти)самодуальных обобщённых булевых бент-функций от n переменных порождают собственные подпространства матрицы $\mathcal{H}_n$, то есть имеют размерность 2^{n-1} .

Доказательство. Достаточно заметить, что в силу чётности q справедливо $(-1) = \omega^{q/2} \in \{\omega, \omega^2, \dots, \omega^{q-1}\}$. ■

В случае $n = 2$ и $q = 2$ есть только две самодуальные обобщённые бент-функции: x_1x_2 и $x_1x_2 \oplus 1$, имеющие характеристические векторы $(1, 1, 1, -1)$ и $(-1, -1, -1, 1)$ соответственно. Данные векторы, очевидно, линейно зависимы в $\mathbb{R}^4$. Рассматривая случай произвольного чётного q , получаем систему

$$\frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix} = \begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix}$$

с переменными $d_1, d_2, d_3, d_4 \in \mathbb{Z}_q$. Все её решения имеют вид

$$(\omega^d, \omega^d, \omega^d, \omega^{d+q/2}) = \omega^d (1, 1, 1, -1) \in \mathbb{C}^4,$$

где $d \in \mathbb{Z}_q$.

Случай антисамодуальных бент-функций рассматривается аналогично. Таким образом, характеристические векторы из множеств $\mathcal{SB}_2^{q,\pm}$ также линейно зависимы в $\mathbb{C}^4$.

3. Изометричные отображения и унитарные операторы

Пусть на множестве всех обобщённых булевых функций определена метрика ρ . Взаимно однозначное отображение φ множества обобщённых булевых функций от n переменных в себя называется *изометричным* относительно метрики ρ , если для любой пары обобщённых булевых функций f, g от n переменных выполняется соотношение

$$\rho(\varphi(f), \varphi(g)) = \rho(f, g).$$

Группой автоморфизмов множества всех обобщённых булевых функций от n переменных относительно метрики ρ называется группа изометричных отображений множества всех обобщённых булевых функций от n переменных в себя.

В булевом случае, как правило, в качестве метрики ρ рассматривается расстояние Хэмминга. В случае обобщённых булевых функций далее рассматриваются две метрики — расстояние Хэмминга и расстояние Ли.

В данном пункте приведено определение действия линейного оператора $\mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ на множестве обобщённых булевых функций от n переменных; охарактеризована группа всех унитарных операторов, отображающих множество всех обобщённых булевых функций от n переменных в себя; показано, что каждый оператор из этой группы соответствует некоторому изометричному отображению. Для двоичного случая отмечается связь с известными результатами применительно к группе автоморфизмов множества всех булевых функций от n переменных.

3.1. Линейные операторы и обобщённые булевы функции

Всюду далее подразумевается использование стандартного базиса пространства $\mathbb{C}^{2^n}$, который состоит из векторов $e_i \in \mathbb{C}^{2^n}$, $i = 1, \dots, 2^n$, где e_i имеет 1 на позиции i , а остальные координаты равны нулю.

Пусть $\varphi : \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ — линейный оператор с матрицей M_φ в стандартном базисе пространства $\mathbb{C}^{2^n}$. Будем говорить, что φ отображает обобщённую булеву функцию f от n переменных с характеристическим вектором F в обобщённую булеву функцию f' от n переменных с характеристическим вектором F' , если $F' = M_\varphi F$, т.е. действие отображения определено на характеристических векторах длины 2^n следующим образом: $F' = M_\varphi F = \varphi(F)$.

Линейный оператор φ называется *унитарным*, если $\varphi\varphi^* = \varphi^*\varphi = \text{id}$, где φ^* — эрмитово сопряжённый к φ оператор. Матрица отображения φ в этом случае является унитарной. Через $\mathcal{U}_n^q$ обозначим группу всех унитарных операторов $\mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$, которые отображают множество всех обобщённых булевых функций от n переменных в себя.

Следующий результат полностью характеризует группу $\mathcal{U}_n^q$. Напомним, что квадратная матрица над полем $\mathbb{F}$ называется *обобщённой перестановочной* или *мономимальной*, если в каждой её строке, а также в каждом столбце присутствует ровно один ненулевой элемент поля $\mathbb{F}$.

Теорема 1. Существует взаимно однозначное соответствие между элементами группы $\mathcal{U}_n^q$ и обобщёнными перестановочными матрицами порядка 2^n с ненулевыми элементами из множества $\{1, \omega, \omega^2, \dots, \omega^{q-1}\}$.

Доказательство. Нетрудно видеть, что операторы, которым соответствуют обобщённые перестановочные матрицы с элементами указанного вида, отображают множество обобщённых булевых функций от n переменных в себя. Более того, каждый такой оператор является унитарным.

Обратно, положим $\varphi \in \mathcal{U}_n^q$ и пусть $U = (u_{ij})$ — его матрица в стандартном базисе. Обозначим через $v_0 \in \mathbb{C}^{2^n}$ вектор из всех единиц, а через $v_i \in \mathbb{C}^{2^n}$, $i = 1, \dots, 2^n$, — вектор с 1 на позиции i , все остальные координаты которого равны (-1) . Пусть $v_{ij} \in \mathbb{C}^{2^n}$, $i, j = 1, \dots, 2^n$, $i \neq j$, — вектор с единицами на позициях с номерами i и j , в то время как оставшиеся равны (-1) .

Зафиксируем некоторые $i, j, k \in \{1, \dots, 2^n\}$, $i < j$. Обозначим $(Uv_0)_k = \omega^{d_0}$, $(Uv_i)_k = \omega^{d_i}$, $(Uv_j)_k = \omega^{d_j}$ и $(Uv_{ij})_k = \omega^{d_{ij}}$ для некоторых $d_0, d_i, d_j, d_{ij} \in \mathbb{Z}_q$. Их суммы равны

$$\begin{aligned} (Uv_0)_k + (Uv_i)_k &= 2u_{ki} = \omega^{d_0} + \omega^{d_i}, \\ (Uv_0)_k + (Uv_j)_k &= 2u_{kj} = \omega^{d_0} + \omega^{d_j}, \\ (Uv_0)_k + (Uv_{ij})_k &= 2(u_{ki} + u_{kj}) = \omega^{d_0} + \omega^{d_{ij}}. \end{aligned}$$

После перегруппировки получаем

$$u_{ki} = (\omega^{d_0} + \omega^{d_i})/2, \quad u_{kj} = (\omega^{d_0} + \omega^{d_j})/2, \quad u_{ki} + u_{kj} = (\omega^{d_0} + \omega^{d_{ij}})/2,$$

то есть

$$\omega^{d_0} + \omega^{d_i} + \omega^{d_0} + \omega^{d_j} = \omega^{d_0} + \omega^{d_{ij}},$$

или, после сокращения подобных,

$$\omega^{d_0} + \omega^{d_i} + \omega^{d_j} = \omega^{d_{ij}}.$$

Это возможно лишь в случае, когда число $\omega^{d_{ij}}$ совпадает с одним из чисел $\omega^{d_0}, \omega^{d_i}, \omega^{d_j}$, в то время как два оставшихся отличаются друг от друга лишь знаком, что всегда допустимо, так как q — чётное число.

Рассмотрим два случая:

С л у ч а й 1. Пусть $\omega^{d_{ij}} = \omega^{d_0}$ и $\omega^{d_i} + \omega^{d_j} = 0$, тогда k -я строка матрицы U есть

$$U_k = (u_{k,1}, \dots, u_{k,i-1}, (\omega^{d_0} - \omega^{d_j})/2, u_{k,i+1}, \dots, u_{k,j-1}, (\omega^{d_0} + \omega^{d_j})/2, u_{k,j+1}, \dots, u_{k,2^n}).$$

В этом случае справедливо

$$\begin{aligned} |u_{ki}|^2 + |u_{kj}|^2 &= \frac{1}{4} (|\omega^{d_0} - \omega^{d_j}|^2 + |\omega^{d_0} + \omega^{d_j}|^2) = \\ &= \frac{1}{4} [(\omega^{d_0} - \omega^{d_j})(\omega^{-d_0} - \omega^{-d_j}) + (\omega^{d_0} + \omega^{d_j})(\omega^{-d_0} + \omega^{-d_j})] = \\ &= \frac{1}{4} (2 \cdot \omega^{d_0} \omega^{-d_0} + 2 \cdot \omega^{d_j} \omega^{-d_j}) = \frac{1}{4} (2 + 2) = 1 \end{aligned}$$

и в силу того, что U — унитарная матрица, имеем $\|U_k\|^2 = 1$ для всех $k \in \{1, \dots, 2^n\}$. Следовательно, все координаты U_k , кроме, может быть, $u_{ki} = (\omega^{d_0} - \omega^{d_j})/2$, $u_{kj} = (\omega^{d_0} + \omega^{d_j})/2$, должны быть равны нулю.

С л у ч а й 2. Без ограничения общности предположим, что $\omega^{d_{ij}} = \omega^{d_i}$ и $\omega^{d_0} + \omega^{d_j} = 0$, тогда $u_{kj} = 0$.

Таким образом, для любых различных индексов $i, j \in \{1, \dots, 2^n\}$ возможны две ситуации: либо по крайней мере один из элементов u_{ki}, u_{kj} k -й строки матрицы U нулевой, либо в данной строке не более двух ненулевых элементов, при этом их форма описана в случае 1.

Анализ случаев. Если для каждой строки имеет место только случай 2, то матрица U является обобщённо перестановочной, так как в каждой её строке присутствует ровно один ненулевой элемент. Предположим, что одна из строк матрицы U , например с номером k , имеет вид, описанный в случае 1. Заметим, что в матрице U найдётся ещё как минимум одна строка такого же вида.

Рассмотрим (характеристический) вектор $F \in \mathbb{C}^{2^n}$, чьи координаты с номерами $\ell = 1, \dots, 2^n$ имеют вид

$$F_\ell = \begin{cases} \omega^{r_1}, & \ell = i, \\ \omega^{r_2}, & \ell = j, \\ 1, & \text{иначе,} \end{cases}$$

где $r_1, r_2 \in \mathbb{Z}_q$, при этом $r_1 < r_2$ и $r_2 - r_1 \neq q/2$. Обозначив $\Delta r = r_2 - r_1$, запишем

$$(UF)_k = u_{ki}\omega^{r_1} + u_{kj}\omega^{r_2} = \omega^{r_1} \left(\frac{\omega^{d_0} - \omega^{d_j}}{2} + \frac{\omega^{d_0} + \omega^{d_j}}{2} \omega^{\Delta r} \right).$$

В силу того, что UF — характеристический вектор обобщённой булевой функции от n переменных, для некоторого $s \in \mathbb{Z}_q$ имеем $(UF)_k = \omega^{r_1+s}$. Тогда справедливо

$$\frac{\omega^{d_0} - \omega^{d_j}}{2} + \frac{\omega^{d_0} + \omega^{d_j}}{2} \omega^{\Delta r} = \omega^s.$$

Используем известные тригонометрические соотношения: пусть $\alpha, \beta \in \mathbb{R}$, тогда

$$\begin{aligned}\cos \alpha + \cos \beta &= 2 \cos ((\alpha + \beta)/2) \cos ((\alpha - \beta)/2), \\ \cos \alpha - \cos \beta &= -2 \sin ((\alpha + \beta)/2) \sin ((\alpha - \beta)/2), \\ \sin \alpha \pm \sin \beta &= 2 \sin ((\alpha \pm \beta)/2) \cos ((\alpha \mp \beta)/2), \\ \sin (\alpha \pm \beta) &= \sin \alpha \cos \beta \pm \cos \alpha \sin \beta, \\ \sin 2\alpha &= 2 \cos \alpha \sin \alpha.\end{aligned}$$

Рассмотрим удвоенную вещественную часть числа ω^s :

$$\begin{aligned}2\operatorname{Re}(\omega^s) &= \cos(2\pi d_0/q) - \cos(2\pi d_j/q) + \cos(2\pi(d_0 + \Delta r)/q) + \cos(2\pi(d_j + \Delta r)/q) = \\ &= 2 \cos(\pi(2d_0 + \Delta r)/q) \cos(\pi\Delta r/q) - 2 \sin(\pi(2d_j + \Delta r)/q) \sin(\pi\Delta r/q),\end{aligned}$$

и удвоенную мнимую часть:

$$\begin{aligned}2\operatorname{Im}(\omega^s) &= \sin(2\pi d_0/q) - \sin(2\pi d_j/q) + \sin(2\pi(d_0 + \Delta r)/q) + \sin(2\pi(d_j + \Delta r)/q) = \\ &= 2 \sin(\pi(2d_0 + \Delta r)/q) \cos(\pi\Delta r/q) + \sin(\pi\Delta r/q) \cos(\pi(2d_j + \Delta r)/q).\end{aligned}$$

Обозначим $\alpha = \pi\Delta r/q$, $\beta = \pi(2d_0 + \Delta r)/q$ и $\gamma = \pi(2d_j + \Delta r)/q$. В силу того, что число ω^s является корнем из единицы, его абсолютное значение равно 1, следовательно,

$$\begin{aligned}\operatorname{Re}^2(\omega^s) + \operatorname{Im}^2(\omega^s) &= \cos^2 \alpha \cos^2 \beta - 2 \cos \alpha \sin \alpha \cos \beta \sin \gamma + \sin^2 \alpha \sin^2 \gamma + \\ &\quad + \cos^2 \alpha \sin^2 \beta + 2 \cos \alpha \sin \alpha \sin \beta \cos \gamma + \sin^2 \alpha \cos^2 \gamma = \\ &= \cos^2 \alpha (\cos^2 \beta + \sin^2 \beta) + \sin^2 \alpha (\cos^2 \gamma + \sin^2 \gamma) + 2 \cos \alpha \sin \alpha (\sin \beta \cos \gamma - \cos \beta \sin \gamma) = \\ &= 1 + \sin(2\alpha) \sin(\beta - \gamma) = 1,\end{aligned}$$

то есть $\sin(2\alpha) \sin(\beta - \gamma) = 0$. Если первый множитель равен нулю, то

$$2\alpha = 2\pi\Delta r/q = \pi m, \quad m \in \mathbb{Z}.$$

Тогда $\Delta r = mq/2$, но в силу того, что $\Delta r \in \{1, \dots, q-1\}$, это может иметь место только при $\Delta r = q/2$, что противоречит выбору r_1, r_2 . Если второй множитель нулевой, то

$$\beta - \gamma = 2\pi(d_0 - d_j)/q = \pi m', \quad m' \in \mathbb{Z},$$

и снова $d_0 = d_j$ или $|d_0 - d_j| = q/2$, так как $|d_0 - d_j| \in \{0, 1, \dots, q-1\}$. Но тогда либо $\omega^{d_0} - \omega^{d_j} = 0$, либо $\omega^{d_0} + \omega^{d_j} = 0$, то есть в строке с номером k есть в точности один ненулевой элемент. ■

Следствие 1. Порядок группы $\mathcal{U}_n^q$ равен $|\mathcal{U}_n^q| = (2^n)! \cdot q^{2^n}$.

3.2. Связь с теоремой Маркова для двоичного случая

Из теоремы А. А. Маркова (1956) следует, что общий вид группы автоморфизмов множества всех булевых функций от n переменных в себя есть

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x), \quad x \in \mathbb{F}_2^n,$$

где π — подстановка на пространстве $\mathbb{F}_2^n$ и g — булева функция от n переменных [16]. Группа таких отображений в литературе также именуется как *группа Джевонса* (см., например, [17]).

Теорема 1 может быть переформулирована следующим образом:

Теорема 2. Действие любого элемента группы $\mathcal{U}_n^q$ на множестве всех обобщённых булевых функций от n переменных единственным образом представимо в виде

$$f(x) \longrightarrow f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n,$$

где π — подстановка на пространстве $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных.

Следуя работе [12], будем обозначать такой оператор через $\varphi_{\pi,g} \in \mathcal{U}_n^q$. Для двоичного случая немедленно получаем

Следствие 2. При $q = 2$ группа $\mathcal{U}_n^q$ изоморфна группе автоморфизмов множества булевых функций от n переменных.

Таким образом, группа $\mathcal{U}_n^q$ есть естественное обобщение отображений из группы автоморфизмов множества всех булевых функций от n переменных на случай обобщённых булевых функций. С точки зрения метрических свойств интересно следующее

Утверждение 2. Каждый элемент $\mathcal{U}_n^q$ сохраняет расстояние Хэмминга и расстояние Ли между обобщёнными булевыми функциями от n переменных.

Таким образом, все элементы группы $\mathcal{U}_n^q$ являются изометричными отображениями относительно упомянутых метрик.

3.3. Матричное представление

По теореме 1 при фиксированном (стандартном) базисе существует взаимно однозначное соответствие между элементами группы $\mathcal{U}_n^q$ и множеством всех обобщённо перестановочных матриц размера $2^n \times 2^n$ с ненулевыми элементами из множества $\{1, \omega^1, \omega^2, \dots, \omega^{q-1}\}$. Действительно, рассмотрим произвольное отображение $\varphi_{\pi,g} \in \mathcal{U}_n^q$. Пусть оно отображает обобщённую булеву функцию f от n переменных с характеристическим вектором

$$F = (\omega^{f(\mathbf{v}_0)}, \omega^{f(\mathbf{v}_1)}, \dots, \omega^{f(\mathbf{v}_{2^n-1})}) \in \mathbb{C}^{2^n}$$

в функцию $f' \in \mathcal{GF}_n^q$ с характеристическим вектором

$$F' = (\omega^{f'(\mathbf{v}_0)}, \omega^{f'(\mathbf{v}_1)}, \dots, \omega^{f'(\mathbf{v}_{2^n-1})}) \in \mathbb{C}^{2^n},$$

то есть $F' = UF$, где U — матрица, соответствующая отображению $\varphi_{\pi,g}$:

$$(i+1) \begin{pmatrix} & \pi(\mathbf{v}_i) & \\ & 0 & \\ & \vdots & \\ & 0 & \\ 0 & \dots & 0 & \omega^{g(\mathbf{v}_i)} & 0 & \dots & 0 \\ & 0 & \\ & \vdots & \\ & 0 & \end{pmatrix}.$$

Здесь $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{2^n-1}$ — все векторы пространства $\mathbb{F}_2^n$ в лексикографическом порядке; в строке с номером $(i+1) \in \{1, 2, \dots, 2^n\}$ ненулевой элемент находится в столбце с номером $(j+1)$, где j — число с двоичной записью $\pi(\mathbf{v}_i)$. Тогда i -я координата вектора $F' = UF$ равна

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

или, другими словами,

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

4. Унитарные операторы и (анти)самодуальность обобщённой бент-функции

Обозначим, следуя [18], ортогональную группу порядка n над полем $\mathbb{F}_2$ через

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

где L^T — результат транспонирования L ; I_n — единичная матрица порядка n над полем $\mathbb{F}_2$.

Задача исследования различных типов эквивалентности и нахождения всех соответствующих классов эквивалентности является более сложной для случая обобщённых булевых и обобщённых бент-функций. Различные типы эквивалентности для функций вида $\mathbb{F}_p^n \rightarrow \mathbb{Z}_{p^k}$, где p — простое, такие, как расширенная аффинная эквивалентность (ЕА), а также более общая ССЗ-эквивалентность, изучаются в работе [6]. Для самодуальных обобщённых бент-функций случай $q = 4$ рассматривается в [5].

4.1. Унитарные операторы, сохраняющие (анти)самодуальность обобщённой бент-функции

В работе [10] (см. также [8]) показано, что отображения вида

$$f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c, x \rangle \oplus d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$, сохраняют самодуальность булевой бент-функции. Группа, состоящая из всех таких отображений, названа *расширенной ортогональной* группой и обозначена через $\overline{\mathcal{O}}_n$. Известно, что она является подгруппой группы $\text{GL}(n+2, \mathbb{F}_2)$ [10].

В [12] доказано, что группы автоморфизмов множеств самодуальных и антисамодуальных бент-функций от n переменных в точности равны расширенной ортогональной группе.

Применительно к обобщённым булевым функциям известно несколько примеров отображений, оставляющих классы обобщённых бент-функций, самодуальных обобщённых бент-функций на месте. Расширенное аффинное преобразование обобщённой бент-функции f от n переменных, имеющее вид

$$f(x) \longrightarrow f(Ax \oplus b) + \lambda \langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $A \in \text{GL}(n, \mathbb{F}_2)$; $b, c \in \mathbb{F}_2^n$; $d \in \mathbb{Z}_q$; $\lambda \in \{0, q/2\}$, переводит данную функцию в обобщённую бент-функцию [4]. Случай $q = 4$ самодуальных бент-функций рассмотрен в [5], где показано, что отображение $f \rightarrow (-f) \bmod 4$, а также частный случай аффинного отображения вида

$$f(x) \longrightarrow f(Lx) + d, \quad x \in \mathbb{F}_2^n, \tag{1}$$

где $L \in \mathcal{O}_n$, $d \in \mathbb{Z}_4$, сохраняют самодуальность обобщённой бент-функции.

В настоящей работе предлагается новое расширенное аффинное преобразование, сохраняющее самодуальность обобщённой бент-функции.

Утверждение 3. Отображения множества всех обобщённых булевых функций от n переменных в себя, имеющие вид

$$f(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2} \langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$, сохраняют (анти)самодуальность обобщённой бент-функции от n переменных.

Доказательство. Пусть $f \in \mathcal{SB}_n^{q,+} \cup \mathcal{SB}_n^{q,-}$, то есть $\tilde{f} = f + \frac{q}{2}\varepsilon$ для некоторого $\varepsilon \in \mathbb{F}_2$. Рассмотрим функцию $g(x) = f(L(x \oplus c)) + \frac{q}{2}\langle c, x \rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$. Её коэффициенты Уолша — Адамара имеют вид

$$\begin{aligned} H_g(y) &= \sum_{x \in \mathbb{F}_2^n} \omega^{g(x)} (-1)^{\langle x, y \rangle} = \sum_{x \in \mathbb{F}_2^n} \omega^{f(L(x \oplus c)) + (q/2)\langle c, x \rangle + d + (q/2)\langle x, y \rangle} = \omega^d \sum_{x \in \mathbb{F}_2^n} \omega^{(q/2)\langle x, y \oplus c \rangle + f(L(x \oplus c))} = \\ &= \omega^d \sum_{z \in \mathbb{F}_2^n} \omega^{(q/2)\langle L^{-1}z \oplus c, y \oplus c \rangle + f(z)} = \omega^{d + (q/2)\langle c, y \rangle + (q/2)\langle c, c \rangle} \sum_{z \in \mathbb{F}_2^n} \omega^{(q/2)\langle z, L(y \oplus c) \rangle + f(z)} = \\ &= \omega^{d + (q/2)\langle c, y \rangle} 2^{n/2} \omega^{\tilde{f}(L(y \oplus c))} = 2^{n/2} \omega^{f(L(y \oplus c)) + (q/2)\langle c, y \rangle + d + (q/2)\varepsilon} = 2^{n/2} \omega^{g(y) + (q/2)\varepsilon} = 2^{n/2} \omega^{\tilde{g}(y)}, \end{aligned}$$

следовательно, $\tilde{g}(y) = g(y) + (q/2)\varepsilon$ для каждого $y \in \mathbb{F}_2^n$. ■

Далее охарактеризованы все операторы из множества $\mathcal{U}_n^q$, сохраняющие самодуальность обобщённой бент-функции, и установлена их связь с отображениями из утверждения 3.

Сначала установим взаимосвязь между сохранением отображением самодуальности и антисамодуальности, а также матрицей, соответствующей такому изометричному отображению:

Утверждение 4. Для оператора $\varphi_{\pi, g} \in \mathcal{U}_n^q$ с матрицей U следующие условия эквивалентны:

- 1) $\varphi_{\pi, g}$ сохраняет самодуальность;
- 2) $\varphi_{\pi, g}$ сохраняет антисамодуальность;
- 3) $U\mathcal{H}_n = \mathcal{H}_n U$.

Доказательство. Достаточно заметить, что по утверждению 1 при $n \geq 4$ существует подмножество $\{f_i\}_{i=1}^{2^{n-1}} \subseteq \mathcal{SB}_n^{q,+}$ с линейно независимыми характеристическими векторами $\{F_i\}_{i=1}^{2^{n-1}} \subseteq \text{Ker}(\mathcal{H}_n - I_{2^n})$ и подмножество $\{g_i\}_{i=1}^{2^{n-1}} \subseteq \mathcal{SB}_n^{q,-}$ с линейно независимыми характеристическими векторами $\{G_i\}_{i=1}^{2^{n-1}} \subseteq \text{Ker}(\mathcal{H}_n + I_{2^n})$.

Дальнейшие рассуждения повторяют доказательство [12, Proposition 2]. ■

В работе [12] описаны все изометричные отображения множества всех булевых функций от n переменных в себя, сохраняющие самодуальность, а именно: доказано, что изометричные отображения вида $f(x) \rightarrow f(\pi(x)) \oplus g(x)$ сохраняют самодуальность, если и только если

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

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

Следующее утверждение характеризует все операторы из множества $\mathcal{U}_n^q$, сохраняющие (анти)самодуальность обобщённой бент-функции.

Теорема 3. Оператор $\varphi_{\pi, g} \in \mathcal{U}_n^q$ сохраняет (анти)самодуальность, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2}\langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$.

Доказательство. Достаточность следует из утверждения 3.

Пусть U — матрица оператора $\varphi_{\pi, g} \in \mathcal{U}_n^q$, сохраняющего (анти)самодуальность, то есть $\varphi_{\pi, g}$ имеет вид $f(x) \rightarrow f(\pi(x)) + g(x)$, $x \in \mathbb{F}_2^n$, где π — подстановка на $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных.

Рассмотрим соотношение $UH_n = H_nU$, получаемое из утверждения 4. Как отмечено ранее, все строки матрицы Сильвестра — Адамара есть в точности характеристические векторы линейных булевых функций от n переменных. Тогда

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

Выпишем в явном виде строку с номером i и столбец с номером j . Для $i = 1, 2, \dots, 2^n$ i -я строка матрицы U является вектором с единственным ненулевым элементом $\omega^{g(\mathbf{v}_{i-1})}$ в столбце с номером j , где $(j-1)$ — число с двоичной записью $\pi(\mathbf{v}_{i-1})$. Таким образом, i -я строка имеет вид

$$(0 \quad \dots \quad 0 \quad \overset{j}{\omega^{g(\mathbf{v}_{i-1})}} \quad 0 \quad \dots \quad 0).$$

Для $j = 1, 2, \dots, 2^n$ j -й столбец матрицы U есть вектор с единственным ненулевым элементом $\omega^{g(\pi^{-1}(\mathbf{v}_{j-1}))}$ в строке с номером i , где $(i-1)$ — число с двоичной записью $\pi^{-1}(\mathbf{v}_{j-1})$. Тогда столбец j есть

$$i \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \omega^{g(\pi^{-1}(\mathbf{v}_{j-1}))} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Отсюда ясно, что

$$(H_nU)_{i+1,j+1} = (-1)^{\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \rangle} \omega^{g(\pi^{-1}(\mathbf{v}_j))}.$$

Таким образом, для любых $i, j \in \{0, 1, \dots, 2^n - 1\}$ получаем

$$\omega^{g(\mathbf{v}_i)} (-1)^{\langle \pi(\mathbf{v}_i), \mathbf{v}_j \rangle} = (-1)^{\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \rangle} \omega^{g(\pi^{-1}(\mathbf{v}_j))},$$

или, эквивалентно, для любых $x, y \in \mathbb{F}_2^n$ в кольце $\mathbb{Z}_q$ должно выполняться соотношение

$$g(x) + \frac{q}{2} \langle \pi(x), y \rangle = \frac{q}{2} \langle x, \pi^{-1}(y) \rangle + g(\pi^{-1}(y)). \quad (2)$$

Подставив нулевой вектор $y = \mathbf{0} \in \mathbb{F}_2^n$ в (2), получим, что g — обобщённая булева функция вида

$$g(x) = \frac{q}{2} \langle x, \pi^{-1}(\mathbf{0}) \rangle + g(\pi^{-1}(\mathbf{0})).$$

Подставим данное выражение в (2):

$$\frac{q}{2} \langle x, \pi^{-1}(\mathbf{0}) \rangle + g(\pi^{-1}(\mathbf{0})) + \frac{q}{2} \langle \pi(x), y \rangle = \frac{q}{2} \langle x, \pi^{-1}(y) \rangle + \frac{q}{2} \langle \pi^{-1}(y), \pi^{-1}(\mathbf{0}) \rangle + g(\pi^{-1}(\mathbf{0})),$$

после преобразований получим

$$\frac{q}{2} \langle x, \pi^{-1}(\mathbf{0}) \rangle + \frac{q}{2} \langle \pi(x), y \rangle = \frac{q}{2} \langle x, \pi^{-1}(y) \rangle + \frac{q}{2} \langle \pi^{-1}(y), \pi^{-1}(\mathbf{0}) \rangle. \quad (3)$$

В силу того, что условие (3) рассматривается в кольце $\mathbb{Z}_q$, имеет значение только чётность обеих частей равенства, то есть для всех $x, y \in \mathbb{F}_2^n$ получаем

$$\langle x, \pi^{-1}(\mathbf{0}) \rangle \oplus \langle \pi(x), y \rangle = \langle x, \pi^{-1}(y) \rangle \oplus \langle \pi^{-1}(y), \pi^{-1}(\mathbf{0}) \rangle.$$

Нетрудно видеть, что подстановка π должна быть аффинной. Это следует из того, что левая часть линейная по переменной y , тогда как правая часть линейна по x . Положим $\pi(x) = L(x \oplus c)$, $x \in \mathbb{F}_2^n$, для некоторых $L \in \text{GL}(n)$ и $c \in \mathbb{F}_2^n$, тогда

$$\langle x, c \rangle \oplus \langle L(x \oplus c), y \rangle = \langle x, L^{-1}y \oplus c \rangle \oplus \langle L^{-1}y \oplus c, c \rangle,$$

то есть

$$\langle L(x \oplus c), y \rangle = \langle x, L^{-1}y \rangle \oplus \langle L^{-1}y, c \rangle \oplus \langle c, c \rangle. \quad (4)$$

Дальнейшие рассуждения повторяют доказательство [12, теорема 1]. ■

4.2. Классификация самодуальных обобщённых бент-функций от четырёх переменных для $q = 4$ в рамках группы $\mathcal{U}_n^q$

Используя отображение из утверждения 3, можно уточнить известную классификацию самодуальных обобщённых бент-функций от четырёх переменных для $q = 4$, приведённую в работе [5] и состоящую из восьми классов эквивалентности. В [5] эквивалентными считаются такие функции, которые могут быть получены друг из друга преобразованиями вида (1).

С использованием отображения более общего вида можно показать, что функции с векторами значений (0330302132010110) и (3123231322030300) из классов 4 и 5 (см. [5]) соответственно связаны преобразованием

$$g(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2} \langle c, x \rangle + d,$$

где

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad c = (1001), \quad d = 3.$$

Аналогично, представители (2022220222020200) и (2123230332121210) классов 2 и 7 соответственно связаны преобразованием

$$f(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2} \langle c, x \rangle + d,$$

где

$$L = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad c = (0101), \quad d = 1.$$

Уточнённая классификация приведена в таблице; всего существует 400 самодуальных обобщённых бент-функций от четырёх переменных для $q = 4$.

**Классификация самодуальных обобщённых
бент-функций от четырёх переменных для $q = 4$**

Представитель класса эквивалентности	Мощность класса
022020222000000	24
202222022202000	64
0330313133110110	48
0330302132010110	120
1321213122010100	96
0220213023100000	48

**4.3. Унитарные операторы и множества самодуальных
и антисамодуальных обобщённых бент-функций**

Охарактеризуем элементы группы $\mathcal{U}_n^q$, определяющие взаимно однозначные соответствия между множествами самодуальных и антисамодуальных обобщённых бент-функций от n переменных.

Изменением одного из параметров отображений, описанных в утверждении 3, можно «переключать» сохранение (анти)самодуальности на соответствие другого характера:

Утверждение 5. Отображения множества всех обобщённых булевых функций от n переменных в себя, имеющие вид

$$f(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2}\langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$, определяют взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

Доказательство. Пусть $f \in \mathcal{SB}_n^{q,+} \cup \mathcal{SB}_n^{q,-}$ и $\tilde{f} = f + (q/2)\varepsilon$ для некоторого $\varepsilon \in \mathbb{F}_2$. Нетрудно видеть, что для $g(x) = f(L(x \oplus c)) + (q/2)\langle c, x \rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$, справедливо $H_g(y) = 2^{n/2}\omega^{\tilde{g}(y)+q/2}$, $y \in \mathbb{F}_2^n$. ■

Из существования такого взаимно однозначного соответствия можно получить

Следствие 3. Справедливо $|\mathcal{SB}_n^{q,+}| = |\mathcal{SB}_n^{q,-}|$.

Аналогично утверждению 4, установим взаимосвязь между рассматриваемыми отображениями, а также матрицами, соответствующими таким изометричным отображениям:

Утверждение 6. Оператор $\varphi_{\pi,g} \in \mathcal{U}_n^q$ с матрицей U определяет взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$, если и только если $U\mathcal{H}_n = -\mathcal{H}_nU$.

Доказательство. Достаточность следует из того, что если $\mathcal{H}_nA = -A\mathcal{H}_n$, то для любых характеристических векторов F, G функций $f \in \mathcal{SB}_q^+(n)$ и $g \in \mathcal{SB}_q^-(n)$ соответственно выполняется

$$\mathcal{H}_n(AF) = -A(\mathcal{H}_nF) = -AF, \quad \mathcal{H}_n(AG) = -A(\mathcal{H}_nG) = AG,$$

следовательно, рассматриваемое отображение определяет взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

Необходимость доказывается аналогично утверждению 4. ■

Далее показано, что множество всех элементов группы $\mathcal{U}_n^q$, определяющих взаимно однозначные соответствия между множествами самодуальных и антисамодуальных

обобщённых бент-функций от n переменных, исчерпывается отображениями, описанными в утверждении 5. Отметим, что случай булевых функций ранее изучен в работе [12], где доказано, что изометричные отображения множества всех булевых функций от n переменных в себя, имеющие вид

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x) \quad x \in \mathbb{F}_2^n,$$

определяют взаимно однозначные соответствия между множествами самодуальных и антисамодуальных бент-функций, если и только если

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

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — нечётное число; $d \in \mathbb{F}_2$.

Следующий результат характеризует все элементы группы $\mathcal{U}_n^q$, определяющие взаимно однозначные соответствия между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

Теорема 4. Оператор $\varphi_{\pi,g} \in \mathcal{U}_n^q$ определяет взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2} \langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$.

Доказательство. Достаточность следует из утверждения 5.

Пусть U — матрица оператора $\varphi_{\pi,g} \in \mathcal{U}_n^q$, определяющего взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,+}$. Как и в доказательстве теоремы 3, используем соотношения

$$\begin{aligned} (UH_n)_{i+1,j+1} &= \omega^{g(\mathbf{v}_i)} (-1)^{\langle \pi(\mathbf{v}_i), \mathbf{v}_j \rangle}, \\ (H_n U)_{i+1,j+1} &= (-1)^{\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \rangle} \omega^{g(\pi^{-1}(\mathbf{v}_j))}, \end{aligned}$$

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

Из утверждения 6 следует, что $UH_n = -H_n U$, откуда получаем $(UH_n)_{i+1,j+1} = -(H_n U)_{i+1,j+1}$ для всех $i, j \in \{0, 1, \dots, 2^n - 1\}$. Следовательно, должно выполняться соотношение

$$-\omega^{g(\mathbf{v}_i)} (-1)^{\langle \pi(\mathbf{v}_i), \mathbf{v}_j \rangle} = (-1)^{\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \rangle} \omega^{g(\pi^{-1}(\mathbf{v}_j))}$$

или, что то же самое,

$$g(x) + \frac{q}{2} \langle \pi(x), y \rangle + \frac{q}{2} = \frac{q}{2} \langle x, \pi^{-1}(y) \rangle + g(\pi^{-1}(y))$$

для всех $x, y \in \mathbb{F}_2^n$, при этом все вычисления проводятся в кольце $\mathbb{Z}_q$.

Дальнейшие рассуждения повторяют доказательство теоремы 3 с отличием в соотношении (4):

$$\langle L(x \oplus c), y \rangle = \langle x, L^{-1}y \rangle \oplus \langle L^{-1}y, c \rangle \oplus \langle c, c \rangle \oplus 1,$$

и выражении для функции g :

$$g(x) = \frac{q}{2} \langle c, x \rangle + g(c) + \frac{q}{2}, \quad x \in \mathbb{F}_2^n,$$

при этом значение $g(c)$ можно фиксировать произвольным элементом кольца $\mathbb{Z}_q$. ■

4.4. И т о г и

Пусть $n \geq 4$ — чётное число и $\varphi_{\pi,g} \in \mathcal{U}_n^q$ — оператор с матрицей U , а именно:

$$\varphi_{\pi,g} : f(x) \longrightarrow f(\pi(x)) + g(x),$$

где π — подстановка на $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных. Матрица U есть

$$(i+1) \begin{pmatrix} & \pi(\mathbf{v}_i) \\ & 0 \\ & \vdots \\ & 0 \\ 0 & \dots & 0 & \omega^{g(\mathbf{v}_i)} & 0 & \dots & 0 \\ & 0 \\ & \vdots \\ & 0 \end{pmatrix}.$$

Здесь, как и ранее, $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{2^n-1}$ — все векторы пространства $\mathbb{F}_2^n$ в лексикографическом порядке; в строке с номером $(i+1) \in \{1, 2, \dots, 2^n\}$ ненулевой элемент находится в столбце с номером $(j+1)$, где j — число с двоичной записью $\pi(\mathbf{v}_i)$. Тогда:

I. Следующие условия эквивалентны:

- 1) $\varphi_{\pi,g}$ сохраняет самодуальность;
- 2) $\varphi_{\pi,g}$ сохраняет антисамодуальность;
- 3) $\pi(x) = L(x \oplus c)$, $g(x) = (q/2)\langle c, x \rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$;
- 4) $U\mathcal{H}_n = \mathcal{H}_n U$.

II. Следующие условия эквивалентны:

- 1) $\varphi_{\pi,g}$ определяет взаимно однозначное соответствие между множествами $\mathcal{SB}^{q,+}$ и $\mathcal{SB}^{q,-}$;
- 2) $\pi(x) = L(x \oplus c)$, $g(x) = (q/2)\langle c, x \rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$;
- 3) $U\mathcal{H}_n = -\mathcal{H}_n U$.

Из полученных результатов следует, что подход к классификации самодуальных обобщённых бент-функций от $n \geq 4$ переменных на основе частного случая расширенного аффинного отображения, упомянутого в утверждении 3, является наиболее общим в рамках группы $\mathcal{U}_n^q$.

5. Отображение, соответствующее комплексному сопряжению характеристического вектора

Ещё одним изометричным отображением множества всех обобщённых булевых функций от n переменных в себя, сохраняющим самодуальность, является отображение, соответствующее комплексному сопряжению характеристического вектора. В терминах функций оно представляется как

$$f(x) \longrightarrow q - f(x), \quad x \in \mathbb{F}_2^n, \quad (5)$$

или, кратко, $f \rightarrow (-f) \bmod q$. Функцию, характеристический вектор которой комплексно сопряжён характеристическому вектору функции f , будем обозначать через $\bar{f}$.

Утверждение 7. Отображение (5) является изометричным, переводит каждую обобщённую бент-функцию в обобщённую бент-функцию и, кроме того, сохраняет (анти)самодуальность.

Доказательство. Сохранение (анти)самодуальности следует из того, что матрица Сильвестра — Адамара является вещественной. ■

Неподвижными точками отображения (5) являются обобщённые булевы функции с вещественными характеристическими векторами, и только они. Такие характеристические векторы имеют, очевидно, только обобщённые булевы функции, представимые в виде $\frac{q}{2}f$, где f — некоторая булева функция от того же числа переменных.

Таким образом, в булевом случае данное отображение является тождественным и не представляет интереса, тогда как для обобщённых булевых функций оно предлагает ряд отображений, отличных от предложенных в предыдущем пункте. Это следует из того, что комплексное сопряжение определяет антилинейное отображение, поэтому ему не может соответствовать никакой линейный оператор $\mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ и, следовательно, никакой элемент исследованной группы $\mathcal{U}_n^q$.

Отметим также, что данное отображение является частным случаем отображений вида $f \rightarrow (\gamma \cdot f) \bmod q$ для $\gamma \in \mathbb{Z}_q^*$, которые изучаются в [6].

Рассмотрим более общий вид отображений типа (5), а именно отображения

$$f(x) \longrightarrow -f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n, \quad (6)$$

где π — подстановка на пространстве $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных. Данная форма отображений с точностью до множителя перед функцией f аналогична форме, упомянутой в теореме 2. Легко видеть, что верно

Утверждение 8. Отображение вида (6) определяет изометрию в метриках Хэмминга и Ли на множестве всех обобщённых булевых функций от n переменных.

Следующий результат характеризует все отображения вида (6), сохраняющие (анти)самодуальность обобщённой бент-функции.

Теорема 5. Отображение вида (6) сохраняет (анти)самодуальность, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2}\langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\text{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$.

Доказательство. Рассмотрим произвольное отображение указанного типа, пусть оно отображает функцию $f \in \mathcal{SB}_n^{q,+}$ в некоторую функцию $h \in \mathcal{SB}_n^{q,+}$, то есть

$$f(x) \longrightarrow h(x) = -f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n.$$

Согласно утверждению 7, функция $\bar{h}$ также является самодуальной, она имеет вид

$$\bar{h}(x) = f(\pi(x)) - g(x), \quad x \in \mathbb{F}_2^n,$$

следовательно, в силу произвольности выбора функции f , должно выполняться $\varphi_{\pi,-g} \in \mathcal{U}_n^q$. ■

Таким образом, самой общей формой изометричных отображений, рассмотренных в настоящей работе, является следующая:

$$f(x) \longrightarrow \gamma \cdot f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n,$$

где $\gamma \in \{1, q-1\}$; π — подстановка на пространстве $\mathbb{F}_2^n$; g — обобщённая булева функция от n переменных.

Закключение

Предложено новое отображение, сохраняющее самодуальность обобщённой бент-функции. Вводится понятие действия унитарного оператора на множестве обобщённых булевых функций от n переменных, представленных своими характеристическими векторами. В рамках рассматриваемого класса унитарных операторов описаны все отображения, сохраняющие самодуальность. Рассмотрен класс отображений, определяемых сопряжением характеристического вектора. Интересным для дальнейшего изучения является вопрос полного описания группы автоморфизмов самодуальных обобщённых бент-функций.

ЛИТЕРАТУРА

1. Rothaus O. S. On “bent” functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. Tokareva N. Bent Functions: Results and Applications to Cryptography. Academic Press, 2015. 220 p.
3. Schmidt K.-U. Quaternary constant-amplitude codes for multicode CDMA // IEEE Trans. Inform. Theory. 2009. V. 55. No. 4. P. 1824–1832.
4. Stănică P., Martinsen T., Gangopadhyay S., and Singh B. K. Bent and generalized bent functions // Des. Codes Cryptogr. 2013. V. 69. No. 1. P. 77–94.
5. Sok L., Shi M., and Solé P. Classification and construction of quaternary self-dual bent functions // Cryptogr. Commun. 2018. V. 10. No. 2. P. 277–289.
6. Çeşmelioglu A. and Meidl W. Equivalence for generalized Boolean functions // Adv. Math. Commun. 2024. V. 18. No. 6. P. 1590–1604.
7. Martinsen T., Meidl W., and Stănică P. Generalized bent functions and their Gray images // LNCS. 2017. V. 10064. P. 160–173.
8. Carlet C., Danielsen L. E., Parker M. G., and Solé P. Self-dual bent functions // Int. J. Inform. Coding Theory. 2010. V. 1. P. 384–399.
9. Hou X.-D. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. No. 2. P. 183–198.
10. Feulner T., Sok L., Solé P., and Wassermann A. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. No. 1. P. 395–406.
11. Kutsenko A. Metrical properties of self-dual bent functions // Des. Codes Cryptogr. 2020. V. 88. No. 1. P. 201–222.
12. Kutsenko A. The group of automorphisms of the set of self-dual bent functions // Cryptogr. Commun. 2020. V. 12. No 5. P. 881–898.
13. Kutsenko A. Decomposing self-dual bent functions // Des. Codes Cryptogr. 2024. V. 92. No 1. P. 113–144.
14. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. опер. 2010. Т. 17. № 1. С. 34–64.
15. Davis J. A. and Jedwab J. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed — Muller codes // IEEE Trans. Inform. Theory. 1999. V. 45. No. 7. P. 2397–2417.
16. Марков А. А. О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
17. Погорелов Б. А., Пудовкина М. А. Классификация дистанционно транзитивных графов орбиталов надгрупп группы Джевонса // Дискретная математика. 2018. Т. 30. № 4. С. 66–87.

18. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices // *Finite Fields Appl.* 2007. V. 13. No. 3. P. 450–491.

REFERENCES

1. *Rothaus O. S.* On “bent” functions. *J. Combin. Theory, Ser. A*, 1976, vol. 20, no. 3, pp. 300–305.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Academic Press, 2015. 220 p.
3. *Schmidt K.-U.* Quaternary constant-amplitude codes for multicode CDMA. *IEEE Trans. Inform. Theory*, 2009, vol. 55, no. 4, pp. 1824–1832.
4. *Stănică P., Martinsen T., Gangopadhyay S., and Singh B. K.* Bent and generalized bent functions. *Des. Codes Cryptogr.*, 2013, vol. 69, no. 1, pp. 77–94.
5. *Sok L., Shi M., and Solé P.* Classification and construction of quaternary self-dual bent functions. *Cryptogr. Commun.*, 2018, vol. 10, no. 2, pp. 277–289.
6. *Çeşmelioglu A. and Meidl W.* Equivalence for generalized Boolean functions. *Adv. Math. Commun.*, 2024, vol. 18, no. 6, pp. 1590–1604.
7. *Martinsen T., Meidl W., and Stănică P.* Generalized bent functions and their Gray images. *LNCS*, 2017, vol. 10064, pp. 160–173.
8. *Carlet C., Danielsen L. E., Parker M. G., and Solé P.* Self-dual bent functions. *Int. J. Inform. Coding Theory*, 2010, vol. 1, pp. 384–399.
9. *Hou X.-D.* Classification of self dual quadratic bent functions. *Des. Codes Cryptogr.*, 2012, vol. 63, no. 2, pp. 183–198.
10. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables. *Des. Codes Cryptogr.*, 2013, vol. 68, no. 1, pp. 395–406.
11. *Kutsenko A.* Metrical properties of self-dual bent functions. *Des. Codes Cryptogr.*, 2020, vol. 88, no. 1, pp. 201–222.
12. *Kutsenko A.* The group of automorphisms of the set of self-dual bent functions. *Cryptogr. Commun.*, 2020, vol. 12, no. 5, pp. 881–898.
13. *Kutsenko A.* Decomposing self-dual bent functions. *Des. Codes Cryptogr.*, 2024, vol. 92, no. 1, pp. 113–144.
14. *Tokareva N. N.* Generalizations of bent functions. A survey. *J. Appl. Industr. Math.*, 2011, vol. 5, no. 1, pp. 110–129.
15. *Davis J. A. and Jedwab J.* Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed — Muller codes. *IEEE Trans. Inform. Theory*, 1999, vol. 45, no. 7, pp. 2397–2417.
16. *Markov A. A.* О преобразованіях, не распроstranyayushchikh iskazheniya [On transformations without error propagation]. *Izbrannye Trudy. T. II. Teoriya Algorifmov i Konstruktivnaya Matematika, Matematicheskaya Logika, Informatika i Smezhnye Voprosy.* Moscow, MCCME, 2003, pp. 70–93. (in Russian)
17. *Pogorelov B. A. and Pudovkina M. A.* Classification of distance-transitive orbital graphs of overgroups of the Jevons group. *Discrete Math. Appl.*, 2018, vol. 30, no. 1, pp. 7–22.
18. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices. *Finite Fields Appl.*, 2007, vol. 13, no. 3, pp. 450–491.