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

На правах рукописи
УДК 519.7

Шапоренко Александр Сергеевич

Построение бент-функций на основе их производных и связанные открытые вопросы

Специальность 1.2.3 —
«Теоретическая информатика, кибернетика»

Диссертация на соискание ученой степени
кандидата физико-математических наук

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

Новосибирск — 2024

Оглавление

Стр.

Введение 4

Глава 1. Бент-функции: основные понятия и связанные открытые проблемы 18

1.1 Булевы функции 18

1.2 Криптографические свойства булевых функций 20

1.3 Бент-функции 21

1.4 Обобщения бент-функций 23

1.5 Проблема о разложении булевых функций в сумму двух бент-функций 25

1.6 Гипотеза о производных бент-функций 27

Глава 2. Конструкция уравновешенных функций с высокой нелинейностью и другими криптографическими свойствами . 29

2.1 Уравновешенные функции с высокой нелинейностью 29

2.2 Конструкция булевых функций, производная которых линейно зависит от некоторой своей переменной 30

2.3 Криптографические свойства булевых функций, которые имеют аффинные производные 35

2.4 Построение уравновешенных функций с высокой нелинейностью . 39

Глава 3. Производные бент-функций 42

3.1 Связь с проблемой о разложении булевых функций в сумму двух бент-функций 42

3.2 Аффинные производные бент-функций 47

3.3 Итеративная нижняя оценка числа бент-функций 49

3.4 Квадратичные производные бент-функций 51

Глава 4. Бент-функции и их обобщения 53

4.1 Связь между обобщенными и булевыми бент-функциями 53

4.2 Связь между кватернарными и булевыми бент-функциями 58

4.3 Связь между кватернарными и обобщенными бент-функциями . . . 65

Глава 5. Исследование однородных бент-функций с помощью графов . 67

Стр.

5.1 Известные методы классификации бент-функций с помощью теории графов 67
5.2 Графы Нэги и однородные бент-функции 68

Заключение 72

Список литературы 73

Введение

Работа посвящена исследованию класса булевых функций от четного числа переменных, отличительным свойством которых является достижение верхней границы значения нелинейности. Такие булевы функции называются бент-функциями. Максимальное значение нелинейности представляет большой интерес для симметричной криптографии, однако бент-функции также связаны с некоторыми объектами теории кодирования, алгебры и комбинаторики. В работе исследуется построение бент-функций с помощью их производных, а также связь между известными открытыми проблемами, посвященными бент-функциям, и производными бент-функций.

Приведем необходимые определения.

Пусть $\mathbb{Z}_q = \{0,\ldots,q-1\}$, где q – целое положительное число. Пространство векторов длины n над $\mathbb{Z}_q$ обозначается $\mathbb{Z}_q^n$. Пусть $\oplus$ обозначает сложение по модулю 2. Для $x, y \in \mathbb{Z}_2^n$, мы будем использовать следующее произведение:

$$\langle x,y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n,$$

где x_i – i-ая координата x, $i = 1,\ldots,n$.

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Обозначим через $\mathcal{F}_n$ множество всех булевых функций от n переменных. *Весом Хэмминга* $wt(y)$ вектора $y \in \mathbb{Z}_2^n$ называется количество ненулевых координат y: $wt(y) = |\{i : y_i = 1\}|$. *Весом Хэмминга* $wt(f)$ функции $f \in \mathcal{F}_n$ называется количество ненулевых значений f: $|\{x \in \mathbb{Z}_2^n : f(x) = 1\}|$. Функция $f \in \mathcal{F}_n$ называется *уравновешенной*, если $wt(f) = 2^{n-1}$. *Расстояние Хэмминга* $\mathrm{dist}(f,g)$ между двумя булевыми функциями $f, g \in \mathcal{F}_n$ вычисляется следующим образом: $\mathrm{dist}(f,g) = |\{x \in \mathbb{Z}_2^n : f(x) \neq g(x)\}|$.

Каждую булеву функцию f от n переменных можно единственным образом представить в виде *полинома Жегалкина* (*алгебраической нормальной формы или АНФ*):

$$f(x_1,\ldots,x_n) = a_0 \oplus \bigoplus_{k=1}^{n} \bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} x_{i_1} \cdot \ldots \cdot x_{i_k},$$

где при каждом k индексы $i_1,\ldots,i_k$ различны и в совокупности пробегают все k-элементные подмножества $\{1,\ldots,n\}$, а коэффициенты $a_{i_1},\ldots,a_{i_k},a_0$ принимают значение 0 или 1.

Алгебраической степенью (степенью) $\deg(f)$ функции f называется количество переменных в самом длинном слагаемом ее полинома Жегалкина, при котором коэффициент не равен нулю. Функции степени два называются *квадратичными*. Булева функция называется *однородной*, если все мономы ее полинома Жегалкина имеют одинаковые степени.

Функция f от n переменных *линейно зависит от переменной* x_i, если $f(x_1,\dots,x_n) = g(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n) \oplus x_i$, где $g \in \mathcal{F}_{n-1}$ и $1 \leqslant i \leqslant n$. Если переменная не входит в АНФ булевой функции, то эта переменная называется *фиктивной*.

Производной булевой функции $f \in \mathcal{F}_n$ по *направлению* $y \in \mathbb{Z}_2^n$ называется функция $D_y f(x) = f(x) \oplus f(x \oplus y)$. Булева функция f *имеет линейную структуру*, если существует ненулевое направление $y \in \mathbb{Z}_2^n$ такое, что $D_y f(x) \equiv \text{const}$.

Булева функция $\ell_{a,b} = \langle x, a\rangle \oplus b$, где $a \in \mathbb{Z}_2^n$ и $b \in \mathbb{Z}_2$, называется *аффинной функцией* от n переменных. Множество всех аффинных функций от n переменных обозначим $\mathcal{A}_n$.

Булева функция $g \in \mathcal{F}_n$ получена из функции $f \in \mathcal{F}_n$ *аффинным преобразованием переменных*, если существует невырожденная квадратная двоичная матрица A порядка $n \times n$ и вектор $b \in \mathbb{Z}_2^n$ такие, что $g(x) = f(Ax \oplus b)$.

Нелинейностью N_f булевой функции $f \in \mathcal{F}_n$ называется расстояние Хэмминга от данной функции до множества всех аффинных функций, а именно

$$N_f = \text{dist}(f,\mathcal{A}_n) = \min_{a\in\mathbb{Z}_2^n, b\in\mathbb{Z}_2} \text{dist}(f, \ell_{a,b}),$$

где $\ell_{a,b}(x) = \langle a, x\rangle \oplus b$, $a \in \mathbb{Z}_2^n$ и $b \in \mathbb{Z}_2$.

Для каждого $y \in \mathbb{Z}_2^n$ *коэффициентом Уолша–Адамара* $W_f(y)$ булевой функции $f \in \mathcal{F}_n$ называется величина, определяемая равенством

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

С помощью коэффициентов Уолша–Адамара можно определять расстояние от функции $f \in \mathcal{F}_n$ до аффинных функций:

$$\text{dist}(f,\ell_{a,0}) = 2^{n-1} - \frac{1}{2} W_f(a).$$

Поскольку $\text{dist}(f,\ell_{a,1}) = 2^n - \text{dist}(f,\ell_{a,0})$, то справедливо следующее:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{Z}_2^n} |W_f(a)|.$$

Для коэффициентов Уолша–Адамара справедливо равенство Парсеваля:

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

Из него следует, что $\max\limits_{a\in\mathbb{Z}_2^n} |W_f(a)| \geqslant 2^{n/2}$. Таким образом, $N_f \leqslant 2^{n-1} - 2^{\frac{n}{2}-1}$.

Булева функция от четного числа n переменных, значение нелинейности которой достигает наибольшего значения $2^{n-1} - 2^{\frac{n}{2}-1}$, называется **бент-функцией**. Известен также следующий критерий: функция $f \in \mathcal{F}_n$ является бент-функцией, если и только если ее производные по всем ненулевым направлениям уравновешены. Обозначим через $\mathcal{B}_n$ множество всех бент-функций от n переменных.

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ – *обобщенная булева функция* от n переменных, где $q \geqslant 2$ – целое положительное число. *Преобразование Уолша–Адамара* обобщенной функции от n переменных определяется следующим образом:

$$W_f(x) = \sum_{y\in\mathbb{Z}_2^n} \omega^{f(y)}(-1)^{\langle x,y\rangle},$$

где $x \in \mathbb{Z}_2^n$ и $\omega = e^{2\pi i/q}$. В случае $q = 4$ получаем $\omega = i$.

Обобщенная булева функция f от n переменных является *обобщенной бент-функцией*, если $|W_f(x)| = 2^{n/2}$ для любого $x \in \mathbb{Z}_2^n$. Отметим, что обобщенные бент-функции существуют и при нечетных n. В работе мы будем рассматривать только случай $q = 4$. Для $q = 4$ множество всех обобщенных булевых функций и множество всех обобщенных бент-функций от n переменных обозначим $\mathcal{GF}_n$ и $\mathcal{GB}_n$ соответственно.

Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *q-значной функцией* от n переменных, где $q \geqslant 2$ – целое положительное число. Для $x, y \in \mathbb{Z}_q^n$, мы будем использовать следующее произведение:

$$x.y = x_1y_1 + \cdots + x_ny_n \bmod q.$$

Преобразование Уолша–Адамара q-значной функции f от n переменных определяется следующим образом:

$$W_f(x) = \sum_{y\in\mathbb{Z}_q^n} \omega^{f(y)+x.y},$$

где $x \in \mathbb{Z}_q^n$ и $\omega = e^{2\pi i/q}$. В случае $q = 4$ такие функции называются *кватернарными функциями*.

Пусть f – q-значная булева функция от n переменных. Тогда f является *q-значной бент-функцией*, если $|W_f(x)| = q^{n/2}$ для любого $x \in \mathbb{Z}_q^n$. Отметим, что q-значные бент-функции также существуют и при нечетных n. В данной работе мы будем рассматривать только кватернарные функции. Множество всех кватернарных функций и множество всех кватернарных бент-функций от n переменных обозначим $\mathcal{QF}_n$ и $\mathcal{QB}_n$ соответственно.

За годы использования булевых функций в системах шифрования были сформулированы математические требования, которые на них накладываются, для противодействия различным криптографическим атакам. Такие свойства булевых функций называют криптографическими. Одной из наиболее важных криптографических характеристик булевой функции является ее нелинейность. Шифры, которые используют функции с высокой нелинейностью в качестве своих компонент, являются более стойкими к линейному криптоанализу [61—63]. Большой интерес, конечно, представляют булевы функции с максимальным значением нелинейности.

Бент-функции определил в 1960-х годах O. S. Rothaus в работе, опубликованной в 1976 году [79]. Однако известно, что бент-функции также исследовались в Советском Союзе математиками В. А. Елисеевым и О. П. Степченковым, которые использовали термин “минимальная функция”.

Бент-функции использовались в построении блочного шифра CAST-128 [14], поточного шифра Grain [41] и хэш-функции HAVAL [92].

К основным криптографическим свойствам относятся также уравновешенность, корреляционная иммунность, строгий лавинный критерий, критерий распространения, алгебраическая иммунность, отсутствие линейных структур. Очевидно, что для криптографических приложений интересны функции, которые обладают сразу несколькими криптографическими свойствами. Исследованию булевых функций с “хорошими” криптографическими свойставами посвящены следующие работы: нелинейность [57; 78; 79], корреляционная иммунность [24; 82], линейные структуры [36], нелинейность и корреляционная иммунность [25; 37; 85], нелинейность и алгебраическая иммунность [1; 5; 38; 47; 89], нелинейность и уравновешенность [26; 34; 35; 40; 47; 70; 81].

Однако не все свойства хорошо сочетаются друг с другом. Так, например, основным криптографическим недостатком бент-функций является тот факт, что бент-функции не являются уравновешенными. Одним из способов решения этой проблемы является преобразование бент-функций с целью получения

уравновешенных булевых функций, которые сохраняют высокие значения нелинейности [34; 35].

Бент-функции также связаны с другими математическими объектами. Так, например, R. L. McFarland [64] и J. F. Dillon [31] исследовали бент-функции в терминах разностных множеств. Описанию бент-функции с помощью графов посвящены работы [2—4; 17; 18; 49]. Бент-функции могут быть использованы для построения последовательностей, которые будут иметь предельно низкую автокорреляцию и взаимную корреляцию [69; 91]. Хорошо известной задачей теории кодирования является определение радиуса покрытия кода Рида–Маллера $RM(\ell, n)$. Если код имеет порядок 1, то эта задача связана с задачей поиска булевых функций с максимально возможной нелинейностью [48; 57].

Несмотря на то, что бент-функции были определены почти 50 лет назад, до сих пор остается множество открытых теоретических вопросов, посвященных этим функциям. Основным открытым вопросом остается точное число бент-функций, которое известно только для $n \leqslant 8$. Приведем ряд работ, которые посвящены нижним и верхним оценкам числа бент-функций [15; 25; 28; 29; 72; 74; 86]. Множество исследований посвящены конструкциям бент-функций. Одной из самых известных конструкций является конструкция Мэйорана–МакФарланда [64]. К ранним конструкциям также относится частичное расщепление [31]. Также были предложены ряд итеративных и алгебраических конструкций [19; 20; 23; 31; 32; 35; 54; 55; 79; 86]. На бент-функции также накладываются дополнительные условия, тем самым выделяя подклассы бент-функций такие, как однородные бент-функции [27; 66; 76; 90], квадратичные бент-функции [4; 31; 75; 77], нормальные бент-функции [21; 34; 35], мономиальные бент-функции [13; 20; 32; 54; 55].

В 2006 году K.-U. Schmidt [80] в контексте построения четверичных кодов постоянной амплитуды (quaternary constant-amplitude codes) для мультикодовых систем CDMA предложил новое обобщение бент-функций – отображения из $\mathbb{Z}_2^n$ в $\mathbb{Z}_4$ с некоторыми специальными спектральными свойствами. Обобщенным бент-функциям посвящены, например, работы [39; 43; 44; 59; 60; 65; 80; 84; 93], причем в работах [43; 59; 84] исследуется связь между обобщенными и булевыми бент-функциями. В 1985 году P. V. Kumar, R. A. Scholtz и L. R. Welch в работе [51] с целью построения q-значных бент-последовательностей [69], применимых в системах CDMA, предложили обобщение бент-функций для отображений из $\mathbb{Z}_q^n$ в

$\mathbb{Z}_q$, которые называются q-значными бент-функциями. Приведем ряд работ посвященных q-значным бент-функциям [16; 42; 45; 46; 51; 65; 83].

В работе [86] была представлена следующая гипотеза: любая булева функция от четного числа переменных n степени не больше $n/2$ может быть представлена как сумма двух бент-функций от n переменных. Кроме того, автором работы [86] также была предложена нижняя оценка числа бент-функций, которая основывается на этой гипотезе, а сама гипотеза была проверена с помощью полного перебора для четных $n \leqslant 6$. Затем исследованием проблемы занимались авторы [77], которые доказали гипотезу для квадратичных булевых функций и нескольких классов бент-функций, среди которых бент-функции из классов Мэйорана–МакФарланда [64] и частичного расщепления [31]. Также разложению дуальных бент-функций в сумму двух бент-функций посвящена работа [11]. Отметим, что данная проблема упоминается в обзорной работе [22], которая посвящена результатам исследования бент-функций за последние 40 лет.

Приведем ряд обзорных работ и монографий, которые посвящены бент-функциям. Монографии S. Mesnager [67] и Н. Н. Токаревой [87], книги О. А. Логачева, А. А. Сальникова, С. В. Смышляева, В. В. Ященко [6], T. W. Cusick и P. Stănică [30], обзор Н. Н. Токаревой [9], учебные пособия И. А. Панкратовой [7] и Ю. В. Таранникова [8]. Различным обобщениям бент-функций посвящены обзорные работы Н. Н. Токаревой [10] и W. Meidl [65].

Целью работы является исследование возможности построения бент-функций на основе их производных. В работе предложена конструкция бент-функций, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных. Также доказано необходимое и достаточное условие того, что функция, которая линейно зависит от некоторой своей переменной, является производной бент-функции. Доказано, что произвольная булева функция от n переменных степени не больше $n/2$ раскладывается в сумму двух бент-функций от n переменных тогда и только тогда, когда любая уравновешенная функция от $n+2$ переменных степени не больше $n/2$, которая линейно зависит от некоторой своей переменной и является производной некоторой булевой функции от $n+2$ переменных, является производной бент-функции от $n+2$ переменных. Тем самым доказана связь проблемы о разложении булевых функций в сумму двух бент-функций и следующей гипотезы о производных бент-функций: любая уравновешенная булева функция от четного числа переменных n степени не больше $n/2-1$, которая является про-

изводной некоторой булевой функции от n переменных, является производной бент-функции от n переменных. Гипотеза о производных бент-функций доказана для квадратичных булевых функций. Получено точное число бент-функций, которые имеют некоторую отличную от константы аффинную функцию своей производной. Этот результат был использован для получения итеративной нижней оценки числа бент-функций. Предложен метод построения уравновешенных функций от четного числа переменных без линейных структур с высокой нелинейностью. Показано, что свойство быть бент-функцией кватернарной функции $f(x+2y) = a(x,y) + 2b(x,y)$ от n переменных, где $a, b \in \mathcal{F}_{2n}$ и $x, y \in \mathbb{Z}_2^n$, не зависит от того, являются ли $b, a \oplus b$ бент-функциями от $2n$ переменных. В работе также исследуется возможность характеризации однородных бент-функций, с помощью клик максимального размера графов $\Gamma(n,k)$, вершинами которых являются неупорядоченные подмножества размера k множества $\{1,\ldots,n\}$, которые соединены ребром, если рассматриваемые подмножества имеют в точности один общий элемент. Было доказано, что если $n = \frac{(k+1)k}{2}$, то максимальный размер клики равен $k+1$, а количество клик максимального размера равно $\frac{n!}{(k+1)!}$.

Основные положения, выносимые на защиту:

1. Предложен метод построения уравновешенных функций от четного числа $n \geqslant 20$ переменных с нелинейностью $2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$ без линейных структур. Полученные значения нелинейности уравновешенных функций являются наибольшими достигнутыми для указанного числа переменных.
2. Представлена конструкция бент-функций, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных. Получено необходимое и достаточное условие того, что уравновешенная функция, которая линейно зависит хотя бы от одной из своих переменных, является производной бент-функции.
3. Доказано, что гипотеза о разложении булевых функций в сумму двух бент-функций верна в том и только том случае, если гипотеза о производных бент-функций верна для уравновешенных функций, которые линейно зависят хотя бы от одной из своих переменных.
4. Доказано, что любая квадратичная уравновешенная функция, которая может быть производной булевой функции, является производной бент-функции. Получено точное число бент-функций, имеющих некоторую

отличную от константы аффинную функцию своей производной. Как следствие получена итеративная нижняя оценка числа бент-функций.

5. Известно, что каждая однородная бент-функция от 6 переменных степени 3 соответствует дополнению клики максимального размера в графе Нэги $\Gamma(6,3)$. Доказано, что для графа Нэги $\Gamma(n,k)$, где $n = \frac{(k+1)k}{2}$, максимальный размер клики равен $k+1$ и точное число клик максимального размера в таких графах равно $\frac{n!}{(k+1)!}$. Установлено, что функции, соответствующие дополнениям клик максимального размера в графах $\Gamma(10,4)$ и $\Gamma(28,7)$, не являются бент-функциями.

Научная новизна: Работа носит теоретический характер. Все результаты диссертации являются новыми и снабжены полными доказательствами. Полученные результаты могут быть использованы для дальнейшего изучения производных бент-функций и их связи с открытыми проблемами из области исследования бент-функций. Например, в работе доказано, что изучение производных бент-функций связано с проблемой разложения булевых функций в сумму двух бент-функций.

Методология и методы исследования. В диссертации используются комбинаторные методы и методы дискретного анализа.

Апробация работы. Основные результаты работы докладывались на следующих конференциях и семинарах: Международная конференция «Boolean Functions and their Applications (BFA 2022)» (Норвегия, г. Балестранд, 2022 г.), Симпозиум «Современные тенденции в криптографии» (CTCrypt 2021) (Московская область, 2021 г.), Пятая конференция по программной инженерии и организации информации (SEIM-2020) (Санкт-Петербург, 2020 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография (SIBECRYPT)» имени Геннадия Петровича Агибалова (г. Абакан, 2018 г.; г. Томск, 2019; г. Новосибирск, 2021 г.), семинары «Дискретный анализ», «Комбинаторика и символьные последовательности», «Теория кодирования», «Криптография и криптоанализ» Института математики им. С. Л. Соболева СО РАН и кафедры теоретической кибернетики ММФ НГУ.

Содержание работы

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

В первой главе представлены основные определения и вспомогательные утверждения, а также ключевые для работы открытые проблемы: о разложении булевых функций в сумму двух бент-функций и о производных бент-функций, а также обзор известных результатов, посвященным им.

Следующая гипотеза была представлена и проверена для $n \leqslant 6$ в работе Н. Н. Токаревой 2011 года [86].

Гипотеза 1. *Пусть n – целое четное число. Тогда любая булева функция от n переменных степени не больше $n/2$ может быть разложена в сумму двух бент-функций от n переменных.*

В 2016 году в [12] была представлена и проверена для $n \leqslant 6$ следующая гипотеза: любая уравновешенная булева функция f от четного числа n переменных степени не больше $n/2 - 1$ такая, что $f(x) = f(x \oplus y)$ для любого $x \in \mathbb{Z}_2^n$ и некоторого ненулевого $y \in \mathbb{Z}_2^n$, является производной бент-функции от n переменных. Мы предлагаем следующее уточнение этой гипотезы.

Гипотеза 2. *Любая уравновешенная булева функция f от четного числа n переменных степени не больше $n/2 - 1$, которая линейно зависит хотя бы от одной из своих переменных, такая, что $f(x) = f(x \oplus y)$ для любого $x \in \mathbb{Z}_2^n$ и некоторого ненулевого $y \in \mathbb{Z}_2^n$, является производной бент-функции от n переменных.*

В работе доказано, что между Гипотезой 2 и проблемой о разложении булевых функций в сумму двух бент-функций существует прямая связь.

Вторая глава посвящена построению уравновешенных функций с высокой нелинейностью и другими криптографическими свойствами. Предложена следующая конструкция.

Конструкция 1. *Пусть* $g_1, g_2 \in \mathcal{F}_n$, $h \in \mathcal{F}_{n+2}$ *и вектор* $y \in \mathbb{Z}_2^n$. *Будем строить функцию* $f \in \mathcal{F}_{n+2}$ *следующим образом:*

$$f(x,x_{n+1},x_{n+2}) = \big((D_y g_1(x) \oplus 1)h(x,x_{n+1},x_{n+2}) \oplus D_y g_2(x)\big)x_{n+1} \\ \oplus\, g_1(x)h(x,x_{n+1},x_{n+2}) \oplus g_2(x),$$

где $x \in \mathbb{Z}_2^n, x_{n+1}, x_{n+2} \in \mathbb{Z}_2$.

Функции g_1, g_2, h *и вектор* y *будем считать параметрами конструкции.*

Доказана следующая теорема, в которой описаны параметры Конструкции 1, при которых функции будут обладать рядом криптографических свойств.

Теорема 1. *Пусть* g_1, $g_2 \in \mathcal{F}_n$, $y \in \mathbb{Z}_2^n$ *и* $h(x,x_{n+1},x_{n+2}) = \langle b,x\rangle \oplus c \oplus x_{n+2}$ *для любого* $x \in \mathbb{Z}_2^n$, *где* $b \in \mathbb{Z}_2^n$ *и* $c \in \mathbb{Z}_2$. *Тогда для функции* $f \in \mathcal{F}_{n+2}$ *из Конструкции 1 справедливо, что*

1. *функция* f *имеет* h *своей производной по направлению* $(y,1,\langle b,y\rangle)$;
2. *функция* f *— уравновешенная функция тогда и только тогда, когда* g_2 *– уравновешенная функция;*
3. $N_f = 2^{n+1} - \max\limits_{a\in\mathbb{Z}_2^n, g\in\{g_2, g_1\oplus g_2\}} |W_g(a)|$;
4. *если* g_2 *и* $g_1 \oplus g_2$ *— корреляционно-иммунные порядка* r, *то функция* f *является корреляционно-иммунной порядка* r.
5. *если* g_2 *и* $g_1 \oplus g_2$ *— уравновешенная функция и бент-функция соответственно, то функция* f *— уравновешенная без линейных структур.*

В [40] было показано, как построить уравновешенную функцию от 16 переменных с нелинейностью 32 598. Обозначим эту функцию f_{16}. Предложен итеративный метод построения уравновешенных функций от четного $n \geqslant 18$ числа переменных с высокой нелинейностью без линейных структур.

Метод 1. *Будем строить булевы функции от* n *переменных, используя Конструкцию 1 со следующими параметрами:*

- *при* $n = 18$ *функция* $g_2 = f_{16}$;
- *при* $n \geqslant 20$ *функция* g_2 *— функция* f *из Конструкции 1, полученная с помощью Метода 1 на предыдущем шаге;*
- *функция* $h(x,x_{n+1},x_{n+2}) = \langle b,x\rangle \oplus c \oplus x_{n+2}$ *для любого* $x \in \mathbb{Z}_2^n$, *где* $b \in \mathbb{Z}_2^n$ *и* $c \in \mathbb{Z}_2$;

– *функция* g_1 *такая, что* $g_1 \oplus g_2$ *— бент-функция;*
– *вектор* $y \in \mathbb{Z}_2^n$ *— произвольный.*

Теорема 2. *Функции от* $n \geqslant 18$ *переменных полученные с помощью Метода 1 являются уравновешенными функциями без линейных структур с нелинейностью* $2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$.

Результаты главы опубликованы в работе [94].

Третья глава посвящена гипотезе о производных бент-функций и ее связи с проблемой о разложении булевых функций в сумму двух бент-функций. Доказана следующая теорема, в которой представлено необходимое и достаточное условие того, что функция, линейно зависящая от некоторой своей переменной, является производной бент-функции. Кроме того, теорема представляет достаточное условие для того, чтобы функции, получаемые с помощью Конструкции 1, были бент-функциями.

Теорема 3. *Пусть* $n \geqslant 2$ *– четное целое число, функции* g_1, g_2, $h_1 \in \mathcal{F}_n$, *вектор* $(y,1,y_{n+2}) \in \mathbb{Z}_2^{n+2}$ *и* $h(x,x_{n+1},x_{n+2}) = (D_y h_1(x) \oplus y_{n+2})x_{n+1} \oplus h_1(x) \oplus x_{n+2}$. *Тогда* $f \in \mathcal{F}_{n+2}$ *из Конструкции 1 является бент-функцией тогда и только тогда, когда* g_2, $g_1 \oplus g_2$, $g_2 \oplus h_1$ *и* $g_1 \oplus g_2 \oplus h_1$ *— бент-функции. При этом любая функция* f *от* $n+2$ *переменных, которая имеет* h *своей производной по направлению* $(y,1,y_{n+2})$, *имеет представление из Конструкции 1. Кроме того, для различных параметров* (g_1, g_2) *получаются различные бент-функции* f.

В данной главе также доказано, что проблемы о разложении булевой функции в сумму двух бент-функций и о производных бент-функций являются эквивалентными.

Теорема 4. *Гипотеза 1 и Гипотеза 2 являются эквивалентными.*

Также в данной главе исследуются аффинные производные бент-функций. Доказана следующая теорема.

Теорема 5. *Пусть* $n \geqslant 2$, $\ell \in \mathcal{A}_{n+2}$ *и не является константой. Тогда* ℓ *является производной* $(2^{n+1} - 1) \mid \mathcal{B}_n \mid^2$ *бент-функций от* $n + 2$ *переменных.*

Таким образом, получено точное число бент-функций, которые имеют некоторую отличную от константы аффинную функцию своей производной. Отметим,

что производные второго порядка бент-функций с аффинными производными являются константами, поскольку производные аффинных функций – константы. Поэтому бент-функции, имеющие аффинные производные, можно использовать при построении бент-функций вида $f \oplus \mathrm{Ind}_U$ [50], где Ind_U – булева функцию от n переменных, принимающая значение 1 на всех элементах множества U и только на них.

Теорема 5 в дальнейшем используется, чтобы получить следующую итеративную нижнюю оценку числа бент-функций.

Теорема 6. *Для любого* $n \geqslant 2$ *справедливо* $|\mathcal{B}_{n+2}| \geqslant (2^{n+2} - 2)\,|\mathcal{B}_n|^2$.

Отметим, что в этой оценке не учитываются бент-функции, которые не имеют аффинных производных. Бент-функциям, которые не имеют аффинных производных, посвящены работы [19; 58; 71]. Однако, в приведенных работах не приводятся нижнии оценки или точные числа таких бент-функций, что позволило бы улучшить оценку из Теоремы 6. Также в этой главе представлено сравнение оценки из Теоремы 6 с другими известными итеративными нижними оценками числа бент-функций.

С использованием того факта, что Гипотеза 1 верна для квадратичных булевых функций [77], была доказана следующая теорема.

Теорема 7. *Пусть* f *– квадратичная уравновешенная булева функция от* $n \geqslant 6$ *переменных такая, что* $f(x) \oplus f(x \oplus y) = 0$ *для некоторого ненулевого* $y \in \mathbb{Z}_2^n$ *и произвольного* $x \in \mathbb{Z}_2^n$. *Тогда* f *является производной некоторой бент-функции от* n *переменных.*

Таким образом, Теоремы 5 и 7 дают доказательство Гипотезы 2 для функций степени не больше 2, которые не являются константами.

Результаты главы опубликованы в работах [95; 98; 99].

Четвертая глава посвящена исследованию связи кватернарных и булевых бент-функций. В этой главе доказано, что между свойствами функций $f \in \mathcal{QF}_n$ и $a, b \in \mathcal{F}_{2n}$ таких, что $f(x + 2y) = a(x,y) + 2b(x,y)$, где $x, y \in \mathbb{Z}_2^n$, быть бент-функциями нет зависимости. А именно, доказаны следующие утверждения.

Утверждение 18. *Для любых целых* $n \geqslant 2$ *существует кватернарная бент-функция* $f(x + 2y) = a(x,y) + 2b(x,y)$ *от* n *переменных, где* b *и* $a \oplus b$ *не являются бент-функциями от* $2n$ *переменных.*

Утверждение 19. *Для любых целых* $n \geqslant 1$ *существуют булевы бент-функции* b *и* $a \oplus b$ *от* $2n$ *переменных такие, что функция* $f(x+2y) = a(x,y) + 2b(x,y)$ *от* n *переменных не является кватернарной бент-функцией.*

Результаты главы опубликованы в работах [96; 100—102].

В **пятой главе** мы изучаем связь однородных бент-функций и графов $\Gamma(n,k)$, вершинами которого являются неупорядоченные подмножества размера k множества $\{1,\ldots,n\}$, которые соединены ребром, если рассматриваемые подмножества имеют в точности один общий элемент. В [27] было показано, что все однородные бент-функции от 6 переменных находятся во взаимно однозначном соответствии с дополнениями к кликам максимального размера графа $\Gamma(6,3)$.

Следовательно, возникает вопрос о возможности классификации однородных бент-функций от большего числа переменных с помощью выделения в графе $\Gamma(n,k)$ дополнений к кликам максимального размера. Доказана следующая теорема.

Теорема 8. *Пусть* $n = \frac{(k+1)k}{2}$, *где* $k > 1$. *Тогда максимальный размер клики в графе* $\Gamma(n,k)$ *равен* $k+1$. *При этом количество клик максимального размера равно* $\frac{n!}{(k+1)!}$.

В данной главе установлено, что булевы функции, которые соответствуют дополнениям клик максимального размера в графах $\Gamma(10,4)$ и $\Gamma(28,7)$, не являются бент-функциями.

Результаты главы были представлены в работах [97; 103].

В **заключении** приведены основные результаты работы.

Благодарности. Автор выражает признательность своему научному руководителю Наталье Николаевне Токаревой за постановку интересных задач, постоянное внимание к работе и поддержку. Также автор хотел бы выразить благодарность Николаю Александровичу Коломейцу и Александру Владимировичу Куценко за ценные советы и интересные обсуждения по теме работы.

Публикации. Основные результаты по теме диссертации изложены в 10 печатных изданиях, 4 из которых изданы в журналах, рекомендованных ВАК, 6 — в тезисах докладов. Статья [96] опубликована в соавторстве с Н. Н. Токаревой и P. Solé, при этом результаты параграфов 4, 5 и 8.2 статьи [96] получены автором лично.

Объем и структура работы. Диссертация состоит из введения, 5 глав и заключения. Полный объём диссертации составляет 82 страницы, включая 6 таблиц. Список литературы содержит 103 наименования.

Глава 1. Бент-функции: основные понятия и связанные открытые проблемы

В этой главе мы приводим необходимые определения и вспомогательные утверждения. Также в этой главе приводятся две ключевые для работы проблемы: о разложении булевых функций в сумму двух бент-функций и о производных бент-функций, а также обзор известных результатов, посвященным им.

1.1 Булевы функции

Пусть $\mathbb{Z}_q = \{0, \ldots, q-1\}$, где q – целое положительное число. Пространство векторов длины n над $\mathbb{Z}_q$ обозначается $\mathbb{Z}_q^n$.

Пусть $\oplus$ обозначает сложение по модулю 2. Для $x, y \in \mathbb{Z}_2^n$, мы будем использовать следующее произведение:

$$\langle x,y \rangle = x_1 y_1 \oplus \cdots \oplus x_n y_n,$$

где x_i – i-ая координата x, $i = 1, \ldots, n$.

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Множество всех булевых функций от n переменных обозначим $\mathcal{F}_n$. С каждой булевой функцией f от n переменных можно связать ее *носитель*:

$$\text{supp}(f) = \{x \in \mathbb{Z}_2^n : f(x) = 1\}.$$

Вес Хэмминга $wt(y)$ вектора $y \in \mathbb{Z}_2^n$: $wt(y) = |\{i : y_i = 1\}|$. *Весом Хэмминга* $wt(f)$ функции $f \in \mathcal{F}_n$ называется количество ненулевых значений f: $|\{x \in \mathbb{Z}_2^n : f(x) = 1\}|$.

Расстояние Хэмминга $\text{dist}(f, g)$ между двумя функциями $f, g \in \mathcal{F}_n$ вычисляется следующим образом:

$$\text{dist}(f, g) = |\{x \in \mathbb{Z}_2^n : f(x) \neq g(x)\}|.$$

Каждую булеву функцию f от n переменных можно единственным образом представить в виде *полинома Жегалкина* (*алгебраической нормальной формы или АНФ*):

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{k=1}^{n} \bigoplus_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} x_{i_1} \cdot \ldots \cdot x_{i_k},$$

где при каждом k индексы $i_1,...,i_k$ различны и в совокупности пробегают все k-элементные подмножества $\{1,...,n\}$, а коэффициенты $a_{i_1},...,a_{i_k},a_0$ принимают значение 0 или 1.

Алгебраической степенью (степенью) $\deg(f)$ функции f называется количество переменных в самом длинном слагаемом ее полинома Жегалкина, при котором коэффициент не равен нулю. Функция степени не выше 1 называется *аффинной*. Аффинную функцию от n переменных также можно представить в виде $\ell = \langle x, a\rangle \oplus b$, где $a \in \mathbb{Z}_2^n$ и $b \in \mathbb{Z}_2$. Множество всех аффинных функций от n переменных обозначим $\mathcal{A}_n$. Функции степени два называются *квадратичными*. Булева функция называется *однородной*, если все мономы ее полинома Жегалкина имеют одинаковые степени.

Функция f от n переменных *линейно зависит от переменной* x_i, если $f(x_1,\ldots,x_n) = g(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n) \oplus x_i$, где $g \in \mathcal{F}_{n-1}$ и $1 \leqslant i \leqslant n$. Если переменная не входит в АНФ булевой функции, то эта переменная называется *фиктивной*.

Производной булевой функции $f \in \mathcal{F}_n$ по *направлению* $y \in \mathbb{Z}_2^n$ называется функция $D_y f(x) = f(x) \oplus f(x \oplus y)$. Легко убедиться, что $D_y\big(f \oplus g\big) = D_y f \oplus D_y g$.

Приведем следующий хорошо известный вспомогательный факт.

Лемма 1. *Пусть* $f \in \mathcal{F}_n$ *такая, что* $\deg f \geqslant 1$. *Тогда для любого* $y \in \mathbb{Z}_2^n$ *верно* $\deg(D_y f) \leqslant \deg(f) - 1$.

Доказательство этого факта можно найти, например, в [7].

Приведем необходимое и достаточное условие того, что функция является производной некоторой булевой функции, которое было представлено в [12].

Лемма 2. *Булева функция* $f \in \mathcal{F}_n$ *является производной функции* $g \in \mathcal{F}_n$ *по ненулевому направлению* $y \in \mathbb{Z}_2^n$ *тогда и только тогда, когда* $D_y f(x) = 0$ *для всех* $x \in \mathbb{Z}_2^n$.

Для каждого $y \in \mathbb{Z}_2^n$ *коэффициентом Уолша–Адамара* $W_f(y)$ булевой функции $f \in \mathcal{F}_n$ называется величина, определяемая равенством

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

Неупорядоченный набор абсолютных значений коэффициентов Уолша–Адамара булевой функции называется её *спектром Уолша–Адамара*.

Нам понадобится следующие хорошо известные факты.

Лемма 3. *Для любой булевой функции f от n переменных справедливо, что* $\max\limits_{a\in\mathbb{Z}_2^n} |W_f(a)| \geqslant 2^{n/2}$.

Лемма 4. *Пусть $f \in \mathcal{F}_n$, $\ell \in \mathcal{A}_n$ и $\ell(x) = \langle a,x\rangle \oplus b$, где $a \in \mathbb{Z}_2^n, b \in \mathbb{Z}_2$. Тогда для любого $c \in \mathbb{Z}_2^n$ справедливо, что $W_{f\oplus\ell}(c) = (-1)^b \cdot W_f(a \oplus c)$.*

Булева функция $g \in \mathcal{F}_n$ получена из функции $f \in \mathcal{F}_n$ *аффинным преобразованием переменных*, если существует невырожденная квадратная двоичная матрица A порядка $n \times n$ и вектор $b \in \mathbb{Z}_2^n$ такие, что $g(x) = f(Ax \oplus b)$.

Следующий факт известен как теорема Диксона. Его доказательство приведено, например, в [56].

Лемма 5. *Любую квадратичную булеву функцию можно привести аффинным преобразованием переменных к следующему виду:*

$$x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2t-1}x_{2t} \oplus \ell(x)$$

для некоторой аффинной ℓ, и t, $1 \leqslant t \leqslant n/2$.

1.2 Криптографические свойства булевых функций

Функция $f \in \mathcal{F}_n$ называется *уравновешенной*, если $wt(f) = 2^{n-1}$.

Нам понадобится следующие хорошо известные факты.

Лемма 6. *Булева функция $f \in \mathcal{F}_n$ является уравновешенной тогда и только тогда, когда $W_f(0) = 0$.*

Лемма 7. *Пусть f является уравновешенной булевой функцией от n переменных. Тогда любая булева функция, полученная из f аффинным преобразованием переменных, также является уравновешенной.*

Доказательство этого утверждения следует из Леммы 6.

Булева функция f *имеет линейную структуру*, если существует ненулевое направление $y \in \mathbb{Z}_2^n$ такое, что $D_yf(x) \equiv$ const. Следующее факт объясняет интерес к удаленности от класса функций, которые имеют линейную структуру.

Лемма 8. *Пусть $f \in \mathcal{F}_n$ имеет линейную структуру. Тогда существует функция $g \in \mathcal{F}_n$, которая получена из f аффинным преобразованием переменных и имеет фиктивную переменную или линейно зависит от некоторой своей переменной.*

Доказательство этого утверждения можно найти, например, в [7].

Булева функция $f \in \mathcal{F}_n$ называется *корреляционно-иммунной порядка* r, $1 \leqslant r \leqslant n$, если для любой ее подфункции $g = f_{i_1,\dots,i_r}^{a_1,\dots,a_r}$, полученной из f подстановкой констант $a_1, \dots, a_r$ вместо переменных $x_{i_1}, \dots, x_{i_r}$, верно $wt(g) = wt(f)/2^r$. Требование корреляционной-иммунности функции связано с противостоянием корреляционной атаке [82].

Лемма 9. *Функция $f \in \mathcal{F}_n$ является корреляционно-иммунной порядка r тогда и только тогда, когда $W_f(a) = 0$ для всех $a \in \mathbb{Z}_2^n$ таких, что $1 \leqslant wt(a) \leqslant r$.*

Доказательство этого факта приведено в [82].

1.3 Бент-функции

Нелинейностью N_f булевой функции $f \in \mathcal{F}_n$ называется расстояние Хэмминга от данной функции до множества всех аффинных функций, а именно

$$N_f = \operatorname{dist}(f, \mathcal{A}_n) = \min_{a \in \mathbb{Z}_2^n, b \in \mathbb{Z}_2} \operatorname{dist}(f, \ell_{a,b}),$$

где $\ell_{a,b}(x) = \langle a, x \rangle \oplus b$, $a \in \mathbb{Z}_2^n$ и $b \in \mathbb{Z}_2$.

Приведем хорошо известный факт о связи нелинейности булевой функции и ее коэффициентов Уолша–Адамара, доказательство которого можно найти, например, в [87].

Лемма 10. *Пусть $f \in \mathcal{F}_n$. Тогда $N_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{Z}_2^n} |W_f(a)|$.*

Булева функция от четного числа переменных n называется *бент-функцией*, если ее значение нелинейности достигает наибольшего значения $2^{n-1} - 2^{\frac{n}{2}-1}$ (см., например, [87]). Обозначим через $\mathcal{B}_n$ множество всех бент-функций от n переменных.

Приведем хорошо известные факты о бент-функциях, которые будут использоваться в работе. Доказательство следующих утверждений можно найти, например, в [87].

Лемма 11. *Пусть* $f \in \mathcal{B}_n$ *и* $n \geqslant 4$. *Тогда* $\deg(f) \leqslant n/2$.

Лемма 12. *Пусть* $f \in \mathcal{B}_n$. *Тогда* $wt(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.

Следовательно, бент-функции никогда не являются уравновешенными.

Лемма 13. *Булева функция* $f \in \mathbb{Z}_n$ *является бент-функцией тогда и только тогда, когда* $W_f(y) = \pm 2^{n/2}$ *для любого* $y \in \mathbb{Z}_2^n$.

Лемма 14. *Пусть* $f \in \mathcal{B}_n$. *Тогда*

1. *любая булева функция, полученная из* f *аффинным преобразованием переменных, также является бент-функцией;*
2. *функция* $f \oplus \ell$ *является бент-функцией от* n *переменных для любой аффинной функции* ℓ.

Для бент-функции f от n переменных *дуальная функция* $\widetilde{f}$ определяется с помощью равенств $W_f(y) = 2^{n/2}(-1)^{\widetilde{f}(y)}$ для всех $y \in \mathbb{Z}_2^n$. Отметим, что $\widetilde{f}$ также является бент-функцией (см., например, [87]). Исследованию дуальных бент-функций посвящены, например, работы [11; 52; 53].

Приведем эквивалентное определение бент-функций.

Лемма 15. *Булева функция* $f \in \mathcal{F}_n$ *является бент-функцией тогда и только тогда, когда для любого ненулевого направления* y *ее производная* $D_y f(x)$ *является уравновешенной.*

Доказательство этого утверждения можно найти, например, в [87].

Так как следующее вспомогательное утверждение было представлено в [12] без доказательства, мы приведем его здесь.

Лемма 16. *Пусть* f *является булевой функцией от* n *переменных. Положим, что* f *является производной некоторой булевой функции по направлению* $y \neq 0$. *Тогда* $f_1(x) = f(Ax \oplus b)$ *также является производной некоторой булевой функции по направлению* $A^{-1}y \neq 0$, *где* $b \in \mathbb{Z}_2^n$ *и* A *– невырожденная двоичная* $n \times n-$*матрица. Более того, если* f_1 *является производной некоторой бент-функции, тогда* f *также является производной некоторой бент-функции.*

Доказательство. Из Леммы 2 следует, что $f(x) \oplus f(x \oplus y) = 0$ для всех $x \in \mathbb{Z}_2^n$. Следовательно, $f(Ax \oplus b) \oplus f(Ax \oplus b \oplus y) = f(Ax \oplus b) \oplus f(A(x \oplus A^{-1}y) \oplus b) =$

$f_1(x) \oplus f_1(x \oplus A^{-1}y) = 0$. Из Леммы 2 следует, что f_1 является производной некоторой булевой функции для ненулевого направления $A^{-1}y$.

Теперь положим, что g – бент-функция и $g(x) \oplus g(x \oplus A^{-1}y) = f_1(x)$. Тогда $g(A^{-1}x \oplus b) \oplus g(A^{-1}x \oplus A^{-1}y \oplus b) = f_1(A^{-1}x \oplus b) = f(x)$. Из Леммы 14 следует, что $g(A^{-1}x \oplus b)$ – бент-функция. □

Далее приведем известные конструкции бент-функций, которые будут использоваться в работе. Одной из самых простых итеративных конструкций бент-функций является контструкция, которая была представлена в [79].

Лемма 17. *Пусть $x \in \mathbb{Z}_2^r$ и $y \in \mathbb{Z}_2^k$, где $r,k \geqslant 2$ – четные. Булева функция $f(x,y) = f_1(x) \oplus f_2(y) \in \mathcal{B}_{r+k}$ тогда и только тогда, когда f_1 и f_2 являются бент-функциями от r и k переменных соответственно.*

Хорошо известно, что бент-функциями от двух переменных являются квадратичные функции и только они. Тогда согласно Лемме 17 справедливо следующее утверждение.

Лемма 18. *Булева функция g от четного числа n переменных, которая имеет следующее представление: $x_1x_2 \oplus \cdots \oplus x_{n-1}x_n$, является бент-функцией.*

Далее приведем описание одного из самых известных классов бент-функций – класса Мэйорана–МакФарланда.

Лемма 19. *Пусть n – положительное целое число, g – произвольная функция от n переменных и π – взаимно-однозначное отображение на $\mathbb{Z}_2^n$. Тогда для $x, y \in \mathbb{Z}_2^n$ функция $f(x,y) = \langle \pi(x), y \rangle \oplus g(x)$ – бент-функция от $2n$ переменных.*

Доказательство этого утверждения можно найти, например, в [7].

1.4 Обобщения бент-функций

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ – *обобщенная булева функция* от n переменных, где $q \geqslant 2$ – целое положительное число. *Преобразование Уолша–Адамара* обобщенной функции f от n переменных определяется следующим образом:

$$W_f(x) = \sum_{y \in \mathbb{Z}_2^n} \omega^{f(y)} (-1)^{\langle x,y \rangle},$$

где $x \in \mathbb{Z}_2^n$ и $\omega = e^{2\pi i/q}$. В случае $q = 4$ получаем $\omega = i$.

Обобщенная булева функция f от n переменных является *обобщенной бент-функцией*, если $|W_f(x)| = 2^{n/2}$ для любого $x \in \mathbb{Z}_2^n$. Отметим, что обобщенные бент-функции существуют и при нечетных n.

K.-U. Schmidt в работе [80] подробно разбирает случай обобщенных бент-функций для $q = 4$. Мы будем рассматривать именно этот случай. Для $q = 4$ множество всех обобщенных булевых функций и множество всех обобщенных бент-функций от n переменных обозначим $\mathcal{GF}_n$ и $\mathcal{GB}_n$ соответственно.

Обобщенным бент-функциям посвящены следующие работы [39; 43; 59; 60; 65; 80; 84; 93].

Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *q-значной функцией* от n переменных, где $q \geqslant 2$ – целое положительное число. Для $x, y \in \mathbb{Z}_q^n$, мы будем использовать следующее произведение:

$$x.y = x_1y_1 + \cdots + x_ny_n \bmod q,$$

где x_i – i-ая координата x, $i = 1, \ldots, n$.

Преобразование Уолша–Адамара q-значной функции f от n переменных определяется следующим образом:

$$W_f(x) = \sum_{y \in \mathbb{Z}_q^n} \omega^{f(y)+x.y},$$

где $x \in \mathbb{Z}_q^n$ и $\omega = e^{2\pi i/q}$. В случае $q = 4$ получаем $\omega = i$. В этом случае такие функции называются *кватернарными функциями*.

Пусть f – q-значная булева функция от n переменных. Тогда f является *q-значной бент-функцией*, если $|W_f(x)| = q^{n/2}$ для любого $x \in \mathbb{Z}_q^n$. Отметим, что q-значные бент-функции также существуют и при нечетных n [51]. В данной работе мы будем рассматривать только кватернарные функции. Множество всех кватернарных функций и множество всех кватернарных бент-функций от n переменных обозначим $\mathcal{QF}_n$ и $\mathcal{QB}_n$ соответственно.

Пусть f – q-значная бент-функция от n переменных. Тогда f называется *регулярной*, если для любого $x \in \mathbb{Z}_q^n$ выполняется $W_f(x) = q^{n/2}\omega^{h(x)}$, где h – q-значная функция от n переменных.

Лемма 20. *Все кватернарные бент-функции являются регулярными.*

Это утверждение было доказано в [51].

Также приведем аналог конструкции Ротхауса для кватернарных функций.

Лемма 21. *Пусть* $x \in \mathbb{Z}_4^r$ *и* $y \in \mathbb{Z}_4^k$ *для целых* $r,k \geqslant 1$. *Кватернарная функция* $f(x,y) = f_1(x) \oplus f_2(y)$ *– кватернарная бент-функция от* $r+k$ *переменных тогда и только тогда, когда функции* f_1 *и* f_2 *– кватернарные бент-функции от* r *и* k *переменных соответственно.*

Доказательство этого утверждения приведено в [83].

Данное обобщение было предложено в работе [51]. Этому обобщению бент-функций посвящены следующие работы [16; 42; 45; 46; 51; 65; 83].

Подробнее об этих и других обобщениях можно прочитать в обзорной работе Н. Н. Токаревой [10].

1.5 Проблема о разложении булевых функций в сумму двух бент-функций

В [86] была представлена следующая гипотеза.

Гипотеза 1. *Пусть* n *– целое четное число. Тогда любая булева функция от* n *переменных степени не больше* $n/2$ *может быть разложена в сумму двух бент-функций от* n *переменных.*

Отметим, что ограничение на степень следует из Леммы 11. В работе [86] Гипотеза 1 была проверена с помощью полного перебора для $n \leqslant 6$. Согласно [86], если Гипотеза 1 верна, то справедлива следующая нижняя оценка для числа бент-функций от n переменных:

$$| \mathcal{B}_n | \geqslant 2^{2^{n-2}+\frac{1}{4}\binom{n}{n/2}}.$$

Отметим также, что справедливость представленной гипотезы будет свидетельствовать о многообразии класса бент-функций, поскольку разнообразными являются булевы функции степени не больше $n/2$.

В [77] гипотеза была доказана для квадратичных функций и некоторых классов бент-функций, среди которых бент-функции из класса Мэйорана–МакФарланда.

Утверждение 1. *Пусть* $n \geqslant 4$ *– целое положительное число. Справедливы следующие утверждения:*

1. *любая булева бент-функция от n переменных из класса Мэйорана–МакФарланда раскладывается в сумму двух бент-функций от n переменных;*
2. *любая квадратичная булева функция от n переменных представляется как сумма двух бент-функций от n переменных;*

Доказательство этого утверждения приведено в [77].

Известно, что все бент-функции от восьми переменных степени 3 могут быть получены из функций класса Мэйорана–МакФарланда с помощью аффинного преобразования переменных и добавлением некоторой аффинной функции [33]. Таким образом, из Утверждения 1 и Леммы 14 следует, что все бент-функции от 8 переменных степени не больше 3 раскладываются в сумму двух бент-функций.

Также разложению дуальных бент-функций в сумму двух бент-функций посвящена работа [11]. Отметим, что данная проблема упоминатеся в обзорной работе [22], которая посвящена результатам исследования бент-функций за последние 40 лет.

Отметим, что Гипотеза 1 может быть представлена следующим образом: АНФ любой булевой функции от n переменных степени не больше $n/2$ разделяется на две части, каждая из которых — часть АНФ некоторой бент-функции от n переменных.

Таким образом, проблема о разложении булевых функций в сумму двух бент-функций связана со следующей гипотезой: произвольная однородная булева функция от четного числа n переменных степени $k \leqslant n/2$ является однородной k-частью АНФ некоторой бент-функции от n переменных, где однородная k-часть АНФ функции f – все мономы степени k функции f. Эта гипотеза была представлена и доказана для квадратичных функций в работе 2022 года [88]. Интересно, что обе гипотезы верны для квадратичных функций.

Однородным бент-функциям посвящены, например, работы [27; 66; 76; 90].

1.6 Гипотеза о производных бент-функций

В этом разделе мы представим известную гипотезу о производных бент-функций.

Из Леммы 15 следует, что производная произвольной бент-функции по любого ненулевому направлению является уравновешенной функцией. Это приводит к вопросу о том, всякая ли уравновешенная функция, которая является производной булевой функции, является производной бент-функции. Другими словами, можно сформулировать следующую гипотезу, которая была впервые сформулирована в [12].

Гипотеза. *Любая уравновешенная булева функция f от четного числа n переменных степени не больше $n/2-1$ такая, что $f(x)=f(x\oplus y)$ для любого $x\in\mathbb{Z}_2^n$ и некоторого ненулевого $y\in\mathbb{Z}_2^n$, является производной бент-функции от n переменных.*

В [12] указано, что гипотеза верна для четного числа $n\leqslant 6$ переменных. Покажем откуда следуют ограничения на уравновешенные функции из условия гипотезы. Из Лемм 1 и11 следует, что для любой бент-функции $f\in\mathcal{B}_n$ справедливо, что $\deg(D_yf)\leqslant n/2-1$. Согласно Лемме 2, условие $f(x)=f(x\oplus y)$ для любого $x\in\mathbb{Z}_2^n$ и некоторого ненулевого $y\in\mathbb{Z}_2^n$ является необходимым и достаточным условием того, что $f\in\mathcal{F}_n$ является производной некоторой булевой функции от n переменных.

Тот факт, что множество всех производных бент-функций покрывает множество всех уравновешенных функций, удовлетворяющих условиям гипотезы, свидетельствует о том, что множество всех бент-функций разнообразно, поскольку разнообразным является множество уравновешенных функций. Как будет показано дальше, изучение производных бент-функций может привести к получению оценок числа бент-функций.

В работе [73] В. Н. Потапов показал, что для достаточно больших n найдутся уравновешенные функции, которые удовлетворяют условию гипотезы, но не являются производными бент-функций. Поэтому мы предлагаем следующее уточнение гипотезы о производных бент-функций.

Гипотеза 2. *Любая уравновешенная булева функция f от четного числа n переменных степени не больше $n/2-1$, которая линейно зависит хотя бы от одной*

из своих переменных, такая, что $f(x) = f(x \oplus y)$ *для любого* $x \in \mathbb{Z}_2^n$ *и некоторого ненулевого* $y \in \mathbb{Z}_2^n$*, является производной бент-функции от* n *переменных.*

В дальнейшем будет доказано, что между Гипотезой 2 и проблемой о разложении булевых функций в сумму двух бент-функций существует связь. Отметим, что гипотеза о разложении булевых функций в сумму двух бент-функций верна для квадратичных функций, а справделивость гипотезы о производных бент-функций для квадратичных функций будет доказана в данной работе.

Глава 2. Конструкция уравновешенных функций с высокой нелинейностью и другими криптографическими свойствами

Эта глава посвящена построению уравновешенных функций с высокой нелинейностью. Мы приводим итеративную конструкцию, позволяющую строить уравновешенные булевы функции от четного числа переменных $n \geqslant 18$ с нелинейностью $2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$ без линейных структур. Результаты главы опубликованы в работе [94].

2.1 Уравновешенные функции с высокой нелинейностью

Как уже отмечалось ранее, бент-функции не являются уравновешенными. В связи с этим известной задачей является поиск и построение уравновешенных функций с высокой нелинейностью.

Максимальные значения нелинейности уравновешенных функций неизвестны для $n > 7$. В работе [81] была приведена следующая верхняя оценка нелинейности уравновешенных функций от четного числа переменных.

Утверждение 2. *Пусть $n \geqslant 4$ – четное целое число и f – уравновешенная булева функция от n переменных. Тогда $N_f \leqslant 2^{n-1} - 2^{\frac{n}{2}-1} - 2$.*

Одним из методов получения уравновешенных функций с высокой нелинейностью является преобразование бент-функций, при котором высокое значение нелинейности функции сохраняется, а функция становится уравновешенной. Такому методу посвящены, например, работы [34; 35]. Уравновешенным функциям с высокой нелинейностью также посвящены следующие работы [26; 34; 35; 40; 47; 70; 81].

2.2 Конструкция булевых функций, производная которых линейно зависит от некоторой своей переменной

В данном разделе мы представим конструкцию булевых функций, производная которых по некоторому ненулевому направлению линейно зависит от некоторой своей переменной. Данная конструкция имеет управляемую производную и позволяет строить все булевы функции, имеющие в качестве своей производной по некоторому ненулевому направлению функцию, которая линейно зависит хотя бы от одной из своих переменных. Для $n = 4$ и $n = 6$ мы покажем, что множество функций, которые можно построить с помощью данной конструкции, содержит уравновешенные функции с высокой нелинейностью.

Мы предлагаем следующую итеративную конструкцию булевых функций, которая является ключевой для данной работы.

Конструкция 1. *Пусть $g_1, g_2 \in \mathcal{F}_n$, $h \in \mathcal{F}_{n+2}$ и вектор $y \in \mathbb{Z}_2^n$. Будем строить функцию $f \in \mathcal{F}_{n+2}$ следующим образом:*

$$f(x,x_{n+1},x_{n+2}) = \big((D_y g_1(x) \oplus 1)h(x,x_{n+1},x_{n+2}) \oplus D_y g_2(x)\big)x_{n+1} \\ \oplus g_1(x)h(x,x_{n+1},x_{n+2}) \oplus g_2(x), \tag{2.1}$$

где $x \in \mathbb{Z}_2^n, x_{n+1}, x_{n+2} \in \mathbb{Z}_2$.

Функции g_1, g_2, h и вектор y будем считать параметрами конструкции.

Следующее утверждение показывает, что Конструкция 1 позволяет строить все булевы функции, имеющие в качестве своей производной по некоторому ненулевому направлению функцию, которая линейно зависит хотя бы от одной из своих переменных.

Утверждение 3. *Пусть $n \geqslant 2$ – четное целое число, функции g_1, g_2, $h_1 \in \mathcal{F}_n$, вектор $(y,1,y_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $h(x,x_{n+1},x_{n+2}) = (D_y h_1(x) \oplus y_{n+2})x_{n+1} \oplus h_1(x) \oplus x_{n+2}$. Тогда любая функция $f \in \mathcal{F}_{n+2}$, которая имеет h своей производной по направлению $(y,1,y_{n+2})$, имеет представление из Конструкции 1. При этом для $(a,a_{n+1},a_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $c = \langle a,y\rangle \oplus a_{n+1} \oplus a_{n+2}y_{n+2}$ справедливо*

$$W_f(a,a_{n+1},a_{n+2}) = (-1)^{c\cdot a_{n+2}} \cdot 2 \cdot W_{cg_1 \oplus g_2 \oplus a_{n+2}h_1}(a).$$

Кроме того, для различных параметров (g_1, g_2) получаются различные функции f.

Доказательство. Заметим, что $D_{(y,1,y_{n+2})}h(x,x_{n+1},x_{n+2}) = 0$ для любого $(x,x_{n+1},x_{n+2}) \in \mathbb{Z}_2^{n+2}$. Из Леммы 2 следует, что h является производной булевой функции по направлению $(y,1,y_{n+2})$. Для любой функции $f \in \mathcal{F}_{n+2}$, которая имеет h своей производной по направлению $(y,1,y_{n+2})$, справедливо

$$f(x,x_{n+1},x_{n+2}) \oplus f(x \oplus y,x_{n+1} \oplus 1,x_{n+2} \oplus y_{n+2}) = h(x,x_{n+1},x_{n+2}). \tag{2.2}$$

Поскольку $h(x,x_{n+1},x_{n+2}) = h(x \oplus y,x_{n+1} \oplus 1, x_{n+2} \oplus y_{n+2})$, мы получаем, что

$$h(x,x_{n+1},x_{n+2}) = 1 \iff h(x \oplus y,x_{n+1} \oplus 1, x_{n+2} \oplus y_{n+2}) = 1. \tag{2.3}$$

Если $h(x,x_{n+1},x_{n+2}) = 1$, то, поскольку h линейно зависит от переменной x_{n+2}, имеем $h(x,x_{n+1},x_{n+2} \oplus 1) = 0$. Тогда из (2.3) следует, что

$$\begin{aligned}
&\{x : \exists x_{n+2} \in \mathbb{Z}_2 \text{ такой, что } h(x,0,x_{n+2}) = 0\}\\
=&\{x : \exists x_{n+2} \in \mathbb{Z}_2 \text{ такой, что } h(x,0,x_{n+2}) = 1\}\\
=&\{x : \exists x_{n+2} \in \mathbb{Z}_2 \text{ такой, что } h(x,1,x_{n+2}) = 0\}\\
=&\{x : \exists x_{n+2} \in \mathbb{Z}_2 \text{ такой, что } h(x,1,x_{n+2}) = 1\} = \mathbb{Z}_2^n.
\end{aligned} \tag{2.4}$$

Таким образом, из (2.2) и (2.4) следует, что любая булева функция f, для которой $D_{(y,1,y_{n+2})}f(x,x_{n+1},x_{n+2}) = h(x,x_{n+1},x_{n+2})$, имеет следующее представление:

$$\begin{cases}
f(x,0,x_{n+2}) = f_1(x), & \text{если } h(x,0,x_{n+2}) = 1,\\
f(x,1,x_{n+2}) = f_1(x \oplus y) \oplus 1, & \text{если } h(x,1,x_{n+2}) = 1,\\
f(x,0,x_{n+2}) = f_2(x), & \text{если } h(x,0,x_{n+2}) = 0,\\
f(x,1,x_{n+2}) = f_2(x \oplus y), & \text{если } h(x,1,x_{n+2}) = 0,
\end{cases} \tag{2.5}$$

где f_1 и f_2 – произвольные функции от n переменных. Следовательно, перебирая все возможные f_1 и f_2, мы получим все различные булевы функции от $n+2$ переменных, которые имеют $h(x,x_{n+1},x_{n+2})$ своими производными по направлению $(y,1,y_{n+2})$.

Положим, что $g_1 = f_1 \oplus f_2$ и $g_2 = f_2$. Несложно проверить, что из представления (2.5) следует, что f имеет представление из Конструкции 1.

Отметим, что для $(x,x_{n+1},x_{n+2}) \in \mathbb{Z}_2^{n+2}$ выполняется

$$x_{n+2} = h(x,x_{n+1},x_{n+2}) \oplus (D_y h_1(x) \oplus y_{n+2})x_{n+1} \oplus h_1(x). \tag{2.6}$$

Теперь проверим, чему равны коэффициенты Уолша–Адамара функции f для каждого $(a,a_{n+1},a_{n+2}) \in \mathbb{Z}_2^{n+2}$.

Заметим, что

$$\langle (x,x_{n+1},x_{n+2}),(a,a_{n+1},a_{n+2})\rangle = \langle a,x\rangle \oplus a_{n+1}x_{n+1} \oplus a_{n+2}x_{n+2}.$$

Тогда из (2.2) следует, что

$$\begin{aligned}
&W_f(a,a_{n+1},a_{n+2}) \\
&= \sum_{(x,x_{n+1},x_{n+2})\in\mathbb{Z}_2^{n+2}} (-1)^{f(x,x_{n+1},x_{n+2})\oplus\langle (x,x_{n+1},x_{n+2}),(a,a_{n+1},a_{n+2})\rangle} \\
&= \sum_{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}} \Big((-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}} \\
&+ (-1)^{f(x\oplus y,1,x_{n+2}\oplus y_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}\oplus\langle a,y\rangle\oplus a_{n+1}\oplus a_{n+2}y_{n+2}} \Big) \\
&= \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2} \\ h(x,0,x_{n+2})=1}} \Big((-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}} \\
&+ (-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}\oplus\langle a,y\rangle\oplus a_{n+1}\oplus a_{n+2}y_{n+2}\oplus 1} \Big) \\
&+ \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2} \\ h(x,0,x_{n+2})=0}} \Big((-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}} \\
&+ (-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}\oplus\langle a,y\rangle\oplus a_{n+1}\oplus a_{n+2}y_{n+2}} \Big).
\end{aligned}$$

Допустим, что $\langle a,y\rangle \oplus a_{n+1} \oplus a_{n+2}y_{n+2} = 0$. Тогда

$$W_f(a,a_{n+1},a_{n+2}) = 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2} \\ h(x,0,x_{n+2})=0}} (-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}}.$$

Из (2.4) и (2.5) следует, что если $a_{n+2} = 0$, тогда

$$\begin{aligned}
W_f(a,a_{n+1},0) &= 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2} \\ h(x,0,x_{n+2})=0}} (-1)^{f_2(x)\oplus\langle a,x\rangle} \\
&= 2 \cdot \sum_{x\in\mathbb{Z}_2^n} (-1)^{f_2(x)\oplus\langle a,x\rangle} = 2 \cdot W_{f_2}(a) = 2 \cdot W_{g_2}(a).
\end{aligned}$$

Если $a_{n+2} = 1$, тогда из (2.5) и (2.6) следует, что

$$W_f(a,a_{n+1},1) = 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} (-1)^{f_2(x)\oplus\langle a,x\rangle\oplus x_{n+2}}$$
$$= 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} (-1)^{f_2(x)\oplus\langle a,x\rangle\oplus h_1(x)}.$$

Тогда согласно (2.4) справедливо

$$W_f(a,a_{n+1},1) = 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} (-1)^{f_2(x)\oplus\langle a,x\rangle\oplus h_1(x)}$$
$$= 2 \cdot \sum_{x\in\mathbb{Z}_2^n} (-1)^{f_2(x)\oplus h_1(x)\oplus\langle a,x\rangle} = 2 \cdot W_{f_2\oplus h_1}(a) = 2 \cdot W_{g_2\oplus h_1}(a).$$

Теперь пусть $\langle a,y\rangle \oplus a_{n+1} \oplus a_{n+2}y_{n+2} = 1$. Тогда

$$W_f(a,a_{n+1},a_{n+2}) = 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}}.$$

Из (2.4) и (2.5) следует, что если $a_{n+2} = 0$, тогда

$$W_f(a,a_{n+1},0) = 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f_1(x)\oplus\langle a,x\rangle}$$
$$= 2 \cdot \sum_{x\in\mathbb{Z}_2^n} (-1)^{f_1(x)\oplus\langle a,x\rangle} = 2 \cdot W_{f_1}(a) = 2 \cdot W_{g_1\oplus g_2}(a).$$

Если $a_{n+2} = 1$, тогда из (2.5) и (2.6) следует, что

$$W_f(a,a_{n+1},1) = 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f_1(x)\oplus\langle a,x\rangle\oplus x_{n+2}}$$
$$= 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f_1(x)\oplus h_1(x)\oplus\langle a,x\rangle\oplus 1}.$$

Тогда согласно (2.4) справедливо

$$W_f(a,a_{n+1},1) = 2 \cdot \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f_1(x)\oplus h_1(x)\oplus\langle a,x\rangle\oplus 1}$$
$$= 2 \cdot \sum_{x\in\mathbb{Z}_2^n} (-1)^{f_1(x)\oplus h_1(x)\oplus\langle a,x\rangle\oplus 1} = -2 \cdot W_{f_1\oplus h_1}(a) = -2 \cdot W_{g_1\oplus g_2\oplus h_1}(a).$$

□

Отметим, что произвольная функция $h \in \mathcal{F}_{n+2}$, которая линейно зависит от переменной x_{n+2}, может быть представлена следующим образом: $h(x,x_{n+1},x_{n+2}) = h_2(x)x_{n+1} \oplus h_1(x) \oplus x_{n+2}$, где $h_1, h_2 \in \mathcal{F}_n$ и $x \in \mathbb{Z}_2^n$. Тогда из Леммы 2 функция h является производной некоторой функции по направлению $(y,1,y_{n+2})$ тогда и только тогда, когда $D_{(y,1,y_{n+2})}h(x,x_{n+1},x_{n+2}) = 0$. Откуда несложно получить, что $h_2(x) = D_y h_1(x) \oplus y_{n+2}$. Таким образом, Утверждение 3 описывает все функции от n переменных, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных.

Полным перебором было проверено, что для $n = 4$ множество всех функций, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных, состоит из 28896 функций. Это множество содержит все 896 бент-функций от 4 переменных. Кроме того, все 10920 уравновешенных функций от 4 переменных, которые имеют нелинейность 4 – максимальное значение нелинейности уравновешенных функций от 4 переменных, имеют производную по некоторому ненулевому направлению, которая линейно зависит хотя бы от одной из своих переменных. Более того, все уравновешенные функции, производная которых по некоторому ненулевому направлению зависит линейно хотя бы от одной из своих переменных, имеют нелинейность равную 4.

Булева функция от шести переменных

$$x_3x_4x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_2x_5x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_4$$

является уравновешенной и имеет нелинейность 24, тогда как верхняя оценка нелинейности для уравновешенных функций от четного числа переменных из Утверждения 2 дает 26. Ее производная по направлению $(1,0,\ldots,0)$ является аффинной. Отметим, что оценка 26 нелинейности уравновешенных функций от шести переменных достижима [81].

Таким образом, для $n = 6$ существует уравновешенная функция, производная которой по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных, с нелинейностью на два меньше, чем значение оценки нелинейности из Утверждения 2. Более того, можно доказать следующий факт.

Утверждение 4. *Пусть $n \geqslant 4$ – четное целое число и $f \in \mathcal{F}_{n+2}$, производная которой по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных. Тогда $N_f \leqslant 2^{n+1} - 2^{\frac{n}{2}} - 4$.*

Доказательство. Из Утверждения 3 известно, что f имеет форму (2.1) и $W_f(0) = W_{g_2}(0)$. Из Леммы 6 следует, что g_2 из (2.1) является уравновешенной функцией от n переменных. Тогда из Утверждения 2 имеем $N_{g_2} \leqslant 2^{n-1} - 2^{\frac{n}{2}-1} - 2$ и, таким образом, из Леммы 10 следует $\max\limits_{a \in \mathbb{Z}_2^n} |W_{g_2}| \geqslant 2^{\frac{n}{2}} + 4$.

Тогда из Утверждения 3 следует, что $\max\limits_{a \in \mathbb{Z}_2^{n+2}} |W_f(a)| \geqslant 2(2^{\frac{n}{2}} + 4)$. Следовательно, из Леммы 10 следует $N_f \leqslant 2^{n+1} - 2^{\frac{n}{2}} - 4$. □

2.3 Криптографические свойства булевых функций, которые имеют аффинные производные

В данном разделе мы рассмотрим частный случай Конструкции 1 – итеративную конструкцию функций, которые имеют аффинные производные. Мы также приводим достаточные условия, при которых функции, полученные с помощью этой конструкции, будут обладать такими криптографическими свойствами, как уравновешенность, отсутствие линейных структур и корреляционная иммунность.

Утверждение 5. *Пусть $n \geqslant 2$ – четное целое число, g_1, $g_2 \in \mathcal{F}_n$, $y, b \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$ и $h(x,x_{n+1},x_{n+2}) = \langle b,x \rangle \oplus c \oplus x_{n+2}$. Тогда для функции $f \in \mathcal{F}_{n+2}$, построенной с помощью Конструкции 1, справедливо, что*

1. *функция f является уравновешенной функцией от $n+2$ переменных тогда и только тогда, когда g_2 – уравновешенная функция от n переменных;*
2. $N_f = 2^{n+1} - \max\limits_{a \in \mathbb{Z}_2^n, g \in \{g_2, g_1 \oplus g_2\}} |W_g(a)|$;
3. *если g_2 и $g_1 \oplus g_2$ являются корреляционно -иммунными порядка r функциями от n переменных, то булева функция f является корреляционно-иммунной порядка r.*

Доказательство. Пусть $\ell_1(x) = \langle b,x\rangle \oplus c$, где $x \in \mathbb{Z}_2^n$. Можно убедиться, что $D_y\ell_1(x) = \langle b,y\rangle$ для любого $x \in \mathbb{Z}_2^n$. Пусть $y_{n+2} = \langle b,y\rangle$. Тогда

$$h(x,x_{n+1},x_{n+2}) = (D_y\ell_1(x) \oplus y_{n+2})x_{n+1} \oplus \ell_1(x) \oplus x_{n+2}.$$

Из Утверждения 3 и Леммы 4 для $f \in \mathcal{F}_{n+2}$ из (2.1) следует, что

$$|W_f(a,a_{n+1},a_{n+2})|$$
$$= \begin{cases} 2 \cdot |W_{g_2}(a)|, & \text{если } \langle a,y\rangle = a_{n+1} \text{ и } a_{n+2} = 0, \\ 2 \cdot |W_{g_2}(a \oplus b)|, & \text{если } \langle a,y\rangle = a_{n+1} \oplus y_{n+2} \text{ и } a_{n+2} = 1, \\ 2 \cdot |W_{g_1 \oplus g_2}(a)|, & \text{если } \langle a,y\rangle = a_{n+1} \oplus 1 \text{ и } a_{n+2} = 0, \\ 2 \cdot |W_{g_1 \oplus g_2}(a \oplus b)|, & \text{если } \langle a,y\rangle = a_{n+1} \oplus y_{n+2} \oplus 1 \text{ и } a_{n+2} = 1. \end{cases}$$

Тогда $W_f(\mathbf{0}) = W_{g_2}(0)$ и первое утверждение следует из Леммы 6. Второе утверждение следует из Леммы 10, а третье из Леммы 9. □

Теперь приведем достаточные условия для того, чтобы функции из Конструкции 1 не имели линейных структур.

Утверждение 6. *Пусть $n \geqslant 2$ – четное целое число, g_1, g_2 – булевы функции от n переменных, $y \in \mathbb{Z}_2^n$ и $h(x,x_{n+1},x_{n+2}) = \ell_1(x) \oplus x_{n+2}$, где $\ell_1 \in \mathcal{A}_n$. Тогда если g_2 и $g_1 \oplus g_2$ являются уравновешенной функцией и бент-функцией от n переменных соответственно, то булева функция $f \in \mathcal{F}_{n+2}$, построенная с помощью Конструкции 1, является уравновешенной и не имеет линейных структур.*

Доказательство. Рассмотрим производную функции f из (2.1) по направлению $(z,z_{n+1},z_{n+2}) \in \mathbb{Z}_2^{n+2}$.

$$D_{(z,z_{n+1},z_{n+2})}f(x,x_{n+1},x_{n+2}) = \big((D_yg_1(x) \oplus 1)(\ell_1(x) \oplus x_{n+2}) \oplus D_yg_2(x)\big)x_{n+1}$$
$$\oplus g_1(x)(\ell_1(x) \oplus x_{n+2}) \oplus g_2(x)$$
$$\oplus\big((D_yg_1(x \oplus z) \oplus 1)(\ell_1(x \oplus z) \oplus x_{n+2} \oplus z_{n+2}) \oplus D_yg_2(x \oplus z)\big)x_{n+1}$$
$$\oplus\big((D_yg_1(x \oplus z) \oplus 1)(\ell_1(x \oplus z) \oplus x_{n+2} \oplus z_{n+2}) \oplus D_yg_2(x \oplus z)\big)z_{n+1}$$
$$\oplus g_1(x \oplus z)(\ell_1(x \oplus z) \oplus x_{n+2} \oplus z_{n+2}) \oplus g_2(x \oplus z).$$

Пусть $\ell_1(x \oplus z) = \ell_1(x) \oplus d$, где $d \in \mathbb{Z}_2$. Заметим, что если $z = \mathbf{0}$, то $d = 0$. Тогда

$$D_{(z,z_{n+1},z_{n+2})}f(x,x_{n+1},x_{n+2}) = x_{n+1}x_{n+2}\big(D_zD_yg_1(x)\big)$$

$$\oplus x_{n+1}\big(\ell_1(x)D_zD_yg_1(x)\oplus(z_{n+2}\oplus d)D_yg_1(x\oplus z)\oplus D_zD_yg_2(x)\oplus z_{n+2}\oplus d\big)$$
$$\oplus x_{n+2}\big(D_zg_1(x)\oplus z_{n+1}\cdot(D_yg_1(x\oplus z)\oplus 1)\big)\oplus\ell_1(x)D_zg_1(x)$$
$$\oplus z_{n+1}\cdot(D_yg_1(x\oplus z)\oplus 1)\ell_1(x)\oplus z_{n+1}\cdot d\cdot(D_yg_1(x\oplus z)\oplus 1)$$
$$\oplus z_{n+1}\cdot D_yg_2(x\oplus z)\oplus z_{n+1}\cdot z_{n+2}\cdot(D_yg_1(x\oplus z)\oplus 1)$$
$$\oplus(z_{n+2}\oplus d)g_1(x\oplus z)\oplus D_zg_2(x).$$

Докажем, что для любого ненулевого направления (z,z_{n+1},z_{n+2}) функция $D_{(z,z_{n+1},z_{n+2})}f$ не является константой. Предположим обратное. Пусть $D_{(z,z_{n+1},z_{n+2})}f\equiv\text{const}$ для $(z,z_{n+1},z_{n+2})\neq(0,\dots,0)$.

Пусть $z_{n+1}=0$. Тогда $D_zg_1(x)=0$. Если $z_{n+2}=d$, то $z\neq\mathbf{0}$. Тогда $D_{(z,0,d)}f$ имеет слагаемое $D_zg_2(x)=D_z\big(g_1(x)\oplus g_2(x)\big)$, которое не является константой согласно Лемме 15.

Если $z_{n+2}=d\oplus 1$, то $D_{(z,0,d\oplus1)}f$ имеет слагаемое

$$g_1(x\oplus z)\oplus g_2(x\oplus z)\oplus g_2(x),$$

которое для любого z не является константой, поскольку $g_2(x)$ и $g_2(x)\oplus 1$ являются уравновешенными, а $g_1(x\oplus z)\oplus g_2(x\oplus z)$ является бент-функцией согласно Лемме 14.

Пусть $z_{n+1}=1$. Тогда

$$D_zg_1(x)=D_yg_1(x\oplus z)\oplus 1.$$

Заметим, что если $y=z$, то равенство не выполняется.
Если $z_{n+2}=d$, то $D_{(z,1,d)}f$ имеет слагаемое

$$D_yg_2(x\oplus z)\oplus D_zg_2(x)=D_y\big(g_1(x\oplus z)\oplus g_2(x\oplus z)\big)\oplus D_z\big(g_1(x)\oplus g_2(x)\big)\oplus 1$$
$$=D_{y\oplus z}\big(g_1(x)\oplus g_2(x)\big)\oplus 1,$$

которое для $y\neq z$ не является константой согласно Лемме 15.
Если $z_{n+2}=d\oplus 1$, то $D_{(z,1,d\oplus1)}f$ имеет слагаемое

$$g_1(x\oplus y\oplus z)\oplus D_yg_2(x\oplus z)\oplus D_zg_2(x)\oplus 1$$
$$=g_1(x\oplus y\oplus z)\oplus g_2(x\oplus y\oplus z)\oplus g_2(x)\oplus 1,$$

которое для любого z не является константой, поскольку $g_2(x)$ и $g_2(x)\oplus1$ являются уравновешенными, а $g_1(x\oplus y\oplus z)\oplus g_2(x\oplus y\oplus z)$ является бент-функцией согласно Лемме 14. Тогда $D_{(z,z_{n+1},z_{n+2})}f\not\equiv\text{const}$ для любого $(z,z_{n+1},z_{n+2})\neq(0,\dots,0)$.

Пусть $\ell_1(x) = \langle b,x\rangle \oplus c$, где $b \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$. Из Утверждения 5 следует, что f – уравновешенная. □

В следующей теореме мы используем Утверждения полученные выше, чтобы описать параметры Консрукции 1, при которых функции будут обладать рядом криптографических свойств.

Теорема 1. *Пусть g_1, $g_2 \in \mathcal{F}_n$, $y \in \mathbb{Z}_2^n$ и $h(x,x_{n+1},x_{n+2}) = \langle b,x\rangle \oplus c \oplus x_{n+2}$ для любого $x \in \mathbb{Z}_2^n$, где $b \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$. Тогда для функции $f \in \mathcal{F}_{n+2}$ из Конструкции 1 справедливо, что*

1. *функция f имеет h своей производной по направлению $(y,1,\langle b,y\rangle)$;*
2. *функция f — уравновешенная функция тогда и только тогда, когда g_2 – уравновешенная функция;*
3. $N_f = 2^{n+1} - \max\limits_{a\in\mathbb{Z}_2^n, g\in\{g_2, g_1\oplus g_2\}} |W_g(a)|$;
4. *если g_2 и $g_1 \oplus g_2$ — корреляционно-иммунные порядка r, то функция f является корреляционно-иммунной порядка r.*
5. *если g_2 и $g_1 \oplus g_2$ — уравновешенная функция и бент-функция соответственно, то функция f — уравновешенная без линейных структур.*

Доказательство. Пусть $f \in \mathcal{F}_{n+2}$ построена с помощью Конструкции 1. Проверим чему равна производная f по направлению $(y,1,\langle b,y\rangle)$. Если $\ell_1(x) = \langle b,x\rangle \oplus c$, то $\ell_1(x \oplus y) = \langle b,x\rangle \oplus c \oplus \langle b,y\rangle$. Тогда

$$D_{(y,1,\langle b,y\rangle)}f(x,x_{n+1},x_{n+2}) = \big((D_yg_1(x) \oplus 1)(\ell_1(x) \oplus x_{n+2}) \oplus D_yg_2(x)\big)x_{n+1}$$

$$\oplus g_1(x)(\ell_1(x) \oplus x_{n+2}) \oplus g_2(x)$$

$$\oplus\big((D_yg_1(x \oplus y) \oplus 1)(\ell_1(x) \oplus x_{n+2} \oplus \langle b,y\rangle \oplus \langle b,y\rangle) \oplus D_yg_2(x \oplus y)\big)x_{n+1}$$

$$\oplus(D_yg_1(x \oplus y) \oplus 1)(\ell_1(x) \oplus x_{n+2} \oplus \langle b,y\rangle \oplus \langle b,y\rangle) \oplus D_yg_2(x \oplus y)$$

$$\oplus g_1(x \oplus y)(\ell_1(x) \oplus x_{n+2} \oplus \langle b,y\rangle \oplus \langle b,y\rangle) \oplus g_2(x \oplus y) =$$

$$= \ell_1(x) \oplus x_{n+2} = h(x,x_{n+1},x_{n+2}).$$

Из Утверждения 5 следуют второе, третье и четвертое утверждение теоремы. Пятое утверждение следует из Утверждения 6. □

В следующем разделе мы испольуем Теорему 1 для построения уравновешенных функций с высокой нелинейностью без линейных структур.

2.4 Построение уравновешенных функций с высокой нелинейностью

Этот раздел посвящен построению уравновешенных функций с высокой нелинейностью. Мы используем итеративную Конструкцию 1 и уравновешенную функцию от 16 переменных с высокой нелинейностью, представленную в [40], для построения уравновешенных функций от четного числа переменных $n \geqslant 18$ без линейных структур с нелинейностью $2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$. Также мы сравниваем полученные значения нелинейности уравновешенных функций с верхней оценкой нелинейности из Утверждения 2, а также со значениями нелинейности уравновешенных функций, полученных в других работах.

В [40] было показано, как построить уравновешенную функцию от 16 переменных с нелинейностью 32 598. Обозначим эту функцию f_{16}.

Пусть $\sigma_{2,16}$ – булева функция от 16 переменных, которая содержит все квадратичные слагаемые и только их, и $f_q = \sigma_{2,16} \oplus \bigoplus_{i=1}^{n/2} x_i$. Тогда f_{16} можно задать с помощью ее носителя: $\mathrm{supp}(f_{16}) = \mathrm{supp}(f_q) \cup S$, где

$$S = \{8256, 2080, 4112, 2049, 36912, 5264, 34840, 10264, 49169, 38400, 1632,$$

$$3075, 2570, 16800, 16908, 1569, 24612, 12417, 29504, 17825, 37413, 18965,$$

$$41410, 16613, 5028, 35122, 21656, 61968, 42122, 8000, 24873, 9546, 21541,$$

$$10763, 35881, 57372, 45256, 42033, 37524, 19529, 7237, 16446, 17888, 20881,$$

$$26817, 49539, 14964, 54452, 51612, 22981, 20723, 989, 46868, 50830, 11884,$$

$$1518, 5363, 36553, 43729, 39321, 50459, 55401, 37771, 52359, 5965, 8511,$$

$$18551,58538, 14987, 53799, 44090, 10156, 29283, 27057, 58443, 61497,$$

$$35782, 44047,22940, 7540, 19865, 43961, 15221, 62179, 43927, 57240, 59741,$$

$$61867, 14190,62511, 44665, 3067, 8107, 61937, 51161, 42937, 31835, 44725,$$

$$30435, 14324, 30381,31964, 56506, 54652, 59951, 61206, 43993, 14310, 58959,$$

$$32494, 24443, 32381,62451, 60915, 60381, 44990, 62845, 36351, 32508, 61147,$$

$$56309, 32351, 48503, 57215, 32751, 63483, 64510, 65535\}$$

и каждому числу из S ставится в соответствие вектор его двоичного представления длины 16.

Далее приведем итеративный метод построения уравновешенных функций от четного числа $n \geqslant 18$ переменных с высокой нелинейностью без линейных структур.

Метод 1. *Будем строить булевы функции от n переменных с помощью Конструкции 1 со следующими параметрами:*

- *при $n = 18$ функция $g_2 = f_{16}$;*
- *при $n \geqslant 20$ функция g_2 — функция f из Конструкции 1, полученная с помощью Метода 1 на предыдущем шаге;*
- *функция $h(x,x_{n+1},x_{n+2}) = \langle b,x\rangle \oplus c \oplus x_{n+2}$ для любого $x \in \mathbb{Z}_2^n$, где $b \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$;*
- *функция g_1 такая, что $g_1 \oplus g_2$ — бент-функция;*
- *вектор $y \in \mathbb{Z}_2^n$ — произвольный.*

Теорема 2. *Функции от $n \geqslant 18$ переменных полученные с помощью Метода 1 являются уравновешенными функциями без линейных структур с нелинейностью $2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$.*

Доказательство. Из Лемм 3 и 13 имеем $\max\limits_{a\in\mathbb{Z}_2^{n-2}} |W_{g_2}(a)| \geqslant \max\limits_{a\in\mathbb{Z}_2^{n-2}} |W_{g_1\oplus g_2}(a)|$ для любого $a \in \mathbb{Z}_2^{n-2}$. Тогда $\max\limits_{a\in\mathbb{Z}_2^{n-2},g\in\{g_2,g_1\oplus g_2\}} |W_g(a)| = \max\limits_{a\in\mathbb{Z}_2^{n-2}} |W_{g_2}(a)|$. Из Леммы 10 следует, что $\max\limits_{a\in\mathbb{Z}_2^{n-2}} |W_{g_2}(a)| = 2^{n-2} - 2 \cdot N_{g_2}$. Таким образом, из Теоремы 1 и Леммы 10 имеем

$$N_f = 2 \cdot 2^{n-2} - 2^{n-2} + 2 \cdot N_{g_2} = 2^{n-2} + 2 \cdot N_{g_2}. \tag{2.7}$$

При $n = 18$ из Теоремы 1 и (2.7) функция f – уравновешенная и

$$N_f = 2^{n-2} + 2 \cdot 32\,598 = 2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7}).$$

При $n \geqslant 20$ мы получаем $N_{g_2} = 2^{n-3} - (2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4} + 2^{\frac{n}{2}-6} + 2^{\frac{n}{2}-8})$. Тогда из Теоремы 1 и (2.7) верно $N_f = 2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$ и при этом функция f является уравновешенной.

Отсутствие линейных структур следует из Теоремы 1. □

В Таблице 1 приводится сравнения значений нелинейности функций, которые можно получить с помощью Теоремы 2, со значениями нелинейности уравновешенных функций, полученных с помощью итеративных конструкций в

работах X. Hu и др. [47] и C. Carlet и др. [26] 2020 и 2022 года соответственно. Отметим, что в [47] рассматриваются $n \leqslant 28$. Также в таблице приводится сравнение с верхней оценкой нелинейности уравновешенных функций из Утверждения 2.

Таблица 1

n	$2^{n-1} - 2^{\frac{n}{2}-1} - 2$	N_f из Теоремы 2		N_f [47]	N_f [26]
18	130814	130732	>	130504	130688
20	523774	523608	>	523154	не приводится
22	2096126	2095792	>	2094980	не приводится
24	8386558	8385888	>	8384490	не приводится
26	33550334	33548992	>	33545992	не приводится
28	134209534	134206848	>	134201460	не приводится

Отметим, что если в Методе 1 при $n = 18$ в качестве g_2 использовать уравновешенную функцию от 16 переменных с большей нелинейностью, нелинейности получаемых с помощью Метода 1 функций будут выше. В работе [70] авторы используют эвристический алгоритм для нахождения уравновешенных функций от 16 переменных, нелинейность которых равна 32638, однако примеры таких функций не приводятся.

В следующей главе будет показано, что если в Теореме 1 в качестве функции g_2 взять бент-функцию, то мы получим бент-функцию. Таким образом, можно считать, что для получения нелинейных уравновешенных функций мы преобразуем бент-функции. Такому методу получения нелинейных уравновешенных функций путем модификации бент-функций посвящены, например, работы [34; 35].

Глава 3. Производные бент-функций

В данной главе предложена конструкция бент-функций, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных. Получено точное число бент-функций, имеющих некоторую отличную от константы аффинную функцию своей производной, а также итеративная нижняя оценка числа бент-функций, основанная на этом результате. Доказано, что любая квадратичная уравновешенная функция, которая может быть производной булевой функции, является производной бент-функции. Результаты главы опубликованы в работах [94; 95; 98; 99].

3.1 Связь с проблемой о разложении булевых функций в сумму двух бент-функций

В этом разделе мы покажем как гиптезы о производных бент-функций и о разложении булевых функций в сумму двух бент-функций связаны между собой.

В следующей теореме представлено необходимое и достаточное условие того, что функция, которая линейно зависит от некоторой своей переменной, является производной бент-функции. Кроме того, теорема представляет достаточное условие для того, чтобы функции, получаемые с помощью Конструкции 1, были бент-функциями.

Теорема 3. *Пусть $n \geqslant 2$ – четное целое число, функции g_1, g_2, $h_1 \in \mathcal{F}_n$, вектор $(y,1,y_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $h(x,x_{n+1},x_{n+2}) = (D_y h_1(x) \oplus y_{n+2})x_{n+1} \oplus h_1(x) \oplus x_{n+2}$. Тогда $f \in \mathcal{F}_{n+2}$ из Конструкции 1 является бент-функцией тогда и только тогда, когда g_2, $g_1 \oplus g_2$, $g_2 \oplus h_1$ и $g_1 \oplus g_2 \oplus h_1$ — бент-функции. При этом любая функция f от $n+2$ переменных, которая имеет h своей производной по направлению $(y,1,y_{n+2})$, имеет представление из Конструкции 1. Кроме того, для различных параметров (g_1, g_2) получаются различные бент-функции f.*

Доказательство. Из Лемм 3, 10 и Утверждения 3 следует, что

$$N_f = 2^{n+1} - \frac{1}{2} \max_{a \in \mathbb{Z}_2^{n+2}} |W_f(a)| = 2^{n+1} - 2^{n/2}$$

тогда и только тогда, когда для любого $b \in \mathbb{Z}_2^n$ справедливо

$$|W_{g_1 \oplus g_2}(b)| = |W_{g_2}(b)| = |W_{g_1 \oplus g_2 \oplus h_1}(b)| = |W_{g_2 \oplus h_1}(b)| = 2^{\frac{n}{2}}.$$

Из Леммы 13 следует, что g_2, $g_1 \oplus g_2$, $g_2 \oplus h_1$, $g_1 \oplus g_2 \oplus h_1$ являются бент-функциями от n переменных.

Второе утверждение следует из Утверждения 3. □

Далее докажем, что между проблемой о разложении булевых функций в сумму двух бент-функций и проблемой о производных бент-функций существует связь.

Утверждение 7. *Пусть $n \geqslant 2$ - целое положительное число. Произвольная булева функция от n переменных степени $d \geqslant 2$ раскладывается в сумму двух бент-функций от n переменных тогда и только тогда, когда любая уравновешенная функция от $n+2$ переменных степени d, которая линейно зависит от некоторой своей переменной и является производной некоторой булевой функции от $n+2$ переменных, является производной бент-функции от $n+2$ переменных.*

Доказательство. Обозначим через e_i вектор веса 1, i-я координата которого равна 1.

($\Rightarrow$) Пусть h является уравновешенной функцией от $n+2$ переменных степени d, которая линейно зависит от переменной x_j, а также является производной некоторой булевой функции. Из Леммы 2 следует, что существует ненулевой вектор $(y,y_{n+1},y_{n+2}) \in \mathbb{Z}_2^{n+2}$ такой, что $D_{(y,y_{n+1},y_{n+2})}h(x,x_{n+1},x_{n+2}) = 0$ для любого $(x,x_{n+1},x_{n+2}) \in \mathbb{Z}_2^{n+2}$. Если $(y,y_{n+1},y_{n+2}) = e_j$, тогда для всех $(x,x_{n+1},x_{n+2}) \in \mathbb{Z}_2^{n+2}$ верно, что $D_{(y,y_{n+1},y_{n+2})}h(x,x_{n+1},x_{n+2}) = 1$. Таким образом, существует индекс $i \neq j$ такой, что $y_i = 1$. Без ограничения общности, положем, что $i = n+1$ и $j = n+2$. Тогда $h(x,x_{n+1},x_{n+2}) = h_2(x)x_{n+1} \oplus h_1(x) \oplus x_{n+2}$, где $h_1, h_2 \in \mathcal{F}_n$.

Поскольку $D_{(y,1,y_{n+2})}h(x,x_{n+1},x_{n+2}) = 0$, справедливо, что $D_y h_2(x) = 0$ и $h_2(x \oplus y) = D_y h_1(x) \oplus y_{n+2}$ для любого $x \in \mathbb{Z}_2^n$.

Если $\deg(h_1) = 0$, тогда $\deg(h) < 2$. В случае если $\deg(h_1) > 0$, из Леммы 1 следует, что $\deg(D_y h_1) \leqslant \deg(h_1) - 1$. Следовательно, если $\deg(h_1) \leqslant d-1$, тогда $\deg(h) \leqslant d-1$. В обоих случаях приходим к противоречию, поскольку h имеет степень $d \geqslant 2$. Таким образом, $\deg(h_1) = d$ и из Теоремы 3 и того факта, что h_1 раскладывается в сумму двух бент-функций от n переменных, следует, что h является производной бент-функции по направлению (y,y_{n+1},y_{n+2}).

($\Leftarrow$) Пусть $h_1 \in \mathcal{F}_n$ и $\deg(h_1) = d$. Покажем, что булева функция $h(x,x_{n+1},x_{n+2}) = h_1(x) \oplus x_{n+2}$ степени d является уравновешенной. Можно заметить, что $|\mathrm{supp}(h)| = 2 \cdot (|\mathrm{supp}(h_1)| + 2^n - |\mathrm{supp}(h_1)|) = 2^{n+1}$.

Поскольку $D_{e_{n+1}}h(x,x_{n+1},x_{n+2}) = 0$ для любого $(x,x_{n+1},x_{n+2}) \in \mathbb{Z}_2^{n+2}$, из Леммы 2 следует, что h является производной булевой функции. Следовательно, из Теоремы 3 и того факта, что h является производной некоторой бент-функции от $n+2$ переменных, мы заключаем, что h_1 раскладывается в сумму двух бент-функций от n переменных. □

Далее используем Утверждение 7 для доказательства эквивалентности Гипотезы 1 и 2.

Теорема 4. *Гипотеза 1 и Гипотеза 2 являются эквивалентными.*

Доказательство. Из Леммы 14 следует, что Гипотеза 1 верная для аффинных функций при всех четных n.

Покажем, что Гипотеза 2 верна для аффинных функций. Пусть $n \geqslant 2$ – четное целое число и $h(x,x_{n+1},x_{n+2}) = \ell(x) \oplus cx_{n+1} \oplus x_{n+2}$, где $\ell \in \mathcal{A}_n$. Пусть h является производной некоторой функции по направлению $(y,1,y_{n+2})$, где вектор $y \in \mathbb{Z}_2^n$ и $y_{n+2} \in \mathbb{Z}_2$. Из Леммы 2 для любого $x \in \mathbb{Z}_2^n$ имеем

$$\ell(x) \oplus cx_{n+1} \oplus x_{n+2} \oplus \ell(x \oplus y) \oplus cx_{n+1} \oplus c \oplus x_{n+2} = 0.$$

Следовательно, $c = D_y\ell(x) \oplus y_{n+2}$. Пусть $g_2, g_1 \oplus g_2$ — произвольные бент-функции от n переменных. Из Леммы 14 следует, что $g_2 \oplus \ell, g_1 \oplus g_2 \oplus \ell \in \mathcal{B}_n$. Тогда из Теоремы 3 следует, что $f \in \mathbb{Z}_2^{n+2}$ из Конструкции 1 имеет h своей производной по направлению $(y,1,y_{n+2})$.

Эквивалентность гипотез для функций степени не меньше 2 следует из Утверждения 7. □

Таким образом, согласно Теореме 4, доказательство Гипотезы 2 приведет к доказательству Гипотезы 1.

Далее исследуем свойства $(f_1 \oplus f_2)h$, где функции h – булева функция от n переменных, f_1, f_2 – бент-функции от n переменных, причем $h \oplus f_1$ и $h \oplus f_2$ также являются бент-функциями от n переменных.

Приведем два вспомогательных утверждения.

Утверждение 8. *Пусть f_1, f_2, f_3, и f_4 являются булевыми функциями от n переменных, причем $f_1, f_2, f_3 \in \mathcal{B}_n$. Тогда функция f, определенная следующим образом:*

$$f(0,0,x) = f_1(x), \qquad f(0,1,x) = f_2(x),$$
$$f(1,0,x) = f_3(x), \qquad f(1,1,x) = f_4(x),$$

является бент-функцией от $n+2$ переменных тогда и только тогда, когда f_4 – бент-функция от n переменных и $\widetilde{f}_1 \oplus \widetilde{f}_2 \oplus \widetilde{f}_3 \oplus \widetilde{f}_4 = 1$.

Доказательство этого утверждения приведено в [86]. Отметим, что Утверждение 8 является упрощенной версией результата из работы A. Canteaut и P. Charpin 2003 года [19]. При этом в [19] также был доказан следующий факт.

Утверждение 9. *Пусть f_1, f_2, f_3 и $f_4 \in \mathcal{F}_n$ и функция f, определенная следующим образом:*

$$f(0,0,x) = f_1(x), \qquad f(0,1,x) = f_2(x),$$
$$f(1,0,x) = f_3(x), \qquad f(1,1,x) = f_4(x),$$

является бент-функцией от $n+2$ переменных. Тогда f_1 является бент-функцией от n переменных тогда и только тогда, когда f_2, f_3 и f_4 – бент-функции от n переменных.

В следующем утверждении приведена верхняя оценка степени булевой функции $(f_1 \oplus f_2)h$, где функции $h \in \mathcal{F}_n$ и f_1, f_2 – бент-функции от n переменных, причем $h \oplus f_1$ и $h \oplus f_2$ также являются бент-функциями от n переменных.

Утверждение 10. *Пусть $n \geqslant 2$ – четное целое число и $h \in \mathcal{F}_n$. Тогда если функции $f_1, f_2, h \oplus f_1, h \oplus f_2$ являются бент-функциями от n переменных, то верно* $\deg((f_1 \oplus f_2)h) \leqslant \frac{n+2}{2}$. *Кроме того, следующие утверждения эквивалентны:*

1. $\varphi_1(x) = \big(f_1(x) \oplus f_2(x)\big)h(x) \oplus f_1(x)$, *где $x \in \mathbb{Z}_2^n$, является бент-функцией от n переменных;*
2. $\varphi_2(x) = \big(f_1(x) \oplus f_2(x)\big)h(x) \oplus f_2(x)$, *где $x \in \mathbb{Z}_2^n$, является бент-функцией от n переменных;*
3. $\varphi_3(x) = \big(f_1(x) \oplus f_2(x)\big)h(x) \oplus f_2(x) \oplus h(x)$, *где $x \in \mathbb{Z}_2^n$, является бент-функцией от n переменных;*
4. $\varphi_4(x) = \big(f_1(x) \oplus f_2(x)\big)h(x) \oplus f_1(x) \oplus h(x)$, *где $x \in \mathbb{Z}_2^n$, является бент-функцией от n переменных;*

5. $\widetilde{\varphi_1} \oplus \widetilde{\varphi_2} \oplus \widetilde{\varphi_3} \oplus \widetilde{\varphi_4} \equiv 0$.

Доказательство. Пусть $y \in \mathbb{Z}_2^n$. Тогда $g \in \mathcal{F}_{n+2}$ такая, что

$$g(x,x_{n+1},x_{n+2}) = \big(h(x) \oplus h(x \oplus y)\big)x_{n+1} \oplus h(x) \oplus x_{n+2},$$

удовлетворяет условию Утверждение 3 для направления $(y,1,0)$. Следовательно, булева функция от $n+2$ переменных

$$f(x,x_{n+1},x_{n+2}) = \big((D_y g_1(x) \oplus 1)g(x,x_{n+1},x_{n+2}) \oplus D_y g_2(x)\big)x_{n+1}$$

$$\oplus g_1(x)g(x,x_{n+1},x_{n+2}) \oplus g_2(x),$$

где $g_1 = f_1 \oplus f_2$ и $g_2 = f_2$, является бент-функцией от $n+2$ переменных. Из Леммы 11 следует, что $\deg(f) \leqslant \frac{n+2}{2}$ и $\deg(g_1 h) = \deg((f_1 \oplus f_2)h) \leqslant \frac{n+2}{2}$.

Легко убедиться в том, что

$$f(x,0,0) = g_1(x)h(x) \oplus g_2(x) = \varphi_2(x),$$

$$f(x,0,1) = g_1(x)h(x) \oplus g_1(x) \oplus g_2(x) = \varphi_1(x),$$

$$f(x,1,0) = g_1(x \oplus y)h(x \oplus y) \oplus g_2(x \oplus y) \oplus h(x \oplus y) = \varphi_3(x \oplus y),$$

$$f(x,1,1) = g_1(x \oplus y)h(x \oplus y) \oplus g_1(x \oplus y) \oplus g_2(x \oplus y) \oplus h(x \oplus y) \oplus 1 = \varphi_4(x \oplus y) \oplus 1.$$

Утверждения 8 и 9 и Лемма 14 завершают доказательство. □

Приведем некоторые следствия из Утверждения 10.

Следствие 1. *Пусть $n \geqslant 2$ – четное целое число, $h, g \in \mathcal{F}_n$ и $\deg(h \cdot g) > \frac{n+2}{2}$. Тогда если $f_1, f_2 \in \mathcal{B}_n$ и $h \equiv f_1 \oplus f_2$, то хотя бы одна из функций $g \oplus f_1$ или $g \oplus f_2$ не является бент-функцией от n переменных.*

Следствие 2. *Пусть $n \geqslant 2$ – четное целое число, h является булевой функцией от n переменных и $f_1, f_2, h \oplus f_1, h \oplus f_2$ – бент-функции от n переменных. Тогда если $(f_1 \oplus f_2)h \equiv h$ или $(f_1 \oplus f_2)h \equiv 0$, при этом $f_3(x) = h(x \oplus y) \oplus f_1(x \oplus y)$ и $f_4(x) = h(x \oplus y) \oplus f_2(x \oplus y)$, где $y \in \mathbb{Z}_2^n$, то справедливо, что $\widetilde{f_1} \oplus \widetilde{f_2} \equiv \widetilde{f_3} \oplus \widetilde{f_4}$.*

В обозначениях Утверждения 10 приведем пример того, как верхняя оценка степени функции $(f_1 \oplus f_2)h$ может быть использована для описания бент-функций f_1, f_2.

Пусть $h(x) = x_1 x_2$ – булева функция от 4 переменных, где $x \in \mathbb{Z}_2^4$, и функции $f_1, f_2 \in \mathcal{B}_4$ такие, что $h \oplus f_1$ и $h \oplus f_2$ являются бент-функциями от 4 переменных.

Положим, что АНФ функции f_1 содержит моном x_3x_4, а АНФ функции f_2 его не содержит. Тогда $\deg((f_1 \oplus f_2)h) = 4 > 3 = \frac{n+1}{2}$. Таким образом, либо каждая бент-функция из разложения функции x_1x_2 от 4 переменных в сумму двух бент-функций имеет моном x_3x_4 в своей АНФ, либо каждая из них его не имеет. Пример достижения оценки можно получить для следующих функций от 4 переменных: $h(x) = x_3$, $f_1(x) = x_1x_2 \oplus x_3x_4$ и $f_2(x) = x_1x_3 \oplus x_2x_4$, где $x \in \mathbb{Z}_2^4$.

3.2 Аффинные производные бент-функций

В этом разделе мы получим точное число бент-функций, которые имеют заданную отличную от константы аффинную функцию своей производной.

Следующий результат показывает точное число направлений, для которых некоторая отличная от константы аффинная функция является производной булевой функции.

Лемма 22. *Пусть $\ell_{a,b}(x) = \langle a, x\rangle \oplus b$, где $a \in \mathbb{Z}_2^n$, a – ненулевой вектор, а $b \in \mathbb{Z}_2$. Тогда $\ell_{a,b}$ является производной булевых функций для $2^{n-1} - 1$ ненулевых направлений. Эти направления – ненулевые вектора y такие, что $\langle a, y\rangle = 0$.*

Доказательство. Если $\langle a, y\rangle = 0$, тогда

$$\ell_{a,b}(x) \oplus \ell_{a,b}(x \oplus y) = \langle a,x\rangle \oplus b \oplus \langle a,x \oplus y\rangle \oplus b = \langle a,y\rangle = 0.$$

Из Леммы 2 следует, что функция $\ell_{a,b}$ является производной булевой функции по направлению y. Поскольку a ненулевой, существует вектор $d \in \mathbb{Z}_2^n$ такой, что $\langle a,d\rangle = 1$. Следовательно,

$$\langle a, y \oplus d\rangle = \langle a, y\rangle \oplus \langle a, d\rangle = \langle a, y\rangle \oplus 1, \text{ для всех } y \in \mathbb{Z}_2^n. \tag{3.1}$$

Разделим $\mathbb{Z}_2^n$ на 2^{n-1} неупорядоченных пар $\{y; y \oplus d\}$. Согласно (3.1), существует 2^{n-1} различных векторов y таких, что $\langle a,y\rangle = 0$, если a – ненулевой вектор. Поскольку один из этих векторов – нулевой вектор, $\ell_{a,b}$ является производной для $2^{n-1} - 1$ ненулевых направлений. □

Докажем следующий вспомогательный результат.

Лемма 23. *Пусть $\ell \in \mathcal{A}_n$ и не является константой, причем ℓ является производной бент-функций f и g от n переменных для различных ненулевых направлений y и z соответственно. Тогда $f \neq g$.*

Доказательство. Пусть $f \in \mathcal{B}_n$ такая, что $D_y f(x) = D_z f(x) = \ell(x)$ для ненулевых $y \neq z$ и всех $x \in \mathbb{Z}_2^n$. Тогда для любого $x \in \mathbb{Z}_2^n$ справедливо, что

$$D_y f(x) \oplus D_z f(x) = f(x) \oplus f(x \oplus y) \oplus f(x) \oplus f(x \oplus z)$$
$$= f(x \oplus y) \oplus f(x \oplus z) = D_{z \oplus y} f(x \oplus y) = 0,$$

что противоречит Лемме 15. □

Следовательно, бент-функция не может иметь одну и ту же аффинную производную для двух различных направлений. Теперь получим точное число бент-функций, которые имеют заданную отличную от константы аффинную функцию своей производной.

Теорема 5. *Пусть $n \geqslant 2$, $\ell \in \mathcal{A}_{n+2}$ и не является константой. Тогда ℓ является производной $(2^{n+1} - 1) \mid \mathcal{B}_n \mid^2$ бент-функций от $n + 2$ переменных.*

Доказательство. Пусть $\ell_{a,b}(x,x_{n+1},x_{n+2}) = \ell_1(x) \oplus c_1 x_{n+1} \oplus c_2 x_{n+2} \oplus b$ для всех $(x,x_{n+1},x_{n+2}) \in \mathbb{Z}_2^{n+2}$, где $\ell_1 \in \mathcal{A}_n$ и $c_1, c_2, b \in \mathbb{Z}_2$. Положим, что $\ell_{a,b}$ является производной некоторой булевой функции по направлению $(y,y_{n+1},y_{n+2}) \neq \mathbf{0}$.

Пусть i – первый ненулевой индекс вектора (y,y_{n+1},y_{n+2}) и j такой индекс, что $j \neq i$ и $\ell_{a,b}$ линейно зависит от переменной x_j. Покажем, что такой индекс j всегда существует. Предположим обратное. Тогда $\ell_{a,b}(x,x_{n+1},x_{n+2}) = x_i \oplus b$ и $D_y l_{a,b}(x,x_{n+1},x_{n+2}) = 1$ для любого $(x,x_{n+1},x_{n+2}) \in \mathbb{Z}_2^{n+2}$, что согласно Лемме 2, противоречит тому, что $\ell_{a,b}$ является производной некоторой булевой функции по направлению (y,y_{n+1},y_{n+2}).

Без ограничения общности, пусть $i = n + 1$ и $j = n + 2$. Тогда функция $\ell_{a,b}(x,x_{n+1},x_{n+2}) = l_1(x) \oplus c_1 x_{n+1} \oplus x_{n+2}$. Из Леммы 14 следует, что сумма аффинной функции и любой бент-функцией дает бент-функцию. Таким образом, из Теоремы 3 получаем, что $\ell_{a,b}$ является производной $\mid \mathcal{B}_n \mid^2$ бент-функций от $n + 2$ переменных.

Из Леммы 23 следует, что для различных направлений (y,y_{n+1},y_{n+2}) мы получаем различные бент-функции, которые имеют $\ell_{a,b}$ своей производной. Тогда из Леммы 22 получаем, что существует в точности $(2^{n+1} - 1) \mid \mathcal{B}_n \mid^2$ бент-функций от $n + 2$ переменных, которые имеют $\ell_{a,b}$ своей производной. □

Поскольку производные аффинных функций являются константами, производные второго порядка бент-функций с аффинными производными – константы. Поэтому бент-функции, имеющие аффинные производные, можно использовать при построении бент-функций вида $f \oplus \mathrm{Ind}_U$ [50], где Ind_U – булева функцию от n переменных, принимающая значение 1 на всех элементах множества U (и только на них). Бент-функции вида $f \oplus \mathrm{Ind}_U$ исследовались также в [49].

3.3 Итеративная нижняя оценка числа бент-функций

В этом разделе мы используем результат Теоремы 5, чтобы получить итеративную нижнюю оценку числа бент-функций от $n \geqslant 4$ переменных.

Теорема 6. *Для любого $n \geqslant 2$ справедливо* $\mid \mathcal{B}_{n+2} \mid \geqslant (2^{n+2} - 2) \mid \mathcal{B}_n \mid^2$.

Доказательство. Пусть $\ell \in \mathcal{A}_{n+2}$ и $\deg(\ell) = 1$. Из Теоремы 5 следует, что существует $(2^{n+1} - 1) \mid \mathcal{B}_n \mid^2$ бент-функций от $n+2$ переменных, которые имеют ℓ своей производной. Таким образом,

$$\mid \mathcal{B}_{n+2} \mid \geqslant (2^{n+1} - 1) \mid \mathcal{B}_n \mid^2 \tag{3.2}$$

Покажем, что бент-функция не может иметь своими производными одновременно ℓ и $\ell \oplus 1$. Пусть $g \in \mathcal{B}_n$ такая, что $D_y g(x) = \ell(x)$ и $D_z g(x) = \ell(x) \oplus 1$ для ненулевых $y \neq z$ и любого $x \in \mathbb{Z}_2^n$. Тогда для любого $x \in \mathbb{Z}_2^n$ справедливо, что

$$\begin{aligned} &D_y g(x) \oplus D_z g(x) = g(x) \oplus g(x \oplus y) \oplus g(x) \oplus g(x \oplus z) \\ &= g(x \oplus y) \oplus g(x \oplus z) = D_{z \oplus y} g(x \oplus y) = \ell(x) \oplus \ell(x) \oplus 1 = 1, \end{aligned}$$

что противоречит Лемме 15. Следовательно, оценку (3.2) можно удвоить. □

Далее сравним полученную итеративную нижнюю оценку с другими известными.

Утверждение 11. *Для любого $n \geqslant 2$ справедливо, что*

$$\mid \mathcal{B}_{n+2} \mid \geqslant 6 \mid \mathcal{B}_n \mid^2 + 2^{n+2}(2^n - 3) \mid \mathcal{B}_n \mid .$$

Данная оценка была доказана в [29].

Бент-функции, которые получаются с помощью конструкции из Утверждения 8, называются *бент итеративными* функциями [86]. Обозначим через $\mathcal{BI}_{n+2}$ класс всех таких функций от $n+2$ переменных.

Следующая итеративная нижняя оценка числа бент-функций основана на Утверждении 8.

Утверждение 12. *Для четного $n \geqslant 2$ справедливо, что*

$$| \mathcal{B}_{n+2} | \geqslant | \mathcal{BI}_{n+2} | \geqslant | \mathcal{B}_n |^4 / | X_n | ,$$

где X_n – множество всех булевых функций от n переменных, которые могут быть представлены как сумма двух различных бент-функций.

Данное утверждение было доказано в [86].

В Таблица 2 представлены количества бент-функций, которые можно получить с помощью Теоремы 6 и Утверждений 11 и 12 для числа переменных $n \leqslant 14$. Для $n \leqslant 10$ количества бент-функций, которые можно получить с помощью Утверждения 12, были приведены в работе [86]. Поскольку число функций, которые раскладываются в сумму двух бент-функций, неизвестно для $n \geqslant 8$, для вычисления количества бент-функций, которые можно получить с помощью Утверждения 12 при $n \geqslant 12$, используется оценка $| X_n | \leqslant 2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$, основанная на числе функций степени не больше $n/2$. Так как число бент-функций неизвестно при $n \geqslant 10$, для вычисления количества бент-функций с помощью оценок при $n \geqslant 12$, мы используем нижние оценки, которые дают лучший результат для $n-2$. Отметим, что при $n \geqslant 14$ оценка из Утверждения 12 дает число между 0 и 1, так как разница между нижней оценкой для $| B_n |$ и верхней оценкой для $| X_n |$ слишком велика. Точные числа бент-функций можно найти, например, в [87].

Таблица 2 — Точные числа бент-функций и нижние оценки, полученные разными методами

Число переменных	4	6	8	10	12	14
Бент-функции	896	$\approx 2^{32.3}$	$\approx 2^{106.29}$	?	?	?
Утверждение 11	512	$\approx 2^{22.4}$	$\approx 2^{67.18}$	$\approx 2^{215.16}$	$\approx 2^{526.9}$	$\approx 2^{1129.3}$
Теорема 6	896	$\approx 2^{25.56}$	$\approx 2^{72.5}$	$\approx 2^{222.5}$	$\approx 2^{563.31}$	$\approx 2^{1140.62}$
Утверждение 12	512	$\approx 2^{28.26}$	$\approx 2^{87.35}$	$\approx 2^{262.16}$	$\approx 2^{410.64}$	0

Можно заметить, что для $4 \leqslant n \leqslant 14$ количество бент-функций получаемое с помощью Теоремы 6 больше чем количество получаемое из Утверждения 11.

Также Таблица 2 показывает, что итеративная нижняя оценка из Утверждения 12 более точная, чем оценка из Теоремы 6 при $6 \leqslant n \leqslant 10$. Однако при $n = 12$ оценка из Теоремы 6 дает большее число, чем оценка из Утверждения 12. Кроме того, как было отмечено выше, оценка из Утверждения 12 дает плохие результаты при $n \geqslant 14$ переменных из-за большой разницы между нижними оценками для $\mid B_n \mid$ и верхней оценкой для $\mid X_n \mid$.

Итеративная нижняя оценка из Теоремы 6 может быть улучшена, если кроме аффинных функций ℓ и $\ell \oplus 1$, мы будем рассматривать другие аффинные функции. К сожалению, тяжело учесть какие бент-функции уже были получены, так как возможен случай, когда $D_y g(x) = \ell(x)$ и $D_z g(x) = h(x)$, где $h \neq \ell$, $h \neq \ell \oplus 1$, и $y \neq z$. В этой оценке мы также не рассматриваем бент-функции, которые не имеют аффинных производных. В последние годы были опубликованы несколько работ, которые были посвящены таким функциям степени 3 [19; 58; 71]. Авторы этих работ исследовали существование бент-функций, которые не имеют аффинных производных, но для того чтобы улучшить оценку из Теоремы 6, необходимо получить нижние оценки числа таких бент-функций или их точное число.

3.4 Квадратичные производные бент-функций

В этом разделе мы докажем, что гипотеза о производных бент-функций верна для квадратичных функций.

Покажем, что любую уравновешенную квадратичную булеву функцию можно привести аффинным преобразованием переменных к квадратичной булевой функции, которая линейно зависит хотя бы от одной из своих переменных.

Лемма 24. *Любую уравновешенную квадратичную булеву функцию можно привести аффинным преобразованием переменных к квадратичной булевой функции, которая линейно зависит хотя бы от одной из своих переменных.*

Доказательство. Пусть f является уравновешенной квадратичной функцией. Из Леммы 5 следует, что $f(Ax \oplus b) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2t-1}x_{2t} \oplus \ell(x)$ для невырожденной квадратной двоичной матрицы A порядка $n \times n$, вектора $b \in \mathbb{Z}_2^n$, $\ell \in \mathcal{A}_n$, $x \in \mathbb{Z}_2^n$ и $1 \leqslant t \leqslant n/2$.

Из Леммы 7 следует, что $f(Ax \oplus b)$ – уравновешенная функция от n переменных. Положим, что $t = n/2$. Тогда из Лемм 12, 14, и 18 следует, что $f(Ax \oplus b)$ является бент-функцией от n переменных и, соответственно, она не является уравновешенной. Таким образом, $t < n/2$.

Покажем, что $f(Ax \oplus b)$ линейно зависит хотя бы от одной из своих переменных $x_{2t+1}, \ldots, x_n$. Положим обратное. Тогда справедливо следующее:

$$f(Ax \oplus b) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus x_{2t-1}x_{2t} \oplus a_{2t-1}x_{2t-1} \oplus a_{2t}x_{2t}.$$

Из Лемм 14 и 18 следует. что $f(Ax \oplus b)$ является бент-функцией от $2t$ переменных. Тогда из Леммы 12 имеем $wt(f(Ax \oplus b)) = 2^{n-2t}(2^{2t-1} \pm 2^{t-1}) = 2^{n-1} \pm 2^{n-t-1}$, а это противоречит тому, что $f(Ax \oplus b)$ является уравновешенной от n переменных. □

Отметим, что из Лемм 1 и 11 следует, что для $n \leqslant 4$ бент-функции не имеют квадратичных производных.

Теорема 7. *Пусть f – квадратичная уравновешенная булева функция от $n \geqslant 6$ переменных такая, что $f(x) \oplus f(x \oplus y) = 0$ для некоторого ненулевого $y \in \mathbb{Z}_2^n$ и произвольного $x \in \mathbb{Z}_2^n$. Тогда f является производной некоторой бент-функции от n переменных.*

Доказательство. Из Леммы 24 следует, что существует квадратичная уравновешенная функция f_1, полученная аффинным преобразованием из f, которая линейно зависит хотя бы от одной из своих переменных.

Из Лемм 2 и 16 следует, что f и f_1 являются производными некоторых булевых функций. Согласно Утверждению 7 и Утверждению 1, f_1 является производной некоторой бент-функции. Тогда из Леммы 16 следует, что f также является производной некоторой бент-функции. □

Таким образом, Гипотеза 2 доказана для квадратичных функций. Отметим также, что Теорема 7 доказывает гипотезу о производных бент-функций для квадратичных функций в том ее виде, в котором она была изначально представлена в работе [12].

Глава 4. Бент-функции и их обобщения

В этой главе связь между обобщенными и булевыми бент-функциями используется для построения булевых бент-функций на основе конструкции обобщенных бент-функций. Также мы исследуем связь между понятиями кватернарных и булевых бент-функций. Мы докажем, что свойство быть бент-функцией кватернарной функции $f(x+2y) = a(x,y)+2b(x,y)$ от n переменных, где $a, b \in \mathcal{F}_{2n}$ и $x, y \in \mathbb{Z}_2^n$, не зависит от того, являются ли $b, a \oplus b$ бент-функциями от $2n$ переменных. Результаты главы опубликованы в работах [96; 100—102].

В этой главе, в зависимости от контекста, мы используем “+” для обозначения сложения над $\mathbb{Z}_4$ и обычного сложения.

4.1 Связь между обобщенными и булевыми бент-функциями

В этом разделе мы используем связь между обобщенными бент-функциями и булевыми функции, которые раскладываются в сумму двух бент-функций, чтобы показать, как на основе конструкций обобщенных бент-функций можно получать конструкции булевых бент-функций.

Пусть $f \in \mathcal{GF}_n$. Тогда функцию f можно единственным образом представить в следующем виде:

$$f(x) = a(x) + 2b(x), \text{ где } a, b \in \mathcal{F}_n, x \in \mathbb{Z}_2^n. \tag{4.1}$$

Приведем два вспомогательных утверждения о связи булевых и обобщенных функций.

Лемма 25. *Пусть n – четное положительное число и $f \in \mathcal{GF}_n$. Тогда коэффициенты Уолша–Адамара функции f и функций $b, a \oplus b \in \mathcal{F}_n$ из представления (4.1) связаны следующим соотношением:*

$$W_f(x) = \frac{1}{2}\left(W_b(x) + W_{a\oplus b}(x)\right) + \frac{i}{2}\left(W_b(x) - W_{a\oplus b}(x)\right), \text{ где } x \in \mathbb{Z}_2^n.$$

Утверждение 13. *Пусть $f \in \mathcal{GF}_{2n}$. Тогда $f \in \mathcal{GB}_{2n} \iff b, a \oplus b \in \mathcal{B}_{2n}$, где $a, b \in \mathcal{F}_n$ – функции из представления (4.1) функции f.*

Доказательства этих двух утверждений приведены в [96].

Отметим, что из Утверждения 13 следует, что для $a \in \mathcal{F}_{2n}$ существует $f \in \mathcal{GB}_{2n}$ такая, что $f(x,y) = a(x,y) + 2b(x,y)$, где $b \in \mathcal{F}_{2n}$, $x, y \in \mathbb{Z}_2^n$, в том и только том случае, если $a \in \mathcal{F}_{2n}$ представляется как сумма двух бент-функций. Таким образом, изучение обобщенных бент-функций также связано с проблемой разложения булевых функций в сумму двух бент-функций. Также из Утверждения 13 следует, что выделение булевых подфункций из конструкций обобщенных бент-функций можно рассматривать как метод построения булевых бент-функций.

Приведем конструкцию обобщенных бент-функций, представленную в [93].

Утверждение 14. *Пусть m,n – целые положительные числа, $f \in \mathcal{GB}_{m+1}$ и $g \in \mathcal{GB}_{n+1}$ такие, что*

$$f(x,x_{m+1}) = (1 \oplus x_{m+1})f_1(x) + x_{m+1}f_2(x),$$

$$g(y,y_{n+1}) = (1 \oplus y_{n+1})g_1(y) + y_{n+1}g_2(y),$$

где $f_1, f_2 \in \mathcal{GF}_m$, $g_1, g_2 \in \mathcal{GF}_n$, $x \in \mathbb{Z}_2^m$ и $y \in \mathbb{Z}_2^n$.

Если $W_{f_1}(u)W_{f_2}(u) = 0$ для всех $u \in \mathbb{Z}_2^m$ или $W_{g_1}(v)W_{g_2}(v) = 0$ для всех $v \in \mathbb{Z}_2^n$, тогда обобщенная функция $h \in \mathcal{GF}_{m+n+2}$, которая имеет следующую форму:

$$\begin{aligned} h(x,y,z_{n+1},z_{n+2}) &= (1 \oplus z_{n+1})f_1(x) + z_{n+1}f_2(x) \\ &+(1 \oplus z_{n+2})g_1(y) + z_{n+2}g_2(y) + 2z_{n+1}z_{n+2}, \end{aligned} \tag{4.2}$$

где $z_{n+1},z_{n+2} \in \mathbb{Z}_2$, является обобщенной бент-функцией от $m+n+2$ переменных.

Докажем вспомогательное утверждение.

Лемма 26. *Пусть $f_1, f_2 \in \mathcal{GF}_n$ и $a_1,a_2,b_1,b_2 \in \mathcal{F}_n$ такие, что*

$$f_1(x) = a_1(x) + 2b_1(x),$$

$$f_2(x) = a_2(x) + 2b_2(x).$$

Тогда $W_{f_1}(u)W_{f_2}(u) = 0$ тогда и только тогда, когда

$$W_{b_2}(u)W_{a_1 \oplus b_1}(u) = -W_{b_1}(u)W_{a_2 \oplus b_2}(u)$$

и

$$W_{b_1}(u)W_{b_2}(u) = W_{a_1 \oplus b_1}(u)W_{a_2 \oplus b_2}(u).$$

Доказательство. Пусть $W_{b_1}(u) = C_1$, $W_{a_1\oplus b_1}(u) = C_2$, $W_{b_2}(u) = C_3$ и $W_{a_2\oplus b_2}(u) = C_4$. Тогда из Леммы 25 следует, что

$$W_{f_1}(u)W_{f_2}(u) = \big(\frac{1}{2}(C_1+C_2)+\frac{i}{2}(C_1-C_2)\big)\big(\frac{1}{2}(C_3+C_4)+\frac{i}{2}(C_3-C_4)\big)$$

$$= \frac{1}{2}(C_2C_3+C_1C_4)+\frac{i}{2}(C_1C_3-C_2C_4).$$

Тогда $W_{f_1}(u)W_{f_2}(u)=0 \iff C_2C_3=-C_1C_4$ и $C_1C_3=C_2C_4$. □

Теперь приведем конструкцию булевых бент-функций, которая следует из Утверждения 14.

Утверждение 15. *Пусть m,n – нечетные целые числа, $a_1,b_1,a_2,b_2 \in \mathcal{F}_m$, $A_1,B_1,A_2,B_2 \in \mathcal{F}_n$ такие, что*

$$a_3(x,x_{m+1}) = (1\oplus x_{m+1})a_1(x)\oplus x_{m+1}a_2(x),$$
$$b_3(x,x_{m+1}) = (1\oplus x_{m+1})b_1(x)\oplus x_{m+1}b_2(x),$$
$$A_3(y,y_{n+1}) = (1\oplus y_{n+1})A_1(y)\oplus y_{n+1}A_2(y),$$
$$B_3(y,y_{n+1}) = (1\oplus y_{n+1})B_1(y)\oplus y_{n+1}B_2(y),$$

где $x\in\mathbb{Z}_2^m$, $y\in\mathbb{Z}_2^n$ и $x_{m+1},y_{m+1}\in\mathbb{Z}_2$.

Положим, что $b_3, a_3\oplus b_3 \in \mathcal{B}_{m+1}$, $B_3, A_3\oplus B_3\in\mathcal{B}_{n+1}$ и выполнено хотя бы одно из следующих условий:

1. *$W_{b_2}(u)W_{a_1\oplus b_1}(u) = -W_{b_1}(u)W_{a_2\oplus b_2}(u)$ и $W_{b_1}(u)W_{b_2}(u) = W_{a_1\oplus b_1}(u)W_{a_2\oplus b_2}(u)$ для всех $u\in\mathbb{Z}_2^m$;*
2. *$W_{B_2}(v)W_{A_1\oplus B_1}(v) = -W_{B_1}(v)W_{A_2\oplus B_2}(v)$ и $W_{B_1}(v)W_{B_2}(v) = W_{A_1\oplus B_1}(v)W_{A_2\oplus B_2}(v)$ для всех $v\in\mathbb{Z}_2^n$.*

Тогда если для $z_{n+1},z_{n+2}\in\mathbb{Z}_2$ булевы функции a и b от $n+m+2$ переменных имеют следующие представления:

$$a(x,y,z_{n+1},z_{n+2}) = a_3(x,z_{n+1})\oplus A_3(y,z_{n+2}), \tag{4.3}$$
$$b(x,y,z_{n+1},z_{n+2}) = b_3(x,z_{n+1})\oplus B_3(y,z_{n+2})\oplus\big(z_{n+1}z_{n+2}\oplus z_{n+1}\big)a_2(x)A_1(y)$$
$$\oplus\big(z_{n+1}z_{n+2}\oplus z_{n+2}\big)a_1(x)A_2(y)\oplus z_{n+1}z_{n+2}\big(a_2(x)A_2(y)\oplus 1\big)$$
$$\oplus\big(z_{n+1}z_{n+2}\oplus z_{n+1}\oplus z_{n+2}\oplus 1\big)a_1(x)A_1(y), \tag{4.4}$$

тогда $b, a\oplus b\in\mathcal{B}_{n+m+2}$.

Доказательство. Пусть $f_1, f_2 \in \mathcal{GF}_m$ и $g_1, g_2 \in \mathcal{GF}_n$ такие, что

$$f_1(x) = a_1(x) + 2b_1(x), \;\; f_2(x) = a_2(x) + 2b_2(x),$$
$$g_1(y) = A_1(y) + 2B_1(y), \;\; g_2(y) = A_2(y) + 2B_2(y),$$

для всех $x \in \mathbb{Z}_2^m$ и $y \in \mathbb{Z}_2^n$.

Из Лемм 25 и 26 следует, что выполнение хотя бы одного из условий (1) или (2) гарантирует, что либо

$$W_{f_1}(u)W_{f_2}(u) = 0 \text{ для всех } u \in \mathbb{Z}_2^m$$

либо

$$W_{g_1}(v)W_{g_2}(v) = 0 \text{ для всех } v \in \mathbb{Z}_2^n.$$

Пусть $f \in \mathcal{GF}_{m+1}$ и $g \in \mathcal{GF}_{n+1}$ такие, что

$$f(x,x_{m+1}) = (1 \oplus x_{m+1})f_1(x) + x_{m+1}f_2(x),$$

$$g(y,y_{n+1}) = (1 \oplus y_{n+1})g_1(y) + y_{n+1}g_2(y),$$

для всех $x \in \mathbb{Z}_2^m$ и $y \in \mathbb{Z}_2^n$. Тогда

$$f(x,x_{m+1}) = a_3(x,x_{m+1}) + 2b_3(x,x_{m+1}),$$

$$g(y,y_{n+1}) = A_3(y,y_{n+1}) + 2B_3(y,y_{n+1})$$

и из Утверждения 13 следует, что $f \in \mathcal{GB}_{m+1}$ и $g \in \mathcal{GB}_{n+1}$.

Тогда из Утверждения 14 следует, что $h \in \mathcal{GF}_{m+n+2}$, которая имеет форму (4.2), является обобщенной бент-функцией от $m + n + 2$ переменных. Дальше определим формы функций $a, b \in \mathcal{F}_{n+m+2}$ из представления (4.1) для функции h. Для h справедливо, что

$$h(x,y,0,0) = f_1(x) + g_1(y) = a_1(x) + A_1(y) + 2\big(b_1 + B_1\big).$$

Отметим, что если $a_1(x) = A_1(y) = 1$, то $a_1(x) + A_1(y) = 2$. Таким образом, для $a, b \in \mathcal{F}_{m+n+2}$ из представления (4.1) функции h справедливо следующее:

$$a(x,y,0,0) = a_1(x) \oplus A_1(y),$$
$$b(x,y,0,0) = b_1(x) \oplus B_1(y) \oplus a_1(x)A_1(y).$$

Аналогично получаем, что

$$\begin{aligned}
&a(x,y,0,1) = a_1(x) \oplus A_2(y),\\
&b(x,y,0,1) = b_1(x) \oplus B_2(y) \oplus a_1(x)A_2(y);\\
&a(x,y,1,0) = a_2(x) \oplus A_1(y),\\
&b(x,y,1,0) = b_2(x) \oplus B_1(y) \oplus a_2(x)A_1(y);\\
&a(x,y,1,1) = a_2(x) \oplus A_2(y),\\
&b(x,y,1,1) = b_2(x) \oplus B_2(y) \oplus a_2(x)A_2(y) \oplus 1.
\end{aligned}$$

Таким образом, нетрудно убедиться, что a и b имеют форму (4.3) и (4.4) соответственно.

Так как $h \in \mathcal{GB}_{m+n+2}$, из Утверждения 13 следует, что $b, a \oplus b \in \mathcal{B}_{m+n+2}$. □

В обозначениях Утверждения 15, положим, что $b_1(x) = b_4(x_1, \ldots, x_{m-1})$, $b_2(x) = b_5(x_1, \ldots, x_{m-1}) \oplus x_m$ и $a_1 \equiv a_2 \equiv 0$, где $b_4, b_5 \in \mathcal{B}_{m-1}$. Тогда из Утверждения 8 следует, что функции $b_3, a_3 \oplus b_3 \in \mathcal{F}_{m+1}$ являются бент-функциями из класса бент итеративных функций. Тогда если для вектора $u \in \mathbb{Z}_2^m$ справедливо, что $u_m = 1$, то верно следующее:

$$W_{b_1}(u) = \sum_{x \in \mathbb{Z}_2^m, x_m = 0} (-1)^{\langle x', u' \rangle \oplus b_4(x')} + \sum_{x \in \mathbb{Z}_2^m, x_m = 1} (-1)^{\langle x', u' \rangle \oplus b_4(x') \oplus 1} = 0,$$

где $x' = (x_1, \ldots, x_{m-1}), u' = (u_1, \ldots, u_{m-1})$. В свою очередь, если для $u \in \mathbb{Z}_2^m$ верно, что $u_m = 0$, то справедливо следующее:

$$W_{b_2}(u) = \sum_{x \in \mathbb{Z}_2^m, x_m = 0} (-1)^{\langle x', u' \rangle \oplus b_5(x')} + \sum_{x \in \mathbb{Z}_2^m, x_m = 1} (-1)^{\langle x', u' \rangle \oplus b_5(x') \oplus 1} = 0.$$

Для функций b_1, b_2, a_1 и a_2 выполнено условие (1) Утверждения 15. По аналогии, для выполнения условия (2) Утверждения 15 предположим, что $A_1 \equiv A_2 \equiv 0$, $B_1(y) = B_4(y_1, \ldots, y_{n-1})$ и $B_2(y) = B_5(y_1, \ldots, y_{n-1}) \oplus y_n$, где $B_4, B_5 \in \mathcal{B}_{n-1}$.

Тогда конструкция из Утверждения 15 принимает следующий вид:

$$b_3(x, z_{n+1}) \oplus B_3(y, z_{n+2}) \oplus z_{n+1} z_{n+2}.$$

Отметим, что бент-функция такого вида может быть получена из следующей конструкции, которая была представлена в [23].

Утверждение 16. *Пусть $r, k \geqslant 2$ – четные целые числа, а также $f_1, f_2 \in \mathcal{B}_r$ и $g_1, g_2 \in \mathcal{B}_k$. Тогда функция $f \in \mathcal{F}_{r+k}$ такая, что*

$$f(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1(x) \oplus f_2(x))(g_1(y) \oplus g_2(y)),$$

где $x \in \mathbb{Z}_2^r$, $y \in \mathbb{Z}_2^k$, *является бент-функцией от* $r + k$ *переменных.*

Действительно, z_{n+1} и z_{n+2} можно представить в виде суммы двух бент-функций следующим образом:

$$z_{n+1} = b_3(x,z_{n+1}) \oplus b_3(x,z_{n+1}) \oplus z_{n+1},$$
$$z_{n+2} = B_3(y,z_{n+2}) \oplus B_3(y,z_{n+2}) \oplus z_{n+2}.$$

Отметим, что для построения бент-функции с помощью Утверждения 15, достаточно выполнения хотя бы одного из условий (1) или (2).

4.2 Связь между кватернарными и булевыми бент-функциями

Данный раздел посвящен исследованию связи между понятиями кватернарных и булевых бент-функций. Мы докажем, что между свойствами кватернарных и булевых функций быть бент-функциями нет прямой связи.

Пусть $f \in \mathcal{QF}_n$. Тогда функцию f единственным образом можно представить в следующем виде:

$$f(x + 2y) = a(x,y) + 2b(x,y), \text{ где } a, b \in \mathcal{F}_{2n}, x, y \in \mathbb{Z}_2^n. \tag{4.5}$$

Докажем следующее вспомогательное утверждение.

Лемма 27. *Пусть* $x, y \in \mathbb{Z}_2^n$. *Если* $x.y \neq \langle x,y\rangle$, *тогда* $x.y = \langle x,y\rangle + 2$.

Доказательство. Если $x.y = 0$ или 1, тогда $x.y = \langle x,y\rangle$. Для остальных двух случаев мы имеем следующие соотношения:

$$x.y = 2 \Rightarrow \langle x,y\rangle = 0 \Rightarrow x.y = \langle x,y\rangle + 2,$$

$$x.y = 3 \Rightarrow \langle x,y\rangle = 1 \Rightarrow x.y = \langle x,y\rangle + 2.$$

□

Дальше мы исследуем связь между коэффициентами Уолша–Адамара кватернарной функции $f \in \mathcal{QF}_n$ и коэффициентами Уолша–Адамара булевых функций $b, a \oplus b \in \mathcal{F}_{2n}$ из представления (4.5) функции f.

Лемма 28. *Пусть $f \in \mathcal{QF}_n$ имеет представление (4.5). Тогда коэффициенты Уолша–Адамара функций f, $a \oplus b$ и b из представления (4.5) связаны следующим соотношением:*

$$W_f(x+2y) = \frac{1}{2}\left(W_b(x \oplus y,x) + W_{a\oplus b}(y,x) - 2c_b(x \oplus y,x) - 2c_{a\oplus b}(y,x)\right)$$

$$+\frac{i}{2}\left(W_b(y,x) - W_{a\oplus b}(x \oplus y,x) - 2c_b(y,x) + 2c_{a\oplus b}(x \oplus y,x)\right),$$

где

$$c_g(u,x) = \sum_{x' \in V_x, y'} (-1)^{f(x',y') \oplus \langle (u,x),(x',y') \rangle}$$

для $x,y,u \in \mathbb{Z}_2^n$, $g \in \mathcal{F}_{2n}$ и $V_x = \{\, x' \in \mathbb{Z}_2^n \mid \langle x,x' \rangle \neq x.x' \,\}$.

Доказательство. Пусть $x,y \in \mathbb{Z}_2^n$. Коэффициенты Уолша–Адамара функции f имеют следующий вид:

$$W_f(x+2y) = \sum_{x',y' \in \mathbb{Z}_2^n} i^{(x+2y).(x'+2y') + a(x',y') + 2b(x',y')}.$$

Поскольку для любых $x,y \in \mathbb{Z}_2^n$ имеем $2\langle x,y \rangle = 2x.y(\bmod 4)$, из Леммы 27 следует, что

$$(x+2y).(x'+2y') = \begin{cases} \langle x,x' \rangle + 2\langle x,y' \rangle + 2\langle y,x' \rangle, & \text{если} \quad x.x' = \langle x,x' \rangle, \\ \langle x,x' \rangle + 2\langle x,y' \rangle + 2\langle y,x' \rangle + 2, & \text{если} \quad x.x' \neq \langle x,x' \rangle. \end{cases}$$

Пусть $U_x = \{\, x' \in \mathbb{Z}_2^n \,:\, x.x' = \langle x,x' \rangle \,\}$ и $V_x = \{\, x' \in \mathbb{Z}_2^n \,:\, x.x' \neq \langle x,x' \rangle \,\}$. Таким образом, $U_x \cap V_x = \varnothing$ и $U_x \cup V_x = \mathbb{Z}_2^n$. Отметим, что в общем случае $|U_x| \neq |V_x|$. Тогда

$$W_f(x+2y) = \sum_{x' \in U_x, y'} (-1)^{\langle x,y' \rangle \oplus \langle y,x' \rangle \oplus b(x',y')} i^{\langle x,x' \rangle + a(x',y')}$$

$$- \sum_{x' \in V_x, y'} (-1)^{\langle x,y' \rangle \oplus \langle y,x' \rangle \oplus b(x',y')} i^{\langle x,x' \rangle + a(x',y')}.$$

Рассмотрим отображения $\beta, \gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$, определяемые следующим образом:

$$\beta : 0,1 \to 0 \text{ и } \beta : 2,3 \to 1;$$

$$\gamma : 0,2 \to 0 \text{ и } \gamma : 1,3 \to 1.$$

Для любых $t \in \mathbb{Z}_4$ справедливо, что

$$i^t = (-1)^{\beta(t)} \left(\frac{1 + (-1)^{\gamma(t)}}{2} + \frac{1 - (-1)^{\gamma(t)}}{2} i \right).$$

Поскольку $\gamma(\langle x,x'\rangle + a(x',y')) = \langle x,x'\rangle \oplus a(x',y')$, то для $t = x.x' + a(x',y')$ мы получаем следующее выражение:

$$W_f(x+2y) = \frac{1}{2}\left(S_1 + S_2 - S_3 - S_4\right) + \frac{i}{2}\left(S_1 - S_2 - S_3 + S_4\right), \tag{4.6}$$

где

$$\begin{aligned}
S_1 &= \sum_{x'\in U_x, y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\beta(\langle x,x'\rangle + a(x',y'))},\\
S_2 &= \sum_{x'\in U_x, y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus\beta(\langle x,x'\rangle + a(x',y'))},\\
S_3 &= \sum_{x'\in V_x, y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\beta(\langle x,x'\rangle + a(x',y'))},\\
S_4 &= \sum_{x'\in V_x, y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus\beta(\langle x,x'\rangle + a(x',y'))}.
\end{aligned}$$

Пусть $M_{\delta,x} = \{\ x' \in \mathbb{Z}_2^n : \langle x,x'\rangle = \delta\ \}$, где $\delta \in \mathbb{Z}_2$. Тогда $M_{0,x} \cup M_{1,x} = \mathbb{Z}_2^n$ и $|M_{0,x}| = |M_{1,x}| = 2^{n-1}$. Разделим суммы S_1, S_2, S_3 и S_4 на две суммы $\sum_{x'\in M_{0,x},y'}$ и $\sum_{x'\in M_{1,x},y'}$. Отметим, что $\beta(a(x',y') + \langle x,x'\rangle)$ равно 0 и $a(x',y')$ для $x' \in M_{0,x}$ и $x' \in M_{1,x}$ соответственно. Таким образом, мы имеем следующие соотношения:

$$\begin{aligned}
S_1 &= \sum_{x'\in U_x\cap M_{0,x}, y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle}\\
&\quad + \sum_{x'\in U_x\cap M_{1,x}, y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus a(x',y')},\\
S_2 &= \sum_{x'\in U_x\cap M_{0,x}, y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle}\\
&\quad + \sum_{x'\in U_x\cap M_{1,x}, y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus a(x',y')},\\
S_3 &= \sum_{x'\in V_x\cap M_{0,x}, y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle}\\
&\quad + \sum_{x'\in V_x\cap M_{1,x}, y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus a(x',y')},\\
S_4 &= \sum_{x'\in V_x\cap M_{0,x}, y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle}\\
&\quad + \sum_{x'\in V_x\cap M_{1,x}, y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle a(x',y')}.
\end{aligned}$$

Группируя слагаемые, мы получаем, что

$$S_1 + S_2 - S_3 - S_4$$
$$= \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle} + \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle}$$
$$- \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle} - \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle}.$$

и

$$S_1 - S_2 - S_3 + S_4$$
$$= \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle} - \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle}$$
$$- \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle} + \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle}.$$

Пусть $g \in \mathcal{F}_{2n}$ и $c_g(u,x) = \sum_{x' \in V_x, y'} (-1)^{g(x',y') \oplus \langle (u,x),(x',y') \rangle}$, где $u \in \mathbb{Z}_2^n$, тогда можно убедиться, что

$$S_1 + S_2 - S_3 - S_4 = \big(W_b(x \oplus y, x) - c_b(x \oplus y, x)\big)$$
$$+ \big(W_{a \oplus b}(y, x) - c_{a \oplus b}(y,x)\big) - c_b(x \oplus y, x) - c_{a \oplus b}(y,x)$$

и

$$S_1 - S_2 - S_3 + S_4 = \big(W_b(y, x) - c_b(y,x)\big)$$
$$- \big(W_{a \oplus b}(x \oplus y, x) - c_{a \oplus b}(x \oplus y, x)\big) - c_b(y,x) + c_{a \oplus b}(x \oplus y, x).$$

Тогда из (4.6) следует необходимое. □

Таким образом, коэффициенты Уолша–Адамара кватернарной функции f не зависят напрямую от коэффициентов Уолша–Адамара булевых функций b и $a \oplus b$ из представления (4.5).

Приведем следующий факт, который следует из Леммы 28. Следующий факт показывает, что кватернарная бент-функция f от $2n$ переменных может быть использована для построения кватернарной бент-функции f' от $2n$ переменных.

Утверждение 17. *Пусть $x, y \in \mathbb{Z}_2^n$, $f, f' \in \mathcal{QF}_n$ и $a, b \in \mathcal{F}_{2n}$ такие, что $f(x + 2y) = a(x,y) + 2b(x,y)$ и $f'(x + 2y) = a(x,y) + 2(a(x,y) \oplus b(x,y))$. Тогда f является кватернарной бент-функцией тогда и только тогда, когда f' является кватернарной бент-функцией.*

Доказательство. Исследуем коэффициенты Уолша–Адамара функций f и f'. Из Леммы 28 следует, что для $x, y \in \mathbb{Z}_2^n$

$$W_f(x+2y) = \frac{1}{2}\left(W_b(x\oplus y,x) + W_{a\oplus b}(y,x) - 2c_b(x\oplus y,x) - 2c_{a\oplus b}(y,x)\right)$$

$$+\frac{i}{2}\left(W_b(y,x) - W_{a\oplus b}(x\oplus y,x) - 2c_b(y,x) + 2c_{a\oplus b}(x\oplus y,x)\right)$$

и

$$W_{f'}(x+2(x\oplus y)) = \frac{1}{2}\left(W_{a\oplus b}(y,x) + W_b(x\oplus y,x) - 2c_{a\oplus b}(y,x) - 2c_b(x\oplus y,x)\right)$$

$$+\frac{i}{2}\left(W_{a\oplus b}(x\oplus y,x) - W_b(y,x) + 2c_b(y,x) - 2c_{a\oplus b}(x\oplus y,x)\right),$$

где

$$c_g(u,x) = \sum_{x'\in V_x, y'} (-1)^{g(x',y')\oplus\langle(u,x),(x',y')\rangle},$$

где $g \in \mathcal{F}_{2n}$, $V_x = \{\, x' \mid \langle x,x'\rangle \neq x.x' \,\}$, и $u \in \mathbb{Z}_2^n$.

Пусть $\Re$ и $\Im$ – вещественная и мнимая часть комплексного числа соответственно. Тогда справедливо, что $\Re(W_f(x+2y)) = \Re(W_{f'}(x+2(x\oplus y)))$ и $\Im(W_f(x+2y)) = -\Im(W_{f'}(x+2(x\oplus y)))$.

Из Леммы 20 следует, что коэффициенты Уолша–Адамара кватернарной бент-функции имеют только вещественную или мнимую часть. Следовательно, если $f \in \mathcal{GB}_n$, тогда $|W_{f'}(x+2(x\oplus y))| = |W_f(x+2y)| = 4^{n/2}$ и, следовательно, f' – кватернарная бент-функция от n переменных. Аналогично мы можем доказать, что если $f' \in \mathcal{QB}_n$, тогда $|W_f(x+2y)| = |W_{f'}(x+2(x\oplus y))| = 4^{n/2}$ и, следовательно, $f \in \mathcal{QB}_n$. □

Далее исследуем связь между свойством быть бент-функциями кватернарной функции f и булевых функций $b, a\oplus b$ из представления (4.5).

Утверждение 18. *Для любых целых $n \geqslant 2$ существует кватернарная бент-функция $f(x+2y) = a(x,y) + 2b(x,y)$ от n переменных, где b и $a\oplus b$ не являются бент-функциями от $2n$ переменных.*

Доказательство. Представление (4.5) функции f от n переменных имеет следующий вид: $f(x_1+2x_{n+1},\ldots,x_n+2x_{2n}) = a(x_1,\ldots,x_{2n}) + 2b(x_1,\ldots,x_{2n})$. Пусть

$$b(x_1,..,x_{2n}) = \bigoplus_{i=3}^{n} x_i x_{i+n} \oplus x_1x_{n+2} \oplus x_2x_{n+1} \oplus x_1x_2x_{n+1},$$

$$a(x_1,..,x_{2n}) = x_1x_{n+1}.$$

Можно заметить, что b раскладывается в сумму $n-2$ булевых функций от двух переменных и одной булевой функции от 4 переменных следующим образом:

$$b(x_1,...,x_{2n}) = b_1(x_1,x_2,x_{n+1},x_{n+2}) \oplus b_2(x_3,x_{n+3}) \oplus ... \oplus b_{n-1}(x_n,x_{2n}),$$

$$b_1(x_1,x_2,x_{n+1},x_{n+2}) = x_1x_{n+2} \oplus x_2x_{n+1} \oplus x_1x_2x_{n+1},$$

$$b_i(x_{i+1},x_{n+i+1}) = x_{i+1}x_{n+i+1}, \ \ i = 2,...,n-1.$$

Из Леммы 17 следует, что b – бент-функция тогда и только тогда, когда b_i – бент-функция, где $i = 1,\ldots,n-1$. Согласно Лемме 11, функция b_1 от 4 переменных не является бент-функцией, так как ее степень равна трем. Следовательно, b не является бент-функцией. Аналогично доказывается, что $a \oplus b$ не является бент-функцией.

Можно убедиться, что

$$2b(x_1,..,x_{2n}) = (2x_3x_{n+3} + ... + 2x_nx_{2n}) + 2x_1x_{n+2} + 2x_2x_{n+1} + 2x_1x_2x_{n+1}.$$

Заметим, что f раскладывается в сумму $n-2$ кватернарных функций от одной переменной и одной кватернарной функции от двух переменных следующим образом:

$$f(x_1 + 2x_{n+1},...,x_n + 2x_{2n}) = f_1(x_1 + 2x_{n+1},x_2 + 2x_{n+2})$$
$$+f_2(x_3 + 2x_{n+3}) + ... + f_{n-1}(x_n + 2x_{2n}),$$

где

$$f_1(x_1 + 2x_{n+1},x_2 + 2x_{n+2}) = x_1x_{n+1} + 2x_1x_{n+2} + 2x_2x_{n+1} + 2x_1x_2x_{n+1},$$

$$f_i(x_{i+1} + 2x_{n+i+1}) = 2x_{i+1}x_{n+i+1}, \ \ i = 2,...,n-1.$$

В Таблицах 3 и 4 представлены коэффициенты Уолша–Адамара функции от одной переменной вида $g(y_1 + 2y_2) = 2y_1y_2$ и функции f_1 соответственно.

Таблица 3

$y \in \mathbb{Z}_4$	0	1	2	3
$W_{2y_1y_2}(y)$	2	$2i$	2	$-2i$

Из определения кватернарных бент-функций и Таблиц 3 и 4 следует, что f_i являются кватернарными бент-функциями, где $i = 1,\ldots,n-1$. Из Леммы 21 следует, что f – кватернарная бент-функция от n переменных. □

Таблица 4

$x \in \mathbb{Z}_4^2$	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
$W_{f_1}(x)$	4	$4i$	4	4	4	$4i$	-4	4	4	$-4i$	4	-4	4	$-4i$	-4	-4

Следующий результат покажет, что в общем случае свойство быть кватернарной бент-функцией не следует из того, что $b, a \oplus b$ – бент-функции.

Утверждение 19. *Для любых целых $n \geqslant 1$ существуют булевы бент-функции b и $a \oplus b$ от $2n$ переменных такие, что функция $f(x + 2y) = a(x,y) + 2b(x,y)$ от n переменных не является кватернарной бент-функцией.*

Доказательство. Представление (4.5) функции f от n переменных имеет следующий вид: $f(x_1 + 2x_{n+1},...,x_n + 2x_{2n}) = a(x_1,...,x_{2n}) + 2b(x_1,...,x_{2n})$.

Пусть $b(x_1,..,x_{2n}) = \bigoplus_{i=1}^{n} x_i x_{i+n}$ и $a(x_1,..,x_{2n}) = x_{n+1}$. Из Лемм 14 и 18 следует, что $b, a \oplus b$ – булевы бент-функции от $2n$ переменных.

Легко убедиться, что $2b(x_1,..,x_{2n}) = 2x_1x_{n+1} + ... + 2x_nx_{2n}$. Тогда f может быть разложена в сумму n кватернарных функций от одной переменной:

$$f(x_1 + 2x_{n+1},...,x_n + 2x_{2n}) = f_1(x_1 + 2x_{n+1}) + ... + f_n(x_n + 2x_{2n}),$$

где

$$f_i(x_i + 2x_{n+i}) = a_i(x_i,x_{n+i}) + 2b_i(x_i,x_{n+i}),\ i = 1,..,n,$$

$$b_i(x_i,x_{n+i}) = x_i x_{n+i},\ i = 1,..,n,$$

$$a_1(x_1,x_{n+1}) = x_{n+1},$$

$$a_i(x_i,x_{n+i}) = 0,\ i = 2,..,n.$$

В Таблице 5 представлены коэффициенты Уолша–Адамара функции f_1.

Таблица 5

$x \in \mathbb{Z}_4$	0	1	2	3
$W_{f_1}(x)$	$2i$	0	$2i$	$2 - 2i$

Из определения кватернарных бент-функций и Таблицы 5 следует, что f_1 не является кватернарной бент-функцией. Тогда из Леммы 21 следует, что f не является кватернарной бент-функцией от n переменных. □

Таким образом, из Утверждений 18 и 19 следует, что свойство быть бент-функцией кватернарных функций f в общем случае не зависит от того являются ли функции $b, a \oplus b$ из представления (4.5) бент-функциями.

4.3 Связь между кватернарными и обобщенными бент-функциями

Данный раздел посвящен исследованию связи между понятиями кватернарных и обобщенных бент-функций.

Пусть $f \in \mathcal{QF}_n$. Тогда функцию f единственном образом можно представить в следующем виде:

$$f(x + 2y) = g(x,y), \text{ где } g \in \mathcal{GF}_{2n}, x, y \in \mathbb{Z}_2^n. \tag{4.7}$$

В следующих двух утверждениях мы покажем, что свойства быть бент-функциями функций f и g из представления (4.7) не следуют одно из другого.

Утверждение 20. *Для любого $n \geqslant 1$ существует обобщенная бент-функция g от $2n$ переменных такая, что кватернарная функция f от n переменных, определенная следующим образом: $f(x + 2y) = g(x,y)$ для всех $x, y \in \mathbb{Z}_2^n$, не является кватернарной бент-функцией.*

Доказательство. Из Утверждения 19 следует, что существует кватернарная функция $f(x + 2y) = a(x,y) + 2b(x,y)$, которая не является кватернарной бент-функцией, когда булевы функции b и $a \oplus b$ являются бент-функциями от $2n$ переменных. При этом из Утверждения 13 следует, что если b и $a \oplus b$ являются бент-функциями, то обобщенная функция $g(x,y) = a(x,y) + 2b(x,y)$ является бент-функцией. □

Утверждение 21. *Для любого $n \geqslant 2$ существует кватернарная бент-функция f от n переменных такая, что обобщенная функция g от $2n$ переменных из представления (4.7) не является бент-функцией.*

Доказательство. Из Утверждения 18 следует, что существует кватернарная бент-функция $f(x + 2y) = a(x,y) + 2b(x,y)$ от $n \geqslant 2$ переменных такая, что функции b и $a \oplus b$ от $2n$ переменных не являются бент-функциями. При этом из

Утверждения 13 следует, что обобщенная функция g является бент-функцией тогда и только тогда, когда b и $a \oplus b$ – булевы бент-функции. Следовательно, g не является бент-функцией. □

Таким образом, подходы Кумара и Шмидта к обобщению бент-функций не являются эквивалентными.

Глава 5. Исследование однородных бент-функций с помощью графов

Данная глава посвящена исследованию связи однородных бент-функций и графов $\Gamma(n,k)$, вершинами которых являются неупорядоченные подмножества размера k множества $\{1,\ldots,n\}$. ве вершины такого графа соединены ребром, если рассматриваемые подмножества имеют в точности один общий элемент. Известно, что между однородными бент-функциями от 6 переменных степени 3 и дополнениями к кликам максимального размера графа Нэги $\Gamma(6,3)$ существует взаимно однозначное соответствие. В главе доказано, что максимальный размер клики в графе $\Gamma(n,k)$, где $n = \frac{(k+1)k}{2}$, равен $k+1$. Кроме того, получено точное число клик максимального размера в таких графах. Также в данной главе установлено, что булевы функции, которые соответствуют дополнениям клик максимального размера в графах $\Gamma(10,4)$ и $\Gamma(28,7)$, не являются бент-функциями. Результаты данной главы были представлены в работах [97; 103].

Для начала приведем обзор известных методов исследования бент-функций с помощью теории графов.

5.1 Известные методы классификации бент-функций с помощью теории графов

Граф называется *регулярным*, если степени всех его вершин равны.

В [17] авторами A. Bernasconi и B. Codenotti был предложен способ классификации бент-функций с помощью *сильно регулярных графов*. Регулярный граф G называется *сильно регулярным*, если существуют неотрицательные целые числа λ и μ такие, что для любых двух вершин x и y число общих смежных им вершин равно λ или μ в зависимости от того, соединены вершины x, y ребром или нет.

Рассмотрим *граф Кэли* G_f булевой функции f. Вершинами графа являются все двоичные векторы длины n. Две вершины x и y соединены ребром, если вектор $x \oplus y$ принадлежит $\mathrm{supp}(f)$.

В [18] было доказано, что булева функция f является бент-функцией тогда и только тогда, когда граф G_f является сильно регулярным, причем $\lambda = \mu$.

Рассмотрим граф GB_n, вершинами которого являются бент-функции от n переменных, где ребрами соединены функции, находящиеся на минимально возможном расстоянии $2^{n/2}$ друг от друга. В [2] Н.А. Коломейцем было доказано, что число бент-функций, которые находятся на расстоянии $2^{n/2}$ от f, где f — бент-функция от n переменных, не больше, чем $2^{n/2}\prod_{i=1}^{n/2}(2^i+1)$. Оценка достигается тогда и только тогда, когда f — квадратичная бент-функция. В [3] было доказано, что GB_n связный для $n = 2, 4, 6$.

Графами квадратичных бент-функций от шести переменных называются графы на шести вершинах, каждая из которых соответствует одной из шести переменных функции. Если две вершины соединены ребром, то в полиноме Жегалкина функции есть произведение соответствующих переменных. В 2013 году Е. П. Корсаковой была получена классификация таких графов [4].

5.2 Графы Нэги и однородные бент-функции

В этом разделе мы исследуем возможность классификации однородных бент-функций с помощью выделения клик максимального размера в графе специального вида, который называется графом Нэги.

В [68] был определен *граф Нэги* $\Gamma(n,k)$, вершины которого соответствуют $\binom{n}{k}$ неупорядоченным подмножествам размера k множества $\{1,...,n\}$. Две вершины такого графа соединены ребром если рассматриваемые подмножества размера k имеют в точности один общий элемент.

Кликой графа G называется полный подграф графа G. Будем называть *дополнением* к клике графа $\Gamma(n,k)$ множество всех вершин этого графа, которые не входят в рассматриваемую клику.

Рассмотрим случай $n = 6$, $k = 3$. В графе $\Gamma(6,3)$ 20 вершин вида $\{a,b,c\}$, где $a,b,c \in \{1,...,6\}$ и различны. В этом графе максимальный размер клики равен $4 = k + 1$, а количество клик максимального размера равно 30 [27].

Рассмотрим клику C с вершинами $\{1,3,6\}$, $\{1,4,5\}$, $\{2,3,5\}$ и $\{2,4,6\}$. Дополнением к этой клике будет множество, состоящее из 16 вершин. Если мы будем сопоставлять вершине $\{\ell,m,n\}$ моном $x_\ell x_m x_n$, где $\ell,m,n = 1,...,6$, то 16 вершин из дополнения к клике C будут соответствовать 16 мономам алгебраической нор-

мальной формы однородной бент-функции от 6 переменных степени 3 [76]. Более того, в [27] было показано, что все однородные бент-функции от 6 переменных находятся во взаимно однозначном соответствии с дополнениями к кликам максимального размера графа $\Gamma(6,3)$.

Встает вопрос о возможности получения однородных бент-функций от большего числа переменных аналогичным методом.

Отметим, что в графе $\Gamma(6,3)$ максимальный размер клики равен $k+1$. Покажем, что в случае произвольных n и k клика размера $k+1$ существует не всегда.

Утверждение 22. *В графе $\Gamma(n,k)$, где n и k — положительные целые числа, не всегда найдется клика размера $k+1$.*

Доказательство. Рассмотрим граф $\Gamma(12,5)$. Предположим, что в графе существует клика размера $k+1$. Пронумеруем все вершины клики и введем обозначение a_i для числа элементов i-ой вершины, которые не являются общими ни для одной из предыдущих $i-1$ вершин. Так a_1 будет равно пяти, а a_2 — четырем. Для третьей вершины это число будет равно трем, если общие элементы этой вершины с первой и второй вершинами не равны, и четырем в противном случае. Остальные значения a_i показаны в Таблице 6.

Таблица 6

i	1	2	3	5	5	6
a_i	5	4	$\geqslant 3$	$\geqslant 2$	$\geqslant 1$	$\geqslant 0$

Сумма всех a_i не должна превосходить $n = 12$. Однако, в нашем случае $\sum\limits_{i=1}^{6} a_i \geqslant 15$, следовательно, клики размера $k+1$ в графе $\Gamma(12,5)$ не существует. □

В следующей теореме выделено множество графов Нэги, для которых был определен максимальный размер клик, а также точное число клик максимального размера.

Теорема 8. *Пусть $n = \frac{(k+1)k}{2}$, где $k > 1$. Тогда максимальный размер клики в графе $\Gamma(n,k)$ равен $k+1$. При этом количество клик максимального размера равно $\frac{n!}{(k+1)!}$.*

Доказательство. Итеративно построим клику размера $k+1$. Пусть первая вершина – $\{1,2,\ldots,k\}$. Из всего множества $\{1,\ldots,n\}$ мы использовали k элементов. Вторая вершина – $\{1,k+1,\ldots,2k-1\}$, где мы используем первый элемент первой вершины и $k-1$ элемент из множества $\{1,\ldots,n\}\backslash\{1,\ldots,k\}$. Пусть b_i - это

количество элементов множества $\{1,\ldots,n\}$, которые не входят ни в одну из i построенных вершин. Тогда $b_1 = n - k$ и $b_2 = n - k - (k-1)$. Для построения l-й вершины, возьмем $(l-1)$-й элемент из каждой ранее построенной вершины. Тогда $b_l = n - k - (k-1) - \ldots - (k-l+1)$. Следовательно, после построения k-й вершины будут использованы все элементы множества $\{1,\ldots,n\}$, так как $1+2+\ldots+k = \frac{k(k+1)}{2} = n$. Для построения $k+1$ вершины будут использоваться k-ые элементы k ранее построенных вершин.

Теперь покажем, что клики большего размера в графе $\Gamma(n,k)$ быть не может. Предположим обратное. Пусть в графе $\Gamma(n,k)$ существует клика размера $k+2$. Тогда любая вершина должна иметь общие элементы с $k+1$ вершинами. Каждая вершина содержит только k элементов, следовательно, есть две другие вершины, которые имеют с ней один и тот же общий элемент.

Как и в случае клики размера $k+1$ будем строить клику размера $k+2$ итеративно. Без ограничения общности в качестве первых трех вершин возьмем следующие: $\{1,\ldots,k\}$, $\{1,k+1,\ldots,2k-1\}$, $\{1,2k,\ldots,3k-2\}$. Пусть b'_i - это количество элементов множества $\{1,\ldots,n\}$, которые не входят ни в одну из i построенных вершин. Поскольку $b'_3 = n - k - 2(k-1) < b_3$, то $b'_i < b_i$ для $i \geqslant 3$. Следовательно, $b_k < 0$ и клики размера $k+2$ в графе $\Gamma(n,k)$ не существует.

Таким образом, клики максимального размера не содержат более двух вершин, которые имеют один и тот же общий элемент. Если мы будем помечать каждое ребро значением элемента, который является общим для двух вершин, которые это ребро соединяет, то в кликах максимального размера не будет ребер, помеченных одинаковыми значениями. Поскольку клика размера $k+1$ имеет $\frac{(k+1)k}{2}$ ребер, ребра помечаются значениями от 1 до n.

Теперь посчитаем количество клик максимального размера в графе $\Gamma(n,k)$, где $n = \frac{(k+1)k}{2}$. Число способов пометить ребра значениями от 1 до n равно $n!$. При этом каждая клика будет встречаться $(k+1)!$ раз. Таким образом, количество клик максимального размера равно $\frac{n!}{(k+1)!}$. □

Отметим, что $\Gamma(6,3)$ принадлежит к числу тех графов $\Gamma(n,k)$, для которых справедливо равенство $n = \frac{(k+1)k}{2}$.

В графе $\Gamma(10,4)$ была выделена клика, вершинами которой являются подмножества $\{1,2,3,4\}$, $\{1,5,6,7\}$, $\{2,5,8,9\}$, $\{3,6,8,10\}$, $\{4,7,9,10\}$. Дополнению этой клики была сопоставлена алгебраическая нормальная форма булевой функции от 10 переменных: каждой вершине $\{a,b,c,d\}$ сопоставляем моном $x_a x_b x_c x_d$, где

$a,b,c,d \in \{1,\ldots,n\}$. Затем все мономы суммируются по модулю два. Дополнению клики с вершинами

$$\{1,2,3,4,5,6,7\}, \{1,8,9,10,11,12,13\}, \{2,8,14,15,16,17,18\},$$
$$\{3,9,14,19,20,21,22\}, \{4,10,15,19,23,24,25\}, \{5,11,16,20,23,26,27\},$$
$$\{6,12,17,21,24,26,28\}, \{7,13,18,22,25,27,28\}$$

графа $\Gamma(28,7)$ была сопоставлена однородная булева функция от 28 переменных степени 7 аналогичным способом. Веса Хэмминга полученных функций равны 628 и $50\ 526\ 464$ соответственно. Из Леммы 12 обе функции не являются бент-функциями.

Отметим, что следующим шагом может быть исследование других значений n и k, при которых максимальный размер клики в графе $\Gamma(n,k)$ будет отличаться от $k+1$.

Заключение

Приведем список основных результатов данной работы.

1. Предложен метод построения уравновешенных функций от четного числа $n \geqslant 20$ переменных с нелинейностью $2^{n-1}-(2^{\frac{n}{2}-1}+2^{\frac{n}{2}-3}+2^{\frac{n}{2}-5}+2^{\frac{n}{2}-7})$ без линейных структур. Полученные значения нелинейности уравновешенных функций являются наибольшими достигнутыми для указанного числа переменных.
2. Представлена конструкция бент-функций, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных. Получено необходимое и достаточное условие того, что уравновешенная функция, которая линейно зависит хотя бы от одной из своих переменных, является производной бент-функции.
3. Доказано, что гипотеза о разложении булевых функций в сумму двух бент-функций верна в том и только том случае, если гипотеза о производных бент-функций верна для уравновешенных функций, которые линейно зависят хотя бы от одной из своих переменных.
4. Доказано, что любая квадратичная уравновешенная функция, которая может быть производной булевой функции, является производной бент-функции. Получено точное число бент-функций, имеющих некоторую отличную от константы аффинную функцию своей производной. Как следствие получена итеративная нижняя оценка числа бент-функций.
5. Известно, что каждая однородная бент-функция от 6 переменных степени 3 соответствует дополнению клики максимального размера в графе Нэги $\Gamma(6,3)$. Доказано, что для графа Нэги $\Gamma(n,k)$, где $n = \frac{(k+1)k}{2}$, максимальный размер клики равен $k+1$ и точное число клик максимального размера в таких графах равно $\frac{n!}{(k+1)!}$. Установлено, что функции, соответствующие дополнениям клик максимального размера в графах $\Gamma(10,4)$ и $\Gamma(28,7)$, не являются бент-функциями.

Список литературы

1. *Коломеец Н. А.* О верхней оценке нелинейности некоторого класса булевых функций с максимальной алгебраической иммунностью // Прикладная дискретная математика. — 2013. — Т. 1, № 19. — С. 14—16.
2. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. — 2014. — Т. 3, № 25. — С. 28—39.
3. *Коломеец Н. А.* О связности графа минимальных расстояний множества бент-функций // Прикладная дискретная математика. Приложение. — 2015. — № 8. — С. 33—34.
4. *Корсакова Е. П.* Классификация графов квадратичных бент-функций от шести переменных // Дискретный анализ и исследование опереаций. — 2013. — Т. 20, № 5. — С. 45—57.
5. *Лобанов М. С.* Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. — 2006. — Т. 18, № 3. — С. 152—159.
6. Булевы функции в теории кодирования и криптологии / О. А. Логачев [и др.]. — ЛЕНАНД, 2015. — 576 с.
7. *Панкратова И. А.* Булевы функции в криптографии: Учебное пособие. — ТГУ, 2014. — 88 с.
8. *Таранников Ю. В.* Комбинаторные свойства дискретных структур и приложения к криптологии. — МЦНМО, 2011. — 152 с.
9. *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. — 2009. — Т. 1, № 3. — С. 15—37.
10. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретный анализ и исследование операций. — 2010. — Т. 17, № 1. — С. 34—64.
11. *Токарева Н. Н.* О разложении дуальной бент-функции в сумму двух бент-функций // Прикладная дискретная математика. — 2014. — Т. 4, № 26. — С. 59—61.
12. *Токарева Н. Н.* О множестве производных булевой бент-функции // Прикладная дискретная математика. Приложение. — 2016. — № 9. — С. 35.

13. *Фролова А. А.* Существенная зависимость бент-функций Касами от произведений переменных // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 1. — С. 77—92.

14. *Adams C. M.* Constructing Symmetric Ciphers Using the CAST Design Procedure // Designs, Codes and Cryptography. — 1997. — Vol. 12, no. 3. — P. 283—316.

15. *Agievich S. V.* On the representation of bent functions by bent rectangles // Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference, Petrozavodsk, Russia, June 1-6, 2000. — Berlin, Boston : De Gruyter, 2002. — P. 121—136.

16. *Agievich S. V.* Bent rectangles // Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Zvenigorod, September 8–18, 2007). — Netherlands : IOS Press, 2008. — P. 3—22.

17. *Bernasconi A.*, *Codenotti B.* Spectral analysis of Boolean functions as a graph eigenvalue problem // IEEE Transactions on Computers. — 1999. — Vol. 48, no. 3. — P. 345—351.

18. *Bernasconi A.*, *Codenottl B.*, *Vanderkam J. M.* A characterization of bent functions in terms of strongly regular graphs // IEEE Transactions on Computers. — 2001. — Vol. 50, no. 9. — P. 984—985.

19. *Canteaut A.*, *Charpin P.* Decomposing bent functions // IEEE Transactions on Information Theory. — 2003. — Vol. 49, no. 8. — P. 2004—2019.

20. *Canteaut A.*, *Charpin P.*, *Kyureghyan G. M.* A new class of monomial bent functions // Finite Fields and Their Applications. — 2008. — Vol. 14, no. 1. — P. 221—241.

21. Finding nonnormal bent functions / A. Canteaut [et al.] // Discrete Applied Mathematics. — 2006. — Vol. 154, no. 2. — P. 202—218.

22. *Carlet C.*, *Mesnager S.* Four decades of research on bent functions // Designs, Codes and Cryptography. — 2016. — Vol. 78. — P. 5—50.

23. *Carlet C.* On the Secondary Constructions of Resilient and Bent Functions // Coding, Cryptography and Combinatorics. — Basel : Birkhäuser Basel, 2004. — P. 3—28.

24. *Carlet C.* Correlation Immune and Resilient Boolean Functions // Encyclopedia of Cryptography and Security. — Boston, MA : Springer US, 2011. — P. 262—264.

25. *Carlet C.*, *Klapper A.* Upper bounds on the numbers of resilient functions and of bent functions // 23rd Symposium on Information Theory. — Benelux, Belgium, 2002. — P. 307—314.

26. Evolving Constructions for Balanced, Highly Nonlinear Boolean Functions / C. Carlet [et al.]. — 2022. — available at https://arxiv.org/abs/2202.08743.

27. *Charnes C.*, *Rötteler M.*, *Beth T.* Homogeneous Bent Functions, Invariants, and Designs // Designs, Codes and Cryptography. — 2002. — Vol. 26, no. 1. — P. 139—154.

28. *Climent J.-J.*, *García F. J.*, *Requena V.* On the construction of bent functions of $n + 2$ variables from bent functions of n variables // Advances in Mathematics of Communications. — 2008. — Vol. 2, no. 4. — P. 421—431.

29. *Climent J.-J.*, *García F. J.*, *Requena V.* A construction of bent functions of $n + 2$ variables from a bent function of n variables and its cyclic shifts // Algebra. — 2014. — Vol. 2014.

30. *Cusick T. W.*, *Stănică P.* Cryptographic Boolean Functions and Applications. — 2nd ed. — Acad. Press, 2017. — 288 p.

31. *Dillon J. F.* Elementary Hadamard difference sets : PhD thesis / Dillon J. F. — Univ. of Maryland, 1974.

32. *Dillon J. F.*, *Dobbertin H.* New cyclic difference sets with Singer parameters // Finite Fields and Their Applications. — 2004. — Vol. 10, no. 3. — P. 342—389.

33. *Dillon J.* A survey of bent functions // NSA Technical Journal. — 1972. — P. 191—215.

34. *Dobbertin H.*, *Leander G.* Cryptographer's toolkit for construction of 8-bit bent functions. — 2005. — Cryptology ePrint Archive, Report 2005/089, available at http://eprint.iacr.org.

35. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1995. — P. 61—74.

36. *Dubuc S.* Linear structures of Boolean functions // Proceedings. 1998 IEEE International Symposium on Information Theory. — 1998. — P. 440.

37. *Fedorova M.*, *Tarannikov Y.* On the Constructing of Highly Nonlinear Resilient Boolean Functions by Means of Special Matrices // Progress in Cryptology — INDOCRYPT 2001. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2001. — P. 254—266. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 2247).

38. On a Conjecture about Binary Strings Distribution / J.-P. Flori [et al.] // Sequences and Their Applications – SETA 2010. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2010. — P. 346—358. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 6338).

39. *Gangopadhyay S.*, *Pasalic E.*, *Stănică P.* A Note on Generalized Bent Criteria for Boolean Functions // IEEE Transactions on Information Theory. — 2013. — Vol. 59, no. 5. — P. 3233—3236.

40. *Gini A.*, *Méaux P.* Weightwise Perfectly Balanced Functions and Nonlinearity // Codes, Cryptology and Information Security. — Cham : Springer Nature Switzerland, 2023. — P. 338—359. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 13874).

41. A Stream Cipher Proposal: Grain-128 / M. Hell [et al.] // 2006 IEEE International Symposium on Information Theory. — 2006. — P. 1614—1618.

42. *Helleseth T.*, *Kholosha A.* Monomial and quadratic bent functions over the finite fields of odd characteristic // IEEE Transactions on Information Theory. — 2006. — Vol. 52, no. 5. — P. 2018—2032.

43. *Hodzic S.*, *Meidl W.*, *Pasalic E.* Full Characterization of Generalized Bent Functions as (Semi)-Bent Spaces, Their Dual, and the Gray Image // IEEE Transactions on Information Theory. — 2018. — Vol. 64, no. 7. — P. 5432—5440.

44. *Hodzic S.*, *Pasalic E.* Generalized Bent Functions - Some General Construction Methods and Related Necessary and Sufficient Conditions // Cryptography and Communications. — 2015. — Vol. 7, no. 4. — P. 469—483.

45. *Hou X.-D.* q-Ary bent functions constructed from chain rings // Finite Fields and Applications. — 1998. — Vol. 4, no. 1. — P. 55—61.

46. *Hou X.-D.* p-Ary and q-ary versions of certain results about bent functions and resilient functions // Finite Fields and Applications. — 2004. — Vol. 10, no. 4. — P. 566—582.

47. *Hu X.*, *Yang B.*, *Huang M.* A construction of highly nonlinear Boolean functions with optimal algebraic immunity and low hardware implementation cost // Discrete Applied Mathematics. — 2020. — Vol. 285. — P. 407—422.

48. *Kavut S.*, *Maitra S.*, *Yucel M. D.* Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class // IEEE Transactions on Information Theory. — 2007. — Vol. 53, no. 5. — P. 1743—1751.

49. *Kolomeec N.* The graph of minimal distances of bent functions and its properties // Designs, Codes and Cryptography. — 2017. — Vol. 85, no. 3. — P. 395—410.

50. *Kolomeec N.* Some general properties of modified bent functions through addition of indicator functions // Cryptography and Communications. — 2021. — Vol. 13, no. 6. — P. 909—926.

51. *Kumar P. V.*, *Scholtz R. A.*, *Welch L. R.* Generalized bent functions and their properties // Journal of Combinatorial Theory, Series A. — 1985. — Vol. 40, no. 1. — P. 90—107.

52. *Kutsenko A.* Metrical properties of self-dual bent functions // Designs, Codes and Cryptography. — 2020. — Vol. 88, no. 1. — P. 201—222.

53. *Kutsenko A. V.*, *Tokareva N. N.* Metrical properties of the set of bent functions in view of duality // Prikladnaya Diskretnaya Matematika. — 2020. — No. 49. — P. 18—34.

54. *Langevin P.*, *Leander G.* Monomial bent functions and Stickelberger's theorem // Finite Fields and Their Applications. — 2008. — Vol. 14, no. 3. — P. 727—742.

55. *Leander N. G.* Monomial bent functions // IEEE Transactions on Information Theory. — 2006. — Vol. 52, no. 2. — P. 738—743.

56. *MacWilliams F. J.*, *Sloane N. J. A.* The Theory of Error-Correcting Codes. — North-Holland Publishing Company, 1977. — 782 p.

57. *Maitra S.*, *Sarkar P.* Maximum nonlinearity of symmetric Boolean functions on odd number of variables // IEEE Transactions on Information Theory. — 2002. — Vol. 48, no. 9. — P. 2626—2630.

58. *Mandal B.*, *Gangopadhyay S.*, *Stănică P.* Cubic Maiorana-McFarland bent functions with no affine derivative // International Journal of Computer Mathematics: Computer Systems Theory. — 2017. — Vol. 2, no. 1. — P. 14—27.

59. *Martinsen T.*, *Meidl W.*, *Stănică P.* Generalized Bent Functions and Their Gray Images // Arithmetic of Finite Fields. — Cham : Springer International Publishing, 2016. — P. 160—173. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 10064).

60. Decomposing Generalized Bent and Hyperbent Functions / T. Martinsen [et al.] // IEEE Transactions on Information Theory. — 2017. — Vol. 63, no. 12. — P. 7804—7812.

61. *Matsui M.* 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).

62. *Matsui M.* The First Experimental Cryptanalysis of the Data Encryption Standard // Advances in Cryptology — CRYPTO '94. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1994. — P. 1—11.

63. *Matsui M.*, *Yamagishi A.* A New Method for Known Plaintext Attack of FEAL Cipher // Advances in Cryptology — EUROCRYPT' 92. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1993. — P. 81—91.

64. *McFarland R. L.* A family of difference sets in non-cyclic groups // Journal of Combinatorial Theory, Series A. — 1973. — Vol. 15, no. 1. — P. 1—10.

65. *Meidl W.* A survey on p-ary and generalized bent functions // Cryptography and Communications. — 2022. — Vol. 14, no. 4. — P. 737—782.

66. On the degree of homogeneous bent functions / Q. Meng [et al.] // Discrete Applied Mathematics. — 2007. — Vol. 155, no. 5. — P. 665—669.

67. *Mesnager S.* Bent functions: Fundamentals and results. — Springer, 2016. — 544 p.

68. *Nagy Z.* A constructive estimation of the Ramsey number // Mat. Lapok. — 1972. — Vol. 23. — P. 301—302. — in Hungarian.

69. *Olsen J.*, *Scholtz R.*, *Welch L.* Bent-function sequences // IEEE Transactions on Information Theory. — 1982. — Vol. 28, no. 6. — P. 858—864.

70. *Picek S.*, *Sisejkovic D.*, *Jakobovic D.* Immunological algorithms paradigm for construction of Boolean functions with good cryptographic properties // Engineering Applications of Artificial Intelligence. — 2017. — Vol. 62. — P. 320—330.

71. *Polujan A. A.*, *A. P.* Cubic bent functions outside the completed Maiorana-McFarland class // Designs, Codes and Cryptography. — 2020. — Vol. 88, no. 9. — P. 1701—1722.

72. *Potapov V. N.* An Upper Bound on the Number of Bent Functions // 2021 XVII International Symposium ”Problems of Redundancy in Information and Control Systems” (REDUNDANCY). — Moscow, Russian Federation, 2021. — P. 95—96.

73. *Potapov V. N.* Existence of balanced functions that are not derivative of bent functions // 2023 XVIII International Symposium ”Problems of Redundancy in Information and Control Systems” (REDUNDANCY). — Moscow, Russian Federation, 2023. — P. 51—53.

74. *Potapov V. N.*, *Taranenko A. A.*, *Tarannikov Y. V.* An asymptotic lower bound on the number of bent functions // Designs, Codes and Cryptography. — 2023.

75. *Preneel B.* Analysis and design of cryptographic hash functions : PhD thesis / Preneel B. — Leuven, Belgium : Katholieke Universiteit Leuven, 1993.

76. *Qu C.*, *Seberry J.*, *Pieprzyk J.* Homogeneous bent functions // Discrete Applied Mathematics. — 2000. — Vol. 102, no. 1. — P. 133—139.

77. New Results on the Boolean Functions That Can Be Expressed as the Sum of Two Bent Functions / L. Qu [et al.] // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. — 2016. — Vol. E99.A, no. 8. — P. 1584—1590.

78. *Rodier F.* Asymptotic Nonlinearity of Boolean Functions // Designs, Codes and Cryptography. — 2006. — Vol. 40, no. 1. — P. 59—70.

79. *Rothaus O. S.* On “bent” functions // Journal of Combinatorial Theory, Series A. — 1976. — Vol. 20, no. 3. — P. 300—305.

80. *Schmidt K.-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // IEEE Transactions on Information Theory. — 2006. — Vol. 55, no. 4. — P. 1824—1832.

81. *Seberry J.*, *Zhang X.-M.*, *Zheng Y.* Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics // Advances in Cryptology — CRYPTO' 93. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1994. — P. 49—60. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 773).

82. *Siegenthaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Transactions on Information Theory. — 1984. — Vol. 30, no. 5. — P. 776—780.

83. *Singh D.*, *Bhaintwal M.*, *Singh B. K.* Some results on q-ary bent functions // International Journal of Computer Mathematics. — 2013. — Vol. 90, no. 9. — P. 1761—1773.

84. Bent and generalized bent Boolean functions / P. Stanica [et al.] // Designs, Codes and Cryptography. — 2013. — Vol. 69, no. 1. — P. 77—94.

85. *Tarannikov Y. V.* On Resilient Boolean Functions with Maximal Possible Nonlinearity // Progress in Cryptology —INDOCRYPT 2000. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2000. — P. 19—30. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 1977).

86. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances in Mathematics of Communications. — 2011. — Vol. 5, no. 4. — P. 609—621.

87. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. — Academic Press, 2015. — 220 p.

88. *Tokareva N. N.* A quadratic part of a bent function can be any // Siberian Electronic Mathematical Reports. — 2022. — Vol. 19, no. 1. — P. 342—347.

89. *Tu Z.*, *Deng Y.* A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity // Designs, Codes and Cryptography. — 2011. — Vol. 60, no. 1. — P. 1—14.

90. Homogeneous bent functions of degree n in 2n variables do not exist for $n > 3$ / T. Xia [et al.] // Discrete Applied Mathematics. — 2004. — Vol. 142, no. 1. — P. 127—132.

91. *Zhang B.*, *Lü S.* I/O correlation properties of bent functions // Science in China Series E: Technological Sciences. — 2000. — Vol. 43, no. 3. — P. 282—286.

92. *Zheng Y.*, *Pieprzyk J.*, *Seberry J.* HAVAL — A one-way hashing algorithm with variable length of output (extended abstract) // Advances in Cryptology — AUSCRYPT '92. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1993. — P. 81—104. — Part of the Lecture Notes in Computer Science book series (LNCS, volume 718).

93. *Zhiyao Y.*, *Pinhui K.*, *Zhixiong C.* New Secondary Constructions of Generalized Bent Functions // Chinese Journal of Electronics. — 2021. — Vol. 30, no. 6. — P. 1022—1029.

Публикации автора по теме диссертации

94. *Шапоренко А. С.* Конструкция уравновешенных функций с высокой нелинейностью и другими криптографическими свойствами // Прикладная дискретная математика. — 2024. — № 63. — С. 8—24.

95. *Shaporenko A.* Derivatives of bent functions in connection with the bent sum decomposition problem // Designs, Codes and Cryptography. — 2023. — Vol. 91, no. 5. — P. 1607—1625.

96. *Tokareva N. N.*, *Shaporenko A. S.*, *Solé P.* Connections between quaternary and Boolean bent functions // Siberian Electronic Mathematical Reports. — 2021. — Vol. 18, no. 1. — P. 561—578.

97. *Шапоренко А. С.* Связь однородных бент-функций и графов Нэги // Дискретный анализ и исследование операций. — 2019. — Т. 26, № 4. — С. 121—131.

98. *Shaporenko A.* New approaches to the study of the "bent sum decomposition problem" // Proceedings of the 7th workshop Boolean Functions and their Applications (BFA 2022), Balestrand, Norway, September 11-16, 2022. — 2022.

99. *Шапоренко А. С.* О производных булевых бент-функций // Прикладная дискретная математика. Приложение. — 2021. — № 14. — С. 57—58.

100. *Shaporenko A.* On relationship between quaternary and Boolean bent functions // Proceedings of Fifth Conference on Software Engineering and Information Management (SEIM-2020), Saint Petersburg, Russia, May 16, 2020. — 2020. — P. 19—23.

101. *Шапоренко А. С.* Связь между кватернарными и компонентными булевыми бент-функциями // Прикладная дискретная математика. Приложение. — 2020. — № 13. — С. 35—37.

102. *Шапоренко А. С.* О взаимосвязи между кватернарными и булевыми бент-функциями // Прикладная дискретная математика. Приложение. — 2019. — № 12. — С. 73—75.

103. *Шапоренко А. С.* Связь однородных бент-функций и графов пересечений // Прикладная дискретная математика. Приложение. — 2018. — № 11. — С. 52—53.