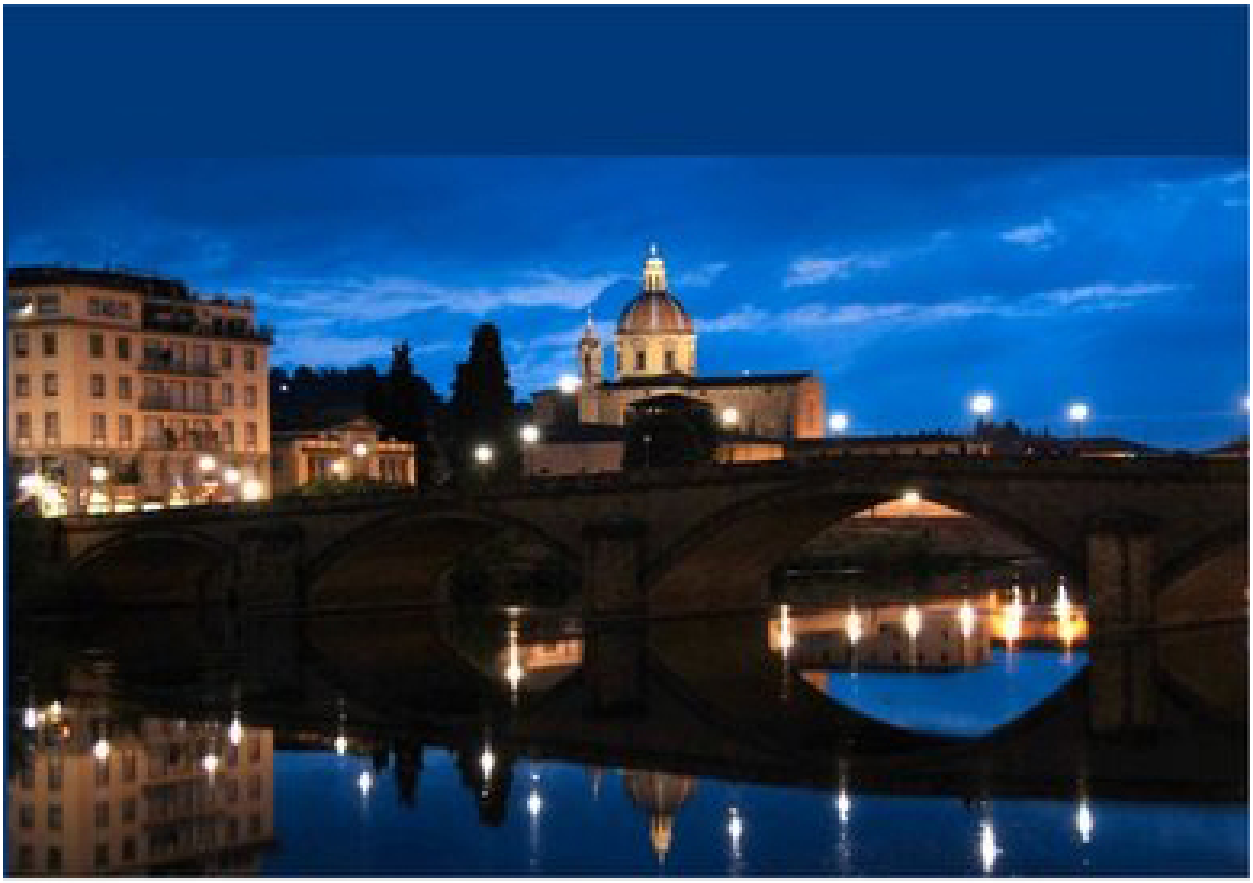


Наталья Токарева

Нелинейные булевы функции: бент-функции и их обобщения

теоретические результаты

LAP LAMBERT Academic Publishing

Наталья Токарева

«Нелинейные булевы функции: бент-функции и их обобщения»

теоретические результаты

Работа относится к такой области дискретной математики, как булевы функции и их приложения в комбинаторике, теории кодирования и криптографии. Исследуется класс булевых функций, обладающих сильными свойствами нелинейности: бент-функции и их обобщения. Впервые бент-функции начали изучаться в 60-х годах XX века в связи с их приложениями в криптографии. Использование нелинейных булевых функций в качестве компонент современных шифров позволяет повышать стойкость шифров к методам линейного и дифференциального криптоанализа. В настоящее время нелинейные булевы функции исследуются по всему миру очень активно. Тем не менее, в этой области остается множество открытых вопросов. В работе приводится подробный обзор основных результатов в области бент-функций; рассматриваются их теоретические и практические приложения; приводится систематический обзор обобщений бент-функций. Устанавливается группа автоморфизмов множества бент-функций. Предлагается новое обобщение бент-функций, позволяющее поэтапно усиливать их нелинейные свойства. Книга предназначена для специалистов в области булевых функций и криптографии, преподавателей и студентов.

LAP LAMBERT Academic Publishing (Saarbrucken, Germany)

ISBN: 978-3-8433-0904-2

2011

Образец цитирования:
Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения // Издательство LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011. ISBN: 978-3-8433-0904-2. 180 с.

Оглавление

Введение

Bent functions deserve
our bent to study them...[1]

Работа относится к такой области дискретной математики, как булевы функции и их приложения в комбинаторике, теории кодирования и криптографии. Исследуется класс булевых функций, обладающих сильными свойствами нелинейности: бент-функции и их обобщения.

Мера нелинейности является важной характеристикой булевой функции в криптографии. Линейность и близкие к ней свойства часто свидетельствуют о простой (в определенном смысле) структуре этой функции и, как правило, представляют собой богатый источник информации о многих других ее свойствах. Задача построения булевых функций, обладающих нелинейными свойствами, естественным образом возникает во многих областях дискретной математики. И часто наибольший интерес вызывают те функции, для которых эти свойства экстремальны. Такие булевы функции называются бент-функциями. Впервые они начали исследоваться в 60-х годах XX века в связи с криптографическими приложениями.

Бент-функцию можно определить как функцию, которая крайне плохо аппроксимируется аффинными функциями. В блочных и поточных шифрах бент-функции и их векторные аналоги способствуют предельному повышению стойкости этих шифров к линейному и дифференциальному методам криптоанализа — основным статистическим методам криптоанализа шифров. Например, в 1993 году была обнаружена существенная слабость к линейному криптоанализу блочного шифра DES. Этот шифр являлся

[1]Игра слов: «Бент-функции заслуживают нашего стремления изучить их...» (англ.)

стандартом симметричного шифрования США на протяжении почти двадцати лет (с 1980 года по 1998 год). Слабость шифра, которая привела к успешной атаке на него, заключалась в плохих криптографических свойствах его нелинейных компонент, так называемых S-блоков. Математически, S-блок — это векторная булева функция, отображающая n входных битов в m выходных битов. Именно эти булевы функции в шифре DES не отвечали необходимым криптографическим требованиям, что и послужило причиной успеха метода линейного криптоанализа. Шифр DES оказался нестойким и к дифференциальному методу криптоанализа. Причина вновь заключалась в слабых S-блоках шифра. Стойкость шифров к упомянутым методам криптоанализа достигается за счет использования бент-функций, их аналогов и обобщений при построении S-блоков. Это было сделано, например, в канадском шифре CAST и новом американском стандарте AES.

В настоящее время нелинейные булевы функции исследуются по всему миру очень активно. Тем не менее, в этой области остается множество открытых вопросов.

В книге приводится подробный обзор основных результатов в области бент-функций, рассматриваются их теоретические и практические приложения (Глава 1); приводится систематический обзор обобщений бент-функций (Глава 2); устанавливается группа автоморфизмов множества бент-функций (Глава 3); предлагается новое обобщение бент-функций, позволяющее поэтапно усиливать их нелинейные свойства (Главы 4, 5).

Глава 1

Бент-функции: результаты и приложения

В данной главе приводится обзор основных результатов в области бент-функций. Рассматриваются их теоретические и практические приложения. Отдельно приводится список нерешенных вопросов.

1.1 Булевы функции

Пусть $\mathbb{Z}_2 = \{0, 1\}$. Через $\mathbb{Z}_2^n$ будем обозначаем множество всех двоичных векторов $\mathbf{v} = (v_1, \ldots, v_n)$ длины n. Будем считать, что все векторы лексикографически упорядочены. Например, при $n = 3$ порядок векторов следующий $(000), (001), (010), (011), (100), (101), (110), (111)$.

Произвольная функция из множества $\mathbb{Z}_2^n$ в множество $\mathbb{Z}_2$ называется *булевой функцией от n переменных*. Например,

$f : \mathbb{Z}_2^2 \to \mathbb{Z}_2$ такая, что $f(00) = 1$, $f(01) = 0$, $f(10) = 0$, $f(11) = 1$;

$g : \mathbb{Z}_2^3 \to \mathbb{Z}_2$ такая, что она принимает значение 1 на векторах с двумя единицами и 0 на всех остальных.

Функции такого вида названы булевыми в честь известного английского математика и философа Джорджа Буля (1815–1864).

Улица, на которой жил Джордж Буль с 1849 по 1855 годы, Корк, Ирландия. Его дом — крайний справа.

Каждую булеву функцию от n переменных можно однозначно определить вектором ее значений длины 2^n. Например, функциям f и g соответствуют векторы (1001) и (00010110). Пусть далее $\boldsymbol{f}$ обозначает вектор значений длины 2^n функции f. Будем считать, что аргументы функции (т. е. векторы длины n) перебираются в лексикографическом порядке.

Пусть $\oplus$ обозначает сложение по модулю 2 (операцию XOR). Известно, что каждая булева функция однозначно может быть задана своей *алгебраической нормальной формой* (АНФ), а именно представлена в виде

$$f(\boldsymbol{v}) = \left(\bigoplus_{k=1}^{n} \bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k}\, v_{i_1} \cdot \ldots \cdot v_{i_k} \right) \oplus a_0,$$

где при каждом k индексы $i_1, \ldots, i_k$ различны и в совокупности пробегают все k-элементные подмножества множества $\{1, \ldots, n\}$. Коэффициенты $a_{i_1,\ldots,i_k}$, a_0 принимают значения 0 или 1. В русскоязычной литературе АНФ также называют *полиномом Жегалкина*.

Например, для функций f и g, приведенных выше, имеем формулы

$f(v_1, v_2) = v_1 \oplus v_2 \oplus 1$,

$g(v_1, v_2, v_3) = v_1v_2v_3 \oplus v_1v_2 \oplus v_1v_3 \oplus v_2v_3$.

Степенью нелинейности $\deg(f)$ булевой функции f называется число переменных в самом длинном слагаемом ее АНФ. Функция называется *аффинной*, *квадратичной*, *кубической* и т. д., если ее степень равна соответственно 1, 2, 3 и т. д. Каждая аффинная функция от n переменных $v_1, \ldots, v_n$ имеет вид $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \oplus a$ для подходящих вектора $\boldsymbol{u}$ и константы a.

1.2 Определение бент-функции

Пусть $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = u_1v_1 \oplus \ldots \oplus u_nv_n$ — скалярное произведение векторов. Через $\mathrm{dist}(f, g)$ обозначим *расстояние Хэмминга* между функциями f и g, т. е. число позиций, в которых различаются векторы $\boldsymbol{f}$ и $\boldsymbol{g}$.

Максимально нелинейной называется булева функция от n переменных (n любое) такая, что расстояние Хэмминга N_f от данной функции до множества всех аффинных функций является максимально возможным. Величину N_f называют *нелинейностью* булевой функции. В случае четного n максимально возможное значение нелинейности равно $2^{n-1} - 2^{(n/2)-1}$. В случае нечетного n точное значение максимального расстояния неизвестно (поиск этого значения или его оценок представляет весьма любопытную и сложную комбинаторную задачу [151, 132]). Термин «максимально нелинейная функция» принят в русскоязычной литературе, тогда как в англоязычной широкое распространение получил термин «бент-функция» (от англ. bent — изогнутый, наклоненный). Аналогия между терминами не полная. При четном числе переменных n бент-функции и максимально нелинейные функции совпадают, а при нечетном n бент-функции (в отличие от максимально нелинейных) не существуют.

Преобразованием Уолша—Адамара булевой функции f от n переменных называется целочисленная функция W_f, заданная на множестве $\mathbb{Z}_2^n$ равен-

ством

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

Справедливо равенство Парсеваля,

$$\sum_{\boldsymbol{v}\in\mathbb{Z}_2^n} \left(W_f(\boldsymbol{v})\right)^2 = 2^{2n}.$$

Поскольку число всех коэффициентов $W_f(\boldsymbol{v})$ равно 2^n, из равенства следует, что максимум модуля коэффициента Уолша—Адамара не может быть меньше величины $2^{n/2}$. Нелинейность N_f произвольной функции f тесно связана с ее коэффициентами Уолша—Адамара, а именно

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

Очевидно, что чем меньше максимум модуля коэффициента $W_f(\boldsymbol{v})$, тем выше нелинейность функции f.

Бент-функцией называется булева функция от n переменных (n четно) такая, что модуль каждого коэффициента Уолша—Адамара этой функции равен $2^{n/2}$. Другими словами, f — бент-функция, если максимум модуля $W_f(\boldsymbol{v})$ достигает своего минимального возможного значения. В силу равенства Парсеваля это имеет место, только если модули всех коэффициентов Уолша—Адамара этой функции совпадают и равны $2^{n/2}$. Таким образом, эквивалентность определению максимально нелинейной функции (при четном n) становится очевидной.

Множество всех бент-функций от n переменных обозначим через $\mathcal{B}_n$.

1.3 Краткая история

Впервые бент-функции были введены О. Ротхаусом в 60-х годах XX века. Выпускник Принстонского университета Оскар Ротхаус (1927–2003) после службы во время Корейской войны в войсках связи поступил на работу математиком в Агентство Национальной Безопасности США. С 1960 по

1966 годы он работал в Институте оборонного анализа (IDA). Его криптографические работы того времени оценивались руководством IDA достаточно высоко. Как и его преподавательская деятельность: «he was one of the most important teachers of cryptology to mathematicians and mathematics to cryptologists» [47]. На это же время приходится и его первая работа о бент-функциях [184]. В открытой печати она появилась только в 1976 году [185]. В ней были установлены базовые свойства бент-функций, предложены их простейшие конструкции и намечена классификация бент-функций от шести переменных. В дальнейшем Оскар Ротхаус не занимался бент-функциями. С 1966 года он работал в Корнелльском Университете (NY).

В Советском Союзе тоже занимались бент-функциями в 60-х годах, однако, имена первых исследователей пока не переданы широкой огласке.

К числу первых работ относятся и исследования американских математиков Дж. Диллона [106] и Р. Л. МакФарланда [157], которые в 70-х годах рассматривали бент-функции в связи с разностными множествами.

С 80-х годов бент-функции начинают интенсивно изучаться по всему миру. В настоящее время известны сотни работ о бент-функциях и близких вопросах. Получены серии конструкций бент-функций, но тем не менее класс всех бент-функций от n переменных до сих пор не описан, для мощности этого класса не найдена асимптотика и не установлено даже приемлемых нижних и верхних оценок. Малый прогресс в этой области связан с тем, что несмотря на простые формулировки задачи здесь очень сложны. Можно сказать, что в действительности класс бент-функций еще не исследован.

Интересно, что в одном из своих последних годовых отчетов (2001–2002) Оскар Ротхаус писал о том, что вернулся к исследованиям своей молодости: к кодам и бент-функциям, и получил новые неожиданные результаты [46]. К сожалению, они так и остались неопубликованными. Тем более жаль, что Оскар Ротхаус, как никто другой, знал цену результатам в этой области.

Стэйт Стрит, ведущая к Корнелльскому университету, Итака, штат Нью-Йорк. В этом университете с 1966 по 2003 год работал Оскар Ротхаус.

1.4 Приложения бент-функций

Впечатляют масштабы исследования бент-функций. В настоящее время множество математиков и инженеров по всему миру регулярно публикуют свои статьи по этой тематике. Результаты обсуждаются на таких международных конференциях, как EUROCRYPT, CRYPTO, SETA, FSE, BFCA, SIBECRYPT и многих других.

Актуальность исследования бент-функций подтверждается их многочисленными теоретическими и практическими приложениями в комбинаторике, алгебре, теории кодирования, теории информации, теории символьных последовательностей, криптографии и криптоанализе. Приведем (далеко не полную) серию таких примеров.

Дискретная математика. Классическая комбинаторная задача построения *матриц Адамара* порядка N, известная с 1893 г., в случае $N = 2^n$

(n четно) при некоторых ограничениях сводится к задаче построения бент-функций от n переменных [185] (см. далее теорему 1).

В теории конечных групп построение *элементарных адамаровых разностных множеств* специального вида эквивалентно построению максимально нелинейных булевых функций (см. [19] и теорему 5).

Теория кодирования. В теории кодирования широко известна задача определения радиуса покрытия произвольного *кода Рида—Маллера*, которая эквивалентна (в случае кодов первого порядка) поиску наиболее нелинейных булевых функций [132,151]. В теории оптимальных кодов специальные семейства квадратичных бент-функций определяют класс *кодов Кердока* [133], обладающих исключительным свойством: вместе с растущим кодовым расстоянием (при увеличении длины кода) каждый код Кердока имеет максимально возможную мощность (см. [27,102]). Этим свойством коды Кердока «обязаны» экстремальной нелинейности бент-функций. Отметим, что задача построения таких семейств бент-функций, задающих код Кердока, несложно переводится в задачу поиска *ортогональных расщеплений* (orthogonal spreads) в конечном векторном пространстве [131], что представляется элегантным примером связи бент-функций с экстремальными геометрическими объектами. Другим примером из теории кодирования служат так называемые *бент-коды* — линейные двоичные коды, каждый из которых определенным образом строится из некоторой бент-функции [78]. В принципе, тем же способом можно строить линейные коды из любых булевых функций, но только бент-коды имеют максимально возможные кодовые размерности.

Теория информации. Семейства *бент-последовательностей* из элементов $+1$ и -1, построенные на основе бент-функций, имеют предельно низкие значения как взаимной корреляции, так и автокорреляции (достигают нижней границы Велча) [170]. Поэтому такие семейства успешно применяются в коммуникационных системах коллективного доступа [173]. Не обходится без бент-функций или их аналогов и в квантовой теории инфор-

мации (см. например, [181]).

Цифровая сотовая связь. Бент-функции применяются в CDMA. Технология цифровой сотовой связи CDMA (Code Division Multiple Access — множественный доступ с кодовым разделением каналов) была стандартизована в 1993 году американской телекоммуникационной промышленной ассоциацией (US TIA) в виде стандарта IS–95. В настоящее время технология используется большинством поставщиков беспроводного оборудования во всем мире согласно стандартам IMT–2000 мобильной связи третьего поколения (в России — стандарты IMT–MC 450 или CDMA–450). Для оценки сигнала в CDMA используется коэффициент отношения пиковой и средней мощностей сигнала PAPR (peak-to-average power ratio). Чем данный коэффициент ниже, тем сигнал считается лучше, так как снижается стоимость на усилители мощности, и повышается надежность связи. Минимальное значение PAPR достигается на кодовых словах специального вида. Такими словами являются векторы значений бент-функций. Коды, состоящие из таких слов, называются *кодами постоянной амплитуды* (см. [173, 200]). Так возникает задача построения кодов постоянной амплитуды наибольшей мощности и обладающих хорошей структурой, т. е. задача выбора специальных подмножеств множества бент-функций.

Криптография. Бент-функцию можно определить как функцию, которая крайне плохо аппроксимируется аффинными функциями. Это базовое свойство бент-функций используется в криптографии. В блочных и поточных шифрах бент-функции и их векторные аналоги способствуют предельному повышению стойкости этих шифров к линейному [154] и дифференциальному [55] методам криптоанализа — основным статистическим методам криптоанализа блочных шифров.

Например, в 1993 году была обнаружена существенная слабость к линейному криптоанализу блочного шифра DES. Этот шифр являлся стандартом симметричного шифрования США на протяжении почти двадцати лет (с 1980 года по 1998 год). Слабость шифра, которая привела к успеш-

ной атаке на него, заключалась в плохих криптографических свойствах его нелинейных компонент, так называемых S-блоков. Математически, S-блок — это векторная булева функция, отображающая n входных битов в m выходных битов. Именно эти булевы функции в шифре DES не отвечали необходимым криптографическим требованиям, что и послужило причиной успеха метода линейного криптоанализа. Шифр DES оказался нестойким и к дифференциальному методу криптоанализа. Причина вновь заключалась в слабых S-блоках шифра.

Стойкость шифров к упомянутым методам криптоанализа достигается за счет использования бент-функций, их аналогов и обобщений при построении S-блоков (см. [41,166]). Это было сделано, например, в шифрах CAST и AES. В канадском шифре CAST S-блоки были изначально спроектированы с использованием бент-функций. Этот шифр был предложен в 1997 году и поддержан правительством Канады в качестве официальной замены шифру DES. В шифре AES — новом стандарте симметричного шифрования США — в качестве S-блока используется специального вида дифференциально 4-равномерная функция, являющаяся одним из обобщений векторных бент-функций. Блочный шифр AES является американским стандартом шифрования с 2002 года.

Бент-функции и их обобщения находят свое применение также в схемах аутентификации [84], хэш-функциях (см. HAVAL) и псевдослучайных генераторах [22]. См. также пример использования бент-функций в поточном шифре Grain.

Обобщения бент-функций. Широко исследуются различные обобщения, подклассы и надклассы бент-функций (см. далее Главу 2). С одной стороны, эти исследования мотивированы высокой сложностью задачи описания бент-функций и являются попытками перехода к более общим (или более частным) ее постановкам — в надежде на частичное решение основной проблемы. С другой стороны, интерес к обобщениям постоянно стимулируется новыми запросами со стороны приложений.

Фотография с одной из криптографических конференций, Франция, 2000-е.

Обзоры некоторых результатов о бент-функциях можно найти в замечательной российской монографии 2004 г. О. А. Логачева, А. А. Сальникова и В. В. Ященко [19], статье немецких криптографов Х. Доббертина и Г. Леандера [113] 2004 г., главах [78,79] французского математика и криптографа К. Карле, написанных для готовящейся к печати книги «Boolean Methods and Models» (2008 г.). См. также более ранние работы Ю. В. Кузнецова и С. А. Шкарина [11] 1996 г., Дж. Ф. Диллона [106] 1972 г. и др.

1.5 Критерии и свойства

Всюду далее n предполагается четным числом.

Напомним, что *матрицей Адамара* называется квадратная $k \times k$-матрица A с элементами ± 1, такая, что $AA^T = kE$, где E — единичная матрица. Строки и столбцы матрицы размера $2^n \times 2^n$ занумеруем векторами $\boldsymbol{u}, \boldsymbol{v}$ длины n. Справедлива [185]

Теорема 1. *Следующие утверждения эквивалентны:*

(i) *булева функция f от n переменных является бент-функцией;*

(ii) *матрица $A = (a_{\boldsymbol{u},\boldsymbol{v}})$, где $a_{\boldsymbol{u},\boldsymbol{v}} = \frac{1}{2^{n/2}} W_f(\boldsymbol{u} \oplus \boldsymbol{v})$, является матрицей Адамара;*

(iii) *матрица $D = (d_{\boldsymbol{u},\boldsymbol{v}})$, где $d_{\boldsymbol{u},\boldsymbol{v}} = (-1)^{f(\boldsymbol{u} \oplus \boldsymbol{v})}$, является матрицей Адамара;*

(iv) *для любого ненулевого вектора $\boldsymbol{u}$ функция $f(\boldsymbol{v}) \oplus f(\boldsymbol{v} \oplus \boldsymbol{u})$* сбалансирована, *т. е. принимает значения 0 и 1 одинаково часто.*

Пункт (iv) теоремы носит название *критерия распространения* $\mathrm{PC}(n)$ *порядка* n. В качестве важного свойства бент-функций можно отметить следующий факт [185]. Согласно [13] он был получен также В. А. Елисеевым и О. П. Степченковым еще в 1962 г.

Теорема 2. *Степень нелинейности* $\deg(f)$ *любой бент-функции f от $n \geqslant 4$ переменных не превосходит числа $n/2$.*

Аффинная функция, как нетрудно видеть, не может быть бент-функцией. Сразу отметим, что бент-функции любой другой возможной степени существуют. Например, квадратичной бент-функцией при любом четном n является функция

$$f(v_1, \ldots, v_n) = v_1 v_2 \oplus v_3 v_4 \oplus \ldots \oplus v_{n-1} v_n. \tag{1.1}$$

Интересно, что любую другую квадратичную бент-функцию g можно получить из f аффинным преобразованием. Приведем необходимое определение. Булевы функции f и g от n переменных *аффинно эквивалентны*, если существуют невырожденная $n \times n$ матрица A, векторы $\boldsymbol{b}, \boldsymbol{c}$ длины n и константа $\lambda \in \mathbb{Z}_2$, такие, что

$$g(\boldsymbol{v}) = f(A\boldsymbol{v} \oplus \boldsymbol{b}) \oplus \langle \boldsymbol{c}, \boldsymbol{v} \rangle \oplus \lambda.$$

Согласно [94] (см. [20,106]), выполняется

Теорема 3. *Любая квадратичная бент-функция от n переменных аффинно эквивалентна функции (1.1).*

Для бент-функций степени 3 и выше подобных результатов нет. Справедлива

Теорема 4. *Класс $\mathcal{B}_n$ бент-функций замкнут относительно*
(i) *любого невырожденного аффинного преобразования переменных;*
(ii) *прибавления любой аффинной функции.*

В силу теоремы 4 имеет смысл вопрос об аффинной классификации бент-функций, который для функций степени $\geqslant 3$ пока остается открытым. Подробнее о методах аффинной и линейной классификации булевых функций можно прочитать в [37].

Часто с бент-функцией f связывают так называемую *дуальную булеву функцию* $\widetilde{f}$ от n переменных, которая определяется равенством $W_f(\boldsymbol{v}) = 2^{n/2}(-1)^{\widetilde{f}(\boldsymbol{v})}$. Определение корректно, поскольку $W_f(\boldsymbol{v}) = \pm 2^{n/2}$ для каждого вектора $\boldsymbol{v}$. Несложно доказать, что булева функция $\widetilde{f}$ является бент-функцией. Справедливо $\widetilde{\widetilde{f}} = f$. Отметим, что если $\deg(f) = n/2$, то степень $\widetilde{f}$ также максимальна: $\deg(\widetilde{f}) = n/2$. Самодуальные бент-функции, т. е. такие, что $f = \widetilde{f}$, изучались в [81].

Дуальные бент-функции потребуются далее в теореме 14.

1.6 Эквивалентные представления бент-функций

Рассмотрим ряд попыток найти бент-функциям комбинаторные или алгебраические «эквиваленты».

1.6.1 Разностные множества и блок-схемы

С самого начала бент-функции изучались в связи с разностными множествами [106]. Пусть конечная абелева группа G имеет порядок v и дана в аддитивной записи. Подмножество $D \subseteq G$ мощности k называется *разностным множеством* с параметрами (v, k, λ), если каждый ненулевой

элемент $g \in G$ можно представить в виде $g = b - d$ ровно λ способами, где b, d — элементы множества D. Справедлива [106]

Теорема 5. *Булева функция f от n переменных является бент-функцией, если и только если множество $D = \{ (\boldsymbol{v}, f(\boldsymbol{v})) \mid \boldsymbol{v} \in \mathbb{Z}_2^n \}$ является разностным множеством с параметрами $(2^{n+1}, 2^n, 2^{n-1})$ в аддитивной группе $\mathbb{Z}_2^{n+1}$.*

Действительно, этот факт несложно следует из пункта (iv) теоремы 1. Разностные множества с приведенными в теореме 5 параметрами называются *элементарными адамаровыми*. Примеры таких множеств были известны еще до появления бент-функций [106].

Известно [36], что разностные множества тесно связаны с блок-схемами. Напомним, что *блок-схемой* с параметрами (v, k, λ) называется система k-элементных подмножеств (или *блоков*) v-элементного множества, такая, что каждая пара различных элементов содержится ровно в λ блоках. Блок-схема *симметрична*, если число блоков равно числу элементов, т. е. равно v. Теорема 5 имеет следующий эквивалентный вид.

Теорема 6. *Булева функция f от n переменных является бент-функцией, если и только если система множеств $D_{\boldsymbol{z}} = D \oplus \boldsymbol{z}$, где вектор $\boldsymbol{z}$ пробегает множество $\mathbb{Z}_2^{n+1}$, является симметричной блок-схемой с параметрами $(2^{n+1}, 2^n, 2^{n-1})$.*

1.6.2 Линейные разветвления

В. В. Ященко [39] в 1997 г. предложил следующее описание класса бент-функций. В его основе лежит тот факт, что любая булева функция f от n переменных может быть представлена в виде *линейного разветвления*

$$f(\boldsymbol{u'}, \boldsymbol{u''}) = \langle \boldsymbol{u'}, h(\boldsymbol{u''}) \rangle \oplus g(\boldsymbol{u''}), \text{ где } \boldsymbol{u'} \in \mathbb{Z}_2^r, \boldsymbol{u''} \in \mathbb{Z}_2^k \qquad (1.2)$$

для подходящих чисел r и k таких, что $n = r + k$, отображения $h : \mathbb{Z}_2^k \to \mathbb{Z}_2^r$ и булевой функции g от k переменных. Максимально возможное значение r

в таком представлении называется *индексом линейности* булевой функции f.

Подмножество M пространства $\mathbb{Z}_2^n$ называется *бент-множеством*, если его мощность равна $2^{2\ell}$ при некотором ℓ и для любого ненулевого вектора $\boldsymbol{z} \in \mathbb{Z}_2^n$ множество $M \cap (\boldsymbol{z} \oplus M)$ либо пусто, либо имеет четную мощность.

Пара $(g; M)$, где g — булева функция от k переменных, M — бент-множество, называется *частичной бент-функцией*, если для любого $\boldsymbol{v'} \in \mathbb{Z}_2^r$ и ненулевого $\boldsymbol{v''} \in \mathbb{Z}_2^k$ функция $g(\boldsymbol{u''}) \oplus g(\boldsymbol{u''} \oplus \boldsymbol{v''})$ сбалансирована на множестве $M \cap ((\boldsymbol{v'}, \boldsymbol{v''}) \oplus M)$.

Теорема 7. *Булева функция f вида (1.2) является бент-функцией тогда и только тогда, когда $n > 2r$ и для любого вектора $\boldsymbol{u'} \in \mathbb{Z}_2^r$ выполняются условия:*

(i) мощность множества $h^{-1}(\boldsymbol{u'})$ равна 2^{n-2r};

(ii) множество $h^{-1}(\boldsymbol{u'})$ является бент-множеством;

(iii) пара $(g; h^{-1}(\boldsymbol{u'}))$ является частичной бент-функцией.

Позднее в 2004 г. К. Карле независимо предложил конструкцию бент-функций, представляющую собой частный случай данного описания (см. далее теорему 17).

1.6.3 Наборы подпространств

Приведем геометрическое описание класса бент-функций, которое предложили в 1998 г. К. Карле и Ф. Гуилло [87] (см. также более раннюю работу [86]).

Пусть f — булева функция от n переменных. Пусть $\mathrm{Ind}_S : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — характеристическая функция подмножества $S \subseteq \mathbb{Z}_2^n$, т. е. Ind_S принимает значение 1 на элементах из S и значение 0 на остальных элементах.

Теорема 8. *Функция f является бент-функцией тогда и только тогда, когда существуют подпространства $E_1, \ldots, E_k$ размерности $n/2$ или*

$(n/2)+1$ *пространства* $\mathbb{Z}_2^n$ *и ненулевые целые числа* $m_1, \ldots, m_k$, *такие, что для любого* $\boldsymbol{v} \in \mathbb{Z}_2^n$ *выполняется*

$$\sum_{i=1}^{k} m_i \mathrm{Ind}_{E_i}(\boldsymbol{v}) = \pm 2^{(n/2)-1} \mathrm{Ind}_{\{\mathbf{0}\}}(\boldsymbol{v}) + f(\boldsymbol{v}).$$

Авторы [87] вводят ограничения на способ выбора пространств $E_1, \ldots, E_k$, при которых такой выбор становится единственным для каждой бент-функции. Таким образом, можно говорить об однозначности такого представления.

1.6.4 Сильно регулярные графы

Другой подход предложили в 1999 г. А. Бернаскони и Б. Коденотти [50], затем к ним присоединился и Дж. Ван-дер-Кам [51].

Пусть f — булева функция от n переменных. Через $\mathrm{supp}(f)$ обозначим ее *носитель*, т. е. множество всех двоичных векторов длины n, на которых функция f принимает значение 1. Рассмотрим *граф Кэли* $G_f = G(\mathbb{Z}_2^n, \mathrm{supp}(f))$ булевой функции f. Вершинами графа являются все векторы длины n. Две вершины $\boldsymbol{u}$, $\boldsymbol{v}$ соединяются ребром, если вектор $\boldsymbol{u} \oplus \boldsymbol{v}$ принадлежит множеству $\mathrm{supp}(f)$.

Регулярный граф G называется *сильно регулярным* (strongly regular), если существуют неотрицательные целые числа λ, μ такие, что для любых двух вершин x, y число общих смежных им вершин равно λ или μ в зависимости от того, соединены вершины x, y ребром или нет. В работе [51] доказана

Теорема 9. *Булева функция* f *является бент-функцией тогда и только тогда, когда граф* G_f *является сильно регулярным, причем* $\lambda = \mu$.

1.6.5 Бент-прямоугольники

С. В. Агиевич в 2000 г. [43] установил биекцию между множеством всех бент-функций от n переменных и множеством *бент-прямоугольников*.

Пусть f — булева функция от n переменных, $n = r + k$. Вектор $\boldsymbol{W}_f$ коэффициентов Уолша—Адамара назовем *спектральным вектором* функции f. Представим двоичный вектор $\boldsymbol{f}$ в виде $\boldsymbol{f} = (\boldsymbol{f}_{(1)}, \ldots, \boldsymbol{f}_{(2^r)})$, где каждый вектор $\boldsymbol{f}_{(i)}$ имеет длину 2^k. Пусть $f_{(i)}$ — булева функция от k переменных, для которой $\boldsymbol{f}_{(i)}$ является вектором значений, $i = 1, \ldots, 2^r$. Свяжем с функцией f матрицу $\mathcal{M}_f$ размера $2^r \times 2^k$, строками которой являются спектральные векторы $\boldsymbol{W}_{f_{(1)}}, \ldots, \boldsymbol{W}_{f_{(2^r)}}$.

Матрица размера $2^r \times 2^k$ называется *бент-прямоугольником*, если каждая ее строка и каждый столбец, домноженный на $2^{r-(n/2)}$, являются спектральными векторами для подходящих булевых функций. Согласно [43], выполняется

Теорема 10. *Булева функция f является бент-функцией тогда и только тогда, когда матрица $\mathcal{M}_f$ является бент-прямоугольником.*

Данный подход позволил [43] дать описание всех бент-функций от шести переменных (см. далее) и получить алгоритм построения специального класса бент-функций от произвольного числа переменных n. В работе [45] С. В. Агиевич исследует соответствие между бент-прямоугольниками и регулярными q-значными бент-функциями [141], описывает аффинные трансформации первых и переводит на язык бент-прямоугольников основные конструкции бент-функций. Дальнейшее развитие этого подхода представляется весьма перспективным.

Здесь перечислены лишь некоторые возможные характеризации бент-функций.

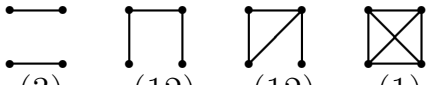
1.7 Бент-функции от малого числа переменных

Задача описания всех бент-функций от n переменных решена лишь при малых значениях n. Приведем эти результаты.

$n = 2$. Функция $v_1 v_2$ является представителем единственного класса

аффинной эквивалентности. Класс $\mathcal{B}_2$ состоит из восьми функций. Это все функции, векторы значений которых содержат нечетное число единиц.

$n = 4$. Множество $\mathcal{B}_4$ состоит из 896 булевых функций, причем каждая функция является квадратичной. Все бент-функции от четырех переменных аффинно эквивалентны функции $v_1v_2 \oplus v_3v_4$. Множество $\mathcal{B}_4$ можно разделить на 28 классов по 32 функции. Алгебраические нормальные формы функций из каждого класса обладают одинаковой квадратичной частью, произвольной линейной частью и любым свободным членом. Если рассмотреть граф на множестве переменных, а ребрами соединить те вершины, которые образуют слагаемое в квадратичной части АНФ функции, то эти 28 типов можно задать следующим образом:



Под каждым графом указано число типов, которые он определяет. Например, имеется 3 типа квадратичной части, состоящей из двух слагаемых: $v_1v_2 \oplus v_3v_4$, $v_1v_3 \oplus v_2v_4$, $v_1v_4 \oplus v_2v_3$, и только один тип из шести слагаемых.

$n = 6$. Аффинная классификация бент-функций от 6 переменных была получена еще в работе О. Ротхауса [185]: множество $\mathcal{B}_6$ состоит из четырех классов аффинной эквивалентности, представителями которых являются следующие функции:

$v_1v_2 \oplus v_3v_4 \oplus v_5v_6$,

$v_1v_2v_3 \oplus v_1v_4 \oplus v_2v_5 \oplus v_3v_6$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_1v_2 \oplus v_1v_4 \oplus v_2v_6 \oplus v_3v_5 \oplus v_4v_5$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_1v_4 \oplus v_2v_6 \oplus v_3v_4 \oplus v_3v_5 \oplus v_3v_6 \oplus v_4v_5 \oplus v_4v_6$.

В работе [204] приводится подобная алгебраическая классификация. Пусть $GF(2^6) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{62}\}$, где α — корень многочлена $x^6 + x + 1$. Пусть булева функция отождествляется с функцией $f(\boldsymbol{v}) : GF(2^6) \to GF(2)$, где $\boldsymbol{v}$ рассматривается как элемент поля $GF(2^6)$. Тогда в качестве представителей классов аффинной эквивалентности множества $\mathcal{B}_6$ можно

выбрать функции: $\mathrm{tr}(\boldsymbol{v}^3 + \alpha^5\boldsymbol{v}^5)$, $\mathrm{tr}(\alpha^3\boldsymbol{v}^7 + \boldsymbol{v}^9)$, $\mathrm{tr}(\alpha\boldsymbol{v}^3 + \alpha^6\boldsymbol{v}^7 + \alpha^{60}\boldsymbol{v}^{13})$, $\mathrm{tr}(\boldsymbol{v}^7 + \alpha\boldsymbol{v}^9 + \boldsymbol{v}^{21})$, где tr — функция следа из $GF(2^6)$ в $GF(2)$.

Дж. Диллоном [106] (см. также [59]) было показано, что любая бент-функция от шести переменных аффинно эквивалентна функции из класса Мэйорана—МакФарланда (см. далее теорему 16).

Класс $\mathcal{B}_6$ содержит $5\,425\,430\,528 \simeq 2^{32,3}$ функций. Описание было дано С. В. Агиевичем [43] с использованием бент-квадратов, т. е. бент-прямоугольников при $r = k$ (см. теорему 10). Скажем, что две бент-функции *квадратно-эквивалентны*, если бент-квадрат одной из них может быть получен из бент-квадрата второй изменением знаков элементов и перестановкой строк и столбцов. Пусть $r = k = 3$. Все функции класса $\mathcal{B}_6$ разбиваются на восемь классов квадратной эквивалентности. Ниже приводятся соответствующие бент-квадраты размера $2^3 \times 2^3$ и количество функций в каждом классе.

8 0 0 0 0 0 0 0	-4 4 4 4 0 0 0 0	-4 4 4 4 0 0 0 0	-4 4 4 4 0 0 0 0
0 8 0 0 0 0 0 0	4-4 4 4 0 0 0 0	4-4 4 4 0 0 0 0	4-4 0 0 4 4 0 0
0 0 8 0 0 0 0 0	4 4-4 4 0 0 0 0	0 0-4 4 4 4 0 0	4 0-4 0 4 0 4 0
0 0 0 8 0 0 0 0	4 4 4-4 0 0 0 0	0 0 4-4 4 4 0 0	4 0 0-4 0 4 4 0
0 0 0 0 8 0 0 0	0 0 0 0 8 0 0 0	4 4 0 0-4 4 0 0	0 4 4 0 0 4-4 0
0 0 0 0 0 8 0 0	0 0 0 0 0 8 0 0	4 4 0 0 4-4 0 0	0 4 0 4-4 0 4 0
0 0 0 0 0 0 8 0	0 0 0 0 0 0 8 0	0 0 0 0 0 0 8 0	0 0 4 4 4-4 0 0
0 0 0 0 0 0 0 8	0 0 0 0 0 0 0 8	0 0 0 0 0 0 0 8	0 0 0 0 0 0 0 8
$(2^{15} \cdot 3^2 \cdot 5 \cdot 7)$	$(2^{18} \cdot 3 \cdot 7^2)$	$(2^{21} \cdot 3 \cdot 7^2)$	$(2^{25} \cdot 3 \cdot 7)$

-4 4 4 4 0 0 0 0	-4 4 4 4 0 0 0 0	-4 4 4 4 0 0 0 0	-6 2 2 2 2 2 2 2
4-4 4 4 0 0 0 0	4-4 4 4 0 0 0 0	4-4 0 0 4 4 0 0	2-6 2 2 2 2 2 2
4 4-4 4 0 0 0 0	0 0-4 4 4 4 0 0	4 0-4 0 4 0 4 0	2 2-6 2 2 2 2 2
4 4 4-4 0 0 0 0	0 0 4-4 4 4 0 0	4 0 0-4 0 4 4 0	2 2 2-6 2 2 2 2
0 0 0 0-4 4 4 4	0 0 0 0-4 4 4 4	0 4 4 0-4 0 0 4	2 2 2 2-6 2 2 2
0 0 0 0 4-4 4 4	0 0 0 0 4-4 4 4	0 4 0 4 0-4 0 4	2 2 2 2 2-6 2 2
0 0 0 0 4 4-4 4	4 4 0 0 0 0-4 4	0 0 4 4 0 0-4 4	2 2 2 2 2 2-6 2
0 0 0 0 4 4 4-4	4 4 0 0 0 0 4-4	0 0 0 0 4 4 4-4	2 2 2 2 2 2 2-6
$(2^{19} \cdot 7^2)$	$(2^{20} \cdot 3^2 \cdot 7^2)$	$(2^{23} \cdot 3 \cdot 7^2)$	$(2^{23} \cdot 3^2 \cdot 5 \cdot 7)$

Отметим, что мощность $\mathcal{B}_6$ была найдена раньше в диссертации Б. Пренела [179]. В 2004 г. авторы [158] перечислили функции класса $\mathcal{B}_6$ способом, отличным от приведенного в [43].

$n = 8$. Аффинная классификация бент-функций от восьми переменных степени не выше 3 была получена в работах [126] и [59], см. также работу [44], посвященную кубическим бент-функциям специального вида. Бент-функции от восьми переменных степени не выше 3 делятся на 10 классов аффинной эквивалентности, представителями которых являются:

$v_1v_2 \oplus v_3v_4 \oplus v_5v_6 \oplus v_7v_8$,

$v_1v_2v_3 \oplus v_1v_4 \oplus v_2v_5 \oplus v_3v_6 \oplus v_7v_8$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4 \oplus v_2v_6 \oplus v_1v_7 \oplus v_5v_8$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_1v_3 \oplus v_1v_5 \oplus v_2v_6 \oplus v_3v_4 \oplus v_7v_8$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_2v_6 \oplus v_2v_5 \oplus v_1v_7 \oplus v_4v_8$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_7 \oplus v_6v_8$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_2v_6 \oplus v_2v_5 \oplus v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_7v_8$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_1v_6 \oplus v_2v_7 \oplus v_4v_8$,

$v_1v_2v_7 \oplus v_3v_4v_7 \oplus v_5v_6v_7 \oplus v_1v_4 \oplus v_3v_6 \oplus v_2v_5 \oplus v_4v_5 \oplus v_7v_8$,

$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_1v_4v_7 \oplus v_3v_5 \oplus v_2v_7 \oplus v_1v_5 \oplus v_1v_6 \oplus v_4v_8$.

В диссертации [59] также показано, что все эти функции аффинно эквивалентны функциям из класса Мэйорана—МакФарланда.

Нижняя $2^{70,4}$ и верхняя $2^{129,2}$ оценки числа всех функций в классе $\mathcal{B}_8$ были получены соответственно в [43] и [146]. Некоторые результаты по частичному описанию класса $\mathcal{B}_8$ на основе исследования групп автоморфизмов бент-функций приводит У. Демпвольф в работах [103, 104]. М. Янг, К. Менг и Х. Жанг [204] показали, что множество $\mathcal{B}_8$ состоит не менее чем из 129 классов аффинной эквивалентности. Представители всех найденных ими классов приводятся в их работе. Это 53 функции вида $\mathrm{tr}(\alpha^i \boldsymbol{v}^{d_1} + \alpha^j \boldsymbol{v}^{d_2} + \alpha^k \boldsymbol{v}^{d_3})$ и 76 функций вида $\mathrm{tr}(\alpha^i \boldsymbol{v}^{d_1} + \alpha^j \boldsymbol{v}^{d_2} + \alpha^k \boldsymbol{v}^{d_3} + \alpha^\ell \boldsymbol{v}^{d_4})$, где $\mathrm{tr} : GF(2^8) \to GF(2)$ — функция следа. Авторы [117] показали, что множество $\mathcal{B}_8 \cap \mathcal{PS}$ содержит функции из не менее чем шести классов аффинной эквивалентности, где $\mathcal{PS}$ — класс бент-функций, полученных методом частичного расщепления (см. далее теорему 18).

По последним данным аффинная классификация бент-функций от вось-

ми переменных четвертой степени завершена [143]. Описаны все 536 возможных вариантов для части четвертой степени[1] АНФ бент-функции от восьми переменных. Установлено точное число всех бент-функций от восьми переменных [143]. Оно равно
$2^9 \times 193\,887\,869\,660\,028\,067\,003\,488\,010\,240 \simeq 2^{106{,}29}$.

При $n \geqslant 10$ класс $\mathcal{B}_n$ не описан, его мощность неизвестна. В работе [204] построено большое число бент-функций от десяти переменных; установлено, что среди них содержится как минимум несколько сотен попарно аффинно неэквивалентных функций. Некоторую информацию о классах $\mathcal{B}_{10}$, $\mathcal{B}_{12}$ можно найти на сайте [104].

1.8 Оценки числа бент-функций

Информации об оценках числа бент-функций от n переменных немного. Приведем нижнюю оценку этого числа, которую дает конструкция Мэйорана—МакФарланда (см. далее теорему 16).

Теорема 11. *Справедливо* $|\mathcal{B}_n| \geqslant 2^{2^{n/2}}(2^{n/2})!$.

Асимптотически, эта оценка имеет вид $(\frac{2^{(n/2)+1}}{e})^{2^{n/2}}\sqrt{2^{(n/2)+1}\pi}$, или, если совсем грубо, $2^{2^{n/2}}$. Следует отметить, что в работе [43] приводится уточнение оценки теоремы 11, являющееся на данный момент лучшим. Однако охарактеризовать асимптотическое поведение оценки [43] достаточно трудно.

Тривиальная верхняя оценка следует из того факта, что, согласно теореме 2, степень бент-функции не превышает $n/2$. Имеем

$$|\mathcal{B}_n| \leqslant 2^{1+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{n/2}} = 2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}.$$

К. Карле и А. Клаппер в 2002 г. [88] немного улучшили эту оценку:

[1] Под *частью степени* i *АНФ функции* понимаем набор всех тех слагаемых ее АНФ, степень которых равна i.

Теорема 12. *Пусть* $n \geqslant 6$ *и выполняется* $\varepsilon = \frac{1}{2^{O(\sqrt{2^n/n})}}$. *Тогда*

$$|\mathcal{B}_n| \leqslant 2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}-2^{n/2}+(n/2)+1}(1+\varepsilon) + 2^{2^{n-1}-\frac{1}{2}\binom{n}{n/2}}.$$

Хотя по-прежнему верхняя оценка близка к тривиальной 2^{2^n}. Верхняя оценка обсуждается также в работе [202].

Кажется интересным, что аналогичная проблема сильного разрыва между нижней и верхней оценками наблюдается и для числа других комбинаторных объектов.

Например, для совершенных двоичных кодов длины $n = 2^s - 1$ с расстоянием 3 (см. определение в [20]). Нижнюю оценку вида $2^{2^{n/2}}$ дает конструкция Ю. Л. Васильева 1962 г. [5], и с ней схожа, на мой взгляд, конструкция Мэйорана—МакФарланда для бент-функций; схожа по своей простоте и изяществу, и той роли основного, базового класса, которую играет в множестве бент-функций. А тип верхней оценки числа совершенных кодов по-прежнему остается тривиальным: 2^{2^n}. Небольшие улучшения нижней и верхней оценок приводятся соответственно в [140] и [1].

1.9 Конструкции бент-функций

Очень сложно не только классифицировать бент-функции, но и предложить отдельные способы их построения. В этом разделе мы следуем в основном работе [78] К. Карле, в которой всевозможные конструкции бент-функций представлены наиболее полно. Конструкции принято делить на *первичные* (primary) и *вторичные* (secondary). К первой группе относят те, с помощью которых бент-функции строятся напрямую, ко второй группе — конструкции, опирающиеся на уже известные бент-функции (например, от меньшего числа переменных).

1.9.1 Итеративные конструкции

Ко вторичным конструкциям относится простая *итеративная конструкция* [185].

Теорема 13. *Функция* $f(\boldsymbol{u'}, \boldsymbol{u''}) = g(\boldsymbol{u'}) \oplus h(\boldsymbol{u''})$, *где векторы* $\boldsymbol{u'}$, $\boldsymbol{u''}$ *имеют четные длины* r, k *соответственно, является бент-функцией тогда и только тогда, когда функции* g, h — *бент-функции.*

Конструкция легко может быть описана в терминах бент-прямоугольников [45]. Приведем следующее обобщение этой простой конструкции, полученное в [71].

Теорема 14. *Пусть* $n = r + k$, *где* r *и* k *четны,* f — *булева функция от* n *переменных. Пусть* $\boldsymbol{u'}$, $\boldsymbol{u''}$ *пробегают* $\mathbb{Z}_2^r$ *и* $\mathbb{Z}_2^k$ *соответственно. Предположим, что функции*

$$f_{\boldsymbol{u''}}(\boldsymbol{u'}) = f(\boldsymbol{u'}, \boldsymbol{u''})$$

являются бент-функциями при любых $\boldsymbol{u''}$. *Определим* $g_{\boldsymbol{u'}}(\boldsymbol{u''}) = \widetilde{f_{\boldsymbol{u''}}}(\boldsymbol{u'})$. *Тогда* f — *бент-функция, если и только если* $g_{\boldsymbol{u'}}$ — *бент-функция для любого* $\boldsymbol{u'}$.

Заметим, что теорема 13 следует из теоремы 14. Итеративный способ построения бент-функций от $n + 2$ переменных из бент-функций от n переменных приводится в [98]. В качестве упражнения можно доказать следующий факт (см. [128]).

Теорема 15. *Пусть* f — *булева функция от* n *переменных,* h — *перестановка на* $\mathbb{Z}_2^n$. *Обозначим через* $h_1, \ldots, h_n$ *булевы функции такие, что* $h(\boldsymbol{v}) = (h_1(\boldsymbol{v}), \ldots, h_n(\boldsymbol{v}))$. *Функция* $f \circ h^{-1}$ *является бент-функцией, если для каждого* $\boldsymbol{u}$ *выполняется*

$$\mathrm{dist}(f, \bigoplus_{i=1}^{n} u_i h_i) = 2^{n-1} \pm 2^{(n/2)-1}.$$

Москва шестидесятых, СССР.

1.9.2 Класс Мэйорана—МакФарланда

К первичным конструкциям принадлежит простая и богатая *конструкция Мэйорана—МакФарланда* 1973 г. [157,107].

Теорема 16. *Пусть h — любая перестановка на $\mathbb{Z}_2^{n/2}$, пусть g — произвольная булева функция от $n/2$ переменных. Тогда функция $f(\boldsymbol{u'}, \boldsymbol{u''}) = \langle \boldsymbol{u'}, h(\boldsymbol{u''}) \rangle \oplus g(\boldsymbol{u''})$ является бент-функцией от n переменных.*

Основной идеей конструкции служит, по выражению К. Карле [78], «конкатенация аффинных функций». Действительно, при каждом фиксированном значении переменных из второй половины функция f является аффинной от $n/2$ первых переменных. С другой стороны, аффинные функции возникают и при рассмотрении соответствующих бент-квадратов. А именно, бент-функция принадлежит классу Мэйорана—МакФарланда, если и только если строки и столбцы ее бент-квадрата являются спектральными векторами аффинных булевых функций [43].

Из теоремы легко следует, что существуют бент-функции с любой степенью нелинейности d, такой, что $2 \leqslant d \leqslant n/2$. Итак, в теореме 16 переменные функции f разбиваются пополам. В 2004 г. К. Карле [75] (см. также [78]) обобщил идею Мэйорана—МакФарланда, рассмотрев разбиение переменных на неравные части.

Теорема 17. *Пусть $n = r + k$. Пусть $h : \mathbb{Z}_2^k \to \mathbb{Z}_2^r$ — любое отображение, такое, что для каждого вектора $\boldsymbol{u}$ длины r множество $h^{-1}(\boldsymbol{u})$ образует подпространство в $\mathbb{Z}_2^k$ размерности $n - 2r$. Пусть g — булева функция от k переменных, сужение которой на $h^{-1}(\boldsymbol{u})$ для каждого $\boldsymbol{u}$ является бент-функцией при $n > 2r$. Тогда булева функция $f(\boldsymbol{u'}, \boldsymbol{u''}) = \langle \boldsymbol{u'}, h(\boldsymbol{u''}) \rangle \oplus g(\boldsymbol{u''})$ является бент-функцией от n переменных.*

Отметим, что конструкция К. Карле имеет сильные сходства с методом описания бент-функций, предложенным В. В. Ященко [39] еще в 1997 г. (см. выше теорему 7).

Теорема 16 представляет частный случай теоремы 17 при $r = k = n/2$.

1.9.3 Partial Spreads

Следующая первичная конструкция Дж. Диллона [107] 1974 г. опирается на специальные семейства подпространств n-мерного пространства и носит название *частичного расщепления* (Partial Spreads).

Пусть $\mathrm{Ind}_S : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — характеристическая функция подмножества $S \subseteq \mathbb{Z}_2^n$.

Теорема 18. *Пусть число q равно $2^{(n/2)-1}$ или $2^{(n/2)-1}+1$. Пусть L_1, …, L_q — линейные подпространства размерности $n/2$ пространства $\mathbb{Z}_2^n$ такие, что любые два из них пересекаются лишь по нулевому вектору. Тогда функция $f(\boldsymbol{v}) = \bigoplus_{i=1}^{q} \mathrm{Ind}_{L_i}(\boldsymbol{v})$ является бент-функцией.*

Случай $q = 2^{(n/2)-1}$ определяет класс бент-функций $\mathcal{PS}^-$.

Случай $q = 2^{(n/2)-1}+1$ задает класс бент-функций $\mathcal{PS}^+$.

Вместе $\mathcal{PS}^-$ и $\mathcal{PS}^+$ составляют класс $\mathcal{PS}$.

Более общие геометрические конструкции можно найти, например, в работе [70].

1.9.4 Алгебраические конструкции

Приведем несколько алгебраических конструкций.

Первая серия конструкций называется *степенные* или *мономиальные бент-функции* (power/monomial bent functions). Пусть векторное пространство $\mathbb{Z}_2^n$ отождествляется с полем Галуа $GF(2^n)$. Булевы функции от n переменных можно рассматривать как функции из $GF(2^n)$ в $GF(2)$, сопоставляя каждому вектору $\boldsymbol{v}$ соответствующий элемент поля $GF(2^n)$, который будем обозначать тем же символом. Пусть $\mathrm{tr} : GF(2^n) \to GF(2)$ — *функция следа*, т. е. $\mathrm{tr}(\boldsymbol{v}) = \boldsymbol{v} + \boldsymbol{v}^2 + \cdots + \boldsymbol{v}^{2^{n-1}}$. Бент-функции, имеющие вид

$$f(\boldsymbol{v}) = \mathrm{tr}(a\boldsymbol{v}^d),$$

где $a \in GF^*(2^n)$ — некоторый параметр, называются *степенными* или *мономиальными*, а целое число d называется *бент-показателем*. Здесь $GF^*(2^n)$ — множество ненулевых элементов поля. Бент-функции такого вида интересны в первую очередь для криптографических приложений в

силу своей простой вычислимости. Хотя криптографы до сих пор не определились: считать простоту вычислимости бент-функции ее достоинством или скорее недостатком [78].

Пусть $\gcd(\cdot,\cdot)$ — наибольший общий делитель двух чисел.

Теорема 19. *Следующие значения d являются бент-показателями:*
$d = 2^{n/2} - 1$ (**Диллон $\diamond$, 1974, [107]**);
$d = 2^i + 1$, *где* $\frac{n}{\gcd(n,i)}$ *четно* (**показатель Голда †**);
$d = 2^{2k} - 2^k + 1$, *где* $\gcd(k,n) = 1$ (**показатель Касами**);
$d = (2^k+1)^2$, *где* $n = 4k$, k *нечетно* (**Канто–Леандер †, 2004, [147]**);
$d = 2^{2k}+2^k+1$, *где* $n = 6k$ (**Канто–Шарпин–Карегян †, 2006, [67]**).

Известно, что три типа степенных бент-функций (в теореме их показатели помечены знаком †) можно описать с помощью конструкции Мэйорана—МакФарланда, а один тип (помечен знаком $\diamond$) содержится в классе $\mathcal{PS}^-$. Существуют ли степенные бент-функции с другими показателями? Можно ли для степенных бент-функций найти простое комбинаторное описание? Ответов на эти вопросы пока нет.

Вторая серия бент-функций состоит из функций вида

$$f(\boldsymbol{v}) = \operatorname{tr}(a_1 \boldsymbol{v}^{d_1} + a_2 \boldsymbol{v}^{d_2}) \tag{1.3}$$

для подходящих элементов $a_1, a_2 \in GF(2^n)$ и показателей d_1, d_2. Известны примеры таких функций со специальными степенными показателями — так называемыми *показателями Нихо* вида $d \equiv 2^i \bmod (2^{n/2} - 1)$. Без ограничения общности [113] пусть первый показатель равен $d_1 = (2^{(n/2)} - 1)\frac{1}{2} + 1$. Справедлива [112]

Теорема 20. *Если выполняется $d_2 = (2^{(n/2)} - 1)\lambda + 1$, где λ равно $1/6$, $1/4$ или 3, то существуют элементы $a_1, a_2 \in GF(2^n)$ такие, что (1.3) является бент-функцией.*

Алгоритмические вопросы построения функций такого вида разбираются в [204]. Бент-функции вида $f(\boldsymbol{v}) = \sum_{i=1}^{(n-1)/2} c_i \operatorname{tr}(\boldsymbol{v}^{1+2^i})$ изучались в [93, 129,

134, 135, 204, 207].

Следует отметить, что алгебраические конструкции бент-функций носят весьма случайный характер: каждый раз исследуются функции лишь некого специального вида. Общий алгебраический подход к описанию бент-функций мог бы основываться на том, что любая булева функция $f : GF(2^n) \to GF(2)$ может быть представлена *с помощью следа* (в так называемой trace form), т. е. в виде

$$f(\boldsymbol{v}) = \mathrm{tr}\left(\sum_{d \in CS} a_d \boldsymbol{v}^d\right) = \sum_{d \in CS} \mathrm{tr}(a_d \boldsymbol{v}^d) \tag{1.4}$$

для подходящих элементов $a_d \in GF(2^n)$, где CS — множество представителей циклотомических классов по модулю $2^n - 1$. Эволюционный алгоритм на основе такого представления был предложен М. Янгом, К. Менгом и Х. Жангом [204]. Эта работа уже упоминалась нами в связи с классификацией бент-функций от 6 и 8 переменных. На основе многочисленных компьютерных исследований авторы делают в этой работе некоторые предположения относительно общего алгебраического вида бент-функций. В частности, они предполагают, что бент-функцию — представителя класса аффинной эквивалентности — можно представить в виде (1.4) с участием небольшого числа мономов. Причем более вероятными ненулевыми коэффициентами a_d в этом представлении авторы [204] считают те, для которых d является бент-показателем (см. теорему 19).

Но общего подхода к алгебраическому описанию бент-функций пока нет.

Более полно (с доказательствами) конструкции бент-функций представлены в обзорах [19, 78, 113], см. также другие конструкции в работах [71, 109].

1.10 Алгоритмы генерации бент-функций

Серия работ посвящена алгоритмическим методам построения бент-функций. Каждый метод основывается, как правило, на одном из возможных

представлений булевой функции и использует те его особенности, которые проявляются в случае, когда булева функция оказывается бент-функцией. К таким базовым представлениям относятся: таблица истинности [158,159], АНФ [115,116], спектральный вектор булевой функции [97], представление с помощью следа [204] и др.

В диссертации Дж. Е. Фаллер [115] подробно разбираются эвристические методы построения бент-функций. Их основная идея заключается в постепенном изменении начальной булевой функции с улучшением тех или иных ее криптографических свойств, включающих нелинейность. Так, для построения бент-функций применяются: генетический алгоритм [162], алгоритмы случайного поиска [163, 115], алгоритм имитации отжига [96]. В диссертации [115] предлагается достаточно быстрый алгоритм построения псевдослучайных бент-функций степени не выше некоторой заданной: функции строятся из случайной квадратичной бент-функции g путем итеративного добавления к АНФ(g) слагаемых более высоких степеней. При этом основная трудность — «отбраковка» бóльшей части слагаемых — преодолевается за счет существенного использования комбинаторных свойств бент-функций.

В 2004 г. К. Менг с соавторами предложили алгоритм [158], позволяющий (теоретически) построить все бент-функции от любого числа переменных n. По сравнению с полным перебором сложность данного алгоритма ниже за счет использования соотношений между отдельными коэффициентами Уолша—Адамара произвольной булевой функции и спектральными векторами ее подфункций, а также за счет оперирования свойствами бент-функций, приведенными в теореме 4. Практически, данный алгоритм и его модификации оказались применимы пока только для генерации всех бент-функций от 6 переменных, всех однородных [180] бент-функций степени 3 от 8 переменных и доказательства несуществования однородных бент-функций степени 4 от 10 переменных.

С. В. Агиевичем [43] приводится алгоритм порождения достаточно боль-

шого числа бент-функций, основанный на использовании бент-прямоугольников (см. теорему 10). Данный алгоритм позволил установить лучшую на данный момент нижнюю оценку числа бент-функций от n переменных. Эволюционный алгоритм на основе представления булевых функций с помощью следа предложен в [204]. Подробнее о применении эволюционных вычислений для генерации бент-функций см. также в [97,116, 159]. Отдельные аспекты порождения случайных бент-функций обсуждаются в работе [119].

1.11 Другие результаты

Случайные булевы функции. В 1998 г. Д. Оледжар и М. Станек [169] исследовали криптографические свойства случайной булевой функции от n переменных. В частности, ими была доказана

Теорема 21. *Существует константа c такая, что при достаточно больших n почти для каждой булевой функции f от n переменных выполняется $N_f \geqslant 2^{n-1} - c\sqrt{n}\,2^{n/2}$.*

Позднее в 2002 г. этот факт был независимо получен К. Карле [74].

Выражение «почти для каждой» следует понимать как «с вероятностью, стремящейся к 1».

Пусть нелинейность произвольной булевой функции g от n переменных имеет вид $N_g = 2^{n-1} - S(g)$, где $S(g)$ — некоторая функция. В 2006 г. Ф. Родье [182] установил асимптотическое значение нелинейности булевой функции. Пусть V^∞ — множество бесконечных двоичных последовательностей, почти все элементы которых равны нулю. Пусть $f : V^\infty \to \mathbb{Z}_2$. Обозначим через f_n сужение функции f на множество $\mathbb{Z}_2^n$ (см. подробнее [182]).

Теорема 22. *Почти для каждой функции $f : V^\infty \to \mathbb{Z}_2$ верно*

$$\lim_{n\to\infty} \frac{S(f_n)}{2^{n/2}\sqrt{n}} = \sqrt{2\ln 2}.$$

Т. е. с ростом n нелинейность случайной булевой функции от n переменных становится достаточно высокой, и даже сопоставимой с нелинейностью бент-функции!

Для криптографических приложений булева функция кроме нелинейности должна обладать целым рядом других свойств. Можно сказать, что теорема 22 «гарантирует» возможность выбора функции с высокой нелинейностью не в ущерб этим свойствам. Но хотя нелинейность почти всех булевых функций высока, это не означает, что такие функции легко построить. Подобные «парадоксы» уже возникали для булевых функций, например при исследовании их сложностных характеристик[2]. В данном случае асимптотическая оценка теоремы 22 задает некий *уровень* нелинейности, с которым имеет смысл сравнивать нелинейность той или иной криптографической булевой функции [183].

Группы автоморфизмов. В 2010 году была установлена [34] группа автоморфизмов множества всех бент-функций. *Группой автоморфизмов* подмножества булевых функций $\mathcal{M}$ называется группа изометричных отображений множества всех булевых функций в себя, оставляющих неподвижным множество $\mathcal{M}$. Напомним, что *полная аффинная группа* $GA(n)$ состоит из всех отображений вида $g(x) \to g(Ax \oplus b)$, где A — невырожденная матрица, b — произвольный вектор. Справедлива [34]

Теорема 23. *Группа автоморфизмов множества всех бент-функций от n переменных равна полупрямому произведению полной аффинной группы $GA(n)$ на $\mathbb{Z}_2^{n+1}$.*

С доказательством этот факт приводится в Главе 3.

В 2006 г. У. Демпвольф [103] предпринял попытку исследования групп автоморфизмов отдельных бент-функций. Более точно — групп автоморфизмов соответствующих элементарных адамаровых разностных множеств

[2]К. Шенноном было доказано, что почти все булевы функции имеют очень большую сложность реализации, асимптотически равную сложности «самой сложной» функции [23], но ни одну такую функцию построить пока не удалось.

(см. теорему 5). У. Демпвольф показал, что каждое такое разностное множество, при наличии определенного свойства у его группы автоморфизмов, относится к одному из пяти указанных им специальных классов. В целом группы автоморфизмов бент-функций исследованы пока крайне мало.

Метрические свойства класса бент-функций. В 2009 году Н. А. Коломейцем и А. В. Павловым было исследовано минимальное расстояние между бент-функциями. Ими был доказан следующий факт [9].

Теорема 24. *Минимальное расстояние между двумя различными бент-функциями от n переменных равно $2^{n/2}$. Две бент-функции находятся на минимальном расстоянии тогда и только тогда, когда они различаются на некотором аффинном подпространстве размерности $n/2$, причем обе функции на нем аффинны.*

1.12 Векторные бент-функции

С 90-х годов XX века стали исследоваться функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, получившие название *векторных булевых функций*, или (n, m)-*функций*. Интерес к ним вызван тем, что нелинейные такие функции имеют непосредственные криптографические приложения. Например, в шифрах они используются в качестве S-блоков.

Рассмотрим нелинейные свойства векторных функций.

Преобразованием Уолша—Адамара (n, m)-функции f называется отображение $W_f^{\mathrm{vect}} : \mathbb{Z}_2^n \times \mathbb{Z}_2^m \to \mathbb{Z}$, заданное равенством

$$W_f^{\mathrm{vect}}(\boldsymbol{a}, \boldsymbol{b}) = \sum_{\boldsymbol{v} \in \mathbb{Z}_2^n} (-1)^{\langle \boldsymbol{a}, \boldsymbol{v} \rangle \oplus \langle \boldsymbol{b}, f(\boldsymbol{v}) \rangle} \text{ для любых } \boldsymbol{a} \in \mathbb{Z}_2^n, \boldsymbol{b} \in \mathbb{Z}_2^m.$$

Нелинейностью (n, m)-функции f называется минимальная из нелинейностей булевых функций $f_{\boldsymbol{b}}$ от n переменных, где $f_{\boldsymbol{b}}(\boldsymbol{v}) = \langle \boldsymbol{b}, f(\boldsymbol{v}) \rangle$ при различных значениях $\boldsymbol{b} \in \mathbb{Z}_2^m$, $\boldsymbol{b} \neq \boldsymbol{0}$. Справедливо

$$N_f = \min_{\boldsymbol{b} \in (\mathbb{Z}_2^m)^*} \mathrm{dist}(f_{\boldsymbol{b}}, \mathfrak{A}_n) = 2^{n-1} - \frac{1}{2} \max_{\boldsymbol{a} \in \mathbb{Z}_2^n, \boldsymbol{b} \in (\mathbb{Z}_2^m)^*} |W_f^{\mathrm{vect}}(\boldsymbol{a}, \boldsymbol{b})|.$$

Здесь через $(\mathbb{Z}_2^m)^*$ обозначено множество ненулевых двоичных векторов длины m. Для нелинейности векторной булевой функции имеется та же самая верхняя оценка, что и в случае обычной булевой функции:

$$N_f \leqslant 2^{n-1} - 2^{(n/2)-1}. \tag{1.5}$$

Векторная (n, m)-функция называется *бент-функцией*, если параметр N_f достигает своего максимального возможного значения, т. е. если каждая булева функция $f_{\boldsymbol{b}}$, где $\boldsymbol{b} \in (\mathbb{Z}_2^m)^*$, является бент-функцией. Справедлива

Теорема 25. *Векторная (n, m)-функция f является бент-функцией тогда и только тогда, когда для любого ненулевого вектора $\boldsymbol{u}$ функция $f(\boldsymbol{v}) \oplus f(\boldsymbol{v} \oplus \boldsymbol{u})$ сбалансирована, т. е. принимает каждое из 2^m возможных значений ровно 2^{n-m} раз.*

Следующий важный факт о существовании векторных бент-функций получила К. Ньюберг [166] в 1991 г.

Теорема 26. *Бент (n, m)-функции существуют тогда и только тогда, когда n четно и $m \leqslant n/2$.*

Легко построить примеры таких функций, например, применяя конструкцию Мэйорана—МакФарланда в новой, векторной, форме, предложенной К. Ньюберг [166]. Отождествим пространство $\mathbb{Z}_2^{n/2}$ с полем Галуа $GF(2^{n/2})$, а пространство $\mathbb{Z}_2^n$ — с прямым произведением $GF(2^{n/2}) \times GF(2^{n/2})$. Пусть n четно, $m \leqslant n/2$. Справедлива

Теорема 27. *Пусть $h : GF(2^{n/2}) \to GF(2^{n/2})$ — любое взаимно однозначное отображение, g — произвольная $(n/2, m)$-функция. Пусть $L : GF(2^{n/2}) \to \mathbb{Z}_2^{n/2}$ — любое линейное или аффинное отображение «на». Тогда векторная (n, m)-функция $f(\boldsymbol{u'}, \boldsymbol{u''}) = L(\boldsymbol{u'} \cdot h(\boldsymbol{u''})) \oplus g(\boldsymbol{u''})$ является бент-функцией.*

Конструкция Мэйорана—МакФарланда является не единственной, которая переносится на векторный случай (см. подробнее [79]).

Поскольку бент (n,m)-функций не существует при $m > n/2$, то оценка (1.5) в этом случае не точна. В 1971 г. В. М. Сидельников [26] и независимо в 1994 г. Ф. Шабат, С. Ваденай [91] установили следующий факт.

Теорема 28. *Пусть $m \geqslant n-1$. Для любой (n,m)-функции f выполняется*

$$N_f \leqslant 2^{n-1} - \frac{1}{2}\sqrt{3(2^n) - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}. \qquad (1.6)$$

При $n/2 < m < n-1$ оценки, улучшающей (1.5), пока не известно.

Случай $n = m$ выделяется особо. В этом случае оценка (1.6) имеет вид

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

Векторная (n,n)-функция f называется *почти бент-функцией* (AB function — almost bent function), если параметр N_f достигает своего максимального возможного значения, $N_f = 2^{n-1} - 2^{(n-1)/2}$. Следует отметить, что по смыслу слово «почти» здесь совершенно лишнее, поскольку речь идет о максимальном значении N_f. Но термин в таком виде уже устоялся. AB-функции существуют, только если n нечетно. К. Карле, П. Шарпин и В. Зиновьев [80] доказали, что степень нелинейности любой такой функции не превышает величины $(n+1)/2$.

Более широким является класс APN-функций.

Эти векторные (n,n)-функции стала рассматривать в 1993 г. К. Ньюберг [167] при исследовании устойчивости шифров к дифференциальному криптоанализу [55]. Стойкость S-блока, заданного векторной функцией f, к дифференциальному криптоанализу тем выше, чем меньше значение $\delta_f = \max_{\boldsymbol{a}\in(\mathbb{Z}_2^n)^*,\boldsymbol{b}\in\mathbb{Z}_2^n} \delta_{f,\boldsymbol{a},\boldsymbol{b}}$, где через $\delta_{f,\boldsymbol{a},\boldsymbol{b}}$ обозначено число решений уравнения $f(\boldsymbol{v}) \oplus f(\boldsymbol{v} \oplus \boldsymbol{a}) = \boldsymbol{b}$. Параметр δ_f и его связи с другими нелинейными характеристиками исследовались в работах [17,40, 63]. Наименьшее возможное значение параметра δ_f равно двум[3]. Векторная (n,n)-функция, для которой этот минимум достигается, называется *почти совершенно нелинейной* (APN function — almost perfectly nonlinear function). И снова, по

[3]Интересно, что при рассмотрении q-значных векторных функций, $q \neq 2$, возможно и $\delta_f = 1$.

иронии, слово «почти» здесь абсолютно ни при чем. Эквивалентно, APN-функция может быть определена как функция, сужение которой на любое двумерное аффинное подпространство пространства $\mathbb{Z}_2^n$ является неаффинной функцией. Подробный обзор результатов о APN-функциях приводится в обзоре М. Э. Тужилина [35], см. также обзор в [79].

AB- и APN- функции тесно связаны.

Теорема 29. *Каждая AB-функция является APN-функцией.*

Теорема 30. *Квадратичная APN-функция является AB-функцией.*

Приведем одно определение для обычных булевых функций. Булева функция f называется *платовидной* (plateaued function), если существует положительное целое число M такое, что любой коэффициент Уолша—Адамара $W_f(\mathbf{v})$ равен 0 или $\pm M$. Из равенства Парсеваля следует, что $M = 2^\beta$, и показатель β может принимать целые значения от $n/2$ до n. Число $2(n-\beta)$ называют *порядком* платовидной функции f. Бент-функции и аффинные функции являются крайними частными случаями платовидных функций (порядков m и 0 соответственно). Справедлива

Теорема 31. *Векторная функция f является AB-функцией тогда и только тогда, когда она APN-функция и все булевы функции $f_{\boldsymbol{b}}$ при $\boldsymbol{b} \neq \mathbf{0}$ являются платовидными, причем одного порядка.*

Более общим понятием по отношению к понятию APN-функции является следующее. Векторная (n,n)-функция f называется *дифференциально δ-равномерной* (differential δ-uniform), δ — целое число, если уравнение $f(\boldsymbol{v}) \oplus f(\boldsymbol{v} \oplus \boldsymbol{a}) = \boldsymbol{b}$ при любых $\boldsymbol{a} \in (\mathbb{Z}_2^n)^*$, $\boldsymbol{b} \in \mathbb{Z}_2^n$ имеет не более δ решений, т. е., другими словами, $\delta_f = \delta$. APN-функции представляют собой частный случай таких функций при $\delta = 2$. Дифференциально 4-равномерные функции (см., например, [60]) используются в S-блоках симметричного алгоритма блочного шифрования AES (или Rijndael), являющегося с 26 мая 2002 г. американским стандартом шифрования.

AB, APN, δ-равномерные функции и вопросы их эквивалентности широко исследуются. В частности [61], уже выдвинута гипотеза, что все степенные AB- и APN-функции найдены (X. Доббертин [110]) и обозначена проблема существования новых комбинаторных конструкций таких функций (см. подробнее [62, 79]). При $n \leqslant 25$ для APN-функций и при $n \leqslant 33$ для AB-функций гипотеза Доббертина уже подтвердилась [111, 148].

За пределами обзора остались *скрюченные функции* (crooked functions) — специальный подкласс APN-функций, введенный в 1998 г. Т. Бендингом и Д. Г. Фон-дер-Флаассом [49]. С помощью таких функций оказалось возможно строить новые дистанционно регулярные графы, симметричные схемы отношений и равномерно упакованные коды типа БЧХ и Препараты [100, 101] (см. также на эту тему работу [65]).

1.13 Открытые вопросы

Приведем серию нерешенных задач в области бент-функций, представляющихся наиболее интересными:

- Получить аффинную классификацию бент-функций (от 10, 12 и т. д. переменных);
- Получить алгебраическую классификацию бент-функций (от 10, 12 и т. д. перем.);
- Получить асимптотику числа бент-функций от n переменных;
- Улучшить нижнюю и верхнюю оценки числа бент-функций;
- Предложить новые конструкции бент-функций. В частности — векторных;
- Разработать эффективные алгоритмы порождения бент-функций;
- Исследовать взаимосвязи между нелинейностью и другими криптографическими характеристиками булевой функции;
- Разработать эффективные методы построения уравновешенных булевых функций с высокой нелинейностью (и др. криптографическими свой-

ствами) из бент-функций;

- Исследовать максимально нелинейные функции от нечетного числа переменных;
- Исследовать метрическую структуру класса бент-функций;
- Получить конструкции оптимальных кодов, кодовые слова которых являются векторами значений бент-функций;
- Исследовать взаимосвязи между различными обобщениями бент-функций;
- Получить новые конструкции обобщенных бент-функций, исследовать их свойства;
- Получить новые эквивалентные представления бент-функций, полнее отражающие содержательную сторону этих объектов;
- Предложить более общие подходы к исследованию бент-функций, за счет установления взаимосвязей с другими дискретными (и не только) объектами;
- Исследовать новые приложения бент-функций в криптографии, теории кодирования и т.д.

Каждому неравнодушному читателю предлагается принять участие в сокращении этого «проблемного» списка!

Глава 2

Обобщения бент-функций: обзор работ

Термин «обобщенная бент-функция» употребляется в статьях довольно часто. И почти каждый раз он означает нечто новое. Бент-функции, в силу своих многочисленных приложений в теории информации, криптографии, теории кодирования и других областях, интенсивно изучаются. Новые постановки задач приводят к возникновению большого числа обобщений бент-функций, разобраться в которых становится все труднее.

В данной главе предлагается систематический обзор существующих обобщений бент-функций и сделана попытка установить (где это возможно) взаимосвязи между различными обобщениями.

Обобщения бент-функций разделены на несколько групп. Сразу отметим, что разделение довольно условное, но оно показалось удобным для изложения материала. При описании каждого обобщения внимание, по возможности, обращается на то когда, кем и почему было введено обобщение; какой вид имеют функции и преобразование Уолша—Адамара (или Фурье), как правило возникающее в каждом случае; какие известны результаты о данном обобщении; как рассматриваемое обобщение связано с другими и пр. По каждому обобщению приводятся соответствующие ссылки.

Приведем краткий список обозначений и определений, использующихся в данной главе.

q, n — натуральные числа;

$+$ — сложение по модулю q;

$x = (x_1, \ldots, x_n)$ — q-значный вектор;

$\mathbb{Z}_q^n$ — множество всех q-значных векторов длины n;

$\mathbb{F}_{q^n}$ — поле Галуа порядка q^n;

$\langle x, y\rangle = x_1 y_1 + \ldots + x_n y_n$ — скалярное произведение векторов;

$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — булева функция от n переменных;

$W_f(y) = \sum\limits_{x \in \mathbb{Z}_2^n} (-1)^{\langle x,y\rangle + f(x)}$ — преобразование Уолша—Адамара;

N_f — *нелинейность* булевой функции f, т. е. расстояние Хэмминга от данной функции до множества всех аффинных функций;

бент-функция (n четное) — булева функция такая, что все ее коэффициенты Уолша—Адамара равны $\pm 2^{n/2}$;

$\mathcal{B}_n$ — класс бент-функций от n переменных.

2.1 Алгебраические обобщения бент-функций

В этом разделе приводятся обобщения, в которых рассматриваемые функции отличаются от булевых. Как правило, это отображения из одной алгебраической системы в другую.

2.1.1 q-Значные бент-функции

Это естественное обобщение бент-функций предложили в 1985 году П. В. Кумар, Р. А. Шольц и Л. Р. Велч [141] с целью построения q-значных бент-последовательностей, применимых в системах CDMA (см. подробнее дальше).

Пусть $q \geqslant 2$ — натуральное число, $i = \sqrt{-1}$ — мнимая единица. Пусть ω — примитивный комплексный корень степени q из единицы, $\omega = e^{2\pi i/q}$. Рассмотрим q-значную функцию $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$.

Преобразованием Уолша—Адамара функции f называется комплексная

функция

$$W_f(y) = \sum_{x \in \mathbb{Z}_q^n} \omega^{\langle x,y \rangle + f(x)}, \text{ для любого } y \in \mathbb{Z}_q^n, \tag{2.1}$$

где скалярное произведение и сложение + рассматриваются по модулю q. Пусть далее $|c|$ обозначает модуль комплексного числа c.

Определение 1. (Кумар, Шольц и Велч, 1985) Пусть q — натуральное число. Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *q-значной бент-функцией*, если $|W_f(y)| = q^{n/2}$ для каждого $y \in \mathbb{Z}_q^n$.

При $q = 2$ это понятие совпадает с понятием булевой бент-функции. Множество всех q-значных бент-функций от n переменных обозначим через $\mathcal{B}_{n,q}$. В [141] были получены следующие результаты.

Теорема 32. *Класс $\mathcal{B}_{n,q}$ замкнут относительно*
(i) *любого невырожденного аффинного преобразования переменных;*
(ii) *прибавления любой q-значной аффинной функции.*

Квадратная $n \times n$-матрица A из целых степеней элемента ω называется *обобщенной матрицей Адамара*, если $A\overline{A}^T = nE$, где E — единичная матрица.

Теорема 33. *Следующие утверждения эквивалентны*
(i) *q-значная функция f является бент-функцией;*
(ii) *матрица $A = (a_{x,y})$, где $a_{x,y} = \omega^{f(x+y)}$, является обобщенной матрицей Адамара.*

Отметим, что при $q = 2$ теоремы 32, 33 представляют собой хорошо известные факты о булевых бент-функциях, см. Главу 1. К особенностям q-значного случая относится тот факт [141], что функция f остается бент-функцией при замене ω в определении $W_f(y)$ на любой другой примитивный корень γ степени q из единицы. Отметим также, что q-значные бент-функции существуют как для четных, так и для нечетных n.

Теорема 34. *Пусть m, n, q — любые. Для произвольных функций $g \in \mathcal{B}_{m,q}$, $h \in \mathcal{B}_{n,q}$ функция $f(x', x'') = g(x') + h(x'')$ является q-значной бент-функцией.*

Имеет место аналог теоремы Мэйорана—МакФарланда [157].

Теорема 35. *Пусть n четно, q — любое число. Тогда функция $f(x', x'') = \langle x', h(x'')\rangle + g(x'')$, где g — произвольная q-значная функция от $n/2$ переменных, h — любая перестановка на множестве $\mathbb{Z}_q^{n/2}$, является q-значной бент-функцией.*

Пусть n нечетно, $q = 2 \bmod 4$, $q > 2$. В [141] показано, что если существует целое число b такое, что $2^b + 1$ делится на $q/2$, то q-значных бент-функций от n переменных не существует.

Для каждого q такого, что $q \neq 2 \bmod 4$, и любого n бент-функции существуют. Они могут быть построены, например, с помощью теоремы 34 из следующих одномерных ($n = 1$) функций:

Теорема 36. *Следующие q-значные функции от одной переменной являются бент-функциями:*
(i) *$f(x) = x^2 + cx$, где $c \in \mathbb{Z}_q$ — любая константа (если q нечетно);*
(ii) *$f(x) = rx'h(x'') + g(x'')$, где $x = rx' + x'' \in \mathbb{Z}_q$, $0 \leqslant x', x'' \leqslant r - 1$, h — любая перестановка на $\mathbb{Z}_r$, g — любая функция вида $\mathbb{Z}_r \to \mathbb{Z}_q$ (если $q = r^2$ для некоторого r).*

См. подробнее [141]. Конструкции q-значных бент-функций, полученные с помощью цепных колец, были предложены К. Хоу [126].

Наиболее полно свойства булевых бент-функций сохраняются для *регулярных q-значных бент-функций*. Бент-функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *регулярной*, если любой ее коэффициент Уолша—Адамара представляется в виде $W_f(y) = q^{n/2}\omega^{g(y)}$ для некоторой q-значной функции g. Можно доказать [141], что g также является регулярной бент-функций, ее называют *дуальной* к функции f.

Приведем несколько примеров.

При $n = 1$, $q = 4$ функция $f(x) = x^3 + 3x^2$ является регулярной бент-функцией. Ее спектр Уолша—Адамара (т. е. набор коэффициентов в порядке возрастания аргумента) имеет вид $(2, 2i, 2, -2i) = (2\omega^0, 2\omega^1, 2\omega^0, 2\omega^3)$, где $\omega = e^{\pi i/2}$; дуальная функция $g(x) = x^3$.

При $n = 1$, $q = 3$ бент-функция $f(x) = x^2$ не является регулярной, ее спектр равен $(\sqrt{3}i, \frac{3}{2} - \frac{\sqrt{3}}{2}i, \frac{3}{2} - \frac{\sqrt{3}}{2}i)$, или, представляя через степени примитивного корня, $(\sqrt{3}\omega^{3/4}, \sqrt{3}\omega^{11/4}, \sqrt{3}\omega^{11/4})$, где $\omega = e^{2\pi i/3}$. При этом все показатели степеней ω не целые.

Несложно заметить, что булева бент-функция ($q = 2$) всегда является регулярной. Бент-функции, построенные в теоремах 35, 36 (при $q = 1 \bmod 4$ в пункте (i)) являются регулярными. При нечетном n и $q = 2, 3 \bmod 4$ регулярных бент-функций не существует [141]. С. В. Агиевичем [45] показано, что регулярные q-значные бент-функции могут быть описаны с помощью *бент-прямоугольников*, — для двоичного случая такое описание приводилось Главе 1.

Далее о q-значных бент-функциях см. например, работы [127, 123], о бент-последовательностях см. [170].

2.1.2 Бент-функции над конечным полем

А. С. Амбросимов [3] в 1994 году предложил другое — вероятностное — определение q-значных бент-функций. В отличие от предыдущего случая здесь рассматриваются только q-значные функции над конечным полем $\mathbb{F}_{q^n}$.

Пусть $q = p^\ell$, где p — простое, ℓ — натуральное. Пусть ω — примитивный комплексный корень степени p из единицы, $\omega = e^{2\pi i/p}$.

Пусть $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ — q-значная функция. Предположим, что вектор $x \in \mathbb{F}_{q^n}$ выбирается случайно и равновероятно. Для случайной величины $\xi = f(x)$ определяется характеристическая функция $\varphi_\xi(z) = \mathbf{E}\,\omega^{\langle \xi, z\rangle}$, $z \in \mathbb{F}_q$, где элементы ξ и z рассматриваются как векторы длины ℓ над полем

$\mathbb{F}_p$, и скалярное произведение $\langle \xi, z \rangle$ берется по модулю p. При фиксированном $z \in \mathbb{F}_q$ *преобразование Уолша—Адамара* функции f определяется как $W_{f,\,z}(y) = q^n\ \varphi_{\langle x,y\rangle + f(x)}(z)$, или, что то же самое,

$$W_{f,\,z}(y) = q^n\ \mathbf{E}\ \omega^{\langle\langle x,y\rangle + f(x), z\rangle},\ \text{для любого } y \in \mathbb{F}_{q^n},$$

где скалярное произведение $\langle x, y \rangle$ рассматривается по модулю q. Расписывая математическое ожидание, получаем

$$W_{f,\,z}(y) = \sum_{x \in \mathbb{F}_{q^n}} \omega^{\langle\langle x,y\rangle + f(x), z\rangle},\ \text{для } y \in \mathbb{F}_{q^n}. \tag{2.2}$$

Отметим, что в определении (2.1) Кумара, Шольца и Велча и определении (2.2) Амбросимова используются примитивные корни из единицы разных степеней — степени q и p соответственно. Параметр z, появившийся в определении (2.2), задает проекцию элемента $\langle x, y \rangle + f(x)$ из поля $\mathbb{F}_q$ в простое поле $\mathbb{F}_p$.

Можно предложить и эквивалентное определение:

$$W'_{f,\,z}(y) = \sum_{x \in \mathbb{F}_{q^n}} \omega^{Tr(\langle x,y\rangle + z f(x))},$$

заменив скалярное произведение на функцию следа $Tr : \mathbb{F}_q \to \mathbb{F}_p$. При таком определении значения $W_{f,\,z}(y)$ и $W'_{f,\,z}(y)$ будут отличаться лишь с точностью до перестановки на элементах z, y.

Согласно [3] для любой функции f и любого ненулевого z выполняется равенство Парсеваля $\sum_{y \in \mathbb{F}_{q^n}} |W_{f,\,z}(y)|^2 = q^{2n}$, из которого следует, что $\max\limits_{y \in \mathbb{F}_{q^n}} |W_{f,z}(y)| \geqslant q^{n/2}$.

Определение 2. (Амбросимов, 1994) Пусть $q = p^\ell$, p — простое. Функция $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ называется *бент-функцией*, если при любых векторах $z \in \mathbb{F}_q \backslash \{0\}$, $y \in \mathbb{F}_{q^n}$ выполняется $|W_{f,\,z}(y)| = q^{n/2}$.

Заметим, что

• При $q = p$, $\ell = 1$ данное определение q-значной бент-функции совпадает с определением 1 Кумара, Шольца и Велча.

• В определении 2 коэффициенты Уолша—Адамара должны быть одинаковыми по модулю при любой ненулевой проекции показателя степени примитивного элемента в (2.2) из поля $\mathbb{F}_q$ в поле $\mathbb{F}_p$. Тогда как в определении 1 они одинаковы по модулю без рассмотрения проекций (кроме того, $\mathbb{Z}_q$ может не быть полем).

Приведем несколько примеров. Любая q-значная функция от одной переменной вида $f(x) = a_2x^2 + a_1x + a_0$, где $a_2 \neq 0$ и $p \neq 2$ является бент-функцией по Амбросимову. Любая функция от двух переменных вида $f(x_1, x_2) = x_1x_2 + a_2x_1^2 + b_2x_2^2 + a_1x_1 + b_1x_2 + c$ над полем характеристики 2 — также бент-функция.

Для бент-функций над полем справедлив [3] критерий Ротхауса.

Теорема 37. *Функция $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ является бент-функцией тогда и только тогда, когда при любом фиксированном $y \in \mathbb{F}_{q^n}$ функция $f(x+y) - f(x)$ имеет равномерное распределение на $\mathbb{F}_q$ при равномерном распределении аргумента x на $\mathbb{F}_{q^n}$.*

В [3] приводится описание всех квадратичных q-значных бент-функций от n переменных и подсчитывается их число, которое обозначим через $M_q(n)$.

Теорема 38. *Пусть $q = p^\ell$. Справедливы утверждения*

(i) *если $p = 2$, $\ell \geqslant 2$, то $M_q(n) = q^{\binom{n}{2}+2n+1} \prod_{j=1}^{n/2}(1 - q^{-2j+1})$ при четном n, и $M_q(n) = 0$, если n — нечетно.*

(ii) *если $p \neq 2$, то $M_q(n) = (q-1)q^n M_q(n-1) + q^{n+1}(q^{n-1} - 1)M_q(n-2)$ при $n \geqslant 3$.*

К сожалению, в [3] не прослеживается явно взаимосвязь между бент-функциями Амбросимова и бент-функциями Кумара, Шольца и Велча. При $q = p^\ell$ не ясно, например, является ли бент-функция в одном смысле бент-функцией в другом.

Вечернее небо. Подмосковье, Россия.

2.1.3 Обобщенные булевы бент-функции Шмидта

Другое обобщение бент-функций стал рассматривать в 2006 году К. Шмидт [188] в связи с построением четверичных кодов постоянной амплитуды (quaternary constant-amplitude codes) для мультикодовых систем CDMA. Остановимся на этом подробнее.

Технология цифровой сотовой связи CDMA (Code Division Multiple Access — множественный доступ с кодовым разделением каналов) была стандартизована в 1993 году американской телекоммуникационной промышленной ассоциацией (US TIA) в виде стандарта IS–95 («Mobile Station — Base Station Compatibility Standard for Dual–Mode Wideband Spread Spectrum Cellular System»). В настоящее время технология активно используется большинством поставщиков беспроводного оборудования во всем мире согласно стандартам IMT–2000 мобильной связи третьего поколения (в России — стандарты IMT–MC 450 или CDMA–450). Отметим, что первая рабо-

та [2], посвященная этой технологии, была опубликована в СССР еще в 1935 г. Д. В. Агеевым. В системах CDMA применяются широкополосные сигналы, при этом вся полоса частот канала одновременно используется многими абонентами. Поскольку каждому абоненту присваивается свой уникальный код, он легко выделяется из общего «шума». В системах CDMA существенно повышается пропускная способность канала, кроме того, они являются весьма экономичными.

Связь между бент-функциями и кодами для CDMA установил в 2000 году Т. Вада [200], см. также работу [174] К. Г. Патерсона.

Рассмотрим простейшую модель передачи информации в мультикодовой системе CDMA. Пусть $N = 2^n$ — степень двойки, $A_N = (a_{jt})$ — матрица Адамара типа Сильвестра размера $N \times N$. Имеются N параллельных потоков данных. Передаваемую информацию можно представить двоичным вектором c длины N (по биту от каждого потока). Сигнал в MC-CDMA моделируется как $S_c(t) = \sum_{j=0}^{N-1}(-1)^{c_j}a_{jt}$, где $t = 0, 1, \ldots, N-1$ — дискретный параметр времени. Т. е. j-я строка матрицы A домножается на $(-1)^{c_j}$, а передаваемый сигнал S_c является суммой этих новых строк. В каждый момент времени передается один бит последовательности S_c. Важным параметром является *отношение пиковой и средней мощностей сигнала* (peak-to-average power ratio), которое определяется как $\mathrm{PAPR}(c) = \frac{1}{N}\max_t |S_c(t)|^2$. Отметим, что $1 \leqslant \mathrm{PAPR}(c) \leqslant N$. Величина $|S_c(t)|^2$ пропорциональна мощности, необходимой для передачи данного сигнала, поэтому наиболее подходящими для передачи являются такие векторы c, для которых $\mathrm{PAPR}(c)$ минимальна. Можно считать, что векторы c выбираются из некоторого двоичного кода C длины N, пусть $\mathrm{PAPR}(C) = \max_{c\in C}\mathrm{PAPR}(c)$. Если $\mathrm{PAPR}(C) = 1$, то C называется *кодом постоянной амплитуды*. Задача построения таких кодов с большой мощностью и большим кодовым расстоянием весьма актуальна. Справедлива [200, 174]

Теорема 39. *Код C длины 2^n является кодом постоянной амплитуды*

тогда и только тогда, когда каждое его кодовое слово — вектор значений некоторой бент-функции от n переменных.

Действительно, заметим, что если c — вектор значений булевой функции f от n переменных, то $\mathrm{PAPR}(c) = \frac{1}{2^n} \max_{x \in \mathbb{Z}_2^n} |W_f(x)|^2$. Таким образом, бент-функции играют существенную роль при построении кодов для CDMA систем.

Обобщение К. Шмидта [188] состоит в следующем. Пусть $q \geqslant 2$ — натуральное число, ω — примитивный комплексный корень степени q из единицы, $\omega = e^{2\pi i/q}$. Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ называется *обобщенной булевой функцией*. Ее *преобразованием Уолша—Адамара* называется комплексная функция

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

Определение 3. (Шмидт, 2006) Пусть q — натуральное. Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ называется *обобщенной бент-функцией*, если для каждого $y \in \mathbb{Z}_2^n$ выполняется $|W_f(y)| = 2^{n/2}$.

С помощью таких функций строятся коды постоянной амплитуды для q-значного варианта MC-CDMA, в котором двоичный вектор c длины N моделируется как $S_{c,q}(t) = \sum_{j=0}^{N-1} \omega^{c_j} a_{jt}$. Отметим также, что для некоторых задач в области циклических кодов определение Шмидта представляется более естественным, чем определение q-значной бент-функции Кумара, Шольца и Велча.

К. Шмидт [188] подробно разбирает случай $q = 4$, исследует взаимосвязи между обобщенными бент-функциями, кодами постоянной амплитуды и известными $\mathbb{Z}_4$-линейными кодами.

Интересным остается вопрос о том, как соотносятся между собой бент-функции Шмидта, q-значные и булевы бент-функции.

В работе [195] был дан ответ на этот вопрос в одном частном случае. Пусть обобщенная булева функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$ ($q = 4$) представляется в

виде $f(x) = a(x) + 2b(x)$, где a, b — булевы функции от n переменных. В [195] показано, что f — обобщенная бент-функция тогда и только тогда, когда функции b и $a + b$ являются обычными бент-функциями.

Отметим, что *действительно-значные бент-функции* (real-valued bent functions) вида $\mathbb{Z}_2^n \to \{0, 1/2, 1, 3/2\}$, рассматривавшиеся в [153], совпадают с обобщенными бент-функциями при $q = 4$.

2.1.4 Бент-функции из конечной абелевой группы в множество комплексных чисел единичной окружности

В 1997 году О. А. Логачев, А. А. Сальников и В. В. Ященко [16] ввели понятие бент-функции на произвольной конечной абелевой группе. В случае, если группа является элементарной абелевой 2-группой, это понятие совпадает с понятием булевой бент-функции.

Пусть $(A, +)$ — конечная абелева группа порядка n и максимальный порядок ее элементов (или *экспонента* группы) равен q. Пусть

$$T_q = \{e^{2\pi ik/q} \mid k = 0, 1, \ldots, q-1\}$$

— группа корней степени q из единицы. Через $\widehat{A}$ обозначим группу гомоморфизмов $\chi : A \to T_q$. Она называется *группой характеров группы* A (или ее *дуальной группой*). Известно, что группы A и $\widehat{A}$ изоморфны, пусть $y \to \chi_y$ — некоторый фиксированный изоморфизм, $y \in A$.

Вместо преобразования Уолша—Адамара удобно ввести *преобразование Фурье* комплекснозначной функции $f : A \to \mathbf{C}$. Оно определяется как

$$\widehat{f}(y) = \sum_{x \in A} f(x)\overline{\chi_y(x)}.$$

Далее рассматриваются только такие функции из A в $\mathbf{C}$, все значения которых лежат на единичной окружности $S_1(\mathbf{C})$ с центром в нуле.

Определение 4. (Логачев, Сальников, Ященко, 1997) Пусть A — конечная абелева группа порядка n. Функция $f : A \to S_1(\mathbf{C})$ называется *бент-функцией*, если $|\widehat{f}(y)|^2 = n$ при любом $y \in A$.

Сделаем следующие замечания:

• Если A — элементарная абелева 2-группа, т. е. $q = 2$, $n = 2^m$ для целого m, то данное понятие совпадает с понятием обычной бент-функции от m переменных.

• Пусть q, m — целые. Тогда q-значные бент-функции Кумара, Шольца и Велча от m переменных (см. определение 1) являются частным случаем бент-функций из определения 4 при $A = \mathbb{Z}_q^m$ и $n = q^m$. Для этого необходима лишь небольшая модификация: от функций вида $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ нужно перейти к функциям $f' : \mathbb{Z}_q^m \to T_q \subset \mathbf{C}$, где $f'(x) = \omega^{f(x)}$. А в качестве изоморфизма между A и ее группой характеров $\widehat{A}$ выбрать соответствие $y \to \chi_y(x) = \omega^{\langle x,y\rangle}$, где $\omega = e^{2\pi i/q}$.

Функция $f : A \to S_1(\mathbf{C})$ называется *уравновешенной*, если выполняется $\sum_{x\in A} f(x) = 0$. Критерий Ротхауса для бент-функций на группе приобретает вид [16]

Теорема 40. *Функция f — бент-функция на группе A тогда и только тогда, когда функция $\overline{f(x)}f(x+y)$ уравновешена для каждого $y \in A$, $y \neq 0$.*

В [16] можно найти и другие критерии.

Для бент-функции f на группе A так же как в булевом случае можно определить *дуальную* функцию $\widetilde{f} : A \to S_1(\mathbf{C})$. Она задается равенством $\widetilde{f}(x) = \frac{1}{\sqrt{n}}\widehat{f}(x)$ и тоже является бент-функцией.

Если для некоторого разложения группы A в прямое произведение групп A_1 и A_2 функция $f : A \to S_1(\mathbf{C})$ может быть представлена в виде $f(x', x'') = f_1(x')f_2(x'')$, где $f_1 : A_1 \to S_1(\mathbf{C})$, $f_2 : A_2 \to S_1(\mathbf{C})$, то функция f называется *разложимой*. Справедлива [16]

Теорема 41. *Разложимая функция f является бент-функцией на группе A тогда и только тогда, когда f_1 и f_2 — бент-функции на группах A_1 и A_2 соответственно.*

2.1.5 Бент-функции из конечной абелевой группы в другую конечную абелеву группу

В. И. Солодовников [28] в 2002 году предложил наиболее общий подход к алгебраическому обобщению бент-функций. При изложении его результатов будем использовать как оригинальные обозначения, так и обозначения работы [82], представляющиеся иногда более удобными. Следует отметить, что в 2004 году К. Карле и К. Динг [82] повторили результаты В. И. Солодовникова, к сожалению, без ссылки на предшественника.

Пусть $(A,+)$ и $(B,+)$ — конечные абелевы группы порядков n и m соответственно, a и b — максимальные порядки элементов в этих группах. Пусть $\widehat{A}$ и $\widehat{B}$ — группы характеров групп A и B. Зафиксируем изоморфизмы $y \to \chi_y$ и $z \to \eta_z$ между A и $\widehat{A}$, B и $\widehat{B}$ соответственно, где $\chi_y : A \to T_a$ и $\eta_z : B \to T_b$ — характеры. Пусть $f : A \to B$ — произвольная функция. Следующие определения из [28] приведем в несколько иной форме (введем нормировочные множители), не искажая при этом их смысл. *Преобразованием Фурье характера функции* f при фиксированном $z \in B$ называется функция

$$\widehat{f_z}(y) = \sum_{x \in A} \eta_z(f(x))\overline{\chi_y(x)}, \text{ где } y \in A. \tag{2.3}$$

При любом z выполняется равенство Парсеваля $\sum_{y \in A} |\widehat{f_z}(y)|^2 = n^2$.

Определение 5. (Солодовников, 2002) Функция $f : A \to B$ называется *бент-функцией*, если для любого $z \in B$, $z \neq 0$ и произвольного $y \in A$ справедливо $|\widehat{f_z}(y)|^2 = n$.

Фиксируя элемент $z \in B$, от функции f можно перейти к комплекснозначной функции $\eta_z \circ f : A \to T_b$. Можно сказать, что (2.3) является разложением этой функции[1] по группе характеров $\widehat{A}$. Функции вида $A \to S_1(\mathbf{C})$ уже рассматривались Логачевым, Сальниковым и Ященко (см. определение 4). Имеет место [28, 82]

[1]Здесь и далее запись $g \circ f(x)$ означает функцию $g(f(x))$.

Теорема 42. *Функция $f : A \to B$ является бент-функцией тогда и только тогда, когда при каждом $z \neq 0$ функция $\eta_z \circ f$ — бент-функция в смысле Логачева, Сальникова и Ященко.*

Производной функции f по направлению $y \in A$ называется функция $D_y f(x) = f(x+y) - f(x)$. Справедлива [28, 82]

Теорема 43. *Функция $f : A \to B$ является бент-функцией, если и только если функция $D_y f(x)$ уравновешена для каждого ненулевого $y \in A$, т. е. мощности всех ее прообразов одинаковы.*

Пусть f — бент-функция. Тогда для любой линейной или аффинной перестановки π на группе A, функция $f \circ \pi : A \to B$ является бент-функцией. Если $\ell : B \to C$ — линейная функция «на» (C — конечная абелева группа), то функция $\ell \circ f : A \to C$ — также бент-функция.

В. И. Солодовниковым [28] определяется функция *близости* двух функций f, $g : A \to B$ как

$$\delta(f,g) = \left(\frac{1}{m} \sum_{y \in B} \Big(\frac{|\{x : f(x) - g(x) = y\}|}{n} - \frac{1}{m} \Big)^2 \right)^{1/2}. \qquad (2.4)$$

С помощью этой функции предполагается оценивать качество (или эффективность) замены одной функции на другую. Чем меньше значение параметра $\delta(f,g)$, тем менее «близки» друг другу функции f и g. Из определения близости следует, что $\delta(f,g) = 0$ тогда и только тогда, когда f и g отличаются на уравновешенную функцию.

Пусть $\mathrm{Hom}(A,B)$ — множество всех гомоморфизмов группы A в группу B. По определению для каждого гомоморфизма h производная $D_y h(x)$ по любому ненулевому направлению $y \in A$ является постоянной функцией. Тогда функцию $f : A \to B$ такую, что для любого ненулевого $y \in A$ функция $D_y f(x)$ уравновешена, естественно называть [28] *абсолютно негоморфной*. Согласно теореме 43 абсолютно негоморфные функции и бент-функции совпадают. Справедлива также

Теорема 44. *Для любой бент-функции f и произвольного гомоморфизма h выполняется $\delta(f,h)=\frac{\sqrt{m-1}}{m\sqrt{n}}$.*

Другими словами, бент-функция находится в одинаковой «близости» от всех гомоморфизмов. Интересно рассмотреть *минимальные функции* — функции наименее близкие к гомоморфизмам, т. е. такие для которых значение

$$\delta_f=\delta(f,\mathrm{Hom}(A,B))$$

минимально. При $A=\mathbb{Z}_q^\ell$, $B=\mathbb{Z}_q^r$ показано [28], что функция f минимальна, если $\delta_f=\frac{\sqrt{m-1}}{m\sqrt{n}}$. Функция называется *абсолютно минимальной*, если ее свойство минимальности инвариантно относительно любых эпиморфизмов группы B.

Теорема 45. *Пусть q — простое, $A=\mathbb{Z}_q^\ell$, $B=\mathbb{Z}_q^r$ и бент-функции из A в B существуют. Тогда*

(i) *любая бент-функция является абсолютно минимальной*;

(ii) *при $q=2$ класс всех бент-функций совпадает с классом всех абсолютно минимальных функций.*

См. далее на эту тему работу [83]. Скоро, видимо, появятся работы о бент-функциях и на конечных неабелевых группах [176].

2.1.6 Векторные G-бент-функции

Идея этого обобщения для функций вида $f:A\to B$ впервые была предложена В. И. Солодовниковым в работе [28] 2002 года. Л. Поинсо и С. Харари [177] в 2004 году подробно ее рассмотрели для случая $A=(\mathbb{Z}_2^k,+)$ и $B=(\mathbb{Z}_2^r,+)$, т. е. векторных булевых функций. Основу обобщения составляет возможность иначе определить производную функции $f:A\to B$.

А именно, пусть $S(A)$ — симметрическая группа A в мультипликативной записи. Перестановка $\sigma\in S(A)$ называется *инволюцией*, если $\sigma\sigma=e$, где e — тождественная перестановка. Перестановка σ *без неподвижных точек*, если для любого $x\in A$ справедливо $\sigma(x)\neq x$. Множество всех инволюций

σ без неподвижных точек обозначим через $Inv(A)$. Подгруппа G группы $S(A)$ такая, что $G \subseteq Inv(A) \cup \{e\}$ называется *группой инволюций группы* A.

Пусть теперь $A = \mathbb{Z}_2^k$, $B = \mathbb{Z}_2^r$. Отметим, что $|Inv(\mathbb{Z}_2^k)| = \frac{2^k!}{2^{k-1}!2^{2^{k-1}}}$. В работе [177] показано, что любая группа инволюций G группы $\mathbb{Z}_2^k$ является абелевой и $|G| \leqslant 2^k$. Будем рассматривать только группы G максимального порядка 2^k. Простым примером такой группы является *группа трансляций* $T(\mathbb{Z}_2^k)$, состоящая из всех перестановок σ_y, $y \in \mathbb{Z}_2^k$, таких, что $\sigma_y(x) = x+y$. Но существуют [177] и другие максимальные группы инволюций.

Пусть $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^r$, G — максимальная группа инволюций группы $\mathbb{Z}_2^k$. *Обобщенной производной f по направлению $\sigma \in G$* называется функция $D_\sigma f(x) = f(\sigma(x)) - f(x)$. Отметим, что, если G — группа трансляций $T(\mathbb{Z}_2^k)$, то обобщенная производная совпадает с обычной, $D_y f(x) = f(x + y) - f(x)$.

Определение 6. (Поинсо, Харари, 2004) Пусть $A = (\mathbb{Z}_2^k, +)$, $B = (\mathbb{Z}_2^r, +)$, G — максимальная группа инволюций группы A. Функция $f : A \to B$ называется *G-бент-функцией*, если обобщенная производная $D_\sigma f(x)$ по каждому направлению $\sigma \in G$, $\sigma \neq e$, уравновешена.

В интерпретации В. И. Солодовникова G-бент-функция — это функция f, которую любая перестановка $\sigma \in G$, $\sigma \neq e$, изменяет настолько сильно, насколько это возможно, т. е. каждый раз выполняется $\delta(f, f \circ \sigma) = 0$.

В работе [177] предлагается перевод определения G-бент-функции на язык обобщенных коэффициентов Фурье, но пока, как представляется, он не вполне доработан и содержит неточности. Не ясно также в какой мере подход [177] применим, если A и B — произвольные абелевы группы.

2.1.7 Многомерные бент-функции на конечной группе

Это прямое обобщение бент-функций О. А. Логачева, А. А. Сальникова и В. В. Ященко [16] предложил рассматривать Л. Поинсо [175] в 2005 году.

Пусть $\mathbf{C}^m$ — m-мерное унитарное пространство с обычным скалярным произведением $\langle x, y\rangle = \sum_{j=1}^{m} x_j \overline{y}_j$, нормой $\|x\|^2 = \langle x, x\rangle$ и метрикой $d(x, y) = \|y - x\|$. Пусть $S_1(\mathbf{C}^m)$ — множество его точек, лежащих на сфере радиуса 1 с центром в нуле.

Пусть, как и выше, A — конечная абелева группа порядка n. Пусть $\widehat{A} = \{\chi_y \mid y \in A\}$ — ее группа характеров.

Преобразованием Фурье функции $f : A \to \mathbf{C}^m$ называется следующая функция из A в $\mathbf{C}^m$:

$$\widehat{f}(y) = \sum_{x \in A} f(x)\overline{\chi_y(x)}.$$

Определение 7. (Поинсо, 2005) Пусть A — конечная абелева группа порядка n. Функция $f : A \to S_1(\mathbf{C}^m)$ называется *многомерной бент-функцией*, если $||\widehat{f}(y)||^2 = n$ для каждого $y \in A$.

При $m = 1$ данное определение полностью совпадает с определением 4. Аналогично, для многомерных бент-функций выполняется критерий Ротхауса, определяется дуальная многомерная бент-функция и т. п. [175]. Но пока не ясно представляют ли многомерные бент-функции самостоятельный интерес, или же являются несколько формальным обобщением бент-функций из определения 4.

2.2 Комбинаторные обобщения бент-функций

В этом разделе рассматриваются довольно естественные обобщения. Можно сказать, что в основу каждого из них заложена простая комбинаторная идея.

2.2.1 Частично определенные бент-функции

Пусть $S \subseteq \mathbb{Z}_2^n$ — произвольное подмножество, $f : S \to \mathbb{Z}_2$ — *частично определенная булева функция*. Ее *неполным преобразованием Уолша—Адамара*

называется отображение

$$W_{f,S}(y) = \sum_{x \in S} (-1)^{\langle x,y \rangle + f(x)}, \text{ для любого } y \in \mathbb{Z}_2^n.$$

Для такого преобразования справедлив аналог равенства Парсеваля:

$$\sum_{y \in \mathbb{Z}_2^n} W_{f,S}^2(y) = 2^n \, |S|.$$

Определение 8. Булева функция f называется *частично определенной бент-функцией*, если $W_{f,S}(y) = \pm\sqrt{|S|}$ для любого $y \in \mathbb{Z}_2^n$.

Подробнее такие функции разбираются в [19, гл. 6]. Здесь отметим лишь, что пока не известно при каких условиях на множество S частично определенные бент-функции существуют.

2.2.2 Платовидные функции

Это достаточно известное обобщение бент-функций, на котором также не будем останавливаться подробно.

Определение 9. Булева функция называется *платовидной*, если все ее ненулевые коэффициенты Уолша—Адамара равны по модулю.

Из равенства Парсеваля следует, что ненулевые коэффициенты должны иметь вид $\pm 2^{n-h}$ для некоторого целого h, где $0 \leqslant h \leqslant n$. Количество таких ненулевых коэффициентов должно быть равно 2^{2h}. Показатель $2h$ и величину 2^{n-h} называют соответственно *порядком* и *амплитудой* платовидной функции. Бент-функции и аффинные функции являются крайними частными случаями платовидных функций (порядков n и 0 соответственно).

Результаты о таких функциях можно найти в обзорах [19, 78], а также в работах [210, 211, 89].

2.2.3 $\mathbb{Z}$-бент-функции

В 2005 году Х. Доббертин, см. [114], предложил исследовать бент-функции в контексте более общего подхода, который можно назвать рекурсивным.

Не будем различать обычную булеву функцию $f(x)$, где $x \in \mathbb{Z}_2^n$, и целочисленную функцию $F(x) = (-1)^{f(x)}$. *Преобразование Фурье* функции $F : \mathbb{Z}_2^n \to \mathbb{Z}$ определяется как

$$\widehat{F}(y) = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x,y \rangle} F(x).$$

Тогда ± 1-значная функция F является бент-функцией, если и только если $\widehat{F}$ также ± 1-значная. Обобщение состоит в следующем.

Определение 10. (Доббертин, 2005) Пусть $T \subseteq \mathbb{Z}$ — любое подмножество. Функция $F : \mathbb{Z}_2^n \to T$ называется *T-бент-функцией*, если все значения функции $\widehat{F}$ принадлежат множеству T.

Доббертин выделил естественную цепочку вложенных друг в друга множеств:

$$T_0 = \{-1, +1\};$$

$$T_r = \{w \in \mathbb{Z} \mid -2^{r-1} \leqslant w \leqslant 2^{r-1}\} \text{ (при } r > 0).$$

T_r-бент-функция называется *$\mathbb{Z}$-бент-функцией уровня r*, а все такие бент-функции (при $r \in \mathbb{Z}$) составляют класс *$\mathbb{Z}$-бент-функций*. В работе [114] исследуются возможности рекурсивного построения (разложения) $\mathbb{Z}$-бент-функций с повышением или понижением их уровня и числа переменных.

2.2.4 Однородные бент-функции

Этот подкласс бент-функций был выделен авторами [180] как состоящий из функций с относительно простыми алгебраическими нормальными формами.

Определение 11. (Ку, Себерри, Пипджик, 2000) Бент-функция называется *однородной*, если все одночлены ее алгебраической нормальной формы имеют одинаковые степени.

В своей работе Ч. Ку, Дж. Себерри и Й. Пипджик перечислили все однородные бент-функции степени 3 от 6 переменных (их оказалось ровно

30) и поставили вопрос о классификации таких бент-функций от большего числа переменных. К. Чарнес, М. Роттелер и Т. Бет [92] доказали, что существуют однородные бент-функции степени 3 от любого числа переменных $n > 2$. В работе [203] Т. Кси, Дж. Себерри, Й. Пипджик и К. Чарнес установили, что однородных бент-функций от n переменных максимальной возможной степени $n/2$ не существует при $n > 3$. Исследователи из Китая К. Менг, Х. Жанг, М. Янг и Дж. Цуи [160, 161] показали, что не существует также однородных бент-функций степени $(n/2) - 1$ при $n > 4$. Но какова же точная верхняя оценка степени нелинейности однородной бент-функции? На этот вопрос нет ответа. Есть только предположение авторов [160] о том, что для любого $k > 1$ найдется такое $N \geqslant 2$, что однородная бент-функция степени k от n переменных существует при каждом $n > N$.

2.2.5 Нормальные бент-функции

Булева функция f от n переменных называется *нормальной* (*слабо нормальной*), если существует $(n/2)$-мерное подпространство пространства $\mathbb{Z}_2^n$, такое что f на нем является константой (аффинной функцией). Впервые такие функции стал рассматривать Х. Доббертин [109] в 1995 году для построения уравновешенных булевых функций с высокой нелинейностью.

Десять лет построить бент-функции, не являющиеся нормальными и слабо нормальными, не удавалось. В 2005 году авторам [68] это удалось.

2.3 Криптографические обобщения бент-функций

Как известно, одной высокой нелинейности для хорошей криптографической функции недостаточно. В этом разделе рассматриваются обобщения, которые возникли путем наложения на множество булевых функций других дополнительных ограничений.

2.3.1 Уравновешенные бент-функции

С точки зрения криптографии, к важным критериям, которым должна удовлетворять булева функция f от n переменных, относятся следующие [18, 78]:

• *уравновешенность* (или *сбалансированность*) — функция f принимает значения 0 и 1 одинаково часто;

• *критерий распространения $PC(k)$ порядка k (Propagation Criterion)* — для любого ненулевого вектора $y \in \mathbb{Z}_2^n$ веса не более k, где $1 \leqslant k \leqslant n$, функция $f(x+y)+f(x)$ уравновешена [178];

• *максимальная нелинейность* — функция f такова, что значение ее нелинейности N_f максимально;

• *равномерность корреляции с линейными функциями*. Значение корреляции между функциями f и g определяется как $c(f,g) = 1 - \frac{\mathrm{dist}(f,g)}{2^{n-1}}$. Для функции f равномерная корреляция означает, что значение $|c(f,g)|$ постоянно при любой линейной функции g.

Но криптографические критерии противоречат друг другу. Бент-функции являются максимально-нелинейными, удовлетворяют критерию $PC(n)$, обладают равномерной корреляцией с линейными функциями (значение равно $\pm 2^{-n/2}$), но не являются уравновешенными. Довольно естественно возникает следующее определение.

Определение 12. Булева функция f от n переменных называется *уравновешенной бент-функций*, если она уравновешена и имеет при этом максимально возможную нелинейность.

В [42] было установлено, что, если n нечетно и f — уравновешенная функция, то $N_f \leqslant 2^{n-1} - 2^{(n-1)/2}$.

В 1994 году С. Чи, С. Ли и К. Ким [95] предложили способ построения уравновешенных бент-функций от нечетного числа переменных, имеющих при этом почти равномерную корреляцию с линейными функциями и удовлетворяющих критерию $PC(k)$ для достаточно большого k. Приве-

дем этот способ.

Пусть n — нечетно, A — невырожденная двоичная матрица размера $(n-1)\times(n-1)$, b — двоичный вектор длины $n-1$.

Теорема 46. *Пусть f_0 — бент-функция от $n-1$ переменной, f_1 — эквивалентная ей бент-функция: $f_1(x) = f_0(Ax+b)+1$. Тогда функция $g(x,z) = f_z(x)$ от n переменных, где $x \in \mathbb{Z}_2^{n-1}$, $z \in \mathbb{Z}_2$,*

(i) *является уравновешенной бент-функцией*;

(ii) *является почти бент-функцией (см. определение далее)*;

(iii) *имеет следующие возможные значения корреляции с любой линейной функцией:* 0, $\pm 2^{-(n-1)/2}$;

(iv) *удовлетворяет критерию PC для любого ненулевого вектора $(y,0)$, где $y \in \mathbb{Z}_2^{n-1}$* ;

(v) *удовлетворяет критерию $PC(n-1)$, если $A = E$ и b — вектор из всех единиц.*

2.3.2 Частично бент-функции

Как уже было отмечено, бент-функции не являются ни уравновешенными, ни корреляционно-иммунными. К. Карле [69] предложил свой способ расширить класс $\mathcal{B}_n$ функциями, обладающими данными свойствами и имеющими при этом достаточно высокую нелинейность. Определение таких *частично бент-функций* дается с помощью следующего экстремального свойства. Пусть $\Delta_f(y) = \sum\limits_{x\in\mathbb{Z}_2^n} (-1)^{f(x)+f(x+y)}$ — *автокорреляция* булевой функции f по направлению y. Пусть NW_f и $N\Delta_f$ — количества ненулевых коэффициентов Уолша—Адамара и коэффициентов автокорреляции булевой функции f, соответственно. Тогда [69] для любой булевой функции выполняется $NW_f \cdot N\Delta_f \geqslant 2^n$.

Определение 13. (Карле, 1993) Булева функция f, для которой $NW_f \cdot N\Delta_f = 2^n$, называется *частично бент-функцией.*

Теорема 47. *Следующие утверждения эквивалентны:*

(i) *функция f — частично бент-функция;*

(ii) *существует вектор z такой, что для любого x значение автокорреляции $\Delta_f(x)$ равно 0 или $(-1)^{\langle x,z\rangle}2^n$;*

(iii) *существуют вектор z и разбиение пространства $\mathbb{Z}_2^n$ в прямую сумму подпространств L и L' такие, что $f|_{L'}$ — частично определенная бент-функция (в смысле определения 8) и для любых $x \in L$, $y \in L'$ выполняется $f(x+y) = \langle x, z\rangle + f(y)$.*

Далее z обозначает вектор, определенный в теореме. Подпространство L для частично бент-функции f определяется как множество векторов x таких, что $\Delta_f(x) \neq 0$. Эквивалентно, можно определить L как пространство линейных структур f, т. е. пространство, состоящее из всех векторов y таких, что $f(x+y)+f(x) = \text{const}$. Подпространство L' для разложения $\mathbb{Z}_2^n$ в прямую сумму выбирается произвольно. Заметим, что размерность подпространства L' должна быть четной, пусть она равна $2h$. Согласно [69] справедливы следующие результаты (необходимые определения см. в [19]).

Теорема 48. *Частично бент-функция является*

(i) *уравновешенной тогда и только тогда, когда $f|_L \neq \text{const}$;*

(ii) *неуравновешенной веса w тогда и только тогда, когда $f|_L$ — константа, причем $w = 2^{n-1} \pm 2^{n-h-1}$, где $\dim L = n - 2h$;*

(iii) *платовидной порядка $2h$;*

(iv) *корреляционно-иммунной порядка k, если и только если смежный класс $z + L^\perp$ не содержит векторов веса w, $1 \leqslant w \leqslant k$;*

(v) *уравновешенной корреляционно-иммунной порядка k, если и только если класс $z + L^\perp$ не содержит векторов веса не больше k;*

(vi) *удовлетворяет критерию распространения $PC(k)$ тогда и только тогда, когда L не содержит векторов веса w, $1 \leqslant w \leqslant k$.*

Отметим, что частично бент-функциями являются все аффинные, квадратичные и бент-функции. Справедлива [69]

Теорема 49. *Пусть f — частично бент-функция,* $\dim L = n - 2h$. *Тогда* $N_f = 2^{n-1} - 2^{n-h-1}$, $W_f(x) = \begin{cases} \pm 2^{n-h}, & \text{если } x \in z + L^{\perp}; \\ 0, & \text{иначе.} \end{cases}$

Очевидно, что чем меньше размерность подпространства L, тем выше нелинейность частично бент-функции.

См. далее на эту тему работы [78, 201].

2.3.3 Гипербент-функции

А. М. Йоссеф и Г. Гонг [205] в 2001 году ввели понятие гипербент-функции[2]. Их работе предшествовала статья С. В. Голомба и Г. Гонга [118] 1999 года, в которой алгоритм шифрования DES рассматривался как регистр сдвига с нелинейными обратными связями и проводился анализ его S-блоков. При таком подходе авторы [118] предложили использовать для приближения координатных функций S-блоков вместо линейных булевых функций собственные мономиальные функции. Эта идея и была развита в [205].

Булеву функцию от n переменных можно рассматривать как функцию из $\mathbb{F}_{2^n}$ в $\mathbb{F}_2$, сопоставляя каждому вектору x соответствующий элемент поля $\mathbb{F}_{2^n}$. Известно, что любая линейная функция $\langle x, y \rangle$ может быть представлена как $Tr(a_x y)$ для подходящего элемента $a_x \in \mathbb{F}_{2^n}$, где $Tr : \mathbb{F}_{2^n} \to \mathbb{F}_2$ — функция следа. Тогда преобразование Уолша—Адамара приобретает следующий, эквивалентный, вид $W_f(y) = \sum\limits_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(yx)+f(x)}$. Функция вида $Tr(a_x y^s)$, где целое число s такое, что $1 \leqslant s \leqslant 2^n - 1$ и $\gcd(s, 2^n - 1) = 1$, называется *собственной мономиальной функцией. Расширенное преобразование Уолша—Адамара* булевой функции f имеет вид

$$W_{f,s}(y) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(yx^s)+f(x)}.$$

Определение 14. (Йоссеф, Гонг, 2001) Булева функция f называется *гипербент-функцией*, если для любого $y \in \mathbb{F}_{2^n}$ и любого целого s,

[2] До этого термин *гипербент-функция* однажды использовался в работе [72] для обозначения другого класса функций, но больше в этом значении он не употребляется.

$\gcd(s, 2^n - 1) = 1$, выполняется $|W_{f,s}(y)| = 2^{n/2}$.

Другими словами, гипербент-функция одинаково плохо приближается всеми собственными мономиальными функциями, ее обобщенная нелинейность

$$NLG(f) = 2^{n-1} - \frac{1}{2} \max_{\substack{y,\, s \\ \gcd(s, 2^n - 1) = 1}} |W_{f,s}(y)|$$

максимальна, т. е. равна $2^{n-1} - 2^{(n/2)-1}$. Авторы [205] для каждого четного n доказали существование гипербент-функций, предложили их векторный вариант, для малого числа переменных рассмотрели уравновешенные гипербент-функции. В 2006 году К. Карле и П. Габори [85] и независимо А. С. Кузьмин, В. Т. Марков, А. А. Нечаев и А. Б. Шишков [12] показали, что степень нелинейности любой гипербент-функции от n переменных равна $n/2$.

А. С. Кузьмин и др. [14, 13] обобщили понятие гипербент-функции: от булевых функций они перешли к функциям над произвольным конечным полем характеристики 2.

А именно, пусть $q = 2^\ell$. В работе [13] рассматривается задача приближения произвольной функции из $\mathbb{F}_q^n$ в $\mathbb{F}_q$ (как и выше она отождествляется с функцией $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$) функциями из некоторого ограниченного класса $\mathcal{A}$. Для оценки эффективности приближения функции f функцией $g \in \mathcal{A}$, вводится параметр *согласие* $\nabla(f, g)$, связанный с функцией близости В. И. Солодовникова, см. (2.4), соотношением $\nabla(f, g) = \frac{q}{\sqrt{q-1}}\delta(f, g)$, если конечные группы выбирать как $A = (\mathbb{F}_{q^n}, +)$ и $B = (\mathbb{F}_q, +)$. Этот параметр представляется более естественным, поскольку $0 \leqslant \nabla(f, g) \leqslant 1$ и при крайних значениях 0 и 1 функции f и g отличаются, соответственно, на уравновешенную функцию и на константу. При $q = 2$ справедливо

$$\left| \mathbf{P}(f = g) - \frac{1}{2} \right| = \frac{\nabla(f, g)}{2}.$$

Т. е., чем меньше согласие между функциями, тем ниже эффективность замены одной на другую. Пусть $\nabla(f, \mathcal{A}) = \max_{g \in \mathcal{A}} \nabla(f, g)$ — *эффективность*

аппроксимации функции f функциями из $\mathcal{A}$. Тогда

• Если $\mathcal{A} = \mathrm{Hom}(A, B)$ — класс всех гомоморфизмов из A в B, то функция $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ такая, что параметр $\nabla(f, \mathrm{Hom}(A, B))$ принимает минимальное возможное значение $q^{-n/2}$, является бент-функцией в смысле определения 5.

• Пусть $\mathcal{A} = \mathcal{M}$ — класс всех собственных обобщенных мономиальных функций, т. е. функций вида $g(x) = h(x^s)$, где $h \in \mathrm{Hom}(A, B)$, s — целое, $\gcd(s, q^n - 1) = 1$.

Определение 15. (Кузьмин и др., 2007) Функция $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ называется *гипербент-функцией*, если параметр $\nabla(f, \mathcal{M})$ принимает минимальное возможное значение $q^{-n/2}$.

При $q = 2$ это определение совпадает с определением 14.

В [14] проведено детальное исследование таких обобщенных гипербент-функций. Приведем здесь лишь одну конструкцию таких функций. Мультипликативная группа поля $\mathbb{F}_{q^n}$ есть прямое произведение $(\mathbb{F}_{q^{n/2}}, \cdot)$ на циклическую группу V порядка $q^{n/2}+1$. Для $a, d \in \mathbb{F}_q$ пусть $z_{a,d}$ равно единице (нулю), если элементы a и d равны (не равны) соответственно.

Теорема 50. *Пусть задана функция $g : V \to \mathbb{F}_q$ такая, что найдется элемент $d \in \mathbb{F}_q$, при котором число решений уравнения $g(x) = a$ в множестве V равно $q^{(n/2)-1} + z_{a,d}$, где $a \in \mathbb{F}_q$. Тогда функция $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ такая, что $f(0) = d$, $f(x) = g(x^{q^{n/2}-1})$ при $x \neq 0$, является гипербент-функцией.*

См. далее на эту тему работы [206, 15]. Мономиальные приближения булевых функций также изучались А. В. Ивановым [6, 7]. Например, им было показано [8], что свойство бент-функции быть гипербент-функцией, вообще говоря, зависит от выбора базиса, при котором рассматривается ее приведенное представление.

2.3.4 Почти бент-функции

Бент-функции существуют только для четного числа переменных. При нечетном n одним из их аналогов можно считать почти бент-функции, обладающие достаточно высокой нелинейностью.

Определение 16. Булева функция f от n переменных называется *почти бент-функцией*, если каждый ее коэффициент Уолша—Адамара равен либо нулю, либо $\pm 2^{(n+1)/2}$.

Почти бент-функции есть ничто иное как платовидные функции максимального порядка $n-1$ от нечетного числа переменных, см. определение 9. Не будем рассматривать их подробно. Отметим лишь, что булевы функции, имеющие три различных значения в спектре Уолша—Адамара, интересны для обеспечения защиты от так называемой soft output joint attack на генераторы псевдошумовых последовательностей (PN-generators), см. [150]. Такие генераторы используются в уже упоминавшемся выше стандарте IS–95 технологии CDMA. Почти бент-функции используются также для построения криптографически стойких S-блоков [105].

См. о почти бент-функциях работы [108, 149].

2.3.5 Бент-функции более высокого порядка нелинейности

Это довольно естественное направление, тесно связанное с нелинейными обобщениями различных методов криптоанализа.

Известно, что эффективность приближения бент-функции любой линейной функцией является самой низкой. Расширяя класс линейных функций, естественно рассматривать для приближения булевы функции степени не выше r, где $2 \leqslant r \leqslant n-1$. При этом возникает понятие *нелинейности r-го порядка* $N_r(f)$ булевой функции f как расстояния Хэмминга от f до всех таких функций.

Определение 17. Булева функция, удаленная от всех функций степени не выше r на максимальное расстояние, называется *бент-функцией*

порядка r.

Но трудность заключается в определении этого максимального возможного значения для $N_r(f)$. При $r \geqslant 2$ это нерешенная задача, более известная в теории кодирования как определение радиуса покрытия кода Рида—Маллера порядка r. Известны пока некоторые оценки для $N_r(f)$, его асимптотическое значение, связь с другими криптографическими параметрами и т. п. Подробнее на эту тему см. обзор К. Карле [77] 2008 года.

2.3.6 k-Бент-функции

В 2007 году автором было введено следующее понятие, см. [29], основной идеей которого было рассмотрение аппроксимирующих функций, отличных от линейных, но являющихся в какой-то степени их аналогами.

Пусть x, y — двоичные векторы длины n. Пусть k — любое целое число, такое что $1 \leqslant k \leqslant n/2$. Определим бинарную операцию

$$\langle x, y\rangle_k = \Big(\sum_{i=1}^{k}\sum_{j=i}^{k}(x_{2i-1}+x_{2i})(x_{2j-1}+x_{2j})(y_{2i-1}+y_{2i})(y_{2j-1}+y_{2j})\Big) + \langle x, y\rangle,$$

которая служит нелинейным аналогом скалярного произведения. Заметим, что компоненты векторов неравноправны в этой операции: $2k$ первых компонент каждого из них входят в квадратичные и линейные слагаемые; остальные — только в линейные.

Функция

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

называется *k-преобразованием Уолша—Адамара* булевой функции f. При $k = 1$ имеем эквивалентную запись обычного преобразования Уолша—Адамара. Справедливо равенство Парсеваля,

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

Функция f называется *k-бент-функцией при фиксированном порядке переменных*, если все ее коэффициенты $W_f^{(j)}(y)$, $j = 1, \ldots, k$ равны $\pm 2^{n/2}$.

Такие функции рассматривались в [29]. Однако, их недостатком являлась зависимость от порядка переменных функции. Приведем более общее определение, избавленное от этого недостатка.

Определение 18. Булева функция f от n переменных называется *k-бент-функцией*, если для произвольной подстановки $\pi \in S_n$, любого $j = 1, \ldots, k$ и любого вектора y выполняется $W^{(j)}_{f\circ\pi}(y) = \pm 2^{n/2}$.

Поясним смысл определения. Рассмотрим множества функций

$$\mathfrak{A}^k_n(\pi) = \{\ \langle \pi(x), y\rangle_k + a \,|\, y \in \mathbb{Z}_2^n, a \in \mathbb{Z}_2\ \}$$

от n переменных. Векторы значений функций из каждого класса $\mathfrak{A}^k_n(\pi)$ образуют двоичный код Адамара. Этот код является нелинейным (при $k > 1$), но у него существует линейный прообраз в пространстве $\mathbb{Z}_4^n$ относительно некоторого простого отображения, см. подробнее [29]. Поэтому функции из $\mathfrak{A}^k_n(\pi)$ можно считать аналогами аффинных функций. Заметим, что они являются квадратичными. *k-Нелинейностью* булевой функции f называется минимальное расстояние Хэмминга $N^{(k)}_f$ от нее до множества всех функций вида $\langle \pi(x), y\rangle_k + a$, где π — любая перестановка. Справедливо равенство

$$N^{(k)}_f = 2^{n-1} - \frac{1}{2} \max_{\pi\in S_n} \max_{y\in\mathbb{Z}_2^n} |W^{(k)}_{f\circ\pi}(y)|.$$

Таким образом, k-бент-функция — это функция, для которой $N^{(j)}_f$ максимально, $N^{(j)}_f = 2^{n-1} - 2^{(n/2)-1}$, при любом $j = 1, \ldots, k$, т. е. она одновременно максимально удалена от всех классов функций $\mathfrak{A}^j_n(\pi)$, $\pi \in S_n$, $j = 1, \ldots, k$. Заметим, что 1-бент-функции совпадают с обычными бент-функциями. С ростом k нелинейные свойства функций усиливаются, поэтому наиболее интересной задачей представляется описание класса всех $(n/2)$-бент-функций. Как следует из [29], этот класс не пуст, при любом четном n ему принадлежат, например, все симметричные бент-функции: $f(x) = \sum_{i=1}^n \sum_{j=i+1}^n x_i x_j$, $f(x) + 1$, $f(x) + \sum_{i=1}^n x_i$, $f(x) + \sum_{i=1}^n x_i + 1$, характеризация которых приводится в [187].

При $n = 4$ все $(n/2)$-бент-функции были описаны в работе [31]. Это 128 квадратичных функций с квадратичной частью одного из четырех видов: $x_1x_2 + x_3x_4$, $x_1x_3 + x_2x_4$, $x_1x_4 + x_2x_3$, $x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$ и произвольной линейной частью. См. также на эту тему [30].

Подробнее k-бент-функции рассматриваются в Главе 4.

2.4 Квантовые обобщения бент-функций

2.4.1 Нега-бент-функции, бент$_4$-функции, I-бент-функции

Бент-функцию часто определяют как функцию, имеющую *плоский* спектр относительно преобразования Уолша—Адамара. Плоский — означает, что модули всех коэффициентов Уолша—Адамара равны. В 2006 году К. Риера и М. Паркер [181] стали исследовать булевы функции, имеющие плоские спектры относительно множества унитарных преобразований специального вида. Напомним, что преобразование пространства $\mathbf{C}^n$, заданное квадратной матрицей A, *унитарно*, если $A\bar{A}^T = E$, где E — единичная матрица. Выбранные преобразования используются при анализе стабилизаторов квантовых состояний [181]. Пусть

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}.$$

Для любой 2×2-матрицы A пусть $A_j = I \otimes \ldots \otimes I \otimes A \otimes I \otimes \ldots \otimes I$ — тензорное (Кронекерово) произведение n матриц, где A встречается на j-ом месте. Рассмотрим следующие множества преобразований:

✓ $\{H\}^n$ — состоящее из одного преобразования $U = \prod_{j=0}^{n-1} H_j$. Если $F = (-1)^f$ — функция *знака* булевой функции f от n переменных, то вектор спектральных значений f относительно преобразования U определяется как $\widehat{F} = UF$. Тогда f — *бент-функция* (в обычном смысле), если ее спектр относительно U — плоский, т. е. каждая компонента $\widehat{F}$ равна ± 1.

✓ $\{N\}^n$ — состоящее из преобразования $U = \prod_{j=0}^{n-1} N_j$.

Определение 19. (Риера, Паркер, 2006) Булева функция с плоским спектром относительно U называется *нега-бент-функцией*.

Отметим, что поскольку U — комплексная матрица, при определении спектра функции здесь возникают свои особенности, см. [172]. Любая аффинная булева функция является нега-бент. М. Паркер (2000, 2007) и А. Потт (2007) изучали нега-бент-функции в работах [171] и [172]. В последней работе исследовался вопрос о пересечении классов бент- и нега-бент-функций, полностью разрешенный для квадратичных функций.

✓ $\{H, N\}^n$ — состоящее из 2^n преобразований вида $\prod\limits_{j\in R_H} H_j \prod\limits_{j\in R_N} N_j$, где R_H и R_N разбивают множество $\{0, 1, \ldots, n-1\}$. Булева функция f от n переменных является *бент$_4$-функцией*, если существует хотя бы одно разбиение R_H, R_N, относительно которого f имеет плоский спектр.

✓ $\{I, H\}^n$ — состоящее из 2^n преобразований вида $\prod\limits_{j\in R_I} I_j \prod\limits_{j\in R_H} H_j$, где R_I и R_H разбивают множество $\{0, 1, \ldots, n-1\}$. Аналогично предыдущему случаю функция f является *I-бент-функцией*, если существует хотя бы одно разбиение R_I, R_H, где $|R_I| < n$, относительно которого спектр f — плоский.

✓ $\{I, H, N\}^n$ — состоящее из 3^n преобразований $\prod\limits_{j\in R_I} I_j \prod\limits_{j\in R_H} H_j \prod\limits_{j\in R_N} N_j$, где R_I, R_H и R_N разбивают $\{0, 1, \ldots, n-1\}$. В этом случае определяются так называемые *I-бент$_4$-функции*, не представляющие, однако, особого интереса, так как этому классу принадлежит любая булева функция.

К. Риера и М. Паркер [181] развивают квантовый мотив своих исследований, изучают свойства бент-функций нового типа и их связь с графами.

Глава 3

Группа автоморфизмов множества бент-функций

Одним из открытых вопросов в области бент-функций долгое время оставался вопрос о группе автоморфизмов множества этих функций. В данной главе дается ответ на этот вопрос.

Пусть A — невырожденная двоичная $n \times n$–матрица, пусть b и c — двоичные векторы длины n, и d — константа. Известно, что любое отображение вида $g(x) \to g(Ax \oplus b) \oplus \langle c, x \rangle \oplus d$, заданное на множестве булевых функций от n переменных, оставляет класс бент-функций на месте. Существуют ли другие изометричные отображения множества булевых функций в себя, оставляющие неподвижным класс бент-функций? Мы покажем, что других таких отображений нет.

Рассмотрим структуру главы. Основная ее часть посвящена доказательству того, что для любой неаффинной функции f найдется такая бент-функция g, что функция $f \oplus g$ не является бент-функцией (теорема 51). Другими словами, множество бент-функций замкнуто относительно прибавления только аффинных булевых функций. Из этого факта будет следовать, что аффинные функции — это в точности все те булевы функции, которые удалены от класса бент-функций на максимально возможное расстояние. Т. е. существует в некотором смысле «дуальность» между определениями бент-функций и аффинных функций. Далее устанавливается, что

множество бент-функций и множество аффинных функций имеют одинаковые группы автоморфизмов. Этой общей группой является полупрямое произведение полной аффинной группы $GA(n)$ на $\mathbb{Z}_2^{n+1}$ (теорема 52).

3.1 Определения и факты

Напомним некоторые определения и обозначения. Пусть $\langle x, y\rangle$ обозначает обычное скалярное произведение двоичных векторов $x, y \in \mathbb{Z}_2^n$ по модулю 2. *Расстоянием Хэмминга* $d(x, y)$ между векторами x и y называется число координат, в которых они различаются.

Под *расстоянием* $dist(f, g)$ между булевыми функциями f и g будем понимать расстояние между их векторами значений. Через $supp(f)$ обозначим *носитель* функции f, т. е. множество тех векторов, на которых f равна единице. Известно, что каждая булева функция f может быть представлена в *алгебраической нормальной форме*, степень которой обозначим через $deg(f)$. Булевы функции степени 1 называются *аффинными* и имеют вид $\langle c, x\rangle \oplus d$ для подходящего вектора c и константы d. Множество всех аффинных функций от n переменных обозначим через $\mathcal{A}_n$.

Преобразованием Уолша—Адамара булевой функции f от n переменных называется целочисленная функция $W_f(y) = \sum_x (-1)^{\langle x,y\rangle \oplus f(x)}$. *Бент-функцией* называется булева функция от n переменных (n четно) такая, что модуль каждого коэффициента Уолша—Адамара $W_f(y)$ этой функции равен $2^{n/2}$. *Производной булевой функции f по направлению y* называется функция $f(x) \oplus f(x \oplus y)$. Заметим, что булева функция f аффинна тогда и только тогда, когда ее производная по любому направлению является константой.

Эквивалентно, бент-функции могут быть определены следующим образом [19]. Напомним, что этот факт не что иное как пункт (iv) теоремы 1 из Главы 1.

Утверждение 1. *Булева функция g является бент-функцией, тогда*

и только тогда, когда ее производная по любому ненулевому направлению y уравновешена, т. е. выполняется $\sum_x (-1)^{g(x)\oplus g(x\oplus y)} = 0$.

Множество всех бент-функций от n переменных обозначим через $\mathcal{B}_n$. Хорошо известно следующее свойство бент-функций (см. теорему 4).

Утверждение 2. *Пусть A — невырожденная двоичная $n\times n$–матрица, b и c — двоичные векторы, d — константа. Любое отображение вида $g(x) \to g(Ax \oplus b) \oplus \langle c, x\rangle \oplus d$, заданное на множестве булевых функций от n переменных, оставляет класс бент-функций на месте.*

Нам потребуется конструкция МакФарланда [157], см. теорему 16, которую приведем здесь еще раз.

Утверждение 3. *Функция $f(x', x'') = \langle x', \pi(x'')\rangle \oplus h(x'')$ является бент-функцией от n переменных, где π — любая перестановка на $\mathbb{Z}_2^{n/2}$ и булева функция h от $n/2$ переменных произвольна.*

Заметим, что разбиение переменных на две равные части x' и x'' может быть любым.

Рассмотрим векторы, у которых фиксированы значения некоторых $n - k$ координат, а значения остальных координат выбираются произвольно. Множество всех таких векторов называется *гранью размерности k* пространства $\mathbb{Z}_2^n$. Например, множество $\Gamma = \{\ (x', x'') : x'' = a\ \}$ является гранью размерности $n/2$, где $x', x'' \in \mathbb{Z}_2^{n/2}$.

3.2 О сдвигах класса бент-функций

Докажем следующий факт, из которого в качестве следствий и будут получены основные результаты главы.

Теорема 51. *Для любой неаффинной функции f найдется такая бент-функция g, что функция $f \oplus g$ не является бент-функцией.*

Доказательство. Предположим, что для некоторой фиксированной функции f такой, что $deg(f) \geqslant 2$, справедливо $f \oplus \mathcal{B}_n = \mathcal{B}_n$. Покажем, что это приведет к противоречию.

Идея доказательства состоит в следующем. Сначала покажем, что некоторая сумма должна быть равна нулю для любой бент-функции, см. далее сумму (3.1). Затем в классе МакФарланда найдем бент-функцию–контрпример g', для которой это равенство не будет выполняться. Бент-функция g' будет получена из специально выбранной бент-функции g инвертированием ее значений на некоторой грани Γ размерности $n/2$. Ключевым условием для возможности выбора такой грани является то, что для некоторого ненулевого y, множество $D = \mathrm{supp}(f(x) \oplus f(x \oplus y))$ будет собственным подмножеством пространства $\mathbb{Z}_2^n$, что возможно тогда и только тогда, когда f неаффинна.

Доказательство удобно разделить на несколько этапов.

Равенство для любой бент-функции. Поскольку $deg(f) \geqslant 2$, то найдется такой ненулевой вектор y, что производная функции f по направлению y не является константой. Можно считать, что $y = 1$. Действительно, так как если y — другой ненулевой вектор, то от функции f перейдем к функции $f'(x) = f(Ax)$, где $A \cdot 1 = y$. Очевидно, что производная функции f' по направлению 1 не константа, и так же как и для f, выполняется равенство $f' \oplus \mathcal{B}_n = \mathcal{B}_n$ (т. е. можно доказывать теорему для f'). Поэтому всюду далее считаем, что $y = 1$.

Пусть g — произвольная бент-функция. Тогда $f \oplus g$ — также бент-функция, и согласно утверждению 1 выполняются равенства

$$\sum_x (-1)^{g(x) \oplus g(x \oplus y)} = 0,$$

$$\sum_x (-1)^{g(x) \oplus f(x) \oplus g(x \oplus y) \oplus f(x \oplus y)} = 0.$$

Вычитая из первого равенства второе, получаем

$$\sum_x (-1)^{g(x) \oplus g(x \oplus y)} (1 - (-1)^{f(x) \oplus f(x \oplus y)}) = 0.$$

Обозначим через D множество $\mathrm{supp}(f(x) \oplus f(x \oplus y))$. Тогда для любой бент-функции g должно выполняться

$$\sum_{x \in D} (-1)^{g(x) \oplus g(x \oplus y)} = 0. \tag{3.1}$$

Выбор грани. Так как функция $f(x) \oplus f(x \oplus y)$ — не константа, то множество D не пусто и не совпадает со всем булевым кубом. Тогда существует $(n/2)$-мерная грань Γ такая, что она имеет непустое пересечение и с множеством D и с его дополнением $\mathbb{Z}_2^n \setminus D$, т. е. выполняется

$$0 < m < |\Gamma| = 2^{n/2}, \tag{3.2}$$

где $m = |\Gamma \cap D|$. Действительно, такую грань всегда можно построить, например, через любой вектор $u \notin D$ и один из векторов v или $v \oplus y$, где $v \in D$, так как либо расстояние $d(u, v)$ либо $d(u, v \oplus y)$ окажется не превосходящим $n/2$.

Заметим, что грань $\Gamma \oplus y$ также имеет пересечение мощности m с множеством D, поскольку, как нетрудно заметить, $D \oplus y = D$. Отметим также, что грани Γ и $\Gamma \oplus y$ не пересекаются (в силу выбора $y = 1$). Имеет место следующее разбиение множества D:

$$D = \Big(\Gamma \cap D\Big) \cup \Big((\Gamma \oplus y) \cap D\Big) \cup \Big(D \setminus (\Gamma \cup (\Gamma \oplus y))\Big), \tag{3.3}$$

которое потребуется нам в дальнейшем.

Без ограничения общности считаем, что грань Γ имеет вид

$$\Gamma = \{(x', x'') : x'' = a\} \text{ для некоторого вектора } a \in \mathbb{Z}_2^{n/2}$$

(в случае, если фиксированные координаты грани расположены иначе, доказательство проводится аналогично). Пусть множество $\Gamma \cap D$ представляется в виде

$$\Gamma \cap D = \{(b^{(1)}, a), (b^{(2)}, a), \ldots, (b^{(m)}, a)\},$$

для подходящих векторов $b^{(1)}, b^{(2)}, \ldots, b^{(m)}$ длины $n/2$.

Специальное подмножество бент-функций. Рассмотрим подмножество G бент-функций вида $g(x', x'') = \langle x', \pi(x'')\rangle$ из класса МакФарланда таких, что перестановки π являются линейными преобразованиями пространства, т. е. каждая π определяется как $\pi(x'') = Ax''$, для подходящей невырожденной матрицы A. Покажем, что в классе G найдется такая бент-функция g, что сумма

$$S = \sum_{x \in \Gamma \cap D} (-1)^{g(x) \oplus g(x \oplus y)}$$

будет не равна нулю. Действительно, распишем эту сумму, подставляя вид произвольной функции из G. Поскольку $\pi(x'' \oplus y'') = A(x'' \oplus y'') = Ax'' \oplus Ay''$, где $y = (y', y'')$, имеем

$$g(x) \oplus g(x \oplus y) = \langle x', Ax''\rangle \oplus \langle x' \oplus y', Ax'' \oplus Ay''\rangle =$$

$$\langle x', Ay''\rangle \oplus \langle y', Ax'' \oplus Ay''\rangle.$$

Тогда, подставляя в сумму S, получаем

$$S = (-1)^{\gamma} \sum_{i=1}^{m} (-1)^{\langle b^{(i)}, Ay''\rangle},$$

где $\gamma = \langle y', Aa \oplus Ay''\rangle$ — константа, зависящая от конкретного выбора матрицы A. Поскольку y'' — ненулевой вектор (по нашему выбору $y'' = 1$), и матрица A может быть любой невырожденной матрицей, то вектор $z = Ay''$ также может быть произвольным ненулевым вектором длины $n/2$. Таким образом, наша задача — показать, что найдется такой ненулевой вектор z, что не равна нулю сумма

$$\sum_{i=1}^{m} (-1)^{\langle b^{(i)}, z\rangle}. \tag{3.4}$$

Поиск вектора z. Предположим обратное. Пусть для каждого ненулевого вектора z сумма (3.4) равна нулю. Рассмотрим двоичную матрицу M размера $(n/2) \times m$, столбцами которой являются все векторы $b^{(1)}, \ldots, b^{(m)}$. Тогда сумма (3.4) есть ни что иное как разность между числом нулей и

числом единиц в линейной комбинации строк матрицы M, определяемой вектором z (строка i входит в комбинацию, если $z_i = 1$). По предположению, матрица M должна удовлетворять условию: *любая ненулевая линейная комбинация строк матрицы M содержит одинаковое число нулей и единиц.* Несложно понять, что с точностью до перестановки столбцов, эта матрица должна иметь вид

$$\begin{pmatrix} \underbrace{0\ldots0}_{m/8} & \underbrace{0\ldots0}_{m/8} & \underbrace{0\ldots0}_{m/8} & \underbrace{0\ldots0}_{m/8} & \underbrace{1\ldots1}_{m/8} & \underbrace{1\ldots1}_{m/8} & \underbrace{1\ldots1}_{m/8} & \underbrace{1\ldots1}_{m/8} \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix}$$

Отсюда сразу замечаем, что число столбцов матрицы должно быть не меньше чем $2^{n/2}$, где $n/2$ — число строк. Таким образом, для существования такой матрицы M необходимо, чтобы выполнялось $m \geqslant 2^{n/2}$. Но это противоречит условию на выбор грани Γ, а именно неравенству (3.2). Следовательно, всегда найдется вектор z такой, что сумма (3.4) не равна нулю. Зафиксируем этот вектор z.

Построение функции–контрпримера. Пусть A — невырожденная матрица такая, что $Ay'' = z$, пусть перестановка π определяется равенством $\pi(x'') = Ax''$. Из условия выбора вектора z следует, что для функции $g(x', x'') = \langle x', \pi(x'')\rangle$ справедливо

$$S = \sum_{x \in \Gamma \cap D} (-1)^{g(x) \oplus g(x \oplus y)} \neq 0. \tag{3.5}$$

Определим новую бент-функцию g', отличающуюся от g лишь на грани Γ. Далее мы увидим, что функции $f \oplus g$ и $f \oplus g'$ не могут одновременно быть бент-функциями, что и приведет к противоречию с основным предположением. Итак, пусть $g'(x', x'') = g(x', x'') \oplus h(x'')$, где

$$h(x'') = \begin{cases} 1, & \text{если } x'' = a; \\ 0, & \text{иначе.} \end{cases}$$

Другими словами, g' получена из функции g инвертированием ее значений на грани Г. Так как g из класса МакФарланда, то функция g' тоже бент-функция. Заметим, что тогда в силу разбиения (3.3) имеем

$$\sum_{x\in D}(-1)^{g'(x)\oplus g'(x\oplus y)} = \Big(\sum_{x\in \Gamma\cap D}(-1)^{g(x)\oplus 1\oplus g(x\oplus y)\oplus 0}\Big)+$$

$$\Big(\sum_{x\in(\Gamma\oplus y)\cap D}(-1)^{g(x)\oplus 0\oplus g(x\oplus y)\oplus 1}\Big)+\Big(\sum_{x\in(D\setminus(\Gamma\cup(\Gamma\oplus y))}(-1)^{g(x)\oplus g(x\oplus y)}\Big)=$$

$$\Big(\sum_{x\in(D\setminus(\Gamma\cup(\Gamma\oplus y))}(-1)^{g(x)\oplus g(x\oplus y)}\Big)-2S.$$

Таким образом,

$$\sum_{x\in D}(-1)^{g'(x)\oplus g'(x\oplus y)} = \sum_{x\in D}(-1)^{g(x)\oplus g(x\oplus y)} - 4S.$$

Отсюда из равенства (3.1) и неравенства (3.5) следует, что

$$\sum_{x\in D}(-1)^{g'(x)\oplus g'(x\oplus y)} \neq 0.$$

Но равенство (3.1) должно выполняться для любой бент-функции, в том числе и для g'. Полученное противоречие доказывает теорему. □

3.3 Дуальность определений бент-функций и аффинных функций

При четном n класс бент-функций $\mathcal{B}_n$ можно определить как множество функций, отстоящих от класса всех аффинных булевых функций $\mathcal{A}_n$ на максимально возможное расстояние $N_{\max}$, т. е.

$$\mathcal{B}_n = \{g : dist(g, \mathcal{A}_n) = N_{\max}\}.$$

При этом известно, что $N_{\max} = 2^{n-1} - 2^{(n/2)-1}$. Но можно ли *обратить* это определение? Другими словами, верно ли, что $\mathcal{A}_n$ — это множество всех булевых функций, отстоящих от класса $\mathcal{B}_n$ на максимально возможное расстояние $N'_{\max}$? Пусть

$$\mathcal{A}'_n = \{f : dist(f, \mathcal{B}_n) = N'_{\max}\}.$$

Покажем, что подобное *обращение* определений действительно возможно, т. е. справедливо $N_{\max} = N'_{\max}$ и $\mathcal{A}_n = \mathcal{A}'_n$.

Утверждение 4. *Справедливо* $N'_{\max} = 2^{n-1} - 2^{(n/2)-1}$.

Доказательство. По определению $N'_{\max} = \max_f \min_{g \in \mathcal{B}_n} dist(f, g)$. Заметим, что $dist(f, g) = 2^{n-1} - \frac{1}{2} W_{f \oplus g}(0)$. Поэтому

$$N'_{\max} = 2^{n-1} - \frac{1}{2} \min_f \max_{g \in \mathcal{B}_n} |W_{f \oplus g}(0)|.$$

Зафиксируем любую бент-функцию g' от n переменных. Поскольку класс $\mathcal{B}_n$ замкнут относительно добавления аффинных функций, то каждая функция вида $g' \oplus \ell_a$, где $\ell_a(x) = \langle a, x \rangle$, является бент-функцией. Заметим, что $W_{f \oplus g' \oplus \ell_a}(0) = W_{f \oplus g'}(a)$. Тогда, очевидно

$$\max_{g \in \mathcal{B}_n} |W_{f \oplus g}(0)| \geqslant \max_{\substack{g \in \mathcal{B}_n,\, g = g' \oplus \ell_a \\ \text{для некоторого } a}} |W_{f \oplus g}(0)| = \max_a |W_{f \oplus g'}(a)|.$$

Но из равенства Парсеваля для булевой функции $f \oplus g'$ следует, что

$$\max_a |W_{f \oplus g'}(a)| \geqslant 2^{n/2}.$$

Отсюда получаем $N'_{\max} \leqslant 2^{n-1} - 2^{(n/2)-1}$. С другой стороны, расстояние $2^{n-1} - 2^{(n/2)-1}$ до класса бент-функций достигается, например, для любой аффинной функции f. Утверждение доказано. $\square$

Утверждение 5. *Выполняется* $\mathcal{A}_n = \mathcal{A}'_n$.

Доказательство. Очевидно, что $\mathcal{A}_n \subseteq \mathcal{A}'_n$. Предположим, что существует функция $f \in \mathcal{A}'_n \setminus \mathcal{A}_n$. Тогда по теореме 51 найдется бент-функция g такая, что $f \oplus g$ не является бент-функцией. Т. е. существует вектор a такой, что $|W_{f\oplus g}(a)| > 2^{n/2}$. Рассмотрим бент-функцию $g'(x) = g(x) \oplus \langle a, x\rangle$. Для нее справедливо $W_{f\oplus g'}(0) = W_{f\oplus g}(a)$ и в силу равенства $dist(f, \mathcal{B}_n) = 2^{n-1} - \frac{1}{2}\max_{g\in\mathcal{B}_n} |W_{f\oplus g}(0)|$ заключаем, что $dist(f, \mathcal{B}_n) < N'_{\max}$, что противоречит выбору f. Таким образом, $\mathcal{A}_n = \mathcal{A}'_n$. □

Заметим, что ключевым фактом, позволившим установить «дуальность» между определениями аффинных функций и бент-функций является теорема 51.

3.4 Автоморфизмы бент-функций

Отображение φ множества всех булевых функций от n переменных в себя называется *изометричным*, если оно сохраняет расстояния между булевыми функциями, т. е. $dist(\varphi(f), \varphi(g)) = dist(f, g)$. Известно, что любое такое отображение однозначно представляется в виде

$$g(x) \to g(s(x)) \oplus f(x), \tag{3.6}$$

где $s : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ — любая подстановка, f — произвольная функция от n переменных.

Группой автоморфизмов подмножества булевых функций $\mathcal{M}$ называется группа изометричных отображений множества всех булевых функций в себя, оставляющих неподвижным множество $\mathcal{M}$. Обозначим эту группу через $Aut(\mathcal{M})$.

Напомним, что *полная аффинная группа* $GA(n)$ состоит из всех отображений вида $g(x) \to g(Ax \oplus b)$, где A — невырожденная матрица, b — произвольный вектор. Справедливо

Утверждение 6. *Группа $Aut(\mathcal{A}_n)$ равна полупрямому произведению полной аффинной группы $GA(n)$ на $\mathbb{Z}_2^{n+1}$.*

Действительно, для любого автоморфизма (3.6) сдвиг на функцию f может определяться только аффинной функцией (т. к. образ нулевой функции — также аффинная функция). Множество всех аффинных функций от n переменных образует группу, изоморфную $\mathbb{Z}_2^{n+1}$. Остается отметить, что каждая перестановка s, как известно, должна принадлежать группе $GA(n)$, см. например, [20].

Теорема 52. *Справедливо* $Aut(\mathcal{B}_n) = Aut(\mathcal{A}_n) = GA(n) \ltimes \mathbb{Z}_2^{n+1}$.

Доказательство. Очевидно, что $Aut(\mathcal{A}_n) \subseteq Aut(\mathcal{B}_n)$. Действительно, для любого отображения $\varphi \in Aut(\mathcal{A}_n)$ и любой бент-функции g имеем $dist(g, \mathcal{A}_n) = dist(\varphi(g), \varphi(\mathcal{A}_n)) = dist(\varphi(g), \mathcal{A}_n)$. А следовательно, любая бент-функция под действием φ переходит в некоторую другую бент-функцию.

Аналогично, $Aut(\mathcal{B}_n) \subseteq Aut(\mathcal{A}_n)$. А именно для любого автоморфизма $\psi \in Aut(\mathcal{B}_n)$ и любой аффинной функции f выполняется $dist(f, \mathcal{B}_n) = dist(\psi(f), \psi(\mathcal{B}_n)) = dist(\psi(f), \mathcal{B}_n)$. Отсюда согласно утверждениям 4 и 5 следует, что $\psi(\mathcal{A}_n) = \mathcal{A}_n$.

Получаем, что $Aut(\mathcal{B}_n) = Aut(\mathcal{A}_n)$. Из утверждения 6 следует конкретный вид этой группы. □

Таким образом, если отображение (3.6) переводит класс бент-функций в себя, то оно имеет вид $g(x) \to g(Ax \oplus b) \oplus \langle c, x \rangle \oplus d$. Напомним, что бент-функции, получающиеся одна из другой с помощью такого отображения называются *аффинно эквивалентными*. Из полученных результатов следует, что более общего подхода к эквивалентности бент-функций на основе изометричных отображений не существует.

Глава 4

Понятие k-бент-функции. Конструкции и свойства

Глава посвящена *k-бент-функциям* — новому обобщению бент-функций. Сначала рассматриваются нелинейные двоичные коды типа Адамара специального вида, на которых возможно задание групповой операции, согласованной с метрикой Хэмминга. Затем на основе этих кодов определяется бинарная операция на множестве всех двоичных векторов, обладающая многими свойствами скалярного произведения. Далее определяется k-преобразование Уолша—Адамара и с его помощью вводится понятие k-бент-функции.

4.1 Определения и обозначения

Введем понятия и обозначения, которые потребуются далее. Вектор длины m с компонентами из кольца $\mathbb{Z}_4$ будем называть *четверичным. Весом Ли* $wt_L(\cdot)$ четверичного вектора называется обычная сумма весов его компонент, где

$$wt_L(0) = 0,\ wt_L(1) = wt_L(3) = 1,\ wt_L(2) = 2.$$

Расстояние Ли $d_L(\mathbf{x}, \mathbf{y})$ между четверичными векторами $\mathbf{x}$ и $\mathbf{y}$ одинаковой длины определяется равенством $d_L(\mathbf{x}, \mathbf{y}) = wt_L(\mathbf{x} - \mathbf{y})$. Пусть $\langle \mathbb{Z}_4^n, d_L \rangle$ —

метрическое пространство на множестве всех четверичных векторов длины n с метрикой Ли. Знаком $+$ будем обозначать операцию сложения по модулю 4. Параметры четверичного кода обозначим через $(n, M, d)_4$. Через $\mathbf{0}, \mathbf{1}, \mathbf{2}$ и $\mathbf{3}$ обозначим векторы со всеми компонентами, равными $0, 1, 2$ и 3 соответственно. Пусть $\beta, \gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$ — следующие отображения:

c	$\beta(c)$	$\gamma(c)$
0	0	0
1	0	1
2	1	1
3	1	0

Пусть $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ — *отображение Грея*: $\varphi(c) = (\beta(c), \gamma(c))$ для $c \in \mathbb{Z}_4$. Отметим, что φ в отличие от β, γ взаимно однозначно. Отображения β, γ и φ покоординатно продолжаются до отображений $\beta, \gamma : \mathbb{Z}_4^i \to \mathbb{Z}_2^i$ и $\varphi : \mathbb{Z}_4^i \to \mathbb{Z}_2^{2i}$ для любого целого i. Напомним, что φ согласно [120] является изометрией, т. е. для любых $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_4^i$

$$d_L(\mathbf{x}, \mathbf{y}) = d_H(\varphi(\mathbf{x}), \varphi(\mathbf{y})).$$

Код длины n над $\mathbb{Z}_4$ называется *линейным*, если он является подгруппой группы $\mathbb{Z}_4^n$ (правильнее такой код было бы называть *групповым*). Двоичный код C называется $\mathbb{Z}_4$-*линейным*, если код $\varphi^{-1}(C)$ линеен.

4.2 Коды с параметрами кодов Адамара

В этом разделе определяются двоичные коды A_m^k типа Адамара с заданной на них групповой операцией.

Пусть m — натуральное, $n = 2^m$, k — фиксированное целое такое, что $0 \leqslant k \leqslant m/2$. Пусть $\mathbf{G}_m^k$ — четверичная матрица размера $(m-k) \times n$, состоящая из лексикографически упорядоченных столбцов $\mathbf{z}^T$, где $\mathbf{z} \in \mathbb{Z}_4^k \times (2\mathbb{Z}_4)^{m-2k}$. Например,

$$\mathbf{G}_1^0 = \begin{pmatrix} 02 \end{pmatrix}, \mathbf{G}_2^0 = \begin{pmatrix} 0022 \\ 0202 \end{pmatrix}, \mathbf{G}_2^1 = \begin{pmatrix} 0123 \end{pmatrix},$$

$$\mathbf{G}_3^0 = \begin{pmatrix} 00002222 \\ 00220022 \\ 02020202 \end{pmatrix}, \mathbf{G}_3^1 = \begin{pmatrix} 00112233 \\ 02020202 \end{pmatrix},$$

$$\boldsymbol{G}_4^1 = \begin{pmatrix} 0000111122223333 \\ 0022002200220022 \\ 0202020202020202 \end{pmatrix}, \mathbf{G}_4^2 = \begin{pmatrix} 0000111122223333 \\ 0123012301230123 \end{pmatrix}.$$

Матрицы такого вида впервые рассматривались Д. С. Кротовым в работах [10] и [139] для построения $\mathbb{Z}_4$-линейных кодов типа Адамара длины $2n$ и получения их полной классификации.

Определим отображение $\varphi_k : \mathbb{Z}_4^k \times \mathbb{Z}_2^{m-2k} \to \mathbb{Z}_2^m$ по правилу:

$$\varphi_k : (\mathbf{u}', \mathbf{u}'') \to (\varphi(\mathbf{u}'), \mathbf{u}'') \text{ для любых векторов } \mathbf{u}' \in \mathbb{Z}_4^k, \mathbf{u}'' \in \mathbb{Z}_2^{m-2k}.$$

Аналогично тому, как это сделано в [57], определим бинарную операцию

$$\star : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$$

следующим образом:

$$\mathbf{u} \star \mathbf{v} = \varphi_k(\varphi_k^{-1}(\mathbf{u}) \dot{+} \varphi_k^{-1}(\mathbf{v})) \text{ для любых векторов } \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m,$$

где $\dot{+}$ обозначает сложение над $\mathbb{Z}_4$ для первых k координат векторов $\varphi_k^{-1}(\mathbf{u})$, $\varphi_k^{-1}(\mathbf{v})$ и сложение над $\mathbb{Z}_2$ для оставшихся $m - 2k$ координат. Пусть четверичный вектор $\mathbf{h}^{\mathbf{u}}$ длины n определяется как

$$\mathbf{h}^{\mathbf{u}} = \varphi_k^{-1}(\mathbf{u}) \cdot \mathbf{G}_m^k. \tag{4.1}$$

Нетрудно заметить, что для любых векторов $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ справедливо

$$\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u} \star \mathbf{v}}. \tag{4.2}$$

Рассмотрим четверичную квадратную матрицу $\mathbf{C}_m^k = (c_{\mathbf{u},\mathbf{v}}^k)$, $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, порядка n, строками которой являются всевозможные векторы $\mathbf{h}^{\mathbf{u}}$, расположенные в порядке лексикографического возрастания векторов $\varphi_k^{-1}(\mathbf{u})$. Например,

$$\mathbf{C}_1^0 = \begin{pmatrix} 00 \\ 02 \end{pmatrix},\ \mathbf{C}_2^0 = \begin{pmatrix} 0000 \\ 0202 \\ 0022 \\ 0220 \end{pmatrix},\ \mathbf{C}_2^1 = \begin{pmatrix} 0000 \\ 0123 \\ 0202 \\ 0321 \end{pmatrix},$$

$$\mathbf{C}_3^0 = \begin{pmatrix} 00000000 \\ 02020202 \\ 00220022 \\ 02200220 \\ 00002222 \\ 02022020 \\ 00222200 \\ 02202002 \end{pmatrix},\ \mathbf{C}_3^1 = \begin{pmatrix} 00000000 \\ 02020202 \\ 00112233 \\ 02132031 \\ 00220022 \\ 02200220 \\ 00332211 \\ 02312013 \end{pmatrix}.$$

Считаем, что столбцы матрицы $\mathbf{C}_m^k$ также нумеруются векторами $\mathbf{v}$ в порядке лексикографического возрастания векторов $\varphi_k^{-1}(\mathbf{v})$. Например, векторы $\mathbf{u}$ для нумерации строк матриц $\mathbf{C}_4^1$ и $\mathbf{C}_4^2$ в нужном порядке приведены в таблицах 1 и 2. При этом каждому вектору $\mathbf{u}$ удобно сопоставлять целое число $\tilde{u} = 8u_1 + 4u_2 + 2u_3 + u_4$.

В таблицах 3 и 4 приведены матрицы $\mathbf{C}_4^1$ и $\mathbf{C}_4^2$ вместе с нумерацией их строк и столбцов.

Пусть J_s — квадратная матрица порядка s (где s — любое натуральное число), состоящая из всех единиц. Для квадратных матриц $A = (a_{i,j})$ и B порядков p и q соответственно обозначим через $A \otimes B$ их кронекерово произведение

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1p}B \\ \dots & \dots & \dots \\ a_{p1}B & \dots & a_{pp}B \end{pmatrix}.$$

$\tilde{u}$	$\mathbf{u}$	$\varphi_1^{-1}(\mathbf{u})$
0	0000	000
1	0001	001
2	0010	010
3	0011	011
4	0100	100
5	0101	101
6	0110	110
7	0111	111
12	1100	200
13	1101	201
14	1110	210
15	1111	211
8	1000	300
9	1001	301
10	1010	310
11	1011	311

Таблица 1. Векторы для $\mathbf{C}_4^1$.

$\tilde{u}$	$\mathbf{u}$	$\varphi_2^{-1}(\mathbf{u})$
0	0000	00
1	0001	01
3	0011	02
2	0010	03
4	0100	10
5	0101	11
7	0111	12
6	0110	13
12	1100	20
13	1101	21
15	1111	22
14	1110	23
8	1000	30
9	1001	31
11	1011	32
10	1010	33

Таблица 2. Векторы для $\mathbf{C}_4^2$.

$c^1_{\mathbf{u},\mathbf{v}}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**12**	**13**	**14**	**15**	**8**	**9**	**10**	**11**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2
3	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0
4	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
5	0	2	0	2	1	3	1	3	2	0	2	0	3	1	3	1
6	0	0	2	2	1	1	3	3	2	2	0	0	3	3	1	1
7	0	2	2	0	1	3	3	1	2	0	0	2	3	1	1	3
12	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
13	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
14	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0
15	0	2	2	0	2	0	0	2	0	2	2	0	2	0	0	2
8	0	0	0	0	3	3	3	3	2	2	2	2	1	1	1	1
9	0	2	0	2	3	1	3	1	2	0	2	0	1	3	1	3
10	0	0	2	2	3	3	1	1	2	2	0	0	1	1	3	3
11	0	2	2	0	3	1	1	3	2	0	0	2	1	3	3	1

Таблица 3. Матрица $\mathbf{C}_4^1$.

$c^2_{\mathbf{u},\mathbf{v}}$	**0**	**1**	**3**	**2**	**4**	**5**	**7**	**6**	**12**	**13**	**15**	**14**	**8**	**9**	**11**	**10**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
3	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
2	0	3	2	1	0	3	2	1	0	3	2	1	0	3	2	1
4	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
5	0	1	2	3	1	2	3	0	2	3	0	1	3	0	1	2
7	0	2	0	2	1	3	1	3	2	0	2	0	3	1	3	1
6	0	3	2	1	1	0	3	2	2	1	0	3	3	2	1	0
12	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
13	0	1	2	3	2	3	0	1	0	1	2	3	2	3	0	1
15	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
14	0	3	2	1	2	1	0	3	0	3	2	1	2	1	0	3
8	0	0	0	0	3	3	3	3	2	2	2	2	1	1	1	1
9	0	1	2	3	3	0	1	2	2	3	0	1	1	2	3	0
11	0	2	0	2	3	1	3	1	2	0	2	0	1	3	1	3
10	0	3	2	1	3	2	1	0	2	1	0	3	1	0	3	2

Таблица 4. Матрица $\mathbf{C}_4^2$.

Далее будут использоваться следующие свойства матриц $\mathbf{C}_m^k$.

Утверждение 7. *При любых целых m, k таких, что $0 \leqslant k \leqslant m/2$, справедливы равенства*

(i) $\mathbf{C}^k_{m+1} = (\mathbf{C}^k_m \otimes J_2) + (J_n \otimes \mathbf{C}^0_1)$;

(ii) $\mathbf{C}^{k+1}_{m+2} = (J_4 \otimes \mathbf{C}^k_m) + (\mathbf{C}^1_2 \otimes J_n)$;

(iii) $(\mathbf{C}^k_m)^T = \mathbf{C}^k_m$.

Доказательство. Пусть $\mathbf{G}^k_m = (\mathbf{z}_1^T, \ldots, \mathbf{z}_n^T)$. Тогда матрица $\mathbf{G}^k_{m+1}$ имеет вид

$$\mathbf{G}^k_{m+1} = \begin{pmatrix} \mathbf{z}_1^T & \mathbf{z}_1^T & \ldots & \mathbf{z}_n^T & \mathbf{z}_n^T \\ 0 & 2 & \ldots & 0 & 2 \end{pmatrix}.$$

Пусть $\mathbf{h}^{\mathbf{u}} = (h_1, \ldots, h_n)$. По определению имеем $\mathbf{h}^{(\mathbf{u},a)} = \varphi_k^{-1}(\mathbf{u}, a) \cdot \mathbf{G}^k_{m+1}$. Используя определение отображения φ_k^{-1}, получаем $\mathbf{h}^{(\mathbf{u},a)} = (\varphi_k^{-1}(\mathbf{u}), a) \cdot \mathbf{G}^k_{m+1} = (h_1, h_1 + 2a, \ldots, h_n, h_n + 2a)$ для любого $a \in \mathbb{Z}_2$. Таким образом, чтобы получить матрицу $\mathbf{C}^k_{m+1}$, каждый элемент $c^k_{\mathbf{u},\mathbf{v}}$ матрицы $\mathbf{C}^k_m$ надо заменить на матрицу $\begin{pmatrix} c^k_{\mathbf{u},\mathbf{v}} & c^k_{\mathbf{u},\mathbf{v}} \\ c^k_{\mathbf{u},\mathbf{v}} & c^k_{\mathbf{u},\mathbf{v}} + 2 \end{pmatrix}$. Другими словами, имеем $\mathbf{C}^k_{m+1} = (\mathbf{C}^k_m \otimes J_2) + (J_n \otimes \mathbf{C}^0_1)$, т. е. справедливо (i).

Пусть $\delta = \varphi^{-1}(a, b)$ для $a, b \in \mathbb{Z}_2$. Непосредственно из вида матрицы

$$\mathbf{G}^{k+1}_{m+2} = \begin{pmatrix} 0 \ldots 0 & 1 \ldots 1 & 2 \ldots 2 & 3 \ldots 3 \\ \mathbf{G}^k_m & \mathbf{G}^k_m & \mathbf{G}^k_m & \mathbf{G}^k_m \end{pmatrix}$$

следует, что $\mathbf{h}^{(a,b,\mathbf{u})} = (\delta, \varphi_k^{-1}(\mathbf{u})) \cdot \mathbf{G}^{k+1}_{m+1} = (\mathbf{h}^{\mathbf{u}}, \mathbf{h}^{\mathbf{u}} + \delta\mathbf{1}, \mathbf{h}^{\mathbf{u}} + \delta\mathbf{2}, \mathbf{h}^{\mathbf{u}} + \delta\mathbf{3})$, откуда получаем соотношение (ii).

Равенство (iii) следует из (i), (ii) и равенства $(A \otimes B)^T = A^T \otimes B^T$. $\square$

Пусть четверичный код $\mathcal{A}^k_m$ состоит из всех векторов $\mathbf{h}^{\mathbf{u}}$ и $\mathbf{h}^{\mathbf{u}} + \mathbf{2}$.

Утверждение 8 [139]**.** *Код $\mathcal{A}^k_m$ линеен и имеет параметры $(n, 2n, n)_4$.*

Определим следующие двоичные коды длин n и $2n$ соответственно:

$$A^k_m = \beta(\mathcal{A}^k_m), \quad H^k_m = \varphi(\mathcal{A}^k_m).$$

Несложно убедиться в том, что мощности этих кодов совпадают и равны $2n$. Код A_m^k можно определить также как $\gamma(\mathcal{A}_m^k)$. Отметим, что согласно [139] любой $\mathbb{Z}_4$-линейный код типа Адамара длины $2n$ эквивалентен одному из кодов $\varphi\left(\mathcal{A}_m^k \cup (\mathcal{A}_m^k + \mathbf{1})\right)$, где k пробегает значения $1, \ldots, \lfloor m/2 \rfloor$.

Ядром двоичного кода C, содержащего нулевой вектор, называется максимальный линейный подкод $\mathrm{Ker}(C)$ кода C такой, что $\mathbf{x} \oplus C = C$ для любого вектора $\mathbf{x} \in \mathrm{Ker}(C)$.

Утверждение 9 [139]**.** *Коды H_m^0 и H_m^1 линейны. При $k > 1$ справедливо равенство $|\mathrm{Ker}(H_m^k)| = 2^{m-k+1}$.*

Нетрудно установить следующий факт.

Утверждение 10. *При любом целом k, $0 \leqslant k \leqslant m/2$, справедливо равенство $\mathrm{Ker}(A_m^k) = \beta(\varphi^{-1}(\mathrm{Ker}(H_m^k)))$.*

Доказательство. Пусть $\varphi(\mathbf{x}) \in \mathrm{Ker}(H_m^k)$ для некоторого $\mathbf{x} \in \mathcal{A}_m^k$. Тогда $\varphi(\mathbf{x}) \oplus H_m^k = H_m^k$ и следовательно, $\beta(\mathbf{x}) \oplus A_m^k = A_m^k$. Отсюда следует, что $\mathrm{Ker}(A_m^k) \supseteq \beta(\varphi^{-1}(\mathrm{Ker}(H_m^k)))$.

Обратно, пусть $\beta(\mathbf{x}) \in \mathrm{Ker}(A_m^k)$ для некоторого $\mathbf{x} \in \mathcal{A}_m^k$. Сначала покажем, что вектор $\gamma(\mathbf{x})$ также принадлежит $\mathrm{Ker}(A_m^k)$. Действительно, из линейности четверичного кода $\mathcal{A}_m^k$ и равенства $\beta(2\mathbf{x} + \mathcal{A}_m^k) = \beta(2\mathbf{x}) \oplus \mathcal{A}_m^k$ следует, что $\beta(2\mathbf{x}) \in \mathrm{Ker}(A_m^k)$. В силу линейности двоичного подкода $\mathrm{Ker}(A_m^k)$ получаем $\gamma(\mathbf{x}) = \beta(\mathbf{x}) \oplus \beta(2\mathbf{x}) \in \mathrm{Ker}(A_m^k)$. Тогда из равенства $A_m^k = \beta(\mathcal{A}_m^k) = \gamma(\mathcal{A}_m^k)$ и того, что векторы $\beta(\mathbf{x}), \gamma(\mathbf{x})$ принадлежат множеству $\mathrm{Ker}(A_m^k)$, следует $\varphi(\mathbf{x}) \in \mathrm{Ker}(H_m^k)$ (для этого достаточно заметить, что если $\beta(\mathbf{x}) \oplus \beta(\mathbf{y}) = \beta(\mathbf{z})$ для некоторых векторов $\mathbf{y}, \mathbf{z}$, то справедливо также равенство $\gamma(\mathbf{x}) \oplus \gamma(\mathbf{y}) = \gamma(\mathbf{z})$). Таким образом, $\mathrm{Ker}(A_m^k) \subseteq \beta(\varphi^{-1}(\mathrm{Ker}(H_m^k)))$. Утверждение 10 доказано. □

Напомним, что двоичные коды C и C' длины n *эквивалентны*, если существуют вектор $\mathbf{x} \in \mathbb{Z}_2^n$ и подстановка τ на n элементах такие, что

выполняется $\mathbf{x} \oplus C = \tau(C')$, где $\tau(C') = \{\ \tau(\mathbf{y}) \mid \mathbf{y} \in C'\ \}$. Отметим, что на множестве A_m^k отображение β обратимо, что, вообще говоря, неверно для $\mathbb{Z}_2^n$. Поэтому из утверждений 9 и 10 следует, что коды $A_m^1, \ldots, A_m^{\lfloor m/2 \rfloor}$ попарно неэквивалентны.

На кодовых словах кода A_m^k определим бинарную операцию

$$\bullet : A_m^k \times A_m^k \to A_m^k,$$

согласованную с операцией $+$ на множестве $\mathcal{A}_m^k$. А именно пусть

$$\mathbf{x} \bullet \mathbf{y} = \beta(\beta^{-1}(\mathbf{x}) + \beta^{-1}(\mathbf{y})) \text{ для любых векторов } \mathbf{x}, \mathbf{y} \in A_m^k. \tag{4.3}$$

Нетрудно видеть, что $(A_m^k, \bullet)$ является абелевой группой. Через $\mathbf{x}^{-1}$ обозначим вектор, обратный вектору $\mathbf{x} \in A_m^k$ относительно операции $\bullet$. Имеет место равенство $\beta^{-1}(\mathbf{x}^{-1}) = -\beta^{-1}(\mathbf{x})$.

Приведем некоторые свойства, которыми обладает операция $\bullet$.

Утверждение 11. *Для любых* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in A_m^k$ *верны соотношения:*
(i) $wt_H(\mathbf{x}) = \frac{1}{2} wt_L(\beta^{-1}(\mathbf{x}))$;
(ii) $d_H(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} \bullet \mathbf{y}^{-1})$;
(iii) $d_H(\mathbf{x}, \mathbf{y}) = \frac{1}{2} d_L(\beta^{-1}(\mathbf{x}), \beta^{-1}(\mathbf{y}))$.

Доказательство. (i) Пусть $\mathbf{x}' = \beta^{-1}(\mathbf{x})$ — соответствующий кодовый вектор кода $\mathcal{A}_m^k$. Обозначим через b_c число координат вектора $\mathbf{x}'$, равных c, где $c \in \mathbb{Z}_4$. Имеем $wt_L(\mathbf{x}') = b_1 + 2b_2 + b_3$ и $wt_H(\mathbf{x}) = b_2 + b_3$. По построению матрицы $\mathbf{G}_m^k$ для любого ее столбца $\mathbf{z}_1^T$ найдется единственный столбец $\mathbf{z}_2^T$ этой матрицы такой, что $\mathbf{z}_2^T = 3\mathbf{z}_1^T$ (возможно $\mathbf{z}_1^T = \mathbf{z}_2^T$). Отсюда следует, что в любом кодовом слове кода $\mathcal{A}_m^k$ число компонент, равных 1, совпадает с числом компонент, равных 3. Таким образом, из того что $b_1 = b_3$, следует требуемое равенство.

(ii) Пусть $\mathbf{x}' = \beta^{-1}(\mathbf{x})$, $\mathbf{y}' = \beta^{-1}(\mathbf{y})$ — соответствующие кодовые векторы кода $\mathcal{A}_m^k$. Тогда

$$wt_H(\mathbf{x} \bullet \mathbf{y}^{-1}) = \frac{1}{2} wt_L(\beta^{-1}(\mathbf{x} \bullet \mathbf{y}^{-1})) = \frac{1}{2} wt_L(\mathbf{x}' - \mathbf{y}').$$

Множество ненулевых компонент произвольного двоичного вектора $\mathbf{v}$ обозначим через $\mathrm{supp}(\mathbf{v})$. Через I_c обозначим множество всех компонент вектора $\mathbf{x}'-\mathbf{y}'$ равных c, $c \in \mathbb{Z}_4$, и пусть $|I_c| = b_c$. Имеем $wt_L(\mathbf{x}'-\mathbf{y}') = b_1+2b_2+b_3$. Согласно (4.3) имеем

$$\mathrm{supp}(\mathbf{x} \bullet \mathbf{y}^{-1}) = I_2 \cup I_3,$$

и, следовательно, $wt_H(\mathbf{x} \bullet \mathbf{y}^{-1}) = b_2 + b_3$. Для любого $c \in \mathbb{Z}_4$ определим подмножество $I_c^{1,3}$ множества I_c, состоящее из всех компонент $s \in I_c$ таких, что $y'_s \in \{1, 3\}$. Тогда, исходя из определения отображения β, получаем

$$\mathrm{supp}(\mathbf{x} \oplus \mathbf{y}) = I_1^{1,3} \cup I_2 \cup (I_3 \setminus I_3^{1,3}).$$

Заметим, что, вообще говоря, вектор $\mathbf{x} \oplus \mathbf{y}$ не принадлежит коду A_m^k. Опираясь на упомянутое в пункте (i) свойство матрицы $\mathbf{G}_m^k$ (для любого ее столбца $\mathbf{z}_1^T$ найдется единственный столбец $\mathbf{z}_2^T$ этой матрицы такой, что $\mathbf{z}_2^T = 3\mathbf{z}_1^T$), получаем, что $|I_1^{1,3}| = |I_3^{1,3}| = r$. Отсюда следует, что $d_H(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} \oplus \mathbf{y}) = r + b_2 + (b_3 - r) = b_2 + b_3 = wt_H(\mathbf{x} \bullet \mathbf{y}^{-1})$.

Равенство (iii) несложно вытекает из (i) и (ii). □

Согласно утверждениям 8 и 11 код A_m^k имеет кодовое расстояние $n/2$. Таким образом, из утверждений 8, 9, 10 и 11 следует

Теорема 53. *При целых m, k, таких что $1 \leqslant k \leqslant m/2$, выполняется*
(i) *код A_m^k является $(n, 2n, n/2)_2$-кодом типа Адамара;*
(ii) *код A_m^1 линеен, при $k \geqslant 2$ справедливо $|\mathrm{Ker}(A_m^k)| = 2^{m-k+1}$, где через $\mathrm{Ker}(A_m^k)$ обозначено ядро кода.*
(iii) *операция $\bullet$, заданная на A_m^k, согласована с метрикой Хэмминга: для любых $\mathbf{x}, \mathbf{y} \in A_m^k$ имеет место $d_H(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} \bullet \mathbf{y}^{-1})$, где $\mathbf{y}^{-1}$ обозначает кодовое слово A_m^k такое, что $\mathbf{y} \bullet \mathbf{y}^{-1} = \mathbf{0}$.*

4.3 Бинарная операция $\langle \mathbf{u}, \mathbf{v} \rangle_k$

Итак, пусть $\mathbf{C}_m^k = (c_{\mathbf{u},\mathbf{v}}^k)$ — выше определенная четверичная квадратная матрица порядка n, где векторы $\mathbf{u}, \mathbf{v}$ пробегают пространство $\mathbb{Z}_2^m$ в порядке лексикографического возрастания векторов $\varphi_k^{-1}(\mathbf{u})$ и $\varphi_k^{-1}(\mathbf{v})$ соответственно. При любом целом k, $0 \leqslant k \leqslant m/2$, определим бинарную операцию

$$\langle \cdot, \cdot \rangle_k : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2$$

следующим образом:

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(c_{\mathbf{u},\mathbf{v}}^k) \text{ для любых } \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m. \tag{4.4}$$

Операция $\langle \cdot, \cdot \rangle_0$ совпадает с обычным скалярным произведением, т. е.

$$\langle \mathbf{u}, \mathbf{v} \rangle_0 = \langle \mathbf{u}, \mathbf{v} \rangle.$$

Далее будем использовать оба эти обозначения.

Пусть π_k обозначает подстановку $(1,2)(3,4)\ldots(2k-1,2k)$ на m элементах, представленную в виде произведения транспозиций. Другими словами, вектор $\pi_k(\mathbf{u})$ получается из вектора $\mathbf{u} \in \mathbb{Z}_2^m$, если поменять местами координаты в каждой паре, образующей (под действием отображения φ_k^{-1}) $\mathbb{Z}_4$-координату. Заметим, что для любого вектора $\mathbf{u} \in \mathbb{Z}_2^m$ сумма строк матрицы $\mathbf{C}_m^k$, отвечающих векторам $\mathbf{u}$ и $\pi_k(\mathbf{u})$, равна нулевому вектору.

Свойства операции $\langle \cdot, \cdot \rangle_k$ приведены в следующем утверждении.

Утверждение 12. *Пусть $m \in \mathbb{N}$, k — целое, $0 \leqslant k \leqslant m/2$. Тогда при любых векторах $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$ выполняются соотношения:*

(i) $\langle \mathbf{u}, \mathbf{v} \rangle_k = \langle \mathbf{v}, \mathbf{u} \rangle_k$;

(ii) $\langle a\mathbf{u}, \mathbf{v} \rangle_k = a\langle \mathbf{u}, \mathbf{v} \rangle_k$ *для любого* $a \in \mathbb{Z}_2$;

(iii) $\displaystyle\sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u},\mathbf{v} \rangle_k \oplus \langle \mathbf{w},\mathbf{v} \rangle_k} = \begin{cases} 2^m, & \text{если } \mathbf{u} = \mathbf{w}, \\ 0 & \text{в противном случае;} \end{cases}$

(iv) $\langle (\mathbf{u}, a), (\mathbf{v}, b) \rangle_k = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus ab$ *для любых* $a, b \in \mathbb{Z}_2$;

(v) $\langle (a,a'),(b,b')\rangle_1 = \langle (a',a),(b,b')\rangle_0$ *для любых* $a,a',b,b' \in \mathbb{Z}_2$;

(vi) $\langle (a,a',\mathbf{u}),(b,b',\mathbf{v})\rangle_{k+1} = \langle (a,a'),(b,b')\rangle_\varepsilon \oplus \langle \mathbf{u},\mathbf{v}\rangle_k$, *для любых* a, a', b, $b' \in \mathbb{Z}_2$, *где параметр* $\varepsilon \in \mathbb{Z}_2$ *определяется как* $\varepsilon = \langle \mathbf{u},\mathbf{v}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{v}\rangle_k \oplus 1$;

(vii) $\langle \mathbf{u},\mathbf{w}\rangle_k \oplus \langle \mathbf{v},\mathbf{w}\rangle_k =$
$$\langle \mathbf{u}\star\mathbf{v},\mathbf{w}\rangle_k \oplus \Big(\langle \mathbf{u},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{w}\rangle_k\Big)\Big(\langle \mathbf{v},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{v}),\mathbf{w}\rangle_k\Big).$$

Доказательство. Соотношение (i) следует из утверждения 7, равенство (ii) — из определения матрицы $\mathbf{C}_m^k$.

(iii) Заметим, что левая часть равенства равна $2^m - 2d_H(\beta(\mathbf{h}^{\mathbf{u}}),\beta(\mathbf{h}^{\mathbf{w}}))$. Отсюда и из теоремы 53 вытекает требуемое. Действительно, если $\mathbf{u} \neq \mathbf{w}$, то кодовые слова $\beta(\mathbf{h}^{\mathbf{u}})$ и $\beta(\mathbf{h}^{\mathbf{w}})$ кода A_m^k типа Адамара находятся друг от друга на расстоянии 2^{m-1}.

(iv) Согласно утверждению 7, см. (i), справедливо равенство $c^k_{(\mathbf{u},a),(\mathbf{v},b)} = c^k_{\mathbf{u},\mathbf{v}} + 2ab$, из которого следует (iv).

(v) Следует из определения, согласно которому

$\langle\cdot,\cdot\rangle_0$	00	01	10	11
00	0	0	0	0
01	0	1	0	1
10	0	0	1	1
11	0	1	1	0

$\langle\cdot,\cdot\rangle_1$	00	01	10	11
00	0	0	0	0
01	0	0	1	1
10	0	1	0	1
11	0	1	1	0

(vi) Из утверждения 7, см. (ii), следует, что $c^{k+1}_{(a,a',\mathbf{u}),(b,b',\mathbf{v})} = \varphi^{-1}(a,a') \cdot \varphi^{-1}(b,b') + c^k_{\mathbf{u},\mathbf{v}}$. Сперва непосредственной проверкой установим, что имеют место равенства

$$\langle (a,a'),(b,b')\rangle_0 = \gamma(\varphi^{-1}(a,a') \cdot \varphi^{-1}(b,b')),$$
$$\langle (a,a'),(b,b')\rangle_1 = \beta(\varphi^{-1}(a,a') \cdot \varphi^{-1}(b,b')).$$

Действительно, эти равенства несложно получить, используя пункт (v). Далее нетрудно видеть, что для любых $p,q \in \mathbb{Z}_4$ выполняется

$$\beta(p+q) = \beta(p) \oplus \begin{cases} \beta(q), & \text{если } p \text{ равно 0 или 2,} \\ \gamma(q) & \text{в противном случае.} \end{cases}$$

Отсюда следует, что $\langle (a,a',\mathbf{u}),(b,b',\mathbf{v})\rangle_{k+1} = \beta(c^{k+1}_{(a,a',\mathbf{u}),(b,b',\mathbf{v})}) = \beta(c^k_{\mathbf{u},\mathbf{v}}) \oplus \langle (a,a'),(b,b')\rangle_\varepsilon$, где ε равно 1, если $c^k_{\mathbf{u},\mathbf{v}} \in \{0,2\}$, и равно 0 в противном случае. Заметим, что $c^k_{\mathbf{u},\mathbf{v}}$ принадлежит $\{0,2\}$ тогда и только тогда, когда $\beta(c^k_{\mathbf{u},\mathbf{v}}) = \gamma(c^k_{\mathbf{u},\mathbf{v}})$. Поскольку из определения подстановки π_k следует равенство

$$c^k_{\pi_k(\mathbf{u}),\mathbf{v}} = 3c^k_{\mathbf{u},\mathbf{v}},$$

и для любого $p \in \mathbb{Z}_4$, как нетрудно заметить, $\beta(3p) = \gamma(p)$, то для параметра ε получаем соотношение $\varepsilon \oplus 1 = \beta(c^k_{\mathbf{u},\mathbf{v}}) \oplus \gamma(c^k_{\mathbf{u},\mathbf{v}}) = \beta(c^k_{\mathbf{u},\mathbf{v}}) \oplus \beta(3c^k_{\mathbf{u},\mathbf{v}}) = \langle \mathbf{u},\mathbf{v}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{v}\rangle_k$.

(vii) Поскольку выполняется $\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u}\star\mathbf{v}}$ (см. (4.2)), имеем $c^k_{\mathbf{u},\mathbf{w}} + c^k_{\mathbf{v},\mathbf{w}} = c^k_{\mathbf{u}\star\mathbf{w}}$. Заметим, что для любых $p,q \in \mathbb{Z}_4$ равенство $\beta(p) \oplus \beta(q) = \beta(p+q)$ справедливо тогда и только тогда, когда хотя бы один из элементов p, q равен 0 или 2. Согласно предыдущему пункту $c^k_{\mathbf{u},\mathbf{w}}$ принадлежит множеству $\{1,3\}$, если и только если $\langle \mathbf{u},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{w}\rangle_k = 1$. Поэтому $\beta(c^k_{\mathbf{u},\mathbf{w}}) \oplus \beta(c^k_{\mathbf{v},\mathbf{w}}) = \beta(c^k_{\mathbf{u}\star\mathbf{v},\mathbf{w}}) \oplus \Big(\langle \mathbf{u},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{w}\rangle_k\Big)\Big(\langle \mathbf{v},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{v}),\mathbf{w}\rangle_k\Big)$, что и требовалось показать. Утверждение 12 доказано. □

Замечание. Операция $\langle \mathbf{u},\mathbf{v}\rangle_k$ не является билинейной формой при $k \geqslant 2$. Это следует из Утверждения 20, которое будет приведено в разделе 5.5.

Найдем явное представление для произведения $\langle \mathbf{u},\mathbf{v}\rangle_k$.

Теорема 54. *Пусть m,k — целые, $1 \leqslant k \leqslant m/2$. Для любого целого i, $1 \leqslant i \leqslant m/2$, и любых $\mathbf{u},\mathbf{v} \in \mathbb{Z}_2^m$ пусть $Y_i = (u_{2i-1} \oplus u_{2i})(v_{2i-1} \oplus v_{2i})$. Тогда*

$$\langle \mathbf{u},\mathbf{v}\rangle_k = \Big(\bigoplus_{i=1}^{k}\bigoplus_{j=i}^{k} Y_iY_j\Big) \oplus \langle \mathbf{u},\mathbf{v}\rangle.$$

Доказательство. Докажем теорему индукцией по k.

При $k = 1$ согласно пунктам (iv) и (v) утверждения 12 имеем

$$\langle \mathbf{u},\mathbf{v}\rangle_1 = u_2v_1 \oplus u_1v_2 \oplus \bigoplus_{i=3}^{m} u_iv_i = (u_1 \oplus u_2)(v_1 \oplus v_2) \oplus \langle \mathbf{u},\mathbf{v}\rangle = Y_1 \oplus \langle \mathbf{u},\mathbf{v}\rangle.$$

Заметим, что для любого j справедливо $Y_j^2 = Y_j$, откуда получаем требуемое.

Пусть теорема справедлива для некоторого k, $1 \leqslant k \leqslant (m-2)/2$. Покажем, что она имеет место и для $k+1$. По утверждению 12, см. пункт (vi), выполняется

$$\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \langle (u_1, u_2), (v_1, v_2) \rangle_\varepsilon \oplus \langle (u_3, \ldots, u_m), (v_3, \ldots, v_m) \rangle_k, \tag{4.5}$$

где $\varepsilon = \langle (u_3, \ldots, u_m), (v_3, \ldots, v_m) \rangle_k \oplus \langle \pi_k(u_3, \ldots, u_m), (v_3, \ldots, v_m) \rangle_k \oplus 1$.

По предположению индукции имеем

$$\langle (u_3, \ldots, u_m), (v_3, \ldots, v_m) \rangle_k = \Big(\bigoplus_{i=2}^{k+1} \bigoplus_{j=i}^{k+1} Y_i Y_j \Big) \oplus \bigoplus_{s=3}^{m} u_s v_s,$$

и, как нетрудно видеть,

$$\langle \pi_k(u_3, \ldots, u_m), (v_3, \ldots, v_m) \rangle_k = \Big(\bigoplus_{i=2}^{k+1} \bigoplus_{j=i}^{k+1} Y_i Y_j \Big) \oplus \bigoplus_{j=2}^{k+1} \big(u_{2j} v_{2j-1} \oplus u_{2j-1} v_{2j} \big) \oplus \bigoplus_{s=2k+3}^{m} u_s v_s.$$

Отсюда следует, что $\varepsilon = \Big(\bigoplus_{j=2}^{k+1} Y_j \Big) \oplus 1$. Тогда первое слагаемое в правой части равенства (4.5) согласно пункту (v) утверждения 12 имеет вид

$$\langle (u_1, u_2), (v_1, v_2) \rangle_\varepsilon = (\varepsilon \oplus 1)(u_1 v_1 \oplus u_2 v_2) \oplus \varepsilon (u_2 v_1 \oplus u_1 v_2) = \varepsilon Y_1 \oplus u_1 v_1 \oplus u_2 v_2.$$

Подставляя выражение для ε и используя равенство $Y_1^2 = Y_1$, получаем

$$\langle (u_1, u_2), (v_1, v_2) \rangle_\varepsilon = \Big(\bigoplus_{j=1}^{k+1} Y_1 Y_j \Big) \oplus u_1 v_1 \oplus u_2 v_2.$$

Таким образом, имеем следующее выражение для $\langle \mathbf{u}, \mathbf{v} \rangle_{k+1}$:

$$\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \left(\Big(\bigoplus_{j=1}^{k+1} Y_1 Y_j \Big) \oplus u_1 v_1 \oplus u_2 v_2 \right) \oplus \left(\Big(\bigoplus_{i=2}^{k+1} \bigoplus_{j=i}^{k+1} Y_i Y_j \Big) \oplus \bigoplus_{s=3}^{m} u_s v_s \right),$$

и следовательно,

$$\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \Big(\bigoplus_{i=1}^{k+1} \bigoplus_{j=i}^{k+1} Y_i Y_j \Big) \oplus \langle \mathbf{u}, \mathbf{v} \rangle.$$

□

Следствие 1. *Для любых векторов* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ *и любого целого* k*, такого что* $1 \leqslant k \leqslant m/2$*, выполняется равенство*

$$\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{v} \rangle_k = \bigoplus_{i=1}^{k} Y_i.$$

Следствие 2. *Для любых* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ *и произвольного целого* k*, такого что* $1 \leqslant k \leqslant (m-2)/2$*, справедливо равенство*

$$\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus Y_{k+1} \Big(\bigoplus_{i=1}^{k+1} Y_i \Big).$$

Как нетрудно заметить, координаты $u_1, \ldots, u_m$ (также как и $v_1, \ldots, v_m$) участвуют в операции $\langle \cdot, \cdot \rangle_k$ неравноправно. А именно при данном k в точности $2k$ первых координат каждого из векторов $\mathbf{u}, \mathbf{v}$ входят в квадратичные и линейные слагаемые; остальные координаты — только в линейные.

Из теоремы 54 легко следует, что

$$\langle \mathbf{u}, \mathbf{v} \rangle_1 = \langle \mathbf{u}, \hat{\mathbf{v}} \rangle, \tag{4.6}$$

где $\hat{\mathbf{v}}$ получен из вектора $\mathbf{v}$ перестановкой координат v_1 и v_2.

В качестве примера приведем выражение для операции $\langle \cdot, \cdot \rangle_2$ при $m = 4$:

$$\langle \mathbf{u}, \mathbf{v} \rangle_2 = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1 \oplus v_2)(v_3 \oplus v_4) \oplus u_2 v_1 \oplus u_1 v_2 \oplus u_4 v_3 \oplus u_3 v_4 \tag{4.7}$$

и операции $\langle \cdot, \cdot \rangle_3$ при $m = 6$:

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle_3 = {} & (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1 v_3 \oplus v_1 v_4 \oplus v_2 v_3 \oplus v_2 v_4) \\ & \oplus (u_1 \oplus u_2)(u_5 \oplus u_6)(v_1 v_5 \oplus v_1 v_6 \oplus v_2 v_5 \oplus v_2 v_6) \\ & \oplus (u_3 \oplus u_4)(u_5 \oplus u_6)(v_3 v_5 \oplus v_3 v_6 \oplus v_4 v_5 \oplus v_4 v_6) \\ & \oplus u_2 v_1 \oplus u_1 v_2 \oplus u_4 v_3 \oplus u_3 v_4 \oplus u_6 v_5 \oplus u_5 v_6. \end{aligned}$$

4.4 Понятие k-аффинной функции

Пусть каждому вектору кода A_m^k, где $m \in \mathbb{N}$, k — целое, $0 \leqslant k \leqslant m/2$, отвечает булева функция $g \in \mathcal{F}_m$, для которой этот вектор является вектором значений, причем $g(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ для некоторых $\mathbf{u} \in \mathbb{Z}_2^m$, $a \in \mathbb{Z}_2$ и произвольного $\mathbf{v} \in \mathbb{Z}_2^m$. Множество всех таких функций от m переменных назовем множеством *k-аффинных функций*[1] и обозначим через $\mathfrak{A}_m^k$. Ясно, что $|\mathfrak{A}_m^k| = 2^{m+1}$. Из теоремы 54 следует

Утверждение 13. *При любом $m \in \mathbb{N}$, целом k, $0 \leqslant k \leqslant m/2$, класс $\mathfrak{A}_m^k$ состоит из функций вида*

$$g(\mathbf{v}) = \Big(\bigoplus_{i=1}^{k} \bigoplus_{j=i}^{k} (u_{2i-1} \oplus u_{2i})(u_{2j-1} \oplus u_{2j})(v_{2i-1} \oplus v_{2i})(v_{2j-1} \oplus v_{2j}) \Big) \oplus \Big(\bigoplus_{s=1}^{m} u_s v_s \Big) \oplus a, \quad (4.8)$$

где вектор $\mathbf{u}$ пробегает $\mathbb{Z}_2^m$ и a — любой элемент поля $\mathbb{Z}_2$.

Например, произвольная функция g из класса $\mathfrak{A}_4^2$ однозначно определяется двоичным вектором (u_1, u_2, u_3, u_4) и элементом $a \in \mathbb{Z}_2$:

$$g(v_1, v_2, v_3, v_4) = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1 v_3 \oplus v_1 v_4 \oplus v_2 v_3 \oplus v_2 v_4) \oplus u_2 v_1 \oplus u_1 v_2 \oplus u_4 v_3 \oplus u_3 v_4 \oplus a.$$

Класс $\mathfrak{A}_4^2$ состоит из 24 аффинных функций и 8 квадратичных функций. Квадратичные функции задаются векторами

$$\mathbf{u} \in \{\, (0101), (0110), (1001), (1010) \,\}$$

и произвольным значением a.

Напомним, что *степенью нелинейности* (или *рангом*) $\deg f$ булевой функции f называется число переменных в самом длинном слагаемом ее

[1] Термин «k-аффинная функция» в другом значении уже использовался М. Л. Буряковым и О. А. Логачевым [4]. Параметр k в их работе не имеет ничего общего с параметром, определяемым здесь. К сожалению, такое совпадение терминов было замечено уже достаточно поздно.

алгебраической нормальной формы (или многочлена Жегалкина). Из утверждения 13 следует, что степень булевой функции из произвольного класса $\mathfrak{A}_m^k$ не превышает 2. Справедливо

Утверждение 14. *Для любого $m \in \mathbb{N}$ и целого k, $0 \leqslant k \leqslant m/2$, класс $\mathfrak{A}_m^k$ содержит ровно $2^{m-k+1}(k+1)$ аффинных функций и $2^{m-k+1}(2^k-k-1)$ квадратичных функций.*

Доказательство. Согласно утверждению 13 функция $g(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ является аффинной тогда и только тогда, когда для вектора $\mathbf{u}$ выполнено любое из следующих условий:

1) для всех j, $1 \leqslant j \leqslant k$, справедливо $u_{2j-1} = u_{2j}$;

2) найдется единственный номер j, $1 \leqslant j \leqslant k$, такой что $u_{2j-1} \neq u_{2j}$.

Число векторов $\mathbf{u}$ первого типа равно 2^{m-k}, второго типа равно $k2^{m-k}$. Отсюда следует, что число аффинных функций в $\mathfrak{A}_m^k$ равно $2^{m-k+1}(k+1)$. Число квадратичных функций получаем как $2^{m+1} - 2^{m-k+1}(k+1)$. $\square$

Таким образом, классы $\mathfrak{A}_m^0$, $\mathfrak{A}_m^1$ совпадают с классом всех аффинных функций. Несложно доказать

Следствие 3. *Доля аффинных функций в $\mathfrak{A}_m^{m/2}$ стремится к нулю с ростом m.*

4.5 Понятие k-бент-функции

Для любого $m \in \mathbb{N}$ и целого k, $0 \leqslant k \leqslant m/2$, целочисленную функцию $W_f^{(k)}$, заданную на множестве $\mathbb{Z}_2^m$ равенством

$$W_f^{(k)}(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus f(\mathbf{u})} \text{ для любого } \mathbf{v} \in \mathbb{Z}_2^m,$$

назовем *k-преобразованием Уолша—Адамара* булевой функции $f \in \mathcal{F}_m$.

Заметим, что $W_f^{(0)}$ является обычным преобразованием Уолша—Адамара W_f. Поскольку матрица $\beta(\mathbf{C}_m^k)$ после замены каждого ее элемента c на $(-1)^c$ является матрицей Адамара (как это следует из теоремы 53), для $W_f^{(k)}$ имеет место аналог равенства Парсеваля, см. например, [19, гл. 6]. Для полноты изложения приведем доказательство этого факта.

Теорема 55. (равенство Парсеваля для $W_f^{(k)}$). *При любом $m \in \mathbb{N}$ и целом k, $0 \leqslant k \leqslant m/2$, для любой функции $f \in \mathcal{F}_m$ выполняется*

$$\sum_{\mathbf{v}\in\mathbb{Z}_2^m} \Big(W_f^{(k)}(\mathbf{v})\Big)^2 = 2^{2m}.$$

Доказательство. По определению преобразования $W_f^{(k)}$ имеем

$$\sum_{\mathbf{v}\in\mathbb{Z}_2^m} (W_f^{(k)}(\mathbf{v}))^2 = \sum_{\mathbf{v}\in\mathbb{Z}_2^m} \Big(\sum_{\mathbf{u}\in\mathbb{Z}_2^m} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle_k \oplus f(\mathbf{u})}\Big)^2 =$$
$$\sum_{\mathbf{v}\in\mathbb{Z}_2^m} \sum_{\mathbf{u},\mathbf{w}\in\mathbb{Z}_2^m} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle_k \oplus f(\mathbf{u}) \oplus \langle \mathbf{w},\mathbf{v}\rangle_k \oplus f(\mathbf{w})} =$$

(меняя порядок суммирования и используя пункт (iii) утверждения 12)

$$= \sum_{\mathbf{u},\mathbf{w}\in\mathbb{Z}_2^m} (-1)^{f(\mathbf{u})\oplus f(\mathbf{w})} \sum_{\mathbf{v}\in\mathbb{Z}_2^m} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle_k \oplus \langle \mathbf{w},\mathbf{v}\rangle_k} = \sum_{\mathbf{u}\in\mathbb{Z}_2^m} 2^m = 2^{2m}.$$

□

Расстояние между функцией $f \in \mathcal{F}_m$ и множеством функций $\mathfrak{A}_m^k$ назовем *k-нелинейностью* функции f и обозначим через $N_f^{(k)}$.

Утверждение 15. *Справедливо равенство* $N_f^{(k)} = 2^{m-1} - \frac{1}{2} \max\limits_{\mathbf{v}\in\mathbb{Z}_2^m} |W_f^{(k)}(\mathbf{v})|$.

Доказательство. Пусть $\mathbf{g}^{\mathbf{v}} = \beta(\mathbf{h}^{\mathbf{v}})$, где $\mathbf{h}^{\mathbf{v}}$ — строка матрицы $\mathbf{C}_m^k$, отвечающая вектору $\mathbf{v} \in \mathbb{Z}_2^m$. Имеем $g^{\mathbf{v}}(\mathbf{u}) = \langle \mathbf{v}, \mathbf{u}\rangle_k$. Тогда

$$N_f^{(k)} = \min_{g\in\mathfrak{A}_m^k} \operatorname{dist}(f,g) = \min_{\mathbf{v}\in\mathbb{Z}_2^m} \{\, d_H(\mathbf{f}, \mathbf{g}^{\mathbf{v}}), d_H(\mathbf{f}, \mathbf{g}^{\mathbf{v}} \oplus \mathbf{1}) \,\}.$$

Из определения $W_f^{(k)}$ и пункта (i) утверждения 12 следуют равенства

$$d_H(\mathbf{f}, \mathbf{g}^{\mathbf{v}}) = 2^{m-1} - \frac{1}{2}W_f^{(k)}(\mathbf{v}), \quad d_H(\mathbf{f}, \mathbf{g}^{\mathbf{v}} \oplus \mathbf{1}) = 2^{m-1} + \frac{1}{2}W_f^{(k)}(\mathbf{v}),$$

из которых получаем

$$N_f^{(k)} = \min_{\mathbf{v}\in\mathbb{Z}_2^m}\Big(2^{m-1} - \frac{1}{2}|W_f^{(k)}(\mathbf{v})|\Big) = 2^{m-1} - \frac{1}{2}\max_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f^{(k)}(\mathbf{v})|.$$

Утверждение 15 доказано. □

Из теоремы 55 следует неравенство

$$\max_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f^{(k)}(\mathbf{v})| \geqslant 2^{m/2}. \tag{4.9}$$

Поэтому k-нелинейность функции f не превышает величины $2^{m-1}-2^{(m/2)-1}$. По аналогии с определениями максимально нелинейной функции и бент-функции введем следующие понятия.

Определение 20. Для любых $m, k \in \mathbb{N}$, $1 \leqslant k \leqslant m/2$, булеву функцию $f \in \mathcal{F}_m$ назовем *максимально k-нелинейной*, если каждый параметр $N_f^{(j)}$, $j = 1, \ldots, k$, принимает максимальное возможное значение.

Другими словами, вектор значений максимально k-нелинейной функции $f \in \mathcal{F}_m$ удален на максимально возможные расстояния от кодов $A_m^1, \ldots, A_m^k$.

Определение 21. Для четного m, целого k, $1 \leqslant k \leqslant m/2$, булеву функцию $f \in \mathcal{F}_m$ назовем *k-бент-функцией*, если все коэффициенты $W_f^{(j)}(\mathbf{v})$, $j = 1, \ldots, k$, равны $\pm 2^{m/2}$.

В случае четного m эти определения, как станет ясно из дальнейшего, эквивалентны. Класс всех k-бент-функций от m переменных обозначим через $\mathcal{B}_m^k$. Из пунктов (iv) и (v) утверждения 12 следует, что

$$W_f^{(1)}(v_1, v_2, v_3, \ldots, v_m) = W_f(v_2, v_1, v_3, \ldots, v_m).$$

Поэтому класс $\mathcal{B}_m^1$ представляет собой класс обычных бент-функций $\mathcal{B}_m$. Таким образом, $\mathcal{B}_m = \mathcal{B}_m^1 \supseteq \cdots \supseteq \mathcal{B}_m^{m/2}$, и, как покажем далее, каждое включение является строгим и $\mathcal{B}_m^{m/2} \neq \emptyset$.

4.6 k-Бент-функции от малого числа переменных

Описание. Рассмотрим малые значения параметра m.

Случай $m = 2$. Класс $\mathcal{B}_2^1$ состоит из всех функций, векторы значений которых имеют нечетный вес Хэмминга; $|\mathcal{B}_2^1| = 8$.

Случай $m = 4$. Сначала приведем пример функции $\xi \in \mathcal{F}_4$ такой, что $\xi \in \mathcal{B}_4^1 \setminus \mathcal{B}_4^2$:

$$\xi(u_1, u_2, u_3, u_4) = u_1u_2 \oplus u_2u_3 \oplus u_3u_4.$$

Используя утверждение 12 и теорему 54, выпишем соответствующие наборы коэффициентов $W_\xi^1(\mathbf{v})$ и $W_\xi^2(\mathbf{v})$ в порядке лексикографического возрастания вектора $\mathbf{v} \in \mathbb{Z}_2^4$. Имеем

$$W_\xi^1 = (4, 4, 4, -4, 4, -4, 4, 4, 4, 4, 4, -4, -4, 4, -4, -4),$$

$$W_\xi^2 = (4, 4, 4, -4, 4, 0, 0, 4, 4, 8, 0, -4, -4, -4, 4, -4).$$

Приведем подробнее, например, вычисление коэффициентов $W_\xi^1(0101)$ и $W_\xi^2(0101)$. Имеем

$$W_\xi^k(0101) = \sum_{u_1,u_2} \Big(\sum_{u_3,u_4} (-1)^{\langle \mathbf{u}, 0101 \rangle_k \oplus \xi(\mathbf{u})} \Big) \text{ для } k = 1, 2.$$

Согласно теореме 54 имеем

$$\langle \mathbf{u}, 0101 \rangle_1 = u_1 \oplus u_4,$$

$$\langle \mathbf{u}, 0101 \rangle_2 = u_1u_3 \oplus u_1u_4 \oplus u_2u_3 \oplus u_2u_4 \oplus u_1 \oplus u_3.$$

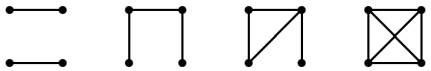
Поэтому

$$W_\xi^1(0101) = \underbrace{(1 - 1 + 1 + 1)}_{(u_1,u_2)=(00)} + \underbrace{(1 - 1 - 1 - 1)}_{(u_1,u_2)=(01)} + \underbrace{(-1 + 1 - 1 - 1)}_{(u_1,u_2)=(10)} + \underbrace{(1 - 1 - 1 - 1)}_{(u_1,u_2)=(11)} = -4,$$

$$W_\xi^2(0101) = (1+1-1+1)+(1-1-1-1)+(-1+1-1-1)+(1+1+1-1) = 0.$$

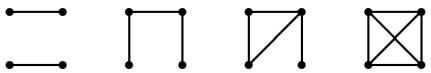
Из данного примера легко заключаем, что множество $\mathcal{B}_4^1 \setminus \mathcal{B}_4^2$ непусто. Рассмотрим теперь каждый класс $\mathcal{B}_4^1$ и $\mathcal{B}_4^2$ в отдельности.

Известно [20], что множество $\mathcal{B}_4^1$ состоит из 896-ти булевых функций, причем каждая функция является квадратичной, т. е. степени нелинейности 2. Множество $\mathcal{B}_4^1$ можно разделить на 28 классов по 32 функции. Алгебраические нормальные формы (или многочлены Жегалкина, а кратко АНФ) функций из каждого класса обладают одинаковой квадратичной частью, произвольной линейной частью и любым свободным членом. Если рассмотреть граф на множестве переменных, а ребрами соединить те вершины, которые образуют слагаемое в квадратичной части АНФ функции, то эти 28 типов можно задать следующим образом:

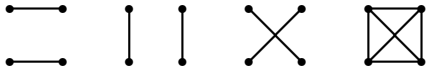


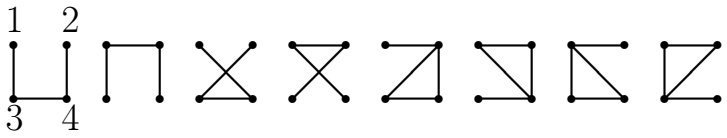
Под каждым графом указано число типов, которые он определяет. Например, имеется 12 типов квадратичной части, состоящей из трех слагаемых, и только один тип из шести слагаемых.

Приведем простое описание класса $\mathcal{B}_4^2$, используя интерпретацию в терминах графов. Рассмотрим граф на четырех вершинах, которые пронумеруем цифрами от 1 до 4. Считаем, что вершина с номером i соответствует переменной v_i. Разделим вершины графа на две доли $\{1, 2\}$ и $\{3, 4\}$. Из 28-ми графов, приведенных выше, выберем только те, в которых число ребер, соединяющих вершины из разных долей, четно. Получим серию из следующих 12-ти графов:



А именно, нумеруя вершины слева направо и сверху вниз, имеем





Покажем, что множество $\mathcal{B}_4^2$ является объединением 12-ти классов 1-бент-функций, каждый из которых отвечает одному из указанных графов. Все функции из одного класса различаются только линейной частью и свободным членом, их число равно 32. Таким образом, $|\mathcal{B}_4^2| = 384$.

Переходя от графов к алгебраическим нормальным формам функций, это утверждение формулируется следующим образом.

Теорема 56. *Пусть параметры i_1, i_2, i_3 и i_4 принимают различные значения от 1 до 4. Тогда множество функций $\mathcal{B}_4^2$ состоит из всех функций степени 2 с квадратичными частями вида:*

$v_{i_1}v_{i_2} \oplus v_{i_3}v_{i_4}$ (3 *типа*);

$v_{i_1}v_{i_2} \oplus v_{i_1}v_{i_3} \oplus v_{i_2}v_{i_4}$ *при* $\{i_1, i_2\} = \{1, 2\}$ *или* $\{3, 4\}$ (4 *типа*);

$v_{i_1}v_{i_2} \oplus v_{i_2}v_{i_3} \oplus v_{i_3}v_{i_4} \oplus v_{i_1}v_{i_3}$ *при* $\{i_1, i_2\} = \{1, 2\}$ *или* $\{3, 4\}$ (4 *типа*);

$v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$ (1 *тип*).

Доказательство. Очевидно, что $\mathcal{B}_4^2$ содержит только функции степени 2. Заметим, что если функция f принадлежит $\mathcal{B}_4^2$, то функция $f \oplus 1$ также содержится в этом классе. Рассмотрим произвольную функцию $f_{\mathbf{w}} \in \mathcal{B}_4^1$ степени 2 вида $f_{\mathbf{w}}(\mathbf{v}) = f(\mathbf{v}) \oplus \langle \mathbf{w}, \mathbf{v} \rangle$, где вектор $\mathbf{w}$ фиксирован и через $f(\cdot)$ обозначена квадратичная часть функции. Выясним при каких условиях функция $f_{\mathbf{w}}$ является 2-бент-функцией, т. е. когда все 2-коэффициенты Уолша-Адамара этой функции равны ± 4. Для произвольного вектора $\mathbf{u} = (u_1, u_2, u_3, u_4)$ рассмотрим коэффициент $W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u})$.

Пусть $\mathbb{Z}_2^4 = V_0 \cup V_1$, где множество V_1 имеет вид

$$V_1 = \{\, (1010), (1001), (0110), (0101) \,\},$$

и множество V_0 содержит все остальные векторы длины 4. Заметим, что для любого вектора $\mathbf{u} \in V_0$ выполняется $(u_1 \oplus u_2)(u_3 \oplus u_4) = 0$, тогда как

$(u_1 \oplus u_2)(u_3 \oplus u_4) = 1$ для любого $\mathbf{u} \in V_1$. По определению имеем

$$\langle \mathbf{u}, \mathbf{v} \rangle_2 = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus \\ u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4.$$

Тогда для любого вектора $\mathbf{u} \in V_0$ выполняется

$$W^{(2)}_{f_\mathbf{w}}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_2 \oplus f_\mathbf{w}(\mathbf{v})} = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{v} \rangle \oplus f_\mathbf{w}(\mathbf{v})} = W_{f_\mathbf{w}}(\tilde{\mathbf{u}}),$$

где $\tilde{\mathbf{u}} = (u_2, u_1, u_4, u_3)$, и следовательно $W^{(2)}_{f_\mathbf{w}}(\mathbf{u}) = \pm 4$, поскольку $f_\mathbf{w}$ является 1-бент-функцией.

Рассмотрим случай $\mathbf{u} \in V_1$. Имеем

$$W^{(2)}_{f_\mathbf{w}}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{v} \rangle \oplus g_\mathbf{w}(\mathbf{v})} = W_{g_\mathbf{w}}(\tilde{\mathbf{u}}), \tag{4.10}$$

где функция $g_\mathbf{w}$ задана равенством $g_\mathbf{w}(\mathbf{v}) = g(\mathbf{v}) \oplus \langle \mathbf{w}, \mathbf{v} \rangle$ и

$$g(\mathbf{v}) = (v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus f(\mathbf{v}).$$

Выясним при каких условиях данные четыре коэффициента

$$W^{(2)}_{f_\mathbf{w}}(1010),\ W^{(2)}_{f_\mathbf{w}}(1001),\ W^{(2)}_{f_\mathbf{w}}(0110),\ W^{(2)}_{f_\mathbf{w}}(0101), \tag{4.11}$$

равны ± 4. Для 12-ти из 28 возможных вариантов функции f функция g является 1-бент-функцией. А именно это 12 квадратичных функций f, указанные в формулировке теоремы:

$f(\mathbf{v})$	$g(\mathbf{v})$
 $v_1v_2 \oplus v_3v_4$	 $v_1v_2 \oplus \ldots \oplus v_3v_4$
 $v_1v_3 \oplus v_2v_4$	 $v_1v_4 \oplus v_2v_3$
 $v_1v_4 \oplus v_2v_3$	 $v_1v_3 \oplus v_2v_4$
 $v_1v_2 \oplus \ldots \oplus v_3v_4$	 $v_1v_2 \oplus v_3v_4$
 $v_1v_3 \oplus v_2v_4 \oplus v_3v_4$	 $v_1v_4 \oplus v_2v_3 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_3 \oplus v_2v_4$	 $v_1v_2 \oplus v_1v_4 \oplus v_2v_3$
 $v_1v_4 \oplus v_2v_3 \oplus v_3v_4$	 $v_1v_3 \oplus v_2v_4 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_4 \oplus v_2v_3$	 $v_1v_2 \oplus v_1v_3 \oplus v_2v_4$
 $v_1v_2 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$	 $v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_4 \oplus v_2v_4 \oplus v_3v_4$	 $v_1v_2 \oplus v_1v_3 \oplus v_2v_3 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_3v_4$	 $v_1v_2 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$
$v_1v_2 \oplus v_1v_3 \oplus v_2v_3 \oplus v_3v_4$	$v_1v_2 \oplus v_1v_4 \oplus v_2v_4 \oplus v_3v_4$

В каждом из этих 12-ти случаев, так как g есть 1-бент-функция, имеем $W^{(2)}_{f_{\mathbf{w}}}(\mathbf{u}) = W_{g_{\mathbf{w}}}(\tilde{\mathbf{u}}) = \pm 4$, и следовательно $f_{\mathbf{w}}$ принадлежит классу 2-бент-функций при любом векторе $\mathbf{w}$. Таким образом, мы показали, что класс $\mathcal{B}_4^2$ содержит по крайней мере $12 \times 32 = 384$ функции. Проверим, что если функция g не является 1-бент-функцией, то модуль хотя бы одного (например, первого) коэффициента среди коэффициентов (4.11) всегда не равен 4, и следовательно, $f_{\mathbf{w}}$ не может быть 2-бент-функцией в этом случае.

Поскольку выполняется

$$g_{\mathbf{w}}(\mathbf{v}) = \begin{cases} f_{\mathbf{w}}(\mathbf{v}), & \text{при } \mathbf{v} \in V_0 \\ f_{\mathbf{w}}(\mathbf{v}) \oplus 1, & \text{при } \mathbf{v} \in V_1, \end{cases}$$

коэффициент $W^{(2)}_{f_{\mathbf{w}}}(1010)$ согласно (4.10) можно представить в виде

$$W^{(2)}_{f_{\mathbf{w}}}(1010) = W_{g_{\mathbf{w}}}(0101) = S_0 - S_1,$$

где

$$S_\delta = \sum_{\mathbf{v} \in V_\delta} (-1)^{\langle (0101), \mathbf{v} \rangle \oplus f_{\mathbf{w}}(\mathbf{v})}, \text{ при } \delta = 0, 1.$$

Так как $f_{\mathbf{w}}$ является 1-бент-функцией, имеем $W_{f_{\mathbf{w}}}(0101) = S_0 + S_1 = \pm 4$. Тогда, как нетрудно заметить, в качестве необходимого условия для равенства $S_0 - S_1 = \pm 4$ величина S_1 должна быть равна ± 4 или 0. Расписывая S_1, получаем

$$S_1 = (-1)^{w_1}\left((-1)^{w_3 \oplus f(1010)} + (-1)^{w_4 \oplus f(1001)}\right) + (-1)^{w_2}\left((-1)^{w_3 \oplus f(0110)} + (-1)^{w_4 \oplus f(0101)}\right).$$

Тогда, как несложно заметить, для выполнения $S_1 \in \{\pm 4, 0\}$ необходимо, чтобы на множестве V_1 функция f принимала значение 1 четное число раз. Но АНФ каждой функции f из оставшихся 16-ти содержит нечетное число одночленов из множества

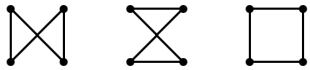
$$\{v_1 v_3, v_1 v_4, v_2 v_3, v_2 v_4\},$$

т. е. при интерпретации на графе — нечетное число ребер между долями $\{1, 2\}$ и $\{3, 4\}$, а следовательно на множестве V_1 каждая такая функция принимает значение 1 нечетное число раз. Таким образом, необходимое условие для $W^{(2)}_{f_{\mathbf{w}}}(1010) = \pm 4$ не выполнено, и следовательно в этом случае функция $f_{\mathbf{w}}$ не является 2-бент-функцией ни при каком векторе $\mathbf{w}$. □

Замечания. Интересным следствием из теоремы 56 является тот факт, что если к 2-бент-функции от четырех переменных прибавить произвольную аффинную функцию, то в результате снова получится 2-бент-функция. Осмелюсь предположить, что причиной этого является «эффект малых значений» и при $m > 4$ подобное свойство для k-бент-функций наблюдаться не будет.

Заметим, что при определении k-бент-функций существенными являются способ разбиения переменных на пары и порядок этих пар. Можно рассматривать более общий подход (см. главу 5), при котором аппроксимации булевых функций ведутся всеми функциями вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, где π — произвольная подстановка на m элементах, и тогда указанные выше ограничения снимаются. Из теоремы 56 следует, что функция $f \in \mathcal{B}_4^1$ является

2-бент-функцией при любом разбиении переменных на пары тогда и только тогда, когда пересечение графа ее квадратичной части с каждым из графов



содержит четное число ребер. Легко видеть, что такому условию удовлетворяют только функции с квадратичной частью вида

Их число равно 128.

m	k	Информация о классах $\mathcal{B}_m^k$
2	1	$\lvert\mathcal{B}_2^1\rvert = 8$
4	1, 2	$\lvert\mathcal{B}_4^1\rvert = 896$, см. описание в [20]; $\lvert\mathcal{B}_4^2\rvert = 384$, описание в [31]; число в [29];
6	1, 2, 3	$\lvert\mathcal{B}_6^1\rvert = 5\,425\,430\,528 \simeq 2^{32,3}$, см. [43, 158, 179]; $\lvert\mathcal{B}_6^2\rvert \geqslant 4 \cdot 896 = 3\,584$, следует из [29]; $\lvert\mathcal{B}_6^3\rvert \geqslant 4 \cdot 384 = 1\,536$, следует из [29];
8	1, 2, 3, 4	$\lvert\mathcal{B}_8^1\rvert \geqslant 1\,559\,994\,535\,674\,013\,286\,400 \simeq 2^{70,4}$, см. [43]; $\lvert\mathcal{B}_8^2\rvert > 2^{34,3}$, следует из [43, 158, 179] и [29]; $\lvert\mathcal{B}_8^3\rvert \geqslant 16 \cdot 896 = 14\,336$, следует из [29]; $\lvert\mathcal{B}_8^4\rvert \geqslant 16 \cdot 384 = 6\,144$, следует из [29];

Таблица 5. Оценки числа k-бент-функций от малого числа переменных.

Несложно теперь заметить, что множество из 28-ми графов квадратичных частей 1-бент-функций разбивается на четыре множества. Одно состоит из четырех указанных выше графов, отвечающих 2-бент-функциям при любом разбиении переменных на пары, и остальные три множества содержат по восемь графов, отвечающих 2-бент-функциям при каждом из трех таких возможных разбиений в отдельности.

В таблице 5 приводится та весьма скромная информация о числе k-бент-функций при малых значениях m, которая известна в настоящий момент. Результаты по 1-бент-функциям и оценки их числа при любом m можно найти в [19] и [78].

4.7 Индуктивный способ построения k-бент-функций

Приведем индуктивную конструкцию k-бент-функций от произвольного числа переменных. А именно с помощью заданной k-бент-функции построим k-бент-функции и $(k+1)$-бент-функции от большего числа переменных, см. соответственно утверждения 16 и 17.

Утверждение 16. *Пусть $m, r \in \mathbb{N}$ четны, $k \in \mathbb{N}$ такое, что $1 \leqslant k \leqslant m/2$, и пусть функция $f \in \mathcal{F}_{m+r}$ представима в виде*

$$f(\mathbf{u}', \mathbf{u}'') = p(\mathbf{u}') \oplus q(\mathbf{u}'') \text{ для любых } \mathbf{u}' \in \mathbb{Z}_2^m,\ \mathbf{u}'' \in \mathbb{Z}_2^r,$$

где $p \in \mathcal{F}_m$, $q \in \mathcal{F}_r$ — функции с непересекающимися множествами переменных. Тогда функция f принадлежит классу $\mathcal{B}_{m+r}^k$, если и только если $p \in \mathcal{B}_m^k$, $q \in \mathcal{B}_r^1$.

Доказательство. Для произвольных $\mathbf{v}' \in \mathbb{Z}_2^m$, $\mathbf{v}'' \in \mathbb{Z}_2^r$ и любого $\ell = 1, \ldots, k$ рассмотрим коэффициент $W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'')$. Используя пункт (iv) утверждения 12, несложно убедиться в справедливости

$$\langle (\mathbf{u}', \mathbf{u}''), (\mathbf{v}', \mathbf{v}'') \rangle_\ell = \langle \mathbf{u}', \mathbf{v}' \rangle_\ell \oplus \langle \mathbf{u}'', \mathbf{v}'' \rangle.$$

Тогда из разложения $f(\mathbf{u}', \mathbf{u}'') = p(\mathbf{u}') \oplus q(\mathbf{u}'')$ следует, что

$$W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'') = W_p^{(\ell)}(\mathbf{v}') \cdot W_q(\mathbf{v}'').$$

Если $p \in \mathcal{B}_m^k$, $q \in \mathcal{B}_r^1 = \mathcal{B}_r$, то, очевидно, $|W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'')| = 2^{m/2} \cdot 2^{r/2} = 2^{(m+r)/2}$ для любого ℓ, $1 \leqslant \ell \leqslant k$, и следовательно, функция f принадлежит классу $\mathcal{B}_{m+r}^k$. С другой стороны, пусть $f \in \mathcal{B}_{m+r}^k$. Для каждого ℓ, $1 \leqslant \ell \leqslant k$, выберем векторы $\mathbf{v}'_\ell$, $\mathbf{v}''$ такими, чтобы значения $|W_p^{(\ell)}(\mathbf{v}'_\ell)|$ и $|W_q(\mathbf{v}'')|$ были максимальны. Тогда из соответствующих равенств Парсеваля получаем

$$|W_p^{(\ell)}(\mathbf{v}'_\ell)| \geqslant 2^{m/2}, \ |W_q(\mathbf{v}'')| \geqslant 2^{r/2}.$$

С учетом того, что верно $|W_f^{(\ell)}(\mathbf{v}'_\ell, \mathbf{v}'')| = 2^{(m+r)/2}$, имеем $|W_p^{(\ell)}(\mathbf{v}'_\ell)| = 2^{m/2}$, $|W_q(\mathbf{v}'')| = 2^{r/2}$ для каждого ℓ, $1 \leqslant \ell \leqslant k$, что выполняется тогда и только тогда, когда $p \in \mathcal{B}_m^k$ и $q \in \mathcal{B}_r = \mathcal{B}_r^1$. Утверждение 16 доказано. $\square$

Напомним, что булева функция называется *симметрической*, если она постоянна на каждом множестве векторов одного веса. Множество всех таких функций от двух переменных обозначим через $\mathcal{F}_2^1$ (смысл этого обозначения будет раскрыт в разделе 4.8).

Утверждение 17. *Пусть $m \in \mathbb{N}$ четно, $k \in \mathbb{N}$ такое, что $1 \leqslant k \leqslant m/2$, и пусть функция $f \in \mathcal{F}_{m+2}$ представима в виде*

$$f(a, a', \mathbf{u}) = s(a, a') \oplus p(\mathbf{u}) \text{ для любых } a, a' \in \mathbb{Z}_2, \ \mathbf{u} \in \mathbb{Z}_2^m,$$

где $s \in \mathcal{F}_2^1$, $p \in \mathcal{F}_m$ — функции с непересекающимися множествами переменных. Тогда функция f принадлежит классу $\mathcal{B}_{m+2}^{k+1}$, если и только если $s \in \mathcal{B}_2^1$, $p \in \mathcal{B}_m^k$.

Доказательство. Рассмотрим коэффициент $W_f^{(\ell+1)}(b, b', \mathbf{v})$, где $\ell \in \mathbb{N}$, $1 \leqslant \ell \leqslant k$, и элементы $b, b' \in \mathbb{Z}_2$, $\mathbf{v} \in \mathbb{Z}_2^m$ — любые. Используя разложение $f(a, a', \mathbf{u}) = s(a, a') \oplus p(\mathbf{u})$, имеем

$$W_f^{(\ell+1)}(b, b', \mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{p(\mathbf{u})} \sum_{a, a' \in \mathbb{Z}_2} (-1)^{\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{\ell+1} \oplus s(a, a')}.$$

Пусть для каждой пары векторов $\mathbf{u}, \mathbf{v}$ параметр $\varepsilon \in \mathbb{Z}_2$ однозначно определяется равенством $\varepsilon = \langle \mathbf{u}, \mathbf{v} \rangle_\ell \oplus \langle \pi_\ell(\mathbf{u}), \mathbf{v} \rangle_\ell \oplus 1$. Согласно пункту (vi) утверждения 12 выполняется равенство

$$\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{\ell+1} = \langle \mathbf{u}, \mathbf{v} \rangle_\ell \oplus \langle (a, a'), (b, b') \rangle_\varepsilon,$$

и следовательно,

$$W_f^{(\ell+1)}(b, b', \mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_\ell \oplus p(\mathbf{u})} \cdot W_s^{(\varepsilon)}(b, b').$$

Поскольку функция s является симметрической, нетрудно проверить, что для любых $b, b' \in \mathbb{Z}_2$ и любого ε имеет место равенство $W_s^{(\varepsilon)}(b, b') = W_s(b, b')$. Таким образом, для каждого ℓ, $1 \leqslant \ell \leqslant k$, справедливо равенство

$$W_f^{(\ell+1)}(b, b', \mathbf{v}) = W_s(b, b') \cdot W_p^{(\ell)}(\mathbf{v}).$$

Рассуждая далее так же как в доказательстве утверждения 16, получаем требуемое. Утверждение 17 доказано. □

Непосредственно из утверждений 16 и 17 вытекает

Теорема 57. . *Пусть числа $m, r \geqslant 0$ четны, $j \geqslant 0$ — любое, k такое, что $1 \leqslant k \leqslant m/2$, и пусть функция $f \in \mathcal{F}_{2j+m+r}$ представима в виде*

$$f(a_1, a'_1, \ldots, a_j, a'_j, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^{j} s_i(a_i, a'_i) \right) \oplus p(\mathbf{u}') \oplus q(\mathbf{u}''),$$

где $s_1, \ldots, s_j \in \mathcal{F}_2^1, p \in \mathcal{F}_m$ и $q \in \mathcal{F}_r$ — функции с непересекающимися множествами переменных. Тогда f принадлежит классу $\mathcal{B}_{2j+m+r}^{j+k}$, если и только если $s_1, \ldots, s_j \in \mathcal{B}_2^1$, $p \in \mathcal{B}_m^k$ и $q \in \mathcal{B}_r^1$.

Следствие 4. *Множество $\mathcal{B}_m^k$ непусто при любом четном m и любом целом k, $1 \leqslant k \leqslant m/2$.*

Доказательство. Рассмотрим любые функции $s_1, \ldots, s_{m/2}$ из $\mathcal{F}_2^1 \cap \mathcal{B}_2^1$. Нетрудно видеть, что класс $\mathcal{F}_2^1 \cap \mathcal{B}_2^1$ состоит из следующих четырех функций от переменных v_1, v_2:

$$v_1 v_2, \ v_1 v_2 \oplus 1, \ v_1 v_2 \oplus v_1 \oplus v_2, \ v_1 v_2 \oplus v_1 \oplus v_2 \oplus 1.$$

Тогда функция $f \in \mathcal{F}_m$ такая, что $f(a_1, a'_1, \ldots, a_{m/2}, a'_{m/2}) = \bigoplus_{i=1}^{m/2} s_i(a_i, a'_i)$, согласно теореме 57 принадлежит классу $\mathcal{B}_m^{m/2}$, и следовательно, каждому классу $\mathcal{B}_m^k$. Следствие 4 доказано. $\square$

Радиусом покрытия двоичного кода называется максимальное расстояние, на которое может быть удален от этого кода двоичный вектор. В общем случае задача нахождения радиуса покрытия произвольного кода типа Адамара длины 2^m (и даже линейного кода Адамара при нечетном m) является открытой, см. некоторые результаты в этом направлении в монографии [19] и работе [132]. Заметим, что согласно следствию 4 радиус покрытия каждого кода A_m^k равен $2^{m-1} - 2^{(m/2)-1}$.

Следствие 5. *При любом четном $m \geqslant 4$ имеют место строгие включения*

$$\mathcal{B}_m^1 \supset \mathcal{B}_m^2 \supset \cdots \supset \mathcal{B}_m^{m/2}.$$

Доказательство. При любом k, $1 \leqslant k \leqslant (m-2)/2$, покажем, что множество $\mathcal{B}_m^k \setminus \mathcal{B}_m^{k+1}$ непусто. Выберем произвольно функцию $\psi \in \mathcal{B}_4^1 \setminus \mathcal{B}_4^2$ (такие функции согласно пункту 4.6 существуют). Пусть $k = 1$. Тогда для любой функции $q \in \mathcal{B}_{m-4}^1$ функция $f \in \mathcal{F}_m$ такая, что $f(\mathbf{u}', \mathbf{u}'') = \psi(\mathbf{u}') \oplus q(\mathbf{u}'')$, по теореме 57 принадлежит множеству $\mathcal{B}_m^1 \setminus \mathcal{B}_m^2$. Пусть далее $k > 1$. Выберем произвольные функции $s_1, \ldots, s_{k-1}$ из множества $\mathcal{F}_2^1 \cap \mathcal{B}_2^1$ и функцию q из множества $\mathcal{B}_{m-2k-2}^1$. Тогда функция $f \in \mathcal{F}_m$, заданная равенством $f(a_1, a'_1, \ldots, a_{k-1}, a'_{k-1}, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^{k-1} s_i(a_i, a'_i)\right) \oplus \psi(\mathbf{u}') \oplus q(\mathbf{u}'')$, является k-бент-функцией, но не принадлежит классу $\mathcal{B}_m^{k+1}$. Следствие 5 доказано. $\square$

Пусть $m \geqslant 4$. Известно (см. например, [19]), что степень нелинейности произвольной бент-функции от m переменных не превышает $m/2$, и для любого d, $2 \leqslant d \leqslant m/2$, существует бент-функция $f \in \mathcal{B}_m$ такая, что $\deg f = d$. Для k-бент-функций имеет место

Следствие 6. *При любом четном m, $m \geqslant 4$, и произвольном $k \in \mathbb{N}$, $1 \leqslant k \leqslant m/2$, существуют k-бент-функции с любой степенью нелинейности d такой, что $2 \leqslant d \leqslant \max\{2, \frac{m}{2} - k + 1\}$.*

Доказательство. Случай $k = 1$ совпадает со случаем обычных бент-функций и не рассматривается. Пусть $2 \leqslant k \leqslant (m-2)/2$. Для любого d, $2 \leqslant d \leqslant \frac{m}{2} - k + 1$, существует функция $p \in \mathcal{B}^1_{m-2k+2}$ такая, что $\deg p = d$. Тогда по теореме 57 для произвольных функций $s_1, \ldots, s_{k-1}$ из множества $\mathcal{F}_2^1 \cap \mathcal{B}_2^1$ функция $f \in \mathcal{F}_m$, заданная равенством $f(a_1, a'_1, \ldots, a_{k-1}, a'_{k-1}, \mathbf{u}) = \left(\bigoplus_{i=1}^{k-1} s_i(a_i, a'_i)\right) \oplus p(\mathbf{u})$, является k-бент-функцией, причем $\deg f = d$. При $k = m/2$ функция $\bigoplus_{i=1}^{m/2} s_i(a_i, a'_i)$, где $s_i \in \mathcal{F}_2^1 \cap \mathcal{B}_2^1$, $i = 1, \ldots, m/2$, является примером $m/2$-бент-функции степени 2. Следствие 6 доказано. □

Вопрос о существовании k-бент-функций со степенью нелинейности выше чем $\frac{m}{2} - k + 1$ остается открытым. Пользуясь следствием 6, можно убедиться в том, что известный класс $\mathcal{HB}_m$ гипер-бент-функций [205] не совпадает ни с одним из классов $\mathcal{B}_m^k$, $1 \leqslant k \leqslant m/2$ (это вытекает из того, что степень нелинейности произвольной гипер-бент-функции от m переменных равна $m/2$, см. [12, 85]).

Как уже отмечалось ранее, мощность класса $\mathcal{B}_m^1$ всех бент-функций от m переменных не известна. Для k-бент-функций непосредственно из теоремы 57 получаем

Следствие 7. *При четном m и любом k, $1 \leqslant k \leqslant m/2$, справедливо неравенство $|\mathcal{B}_m^k| \geqslant 4|\mathcal{B}_{m-2}^{k-1}|$.*

Например для $m = 8$ имеем:

$|\mathcal{B}_8^1| > 2^{70,4}$ (согласно [43]),

$|\mathcal{B}_8^2| > 2^{34,3}$ (как следует из [179], где установлено, что $|\mathcal{B}_6^1| > 2^{32,3}$),

$|\mathcal{B}_8^3| \geqslant 7 \cdot 2^{11}$ (в начале раздела было отмечено, что $|\mathcal{B}_4^1| = 896$),

$|\mathcal{B}_8^4| \geqslant 2^9$ (поскольку $|\mathcal{B}_2^1| = 8$).

Однако даже для $m = 4$ оценка следствия 7 является весьма грубой: имеем $|\mathcal{B}_4^2| \geqslant 32$, хотя точное значение $|\mathcal{B}_4^2|$ равно 384.

4.8 Взаимосвязь k-бент-функций с бент-функциями

Обозначим через $S_{m,k}$ подгруппу группы S_m подстановок на m координатах, порожденную k транспозициями: $(1,2),(3,4),\ldots,(2k-1,2k)$. Очевидно, что группы $S_{m,k}$ и $\mathbb{Z}_2^k$ изоморфны. Для произвольного вектора $\mathbf{w} \in \mathbb{Z}_2^k$ определим подстановку $\sigma_k^{\mathbf{w}}$ на m координатах равенством

$$\sigma_k^{\mathbf{w}} = (1,2)^{w_1} \cdot (3,4)^{w_2} \cdot \ldots \cdot (2k-1,2k)^{w_k},$$

где $(i,j)^0$ обозначает тождественную подстановку. Заметим, что $\pi_k \equiv \sigma_k^{\mathbf{1}}$. Пусть $\mathcal{F}_m^k$ обозначает множество всех функций $f \in \mathcal{F}_m$, постоянных на каждой орбите множества $\mathbb{Z}_2^m$ под действием группы $S_{m,k}$. Поскольку количество орбит множества $\mathbb{Z}_2^m$ равно $3^k 2^{m-2k}$, то справедливо равенство $|\mathcal{F}_m^k| = 2^{3^k 2^{m-2k}} = 2^{2^{m-k\log_2 \frac{4}{3}}}$. Покажем, что на каждом множестве функций $\mathcal{F}_m^k$ понятия k-бент-функции и бент-функции совпадают. А именно верна следующая теорема.

Теорема 58. *При любом четном $m \geqslant 2$ и любом целом k, $1 \leqslant k \leqslant m/2$, справедливо равенство $\mathcal{F}_m^k \cap \mathcal{B}_m^k = \mathcal{F}_m^k \cap \mathcal{B}_m^1$.*

Доказательство. С помощью утверждения 12 найдем следующее представление для произведения $\langle \mathbf{u}, \mathbf{v} \rangle_\ell$, где $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ — произвольные векторы и ℓ такое, что $1 \leqslant \ell \leqslant k$. Определим вектор $\mathbf{w} \in \mathbb{Z}_2^\ell$, зависящий от выбранных векторов $\mathbf{u}, \mathbf{v}$, следующим образом: для каждого $i = 1, \ldots, \ell$ положим

$$w_i = \langle (u_{2i+1}, \ldots, u_m), (v_{2i+1}, \ldots, v_m) \rangle_{\ell-i}$$
$$\oplus \langle \pi_{\ell-i}(\,(u_{2i+1}, \ldots, u_m)\,), (v_{2i+1}, \ldots, v_m) \rangle_{\ell-i} \oplus 1,$$

если $i < \ell$, и пусть $w_\ell = 1$. Тогда в силу пункта (vi) утверждения 12 справедливо равенство

$$\langle \mathbf{u}, \mathbf{v} \rangle_\ell = \left(\bigoplus_{i=1}^{\ell} \langle (u_{2i-1}, u_{2i}), (v_{2i-1}, v_{2i}) \rangle_{w_i} \right) \oplus \langle (u_{2\ell+1}, \ldots, u_m), (v_{2\ell+1}, \ldots, v_m) \rangle$$

(здесь мы считаем, что в случае $\ell = m/2$ последнее слагаемое отсутствует). Отсюда, используя пункты (iv) и (v) утверждения 12, получаем

$$\langle \mathbf{u}, \mathbf{v} \rangle_\ell = \langle \sigma_\ell^{\mathbf{w}}(\mathbf{u}), \mathbf{v} \rangle.$$

Заметим, что если вектор $\mathbf{v} \in \mathbb{Z}_2^m$ фиксирован, а вектор $\mathbf{u}$ пробегает пространство $\mathbb{Z}_2^m$, то вектор $\sigma_\ell^{\mathbf{w}}(\mathbf{u})$ также принимает все возможные значения из $\mathbb{Z}_2^m$. Действительно, предположим обратное. Пусть векторы $\mathbf{u}, \mathbf{u}' \in \mathbb{Z}_2^m$ различны, $\mathbf{w}, \mathbf{w}'$ — соответствующие им векторы из $\mathbb{Z}_2^\ell$, и пусть $\sigma_\ell^{\mathbf{w}}(\mathbf{u}) = \sigma_\ell^{\mathbf{w}'}(\mathbf{u}')$. Очевидно, что векторы $\mathbf{u}, \mathbf{u}'$ могут различаться только в первых 2ℓ координатах. Обозначим через j, $1 \leqslant j \leqslant \ell$, номер последней пары координат $(2j-1, 2j)$ такой, что векторы $\mathbf{u}, \mathbf{u}'$ различаются хотя бы в одной координате из этой пары (в действительности — в обеих координатах). Заметим, что всегда $j < m/2$. Тогда $w_j \neq w'_j$ согласно предположению, что невозможно, поскольку $u_{2j+1} = u'_{2j+1}, \ldots, u_m = u'_m$. Таким образом, из неравенства $\mathbf{u} \neq \mathbf{u}'$ следует, что $\sigma_\ell^{\mathbf{w}}(\mathbf{u}) \neq \sigma_\ell^{\mathbf{w}'}(\mathbf{u}')$.

Пусть $f \in \mathcal{F}_m^k \cap \mathcal{B}_m^1$. Рассмотрим коэффициент $W_f^{(\ell)}(\mathbf{v})$ для произвольного $\mathbf{v} \in \mathbb{Z}_2^m$. С учетом сделанных выше замечаний получаем

$$W_f^{(\ell)}(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \sigma_\ell^{\mathbf{w}}(\mathbf{u}), \mathbf{v} \rangle \oplus f(\mathbf{u})}.$$

Поскольку $f(\mathbf{u}) = f(\sigma_\ell^{\mathbf{w}}(\mathbf{u}))$ для любых $\mathbf{u}, \mathbf{w}$, имеем

$$W_f^{(\ell)}(\mathbf{v}) = \sum_{\mathbf{u}' \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}', \mathbf{v} \rangle \oplus f(\mathbf{u}')}, \text{ где } \mathbf{u}' = \sigma_\ell^{\mathbf{w}}(\mathbf{u}),$$

и следовательно, $W_f^{(\ell)}(\mathbf{v}) = W_f(\mathbf{v})$ для каждого $\ell = 1, \ldots, k$. Теорема 58 доказана. □

Несложно, однако, показать, что функциями из $\mathcal{F}_m^k \cap \mathcal{B}_m^1$ весь класс $\mathcal{B}_m^k$ не исчерпывается. Интересным для дальнейшего исследования представляется вопрос о том, при каких значениях k функции из известных классов бент-функций являются k-бент-функциями. Другими словами, насколько сильно нелинейными (в данном смысле) они являются?

Глава 5

Квадратичные аппроксимации в блочных шифрах

В данной главе исследуется возможность квадратичного криптоанализа блочных шифров (в основу которого положены квадратичные аппроксимации специального вида) и роль k-бент-функций при конструировании таких шифров. Квадратичный криптоанализ является нелинейной модификацией известного метода линейного криптоанализа блочных шифров, предложенного М. Мацуи [154] в 1993 году и являющегося в настоящее время одним из наиболее часто применяемых.

5.1 Линейный криптоанализ и его модификации

В данном разделе представлен обзор результатов по линейному криптоанализу (ЛК) блочных шифров, попыткам его нелинейного обобщения и описанию идеи квадратичного криптоанализа.

5.1.1 Линейный криптоанализ

Метод линейного криптоанализа для блочного шифра FEAL был предложен М. Мацуи и А. Ямагиши [156] в 1992 году, для шифра DES — М. Мацуи [154] в 1993 году; в настоящее время этот метод наряду с методом дифференциального криптоанализа [55] считается одним из наиболее эффектив-

ных.

Идея метода состоит в следующем. Сначала для известного алгоритма шифрования определяется линейное соотношение L на биты открытого текста, шифротекста и ключа, выполняющееся с вероятностью $p = 1/2 + \varepsilon$, достаточно сильно отличающейся от $1/2$. Число ε называется *преобладанием* соотношения L. Затем при фиксированном неизвестном ключе K криптоаналитиком собирается статистика из N пар {открытый текст — соответствующий шифротекст}, и на ее основе с учетом знака ε производится различение двух простых статистических гипотез: выполняется ли соотношение L для данного неизвестного ключа K или нет. В результате для битов ключа K устанавливается новое вероятностное соотношение. Для надежной работы этого метода мощность статистики N должна быть пропорциональна величине $|\varepsilon|^{-2}$.

Большое число работ посвящено различным обобщениям и применениям метода ЛК. Перечислим некоторые из них. Детальное исследование метода ЛК (в частности для DES) провела К. Ниберг [168]; см. также работы [121, 64, 155]. В 1995 году авторы [99] ввели понятие *матрицы корреляций* произвольного булева отображения из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2^m$, удобное для описания его свойств, относящихся к линейному криптоанализу. Для повышения эффективности метода ЛК в [130] было предложено для одной комбинации битов ключа рассматривать одновременно несколько линейных аппроксимаций; эту тему продолжает работа [56]. Авторы [186] привели способ улучшения метода ЛК (в частности для шифра LOKI91), предложив учитывать при аппроксимации вероятностное поведение некоторых битов вместо их фиксированных значений. К числу последних работ о развитии метода ЛК можно отнести [48] и [189].

Серия работ посвящена вопросам стойкости различных алгоритмов шифрования к методу линейного криптоанализа. Л. Кнудсен [137] рассматривал вопросы построения схем шифрования типа Фейстеля, стойких к методам линейного и дифференциального криптоанализа. В. В. Шорин, В. В. Же-

лезняков, Э. М. Габидулин [191] доказали в 2001 году стойкость к этим методам российского алгоритма ГОСТ 28147-89 (с не менее, чем пятью раундами шифрования — при линейном криптоанализе и семью раундами — при дифференциальном). Исследования стойкости шифров RC5, RC6, IDEA, Serpent, AES, Blowfish, Khufu к методу ЛК см. в работах [58, 122, 54, 152, 164].

5.1.2 Проблемы нелинейного криптоанализа

Общий подход к использованию в линейном криптоанализе нелинейных аппроксимаций предложили в 1996 году Л. Кнудсен и М. Робшау [138]. Основная идея его проста: обогатить класс аппроксимирующих функций нелинейными функциями и за счет этого повысить качество аппроксимации. Но при этом криптоаналитику придется столкнуться со следующими трудностями.

Как эффективно выбрать хорошую нелинейную аппроксимацию? В линейном случае возможно решение такой задачи перебором всех 2^m линейных функций от m переменных. В общем случае полный перебор 2^{2^m} булевых функций неосуществим даже при малых значениях m.

Как объединить нелинейные аппроксимации отдельных раундов? Рассмотрим простой пример. Пусть i-й раунд шифрования, переводящий промежуточный шифротекст $C^{(i-1)}$ в $C^{(i)}$, устроен таким образом:

$$C^{(i)} = S^i(C^{(i-1)} \oplus K^{(i)}),$$

где $K^{(i)}$ — подключ i-го раунда, S^i — известное нелинейное преобразование. Пусть криптоаналитик установил приближение преобразования S^i функцией f^i, т. е. с достаточно высокой вероятностью выполняется равенство $S^i(\mathbf{x}) = f^i(\mathbf{x})$ для произвольного $\mathbf{x}$. Тогда, если функция f^i линейна, то для i-го раунда имеем приближение $C^{(i)} = f^i(C^{(i-1)} \oplus K^{(i)}) = f^i(C^{(i-1)}) \oplus f^i(K^{(i)})$. Поскольку зависимость от блока $C^{(i-1)}$ и подключа $K^{(i)}$ здесь выделена явно, такое приближение i-го раунда может участво-

вать в общей цепочке раундовых приближений. В общем случае объединение раундовых приближений затруднено.

В направлении решения первой проблемы можно отметить исследования Т. Шимоямы и Т. Канеко [190], связанные с поиском квадратичных соотношений для конкретных подстановок, использующихся в S-блоках DES; экспериментальные исследования Дж. Накахары и др. [165]; работу Ж. Тапиадора и др. [198] по применению эвристических алгоритмов для поиска хороших нелинейных аппроксимаций (с примерами для S-блоков шифра MARS). Вероятностные аспекты приближения случайной булевой функции множеством всех квадратичных функций исследовались Б. В. Рязановым и С. И. Чечетой в [25]. Вопросы нелинейных аппроксимаций булевых функций (с использованием их приведенного представления) рассматривались А. В. Ивановым [6, 7]. Работы, направленные на решение второй проблемы, автору не известны. В целом метод нелинейного криптоанализа не получил пока должного развития.

5.1.3 Квадратичный криптоанализ

В данной главе исследуются возможности квадратичного криптоанализа блочных шифров, в основу которого положены квадратичные аппроксимации специального вида. Будем аппроксимировать булевы функции функциями вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$ от m переменных $v_1, \ldots, v_m$, где π — любая перестановка на m координатах, параметры $\mathbf{u} \in \mathbb{Z}_2^m, k$ $(1 \leqslant k \leqslant m/2)$ произвольны. Множество таких функций состоит из 2^m (т. е. всех) линейных функций и не более чем $2^{m(1+\log_2 m)}$ квадратичных функций, что не ограничивает криптоаналитика в возможности их полного перебора. Выбор таких функций обусловлен наличием простых формул для вычисления расстояния Хэмминга от произвольной булевой функции до класса функций $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$ при фиксированных π и k, а также свойствами таких функций, близкими к линейным.

Исследования носят теоретический характер. Предложены модифика-

ции алгоритмов 1 и 2 линейного криптоанализа Мацуи [154] для расширенного класса аппроксимирующих функций. Приведены формулы для вычисления абсолютных значений преобладаний и надежности алгоритмов. Показано, что использование k-бент-функций в качестве функций шифрования позволяет снижать максимальное абсолютное значение преобладания до его минимального значения, а следовательно максимально повышать стойкость шифра к данным квадратичным аппроксимациям. Рассмотрены примеры четырехразрядных подстановок, рекомендованных для применения в узлах замены (S-*блоках*) алгоритмов ГОСТ 28147-89, DES, s^3DES; с помощью компьютера показано, что для всех этих подстановок (кроме одной) существуют более вероятные (по сравнению с линейными) квадратичные соотношения специального вида на входные и выходные биты этих подстановок. Рассмотрены свойства аппроксимирующих функций, которые могут быть использованы при согласовании нелинейных раундовых аппроксимаций.

5.2 Класс аппроксимирующих функций Δ_m

Рассмотрим следующий класс булевых функций от переменных $v_1, \ldots, v_m$, где m четно. Для любого k, $1 \leqslant k \leqslant m/2$, и произвольной перестановки $\pi \in S_m$ на m переменных пусть

$$\mathfrak{A}^k_{m,0}(\pi) = \{\langle \mathbf{u}, \pi(\mathbf{v})\rangle_k \,|\, \mathbf{u} \in \mathbb{Z}_2^m\}.$$

Заметим, что для любой перестановки $\pi \in S_m$ множество $\mathfrak{A}^1_{m,0}(\pi)$ состоит из всех линейных функций. Булевы функции от переменных $v_1, \ldots, v_m$, использующиеся при шифровании, будем аппроксимировать функциями из множества

$$\Delta_m = \bigcup_{1 \leqslant k \leqslant m/2} \bigcup_{\pi \in S_m} \mathfrak{A}^k_{m,0}(\pi),$$

которое всюду далее называем *классом аппроксимирующих функций*. Говоря неформально, за счет произвольных перестановок π на переменных

$v_1, \ldots, v_m$ мы снимаем «неравноправие» этих переменных в функции $\langle \mathbf{u}, \mathbf{v} \rangle_k$.

Определим мощность класса Δ_m и способ перечисления его элементов. Основную трудность здесь представляет тот факт, что множества $\mathfrak{A}^{k'}_{m,0}(\pi')$ и $\mathfrak{A}^{k''}_{m,0}(\pi'')$, вообще говоря, имеют непустое пересечение.

Для булевой функции $f \in \mathcal{F}_m$ пусть множество АНФ(f) состоит из всех одночленов ее алгебраической нормальной формы. Например, для функции $g(v_1, v_2, v_3, v_4) = v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_3v_4 \oplus v_2 \oplus v_3 \oplus 1$ имеем АНФ$(g) = \{v_1v_2,\ v_1v_3,\ v_1v_4,\ v_2v_3,\ v_3v_4,\ v_2,\ v_3,\ 1\}$. При фиксированной перестановке $\pi \in S_m$ через f^π обозначим булеву функцию, заданную равенством $f^\pi(\mathbf{v}) = f(\pi(\mathbf{v}))$. Переменные булевой функции $f \in \mathcal{F}_m$ разобьем на пары; паре $\{v_{2i-1}, v_{2i}\}$ сопоставим номер i. Через $\mathrm{Act}(f)$ обозначим подмножество максимальной мощности множества $\{1, 2, \ldots, m/2\}$ такое, что для любых различных элементов i, j из $\mathrm{Act}(f)$ одночлены

$$v_{2i-1}v_{2j-1},\ v_{2i-1}v_{2j},\ v_{2i}v_{2j-1},\ v_{2i}v_{2j}$$

принадлежат множеству АНФ(f). Будем говорить, что пара переменных с номером i *активна* для f, если $i \in \mathrm{Act}(f)$. Заметим, что мощность $\mathrm{Act}(f)$ для любой функции f либо нулевая, либо не меньше двух. Через $\rho = \rho(f)$ обозначим любую перестановку из S_m такую, что $|\mathrm{Act}(f^\rho)| = \max\limits_{\pi \in S_m} |\mathrm{Act}(f^\pi)|$. Рассмотрим, например, множество $\mathrm{Act}(g)$ для функции g, заданной выше. Поскольку одночлены $v_1v_3,\ v_1v_4,\ v_2v_3$ принадлежат АНФ(g), а одночлен v_2v_4 — нет, имеем $\mathrm{Act}(g) = \varnothing$. Однако, при $\rho = (1, 3, 2, 4)$ имеем $\mathrm{Act}(g^\rho) = \{1, 2\}$.

Теорема 59. *Булева функция $f \in \mathcal{F}_m$, степени не больше двух, такая что $f(\mathbf{0}) = 0$, принадлежит классу Δ_m тогда и только тогда, когда f удовлетворяет условиям*

1) *для любых различных чисел i, j $(1 \leqslant i, j \leqslant m/2)$ одночлены*

$$v_{2i-1}v_{2j-1},\ v_{2i-1}v_{2j},\ v_{2i}v_{2j-1},\ v_{2i}v_{2j}$$

одновременно принадлежат / не принадлежат множеству АНФ(f^ρ);

2) *множество* $\text{АНФ}(f^\rho)$ *не содержит одночлены вида* $v_{2i-1}v_{2i}$*;*

3) *в точности одна из переменных* v_{2i-1}, v_{2i} *принадлежит* $\text{АНФ}(f^\rho)$ *для каждого элемента* $i \in \text{Act}(f^\rho)$.

Доказательство. ($\Longleftarrow$) Пусть функция f степени не больше двух, $f(\mathbf{0}) = 0$, удовлетворяет условиям 1), 2), 3) теоремы. Если множество $\text{Act}(f^\rho)$ пусто, то функция f, согласно 1) и 2) линейна и, следовательно, принадлежит множеству Δ_m.

Предположим далее, что множество $\text{Act}(f^\rho)$ не пусто и имеет вид

$$\text{Act}(f^\rho) = \{i_1, \ldots, i_k\},$$

где $2 \leqslant k \leqslant m/2$. Пусть $j_1, \ldots, j_{(m/2)-k}$ — номера неактивных пар переменных функции f^ρ. Рассмотрим перестановку $\tau \in S_m$ такую, что $\tau(i_s) = s$ для любого $s = 1, \ldots, k$ и $\tau(j_s) = k + s$ для любого $s = 1, \ldots, (m/2) - k$. Переставим пары переменных функции f^ρ согласно τ. А именно рассмотрим функцию $f^{\rho\circ\pi}$ (здесь и далее запись $\rho \circ \pi$ означает, что сначала применяется перестановка ρ, а затем π), где $\pi \in S_m$ задается с помощью τ следующим образом: $\pi(2s-1) = 2\tau(s) - 1$, $\pi(2s) = 2\tau(s)$ для любого $s = 1, \ldots, m/2$. Нетрудно заметить, что условия 1), 2), 3) после замены в каждом из них функции f^ρ на $f^{\rho\circ\pi}$ остаются справедливыми, причем множество $\text{Act}(f^{\rho\circ\pi}) = \{1, \ldots, k\}$ также как и $\text{Act}(f^\rho)$ имеет мощность k. Поэтому далее, без ограничения общности, считаем, что $\text{Act}(f^\rho) = \{1, \ldots, k\}$.

Заметим, что число k согласно условиям 1) и 2) однозначно определяет квадратичную часть функции f^ρ, которая имеет вид

$$\bigoplus_{i=1}^{k-1} \bigoplus_{j=i+1}^{k} (v_{2i-1}v_{2j-1} \oplus v_{2i-1}v_{2j} \oplus v_{2i}v_{2j-1} \oplus v_{2i}v_{2j}). \tag{5.1}$$

Покажем, что функция f^ρ принадлежит множеству $\mathfrak{A}^k_{m,0}$. Рассмотрим вектор $\mathbf{u} \in \mathbb{Z}_2^m$ такой, что

$$u_t = 1 \Longleftrightarrow \begin{cases} v_t \notin \text{АНФ}(f^\rho), & \text{при } t = 1, \ldots, 2k; \\ v_t \in \text{АНФ}(f^\rho), & \text{при } t = 2k+1, \ldots, m. \end{cases}$$

Тогда $f^\rho(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k$. Действительно, по теореме 54 имеем

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \left(\bigoplus_{i=1}^{k-1} \bigoplus_{j=i+1}^{k} Y_i Y_j \right) \oplus \left(\bigoplus_{i=1}^{k} (u_{2i} v_{2i-1} \oplus u_{2i-1} v_{2i}) \right) \oplus \left(\bigoplus_{i=k+1}^{m/2} (u_{2i-1} v_{2i-1} \oplus u_{2i} v_{2i}) \right), \qquad (5.2)$$

где $Y_i = (u_{2i-1} \oplus u_{2i})(v_{2i-1} \oplus v_{2i})$. Используя условие 3) и определение вектора $\mathbf{u}$, получаем $u_{2i-1} \oplus u_{2i} = 1$ при $i = 1, \ldots, k$, а значит $Y_i Y_j = v_{2i-1} v_{2j-1} \oplus v_{2i-1} v_{2j} \oplus v_{2i} v_{2j-1} \oplus v_{2i} v_{2j}$, где $1 \leqslant i < j \leqslant k$. Таким образом, квадратичная часть функции $\langle \mathbf{u}, \mathbf{v} \rangle_k$ совпадает с (5.1). Непосредственно из (5.2) получаем, что линейные части функций f^ρ и $\langle \mathbf{u}, \mathbf{v} \rangle_k$ также совпадают. Следовательно, поскольку $f^\rho(\mathbf{0}) = \langle \mathbf{u}, \mathbf{0} \rangle_k = 0$, и обе функции f^ρ и $\langle \mathbf{u}, \mathbf{v} \rangle_k$ имеют степень 2, они равны. Итак, мы показали, что функция f^ρ принадлежит классу $\mathfrak{A}^k_{m,0}(\mathrm{id})$, где id обозначает тождественную перестановку. Осталось заметить, что справедливо

$$f^\sigma \in \mathfrak{A}^k_{m,0}(\mathrm{id}) \Longleftrightarrow f \in \mathfrak{A}^k_{m,0}(\sigma^{-1}), \text{ для любой перестановки } \sigma \in S_m,$$

что вытекает из следующей эквивалентности:

$$\exists \mathbf{u} : \ f^\sigma(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k \Longleftrightarrow \exists \mathbf{u} : \ f(\mathbf{v}) = \langle \mathbf{u}, \sigma^{-1}(\mathbf{v}) \rangle_k.$$

Отсюда, наконец, заключаем, что функция f принадлежит классу $\mathfrak{A}^k_{m,0}(\rho^{-1})$, а следовательно и классу Δ_m.

($\Longrightarrow$) Если функция f линейна, то выполнение условий 1), 2), 3) очевидно. Пусть f имеет нетривиальную квадратичную часть. Тогда, поскольку f принадлежит некоторому классу $\mathfrak{A}^k_{m,0}(\pi)$, мощность квадратичной части f равна $4 \cdot \binom{s}{2}$ для подходящего s, $2 \leqslant s \leqslant k$, что непосредственно следует из теоремы 54. Так как f^ρ также содержится в классе Δ_m, то $|\mathrm{Act}(f^\rho)| = s$ (например, в качестве ρ можно взять перестановку π^{-1}). Тогда квадратичная часть АНФ(f^ρ) исчерпывается одночленами вида $v_{2i-1} v_{2j-1}$, $v_{2i-1} v_{2j}$, $v_{2i} v_{2j-1}$, $v_{2i} v_{2j}$ для любых различных $i, j \in \mathrm{Act}(f^\rho)$,

и следовательно выполнены условия 1) и 2). Справедливость 3) вытекает из теоремы 54. Теорема доказана. □

Следствие 8. *Для любого четного m справедливо равенство*

$$|\Delta_m| = 2^m \left(1 + \sum_{k=2}^{m/2} \binom{m}{2k} \frac{(2k-1)!!}{2^k}\right).$$

Доказательство. Класс Δ_m содержит ровно 2^m линейных булевых функций. С помощью теоремы 59 для каждого фиксированного k, $2 \leqslant k \leqslant m/2$, определим число квадратичных функций f из Δ_m таких, что $|\mathrm{Act}(f^\rho)| = k$. Каждая такая функция f однозначно определяется множеством из k неупорядоченных пар переменных (после действия соответствующей перестановки ρ все эти пары будут активными) и своей линейной частью. Множество из k неупорядоченных пар можно выбрать

$$\frac{1}{k!}\binom{m}{2}\binom{m-2}{2}\cdots\binom{m-2k+2}{2} = \frac{m!}{2^k k!(m-2k)!}$$

способами. Для любой выбранной пары переменных в точности одна переменная из пары входит в множество АНФ(f) согласно условию 3) теоремы 59. Переменные, не содержащиеся в выбранных парах, входят или не входят в АНФ(f) свободно. Таким образом, число функций $f \in \Delta_m$, $|\mathrm{Act}(f^\rho)| = k$, равно

$$\frac{m!}{2^k k!(m-2k)!} \cdot 2^k \cdot 2^{m-2k} = \binom{m}{2k} 2^{m-k}(2k-1)!!$$

Суммируя по всем k, $2 \leqslant k \leqslant m/2$, и учитывая линейные функции, получаем требуемое выражение для мощности класса Δ_m. □

Например, $|\Delta_4| = 28$, $|\Delta_6| = 904$, $|\Delta_8| = 28\,816$, а число линейных функций в каждом из этих классов равно 16, 64 и 256 соответственно. Из следствия 8 несложно вывести, что величина $|\Delta_m|$ не превышает числа $e2^m m!$,

что заведомо меньше, чем $2^{m(1+\log_2 m)}$. Отметим, что число всех квадратичных функций от m переменных пропорционально величине 2^{m^2} и функции вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$ составляют асимптотически малую их часть при $m \to \infty$.

Теорема 59 и следствие 8 предлагают способ перечисления всех элементов множества Δ_m без повторений.

5.3 Квадратичные аппроксимации в блочных шифрах

Основная идея предлагаемого подхода состоит в расширении области поиска наиболее вероятных соотношений для битов открытого текста, шифротекста и ключа: с множества линейных соотношений на множество линейных и квадратичных соотношений специального вида. В обозначениях будем следовать, в основном, книге [19].

Рассмотрим блочный шифр с r раундами шифрования. Пусть

$m = m_{\text{text}}$ — длина открытого текста и шифротекста;

P — открытый текст, $P \in \mathbb{Z}_2^m$;

m_{key} — длина ключа;

K — ключ шифрования, $K \in \mathbb{Z}_2^{m_{\text{key}}}$;

$F : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m_{\text{key}}} \to \mathbb{Z}_2^m$ — преобразование, взаимно однозначное при любом фиксированном втором аргументе;

$C = F(P, K)$ — шифротекст, $C \in \mathbb{Z}_2^m$;

m'_{key} — длина раундового подключа;

$K^{(i)}$ — подключ i-го раунда шифрования, $K^{(i)} \in \mathbb{Z}_2^{m'_{\text{key}}}$, $1 \leqslant i \leqslant r$, определяемый по ключу K;

$F_i : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m'_{\text{key}}} \to \mathbb{Z}_2^m$ — преобразование i-го раунда шифрования, $1 \leqslant i \leqslant r$, взаимно однозначное, если второй аргумент фиксирован;

$C^{(0)} = P$;

$C^{(i)} = F_i(C^{(i-1)}, K^{(i)})$ — промежуточный шифротекст, $C^{(i)} \in \mathbb{Z}_2^m$, $1 \leqslant i \leqslant r$;

$C = C^{(r)}$ — итоговый шифротекст;

Предполагаем, что все открытые тексты P (как и ключи K) равновероятны. Всюду далее считается, что m, m_{key}, m'_{key} — четные числа.

Первый алгоритм. В основе алгоритма лежит следующее равенство

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = \langle \mathbf{d}, \tau(K) \rangle_k, \tag{5.3}$$

где

$\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^m$, $\mathbf{d} \in \mathbb{Z}_2^{m_{\text{key}}}$ — некоторым образом выбранные векторы;

$\pi, \sigma \in S_m$, $\tau \in S_{m_{\text{key}}}$ — фиксированные перестановки;

i, j, k — целые числа такие, что $1 \leqslant i, j \leqslant m/2$, $1 \leqslant k \leqslant m_{\text{key}}/2$.

Считаем, что равенство (5.3) выполняется с вероятностью $p = 1/2 + \varepsilon$, такой, что $0 < |\varepsilon| \leqslant 1/2$. Число ε назовем *преобладанием* равенства (5.3). Отдельной задачей для каждого конкретного алгоритма шифрования является выбор таких значений параметров $\mathbf{a}, \mathbf{b}, \mathbf{d}, \pi, \sigma, \tau, i, j, k$, чтобы величина $|\varepsilon|$ была по возможности максимальной. В данной работе эта задача рассматриваться не будет. Отметим, что выбор параметров i, j, k отражается на виде соотношения (5.3) следующим образом. Если данный параметр (i, j или k) равен 1, то биты соответствующего блока (открытого текста P, шифротекста C или ключа K) входят в соотношение (5.3) линейно, что может быть использовано при добавлении такого соотношения в линейную систему уравнений. С ростом параметра (i, j или k) пропорционально увеличивается число битов блока, участвующих в нелинейной части соотношения.

Пусть фиксирован ключ шифрования K. Рассмотрим набор

$$\{(P_t, C_t) \mid t = 1, \ldots, N\}$$

известных пар открытого и шифрованного текстов, $C_t = F(P_t, K)$. Следующий алгоритм является модификацией алгоритма Мацуи [154] определения

одного бита ключа, основанного на принципе максимального правдоподобия.

Алгоритм 1

- определяем $N_0 = |\{\ t\ :\ \langle \mathbf{a}, \pi(P_t)\rangle_i \oplus \langle \mathbf{b}, \sigma(C_t)\rangle_j = 0\ \}|$;
- полагаем $\langle \mathbf{d}, \tau(K)\rangle_k = \begin{cases} 0, & \text{если } (N_0 - \frac{N}{2}) \cdot \varepsilon > 0; \\ 1, & \text{в другом случае;} \end{cases}$
- с учетом полученного соотношения подбираем ключ.

Конец алгоритма

Напомним, что *надежностью* ξ_0 алгоритма, основанного на процедуре статистической классификации, называется математическое ожидание вероятности его корректной работы. В данном случае под корректной работой алгоритма понимается установление верного соотношения на биты ключа. При этом предполагается, что искомый ключ выбран во всем пространстве ключей случайно, равновероятно и независимо от набора открытых текстов (см. подробнее [19]). Таким образом,

$$\xi_0 = \mathbf{E}\{\xi(K)\} = \frac{1}{2^{m_{\text{key}}}} \sum_{K \in \mathbb{Z}_2^{m_{\text{key}}}} \xi(K),$$

где $\xi(K)$ — вероятность выбора открытых текстов $P_1, \ldots, P_N$ таких, что будет установлено верное соотношение на биты ключа K. Если $p(K) = 1/2 + \varepsilon(K)$, где $\varepsilon(K) \neq 0$, — вероятность выполнения равенства (5.3) для фиксированного ключа K, то

$$\xi(K) = \sum_{s=0}^{N/2} \binom{N}{s} \left(\frac{1}{2} - |\varepsilon(K)|\right)^s \left(\frac{1}{2} + |\varepsilon(K)|\right)^{N-s}.$$

Надежность ξ_0 алгоритма 1 можно оценить в точности так же как и в случае линейного криптоанализа (с привлечением дополнительных криптографических предположений, см. подробнее [154, 19]) с помощью функции

нормального распределения, а именно

$$\xi_0 \simeq \Phi_{0,1}(-2|\varepsilon|\sqrt{N}) = \int\limits_{-2|\varepsilon|\sqrt{N}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy. \tag{5.4}$$

Приведем формулы для вычисления абсолютных значений преобладаний и выделим те свойства булевых функций, использующихся при шифровании, наличие которых придает шифру стойкость к рассматриваемым квадратичным аппроксимациям.

Для фиксированного ключа K, для любых целых i, j таких, что $1 \leqslant i, j \leqslant m/2$, для произвольных перестановок $\pi, \sigma \in S_m$ обозначим через $\varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K;0)$ действительное число из отрезка $[-1/2, 1/2]$ такое, что вероятность выполнения равенства

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(P,K)) \rangle_j = 0 \tag{5.5}$$

равна $1/2 + \varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K;0)$.

Утверждение 18. *Для любого отображения $F(\cdot, K) : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ и любых перестановок $\pi, \sigma \in S_m$ выполняется равенство*

$$2^{m+1} \cdot \varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K;0) = W^{(i)}_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot),K)) \rangle_j}(\mathbf{a}).$$

Доказательство. Пусть $\mathbb{Z}_2^m = M_0 \cup M_1$, где

$$M_x = \{\mathbf{u} \in \mathbb{Z}_2^m \mid \langle \mathbf{a}, \pi(\mathbf{u}) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(\mathbf{u}, K)) \rangle_j = x\}$$

при $x = 0, 1$. Из определения i-коэффициента Уолша — Адамара $W^{(i)}_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot),K)) \rangle_j}(\mathbf{a})$ следует, что

$$W^{(i)}_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot),K)) \rangle_j}(\mathbf{a}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{a}, \pi(\mathbf{u}) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(\mathbf{u},K)) \rangle_j} = |M_0| - |M_1|.$$

С помощью (5.5) получаем $|M_0| = 2^m(1/2 + \varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K;0))$, и следовательно

$$|M_0| - |M_1| = 2^{m+1} \cdot \varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K;0).$$

Утверждение доказано. □

Напомним, что $\varepsilon(K)$ обозначает преобладание, с которым выполняется равенство (5.3) при фиксированном ключе K. Заметим, что для любых k, $\mathbf{d}$ и τ справедливо

$$|\varepsilon(K)| = |\varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K;0)|. \tag{5.6}$$

Теорема 60. *Пусть фиксирован ключ $K \in \mathbb{Z}_2^{m_{\text{key}}}$. Если вектор $\mathbf{b} \in \mathbb{Z}_2^m$, перестановки $\pi, \sigma \in S_m$ и параметр j, $1 \leqslant j \leqslant m/2$, таковы что функция*

$$\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K))\rangle_j : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$$

является $(m/2)$-бент-функцией, то справедливо равенство

$$\max_{i,k,\mathbf{a},\mathbf{d},\tau} |\varepsilon(K)| = \min_{i,k,\mathbf{a},\mathbf{d},\tau} |\varepsilon(K)| = 2^{-(m/2)-1}.$$

Доказательство. Поскольку функция $\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K))\rangle_j$ принадлежит классу $\mathcal{B}_m^{m/2}$, имеем $|W^{(i)}_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K))\rangle_j}(\mathbf{a})| = \pm 2^{m/2}$ для любого $\mathbf{a} \in \mathbb{Z}_2^m$ и каждого i, $1 \leqslant i \leqslant m/2$. Тогда из утверждения 18 и равенства (5.6) сразу следует, что для любых параметров k, $\mathbf{d}$ и τ все значения $|\varepsilon(K)|$ равны $2^{-(m/2)-1}$, откуда и вытекает требуемое. □

Из неравенства (4.9) следует, что $2^{-(m/2)-1}$ является минимальным возможным значением для $\max_{\mathbf{a} \in \mathbb{Z}_2^m} |\varepsilon(K)|$ при любых фиксированных i, j, k, $\mathbf{b}$, $\mathbf{d}$, π, σ и τ. Согласно теореме 60 это минимальное значение достижимо только при использовании $(m/2)$-бент-функций. Задача построения таких функций представляется автору весьма сложной.

Второй алгоритм. Рассмотрим модификацию улучшенного алгоритма Мацуи [154], основанную на исследовании промежуточных шифротекстов. Пусть выбраны целые числа s_1, s_2, такие, что $0 \leqslant s_1 < s_2 \leqslant r$.

Рассмотрим равенство

$$\langle \mathbf{a}, \pi(C^{(s_1)})\rangle_i \oplus \langle \mathbf{b}, \sigma(C^{(s_2)})\rangle_j = \langle \tau(\mathbf{d}), K\rangle_k, \tag{5.7}$$

где $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^m$, $\mathbf{d} \in \mathbb{Z}_2^{m_{\text{key}}}$ — фиксированные векторы; $\pi, \sigma \in S_m$, $\tau \in S_{m_{\text{key}}}$ — заданные перестановки; i, j, k — целые числа такие, что $1 \leqslant i, j \leqslant m/2$, $1 \leqslant k \leqslant m_{\text{key}}/2$. Будем считать, что (5.7) выполняется с вероятностью $\tilde{p} = 1/2 + \tilde{\varepsilon}$, такой, что $0 < |\tilde{\varepsilon}| \leqslant 1/2$.

Обозначим через $\tilde{K}$ часть битов ключа K, которых достаточно для нахождения значений $\langle \mathbf{a}, \pi(C^{(s_1)}) \rangle_i$ и $\langle \mathbf{b}, \sigma(C^{(s_2)}) \rangle_j$ по известным векторам P и C. Пусть m_{s_1,s_2} — число битов в блоке $\tilde{K}$.

Алгоритм 2

- для каждого $\tilde{K} \in \mathbb{Z}_2^{m_{s_1,s_2}}$ определяем

$$N_0(\tilde{K}) = | \{ t : \langle \mathbf{a}, \pi(C_t^{(s_1)}) \rangle_i \oplus \langle \mathbf{b}, \sigma(C_t^{(s_2)}) \rangle_j = 0 \} |;$$

- упорядочим все векторы из $\mathbb{Z}_2^{m_{s_1,s_2}}$: $\tilde{K}_1, \ldots, \tilde{K}_{2^{m_{s_1,s_2}}}$, так, что

$$\left| \frac{N}{2} - N_0(\tilde{K}_1) \right| \geqslant \ldots \geqslant \left| \frac{N}{2} - N_0(\tilde{K}_{2^{m_{s_1,s_2}}}) \right|;$$

- для каждого q от 1 до $2^{m_{s_1,s_2}}$
  - ▷ полагаем $\langle \mathbf{d}, \tau(K) \rangle_k = \begin{cases} 0, & \text{если } (N_0(\tilde{K}_q) - \frac{N}{2}) \cdot \tilde{\varepsilon} > 0; \\ 1, & \text{в другом случае;} \end{cases}$
  - ▷ с учетом полученного соотношения подбираем ключ.

Конец алгоритма

Надежность алгоритма 2 может быть оценена так же как в случае линейного криптоанализа (см. [154, 19]). Для обеспечения требуемой надежности алгоритма размер статистики N должен быть пропорционален величине $|\tilde{\varepsilon}|^{-2}$.

Как и в случае алгоритма 1 имеет место взаимосвязь между абсолютной величиной преобладания $\tilde{\varepsilon}$, k-коэффициентами Уолша — Адамара и k-бент-функциями.

Набор подключей $K^{(s_1+1)}, \ldots, K^{(s_2)}$ обозначим через $K^{(s_1+1,\ldots,s_2)}$. Пусть отображение $F_{s_1+1,s_2} : \mathbb{Z}_2^m \times \left(\mathbb{Z}_2^{m'_{\text{key}}}\right)^{s_2-s_1} \to \mathbb{Z}_2^m$ задано суперпозицией функций $F_{s_1+1}, \ldots, F_{s_2}$:

$$F_{s_1+1,s_2}(C^{(s_1)}, K^{(s_1+1,\ldots,s_2)}) = \\ F_{s_2}(F_{s_2-1}(\ldots \ (F_{s_1+1}(C^{(s_1)}, K^{(s_1+1)}), K^{(s_1+2)})\ldots), K^{(s_2)}).$$

Тогда выполняется

$$C^{(s_2)} = F_{s_1+1,s_2}(C^{(s_1)}, K^{(s_1+1,\ldots,s_2)}).$$

Аналогично тому, как это было сделано для первого алгоритма, рассмотрим равенство

$$\langle \mathbf{a}, \pi(C^{(s_1)})\rangle_i \oplus \langle \mathbf{b}, \sigma(F_{s_1+1,s_2}(C^{(s_1)}, K^{(s_1+1,\ldots,s_2)}))\rangle_j = 0 \tag{5.8}$$

при фиксированном наборе подключей $K^{(s_1+1,\ldots,s_2)}$. Пусть оно выполняется с вероятностью $1/2 + \tilde{\varepsilon}^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K^{(s_1+1,\ldots,s_2)}; 0)$, где $|\tilde{\varepsilon}^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K^{(s_1+1,\ldots,s_2)}; 0)| \leqslant 1/2$. Аналогично утверждению 18 несложно доказать

Утверждение 19. *Для любого отображения* $F_{s_1+1,s_2}(\cdot, K^{(s_1+1,\ldots,s_2)}) : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ *имеем*

$$2^{m+1} \cdot \tilde{\varepsilon}^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K^{(s_1+1,\ldots,s_2)}; 0) = W^{(i)}_{\langle \mathbf{b}, \sigma(F_{s_1+1,s_2}(\pi^{-1}(\cdot), K^{(s_1+1,\ldots,s_2)}))\rangle_j}(\mathbf{a}).$$

Через $\tilde{\varepsilon}(K)$ обозначим преобладание в равенстве (5.7) при фиксированном K. Тогда при любых параметрах k, $\mathbf{d}$ и τ справедливо

$$|\tilde{\varepsilon}(K)| = |\tilde{\varepsilon}^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}(K^{(s_1+1,\ldots,s_2)}; 0)|, \tag{5.9}$$

если $K^{(s_1+1,\ldots,s_2)}$ является набором подключей ключа K.

Теорема 61. *Пусть фиксирован ключ* $K \in \mathbb{Z}_2^{m_{\text{key}}}$ *и целые числа* s_1, s_2, *где* $0 \leqslant s_1 < s_2 \leqslant r$. *Пусть* $K^{(s_1+1,\ldots,s_2)}$ *— набор подключей ключа* K. *Пусть вектор* $\mathbf{b} \in \mathbb{Z}_2^m$, *перестановки* $\pi, \sigma \in S_m$ *и параметр* j, $1 \leqslant j \leqslant m/2$, *таковы, что функция*

$$\langle \mathbf{b}, \sigma(F_{s_1+1,s_2}(\pi^{-1}(\cdot), K^{(s_1+1,\ldots,s_2)}))\rangle_j : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$$

является $(m/2)$*-бент-функцией. Тогда справедливо равенство*

$$\max_{i,k,\mathbf{a},\mathbf{d},\tau} |\tilde{\varepsilon}(K)| = \min_{i,k,\mathbf{a},\mathbf{d},\tau} |\tilde{\varepsilon}(K)| = 2^{-(m/2)-1}.$$

Так же как и для первого алгоритма из теоремы 61 следует, что использование $(m/2)$-бент-функций в качестве промежуточных функций шифрования позволяет снижать величину $\max_{\mathbf{a}\in\mathbb{Z}_2^m} |\tilde{\varepsilon}(K)|$ до минимума.

5.4 Анализ четырехразрядных подстановок в S-блоках алгоритмов ГОСТ, DES, s^3DES

Известно, что стойкость блочного шифра напрямую зависит от стойкости используемых в нем узлов замены (S-блоков). В данном параграфе рассматриваются примеры четырехразрядных подстановок для S-блоков шифров ГОСТ, DES, s^3DES. С помощью компьютера нами показано, что практически во всех случаях существуют более вероятные (по сравнению с линейными) квадратичные соотношения специального вида на входные и выходные биты этих подстановок.

Пример 1. В книге А. Г. Ростовцева и Е. Б. Маховенко [24] приведена серия экстремальных четырехразрядных подстановок, рекомендованных для S-блоков стандарта ГОСТ 28147-89 (см. подстановки $S^1, \ldots, S^{10}$ в таблице 6). Из каждой подстановки путем умножения ее на аффинные подстановки получается целый класс экстремальных подстановок. Все они выбраны так, чтобы максимально повысить стойкость шифра к методам линейного и дифференциального криптоанализа. Рассмотрим их квадратичные аппроксимации функциями из класса Δ_4.

Каждому двоичному вектору $\mathbf{x} = (x_1, x_2, x_3, x_4)$ сопоставим целое число $\tilde{x} = 8x_1 + 4x_2 + 2x_3 + x_4$ от 0 до 15. Пусть $P = (p_1, p_2, p_3, p_4)$ — двоичные входы, $C = (c_1, c_2, c_3, c_4)$ — двоичные выходы некоторой четырехразрядной подстановки S, т. е. $S(\tilde{P}) = \tilde{C}$. Например, действие подстановки S^2 представлено в таблице 7. Найдем наиболее вероятные квадратичные и ли-

нейные зависимости между входными и выходными битами подстановки S, используя класс функций Δ_4. Согласно следствию 8 число функций в Δ_4 равно 28. Из них 16 — линейные функции, 12 — квадратичные, которые можно перечислить следующим образом:

$$\langle 0101, v_1v_2v_3v_4\rangle_2,\quad \langle 0110, v_1v_2v_3v_4\rangle_2,\quad \langle 1001, v_1v_2v_3v_4\rangle_2,\quad \langle 1010, v_1v_2v_3v_4\rangle_2,$$
$$\langle 0101, v_1v_3v_2v_4\rangle_2,\quad \langle 0110, v_1v_3v_2v_4\rangle_2,\quad \langle 1001, v_1v_3v_2v_4\rangle_2,\quad \langle 1010, v_1v_3v_2v_4\rangle_2,$$
$$\langle 0101, v_1v_4v_2v_3\rangle_2,\quad \langle 0110, v_1v_4v_2v_3\rangle_2,\quad \langle 1001, v_1v_4v_2v_3\rangle_2,\quad \langle 1010, v_1v_4v_2v_3\rangle_2.$$

Для этого мы выбрали все различные множества из двух неупорядоченных пар переменных: $\Big\{\{v_1, v_2\}, \{v_3, v_4\}\Big\}, \Big\{\{v_1, v_3\}, \{v_2, v_4\}\Big\}, \Big\{\{v_1, v_4\}, \{v_2, v_3\}\Big\}$; затем для каждого множества составили четыре квадратичные функции, различающиеся только линейной частью.

$$S^1 = (0, 13, 11, 8, 3, 6, 4, 1, 15, 2, 5, 14, 10, 12, 9, 7)$$
$$S^2 = (0, 1, 9, 14, 13, 11, 7, 6, 15, 2, 12, 5, 10, 4, 3, 8)$$
$$S^3 = (0, 1, 11, 13, 9, 14, 6, 7, 12, 5, 8, 3, 15, 2, 4, 10)$$
$$S^4 = (0, 1, 2, 4, 3, 5, 8, 10, 7, 9, 6, 13, 11, 14, 12, 15)$$
$$S^5 = (0, 1, 11, 2, 8, 6, 15, 3, 14, 10, 4, 9, 13, 5, 7, 12)$$
$$S^6 = (0, 1, 11, 2, 8, 3, 15, 6, 14, 10, 4, 9, 13, 5, 7, 12)$$
$$S^7 = (0, 4, 11, 2, 8, 6, 10, 1, 14, 15, 3, 9, 13, 5, 7, 12)$$
$$S^8 = (0, 4, 11, 2, 8, 3, 15, 1, 14, 10, 6, 9, 13, 5, 7, 12)$$
$$S^9 = (0, 11, 15, 9, 1, 5, 6, 8, 3, 10, 4, 12, 14, 13, 7, 2)$$
$$S^{10} = (0, 7, 10, 14, 9, 1, 13, 8, 12, 2, 11, 15, 3, 5, 4, 6)$$
$$S^{11} = (4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3)$$
$$S^{12} = (8, 2, 11, 13, 4, 1, 14, 7, 5, 15, 0, 3, 10, 6, 9, 12)$$
$$S^{13} = (10, 5, 3, 15, 12, 9, 0, 6, 1, 2, 8, 4, 11, 14, 7, 13)$$
$$S^{14} = (5, 10, 12, 6, 0, 15, 3, 9, 8, 13, 11, 1, 7, 2, 14, 4)$$
$$S^{15} = (3, 9, 15, 0, 6, 10, 5, 12, 14, 2, 1, 7, 13, 4, 8, 11)$$
$$S^{16} = (15, 0, 10, 9, 3, 5, 4, 14, 8, 11, 1, 7, 6, 12, 13, 2)$$
$$S^{17} = (12, 6, 3, 9, 0, 5, 10, 15, 2, 13, 4, 14, 7, 11, 1, 8)$$
$$S^{18} = (13, 10, 0, 7, 3, 9, 14, 4, 2, 15, 12, 1, 5, 6, 11, 8)$$

Таблица 6. 4-Разрядные подстановки, с предельно высокой нелинейностью $NL = 4$.

Таблица 7. Подстановка S^2.

входы				выходы			
p_1	p_2	p_3	p_4	c_1	c_2	c_3	c_4
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	1
0	0	1	1	1	1	1	0
0	1	0	0	1	1	0	1
0	1	0	1	1	0	1	1
0	1	1	0	0	1	1	1
0	1	1	1	0	1	1	0
1	0	0	0	1	1	1	1
1	0	0	1	0	0	1	0
1	0	1	0	1	1	0	0
1	0	1	1	0	1	0	1
1	1	0	0	1	0	1	0
1	1	0	1	0	1	0	0
1	1	1	0	0	0	1	1
1	1	1	1	1	0	0	0

Рассмотрим соотношения

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = 0, \tag{5.10}$$

где при $i = 1$ вектору $\mathbf{a}$ соответствуют числа $0, \ldots, 15$ и тождественная перестановка π; при $i = 2$ вектору $\mathbf{a}$ отвечают числа $5, 6, 9, 10$ и перестановки $\pi = \mathrm{id}, (1,3,2,4), (1,3,4,2)$ (аналогично для $\mathbf{b}$ и σ при $j = 1$, $j = 2$). При данных условиях функции $\langle \mathbf{a}, \pi(\cdot) \rangle_i$ и $\langle \mathbf{b}, \sigma(\cdot) \rangle_j$ пробегают все множество функций Δ_4 без повторений. Для подстановки S рассмотрим таблицу, строки которой занумерованы тройками $(i, \tilde{a}, \pi)$, а столбцы — тройками $(j, \tilde{b}, \sigma)$, такую что на пересечении строки и столбца находится преобладание $\varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}$ соответствующего равенства (5.10), умноженное на 16 (т. е. отклонение числа выполнений равенства (5.10) от половины).

И хотя здесь приводится способ построения таблицы для четырехразрядной подстановки, заметим, что он несложно может быть обобщен на случай произвольной t-разрядной подстановки или преобразования $P \to C$, где P и C имеют разное число битов.

Параметром неквадратичности подстановки S назовем число

$$NQ(S) = \min_{i,j} \min_{\mathbf{a}\neq\mathbf{0},\mathbf{b}\neq\mathbf{0}} \min_{\delta\in\mathbb{Z}_2,\pi,\sigma} |\{P \,:\, \langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j \neq \delta\}|.$$

Другими словами, величина $NQ(S)$ равна разности числа 8 и максимальной из абсолютных величин элементов таблицы (кроме элементов первой строки и первого столбца). Соотношение, отвечающее элементу таблицы с абсолютной величиной $8 - NQ(S)$, выполняется с вероятностью $\frac{NQ(S)}{16}$ или $1 - \frac{NQ(S)}{16}$ (т.е. наименее или наиболее вероятно). *Нелинейностью* подстановки S называется величина

$$NL(S) = \min_{\mathbf{a}\neq\mathbf{0},\mathbf{b}\neq\mathbf{0}} \min_{\delta,\pi,\sigma} |\{P \,:\, \langle \mathbf{a}, \pi(P) \rangle_1 \oplus \langle \mathbf{b}, \sigma(C) \rangle_1 \neq \delta\}|.$$

Величину $NL(S)$ можно получить как разность числа 8 и максимальной из абсолютных величин элементов той части таблицы, которая соответствует только линейным соотношениям входных и выходных битов, т. е. где $i = j = 1$ (кроме нулевых комбинаций). Очевидно, что $NQ(S) \leqslant NL(S)$.

Согласно [124] справедливо $NL(S) \leqslant 4$ для любой четырехразрядной подстановки S.

Для подстановки S^2 имеем $NL(S^2) = 4$, $NQ(S^2) = 2$ (см. таблицу 8).

$16 \cdot \varepsilon^{i,\mathbf{a},\pi}_{j,\mathbf{b},\sigma}$		$j=1$ id																$j=2$ id				$j=2$ (1,3,2,4)				$j=2$ (1,3,4,2)			
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	5	6	9	10	5	6	9	10	5	6	9	10
$i=1$ id	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	-2	0	2	-2	0	-2	**4**	0	2	0	-2	2	0	2	**4**	-2	0	0	2	0	2	2	0	0	0	**4**	0
	2	0	0	0	0	0	**4**	**4**	0	2	2	-2	-2	2	-2	2	-2	2	(6)	0	0	2	**4**	-2	0	**4**	2	0	2
	3	0	2	0	-2	-2	0	2	0	-2	**4**	2	**4**	0	-2	0	2	0	2	**4**	2	2	-2	0	0	**4**	-2	0	2
	4	0	-2	0	-2	0	2	0	2	0	-2	**4**	2	0	2	**4**	-2	**4**	-2	0	2	**4**	-2	0	2	0	0	-2	-2
	5	0	0	**4**	0	2	2	-2	2	0	**4**	0	0	-2	2	-2	-2	-2	2	0	**4**	0	0	-2	2	0	**-4**	2	2
	6	0	-2	**4**	2	0	-2	0	-2	2	0	-2	**4**	2	0	2	0	-2	0	0	-2	-2	2	2	-2	0	2	2	0
	7	0	**4**	0	0	2	2	-2	2	-2	-2	-2	2	**4**	0	0	0	0	0	**-4**	0	2	**4**	0	-2	0	2	2	**-4**
	8	0	0	2	-2	0	0	2	-2	0	0	2	-2	**4**	**4**	-2	2	2	0	2	0	**4**	0	2	-2	**4**	2	0	-2
	9	0	2	2	**4**	-2	**4**	0	-2	0	-2	2	0	-2	0	0	2	**4**	0	-2	2	0	2	0	(6)	**-4**	2	0	2
	10	0	0	-2	2	**4**	0	-2	-2	2	2	**4**	0	2	-2	0	0	0	-2	2	**4**	2	0	**4**	2	0	0	**4**	0
	11	0	-2	-2	**4**	2	0	**4**	2	-2	0	0	2	0	2	-2	0	2	2	2	-2	-2	2	2	2	0	**4**	0	**4**
	12	0	2	2	0	0	-2	2	**4**	**4**	-2	2	0	0	-2	-2	0	2	-2	2	-2	0	-2	2	0	0	2	-2	0
	13	0	0	-2	-2	2	2	0	0	**4**	0	-2	2	-2	2	0	**4**	0	2	-2	0	0	0	**-4**	0	0	-2	-2	0
	14	0	2	2	0	**4**	-2	2	0	-2	0	0	-2	-2	0	**4**	2	0	0	2	-2	-2	-2	0	0	0	0	-2	2
	15	0	**4**	-2	2	-2	-2	0	0	2	2	0	0	0	**4**	2	-2	-2	0	2	0	-2	0	2	0	0	0	2	2
$i=2$ id	5	0	-2	2	0	**4**	-2	-2	0	2	**4**	0	2	2	0	0	-2	**-4**	0	2	2	0	0	2	-2	2	-2	**4**	0
	6	0	0	(6)	2	-2	2	0	0	0	0	-2	2	-2	2	0	0	0	2	-2	0	-2	2	-2	2	-2	0	0	2
	9	0	0	0	**4**	0	0	0	**-4**	2	-2	2	2	2	-2	2	2	2	-2	0	0	0	2	**4**	2	-2	**4**	2	0
	10	0	2	0	2	2	**4**	-2	0	0	2	**4**	-2	-2	0	-2	0	2	0	0	(6)	2	0	0	(6)	-2	-2	2	2
$i=2$ (1,3,2,4)	5	0	0	2	2	**4**	0	-2	2	**4**	0	2	-2	0	0	-2	-2	0	-2	0	2	0	0	2	2	-2	0	2	0
	6	0	2	**4**	-2	-2	0	2	**4**	0	2	0	2	-2	0	-2	0	0	2	2	0	0	-2	-2	0	2	-2	-2	2
	9	0	2	-2	0	0	-2	2	0	2	0	**4**	2	2	**-4**	0	2	2	-2	**4**	0	2	-2	**4**	0	2	2	0	0
	10	0	0	0	0	2	2	-2	-2	-2	(6)	2	2	0	0	0	0	-2	2	2	(6)	2	0	0	2	2	**-4**	**4**	2
$i=2$ (1,3,4,2)	5	0	0	**4**	**4**	0	0	0	0	**4**	**-4**	0	0	0	0	0	0	2	-2	-2	-2	-2	2	2	2	**-4**	**4**	0	0
	6	0	0	2	-2	0	**-4**	2	2	2	2	0	**4**	2	-2	0	0	-2	0	**4**	-2	0	-2	2	**-4**	**4**	0	0	0
	9	0	**4**	0	0	-2	2	2	2	0	0	**4**	0	-2	-2	-2	2	**4**	0	2	2	2	-2	0	**4**	0	0	-2	2
	10	0	0	2	2	-2	2	0	**-4**	-2	2	0	**4**	0	0	2	2	0	2	0	2	0	2	0	2	0	0	2	2

Таблица 8. Преобладания для подстановки S^2.

В таблице 8 элементы с абсолютными значениями 4 и 6 выделены полужирным шрифтом и заключены в кружки соответственно. Любые линейные соотношения на входные и выходные биты S^2 выполняются с вероятностью не большей $3/4$, тогда как существуют 7 квадратичных соотношений, вероятность которых составляет $7/8$. Выберем из них соотношение

при $i = 2$, $\tilde{a} = 6$, $\pi = \mathrm{id}$, $j = 1$, $\tilde{b} = 2$, $\sigma = \mathrm{id}$, т.е

$$\langle (0110), (p_1, p_2, p_3, p_4) \rangle_2 \oplus \langle (0010), (c_1, c_2, c_3, c_4) \rangle_1 = 0.$$

Используя формулы (4.6) и (4.7), приходим к равенству для входных и выходных битов

$$c_3 = p_1 p_3 \oplus p_1 p_4 \oplus p_2 p_3 \oplus p_2 p_4 \oplus p_1 \oplus p_4,$$

которое выполняется с вероятностью $(8 + 6)/16$, т.е. $7/8$. Заметим, что полученное соотношение линейно относительно битов c_1, c_2, c_3 и c_4.

Аналогично, если выбрать соотношение при $i = 1$, $\tilde{a} = 9$, $\pi = \mathrm{id}$, $j = 2$, $\tilde{b} = 10$, $\sigma = (1, 3, 2, 4)$, а именно

$$\langle (1001), (p_1, p_2, p_3, p_4) \rangle_1 \oplus \langle (1010), (c_1, c_3, c_2, c_4) \rangle_2 = 0,$$

то после преобразования с помощью (4.6) и (4.7) получаем соотношение

$$p_2 \oplus p_4 = c_1 c_2 \oplus c_1 c_4 \oplus c_2 c_3 \oplus c_3 c_4 \oplus c_3 \oplus c_4,$$

линейное относительно битов p_1, p_2, p_3 и p_4, выполняющееся с вероятностью $7/8$.

В приложении 5.6 приведены наиболее вероятные соотношения на P и C для подстановок $S^1, \ldots, S^{10}$, представленные в компактном виде, который поясним на примере полученных соотношений для S^2. Одно соотношение представлено в таблице как $C\{3\} = P\{13, 14, 23, 24, 1, 4\}$, другое — в виде $C\{12, 14, 23, 34, 3, 4\} = P\{2, 4\}$. Заметим, что для каждой из 10 подстановок удается построить более вероятные (по сравнению с линейными) квадратичные соотношения, используя функции из класса Δ_4. Имеем $NL(S^t) = 4$, $NQ(S^t) = 2$ для каждого $t = 1, \ldots, 10$.

На данном примере можно убедиться в том, что использование соотношений вида (5.10) в составе систем уравнений с неизвестными битами (входными или выходными) может приводить к более вероятным аппроксимациям неизвестных битов, не усложняя при этом решение системы (система по-прежнему может оставаться линейной относительно неизвестных).

Пример 2. В книге Б. Шнайера [38] приведены восемь четырехразрядных подстановок, использовавшихся при шифровании методом ГОСТ в приложении для ЦБ РФ, а также в однонаправленной хэш-функции ГОСТ. Все они имеют параметр NL, равный 2, кроме одной, для которой $NL = 4$ (см. подстановку S^{11} в таблице 6). Для каждой подстановки имеем $NQ = 2$, и в среднем добавляется 5-6 новых наиболее вероятных квадратичных соотношений специального вида на входные и выходные биты каждой подстановки.

Пример 3. Для всех 32 подстановок на 16 элементах, используемых в S-блоках алгоритма DES (см. например, [38]), параметры NL и NQ совпадают и равны 2. Отметим, что для каждой подстановки добавляется от 0 до 11 (в среднем 4-5) новых наиболее вероятных квадратичных соотношений на входные и выходные биты.

Пример 4. Рассмотрим 32 подстановки (см. например, [38]) в S-блоках модифицированного алгоритма s^3DES [136, 53], которые считаются устойчивыми к методам дифференциального и линейного криптоанализа. Среди них только 7 подстановок (это подстановки $S^{12}, \ldots, S^{18}$ в таблице 6) обладают нелинейностью $NL = 4$, для 25-ти остальных параметр NL равен 2. Для шести из семи подстановок с нелинейностью $NL = 4$ выполняется $NQ = 2$, и в среднем для каждой такой подстановки имеется около 6 квадратичных соотношений с вероятностью $7/8$. И лишь для одной подстановки S^{18} имеем $NL = NQ = 4$.

Квадратичные соотношения с вероятностью $7/8$ для подстановок S^{11}, $\ldots$, S^{18} приведены в приложении 5.6.

5.5 Замечания и дополнения

Приведем свойства функций $\langle \mathbf{u}, \mathbf{v} \rangle_k$, которые могут быть использованы при согласовании раундовых аппроксимаций в квадратичном криптоанализе конкретных шифров.

Для вектора $\mathbf{u} = (u_1, \ldots, u_m)$ пусть $\bar{\mathbf{u}}^k = (u_1 \oplus u_2, \ldots, u_{2k-1} \oplus u_{2k})$ — вектор длины k. Через $*$ обозначим обычное покомпонентное умножение векторов. Пусть $|\boldsymbol{u}| = \langle \boldsymbol{u}, \boldsymbol{u} \rangle$. Справедливо

Утверждение 20. *Для любых векторов* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$, *для любого* k, $1 \leqslant k \leqslant m/2$, *верно*

$$\langle \mathbf{u} \oplus \mathbf{v}, \mathbf{w} \rangle_k = \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \langle \bar{\mathbf{u}}^k, \bar{\mathbf{w}}^k \rangle \cdot \langle \bar{\mathbf{v}}^k, \bar{\mathbf{w}}^k \rangle \oplus |\bar{\mathbf{u}}^k * \bar{\mathbf{v}}^k * \bar{\mathbf{w}}^k|.$$

Доказательство. Согласно теореме 54 имеем

$$\langle \mathbf{u} \oplus \mathbf{v}, \mathbf{w} \rangle_k = \langle \mathbf{u}, \mathbf{w} \rangle \oplus \langle \mathbf{v}, \mathbf{w} \rangle \oplus \Big(\bigoplus_{i=1}^{k} \bigoplus_{j=i}^{k} (\bar{u}_i^k \oplus \bar{v}_i^k)(\bar{u}_j^k \oplus \bar{v}_j^k) \bar{w}_i^k \bar{w}_j^k \Big) =$$

$$\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \Big(\bigoplus_{i=1}^{k} \bigoplus_{j=i}^{k} \bar{u}_i^k \bar{v}_j^k \bar{w}_i^k \bar{w}_j^k \Big) \oplus \Big(\bigoplus_{i=1}^{k} \bigoplus_{j=i}^{k} \bar{u}_j^k \bar{v}_i^k \bar{w}_i^k \bar{w}_j^k \Big) =$$

$$\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \Big(\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{k} \bar{u}_i^k \bar{v}_j^k \bar{w}_i^k \bar{w}_j^k \Big) \oplus \Big(\bigoplus_{i=1}^{k} \bar{u}_i^k \bar{v}_i^k \bar{w}_i^k \Big).$$

Осталось заметить, что третье слагаемое совпадает с $\langle \bar{\mathbf{u}}^k, \bar{\mathbf{w}}^k \rangle \cdot \langle \bar{\mathbf{v}}^k, \bar{\mathbf{w}}^k \rangle$, а четвертое равно $|\bar{\mathbf{u}}^k * \bar{\mathbf{v}}^k * \bar{\mathbf{w}}^k|$. Утверждение доказано. □

Из утверждения 20 следует, что чем меньше значение k, тем менее существенной является нелинейная «добавка» при переходе от $\langle \mathbf{u} \oplus \mathbf{v}, \mathbf{w} \rangle_k$ к сумме $\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k$. При согласовании раундовых аппроксимаций (см. раздел 5.1.2) такая добавка может быть оценена с некоторой вероятностью по частичной информации о неизвестных битах.

Аналог линейности. Напомним, что в 4.2 была определена бинарная операция $\star : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ по правилу $\mathbf{u} \star \mathbf{v} = \varphi_k(\varphi_k^{-1}(\mathbf{u}) \dot{+} \varphi_k^{-1}(\mathbf{v}))$ для любых $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, где $\dot{+}$ обозначает сложение над $\mathbb{Z}_4$ для первых k координат векторов $\varphi_k^{-1}(\mathbf{u})$, $\varphi_k^{-1}(\mathbf{v})$ и сложение над $\mathbb{Z}_2$ для $m - 2k$ последних координат. Из формулы (4.2) вытекает

Утверждение 21. *При любых целых m, k, любых $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$ справедливо $c^k_{\mathbf{u},\mathbf{w}} + c^k_{\mathbf{v},\mathbf{w}} = c^k_{\mathbf{u}\star\mathbf{v},\mathbf{w}}$, где $+$ обозначает сложение над $\mathbb{Z}_4$.*

Напомним, что по определению (4.4) выполняется $\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(c^k_{\mathbf{u},\mathbf{v}})$. Из этого следует, что вектор значений булевой функции $\langle \mathbf{u}, \cdot \rangle_k : \mathbb{Z}_2^m \to \mathbb{Z}_2$ является образом (под действием отображения β) вектора значений функции $\langle\langle \mathbf{u}, \cdot \rangle\rangle_k : \mathbb{Z}_2^m \to \mathbb{Z}_4$, такой что $\langle\langle \mathbf{u}, \mathbf{v} \rangle\rangle_k = c^k_{\mathbf{u},\mathbf{v}}$. Другими словами, $\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta\left(\langle\langle \mathbf{u}, \mathbf{v} \rangle\rangle_k\right)$. Заметим, что $\langle\langle \mathbf{u}, \mathbf{v} \rangle\rangle_k = \langle\langle \mathbf{v}, \mathbf{u} \rangle\rangle_k$. Согласно утверждению 21 функции $\langle\langle \mathbf{u}, \mathbf{v} \rangle\rangle_k$, $\mathbf{u} \in \mathbb{Z}_2^m$, обладают свойством линейности над $\mathbb{Z}_4$, т.е. $\langle\langle \mathbf{u}', \mathbf{v} \rangle\rangle_k + \langle\langle \mathbf{u}'', \mathbf{v} \rangle\rangle_k = \langle\langle \mathbf{u}' \star \mathbf{u}'', \mathbf{v} \rangle\rangle_k$. Этот факт можно использовать в квадратичном криптоанализе. В частности, заменив основное соотношение $\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = \langle \mathbf{d}, \tau(K) \rangle_k$ для битов открытого текста, шифротекста и ключа (например, для алгоритма 1) на соотношение над $\mathbb{Z}_4$ вида $\langle\langle \mathbf{a}, \pi(P) \rangle\rangle_k + \langle\langle \mathbf{b}, \pi(C) \rangle\rangle_k = \langle\langle \mathbf{d}, \pi(K) \rangle\rangle_k$, полагая $i = j = k$, а также $\pi = \sigma = \tau$. В соотношениях такого типа напрямую может использоваться линейность функций $\langle\langle \mathbf{u}, \mathbf{v} \rangle\rangle_k$ над $\mathbb{Z}_4$. Однако, этот случай требует дополнительного исследования. В частности, необходимо описать способ выбора по набранной статистике значения $\langle\langle \mathbf{d}, \pi(K) \rangle\rangle_k$ из четырех возможных вариантов 0, 1, 2 и 3 (вместо двух, как было ранее).

5.6 Приложение

S	квадратичные соотношения с вероятностью 7/8
S^1	$C\{1,3,4\} = P\{13,14,23,24,1,3\},$ $C\{1,3,4\} = P\{12,13,24,34,1,3\},$ $C\{13,14,23,24,2,3\} = P\{3,4\},$ $C\{12,14,23,34,2,3\} = P\{3,4\},$
S^2	$C\{3\} = P\{13,14,23,24,1,4\},$ $C\{2,4\} = P\{12,14,23,34,3,4\},$ $C\{13,14,23,24,1,4\} = P\{3\},$ $C\{12,14,23,34,3,4\} = P\{2,4\},$ $C\{13,14,23,24,2,4\} = P\{13,14,23,24,2,4\},$ $C\{12,14,23,34,3,4\} = P\{13,14,23,24,2,4\},$ $C\{13,14,23,24,2,4\} = P\{12,14,23,34,3,4\}$
S^3	$C\{2\} = P\{13,14,23,24,1,4\},$ $C\{1,2,3,4\} = P\{12,14,23,34,3,4\},$ $C\{12,14,23,34,3,4\} = P\{4\},$ $C\{13,14,23,24,1,4\} = P\{1,2\},$
S^4	$C\{12,13,24,34,1,3\} = P\{1,2\}$ $C\{12,14,23,34,3,4\} = P\{1,2,3,4\},$ $C\{12,13,24,34,1,3\} = P\{12,13,24,34,1,3\},$ $C\{12,14,23,34,1,4\} = P\{12,13,24,34,1,3\},$ $C\{12,14,23,34,1,4\} = P\{12,14,23,34,1,4\},$
S^5	$C\{1,2\} = P\{12,14,23,34,2,3\}$ $C\{12,14,23,34,2,3\} = P\{2,3\},$
S^6	$C\{12,14,23,34,1,4\} = P\{1,2,3,4\}$
S^7	$C\{1,3\} = P\{13,14,23,24,2,4\},$ $C\{12,13,24,34,1,2\} = P\{1,3\} \oplus 1$ $C\{12,13,24,34,3,4\} = P\{12,14,23,34,1,2\},$ $C\{13,14,23,24,1,4\} = P\{12,13,24,34,3,4\} \oplus 1,$
S^8	$C\{1,3\} = P\{13,14,23,24,2,4\},$ $C\{12,13,24,34,1,2\} = P\{1,3\} \oplus 1$ $C\{12,13,24,34,3,4\} = P\{12,14,23,34,1,2\},$ $C\{13,14,23,24,1,4\} = P\{12,13,24,34,3,4\} \oplus 1,$
S^9	$C\{1,2\} = P\{12,14,23,34,1,4\}$ $C\{1,2,3\} = P\{13,14,23,24,1,3\}$ $C\{1,2,4\} = P\{12,13,24,34,1,3\}$ $C\{13,14,23,24,2,3\} = P\{1,2,4\},$ $C\{12,14,23,34,1,2\} = P\{12,14,23,34,1,4\},$ $C\{13,14,23,24,1,4\} = P\{12,13,24,34,1,2\},$
S^{10}	$C\{1,4\} = P\{13,14,23,24,1,3\},$ $C\{1,2,3,4\} = P\{12,14,23,34,1,4\},$ $C\{13,14,23,24,1,3\} = P\{1,3\},$ $C\{12,14,23,34,3,4\} = P\{1,3\},$ $C\{13,14,23,24,2,4\} = P\{12,14,23,34,3,4\},$ $C\{13,14,23,24,2,4\} = P\{13,14,23,24,1,3\},$

S	квадратичные соотношения с вероятностью 7/8
S^{11}	$C\{2,3\} = P\{13,14,23,24,1,3\} \oplus 1,$ $C\{2,3\} = P\{12,13,24,34,1,3\} \oplus 1,$ $C\{12,14,23,34,1,4\} = P\{1,4\},$ $C\{13,14,23,24,1,3\} = P\{13,14,23,24,2,4\},$ $C\{13,14,23,24,1,3\} = P\{12,13,24,34,1,3\} \oplus 1,$
S^{12}	$C\{1,2,3\} = P\{13,14,23,24,1,3\} \oplus 1,$ $C\{13,14,23,24,1,3\} = P\{3,4\} \oplus 1,$ $C\{12,14,23,34,1,2\} = P\{3,4\} \oplus 1,$ $C\{13,14,23,24,2,4\} = P\{1,3,4\},$ $C\{12,14,23,34,3,4\} = P\{1,3,4\},$ $C\{13,14,23,24,1,3\} = P\{12,14,23,34,2,3\} \oplus 1,$ $C\{12,13,24,34,1,3\} = P\{12,14,23,34,2,3\} \oplus 1,$
S^{13}	$C\{12,14,23,34,1,4\} = P\{13,14,23,24,2,3\} \oplus 1,$ $C\{12,13,24,34,1,3\} = P\{13,14,23,24,2,3\} \oplus 1,$
S^{14}	$C\{1\} = P\{12,14,23,34,1,4\},$ $C\{3\} = P\{12,14,23,34,3,4\},$ $C\{1,2\} = P\{12,14,23,34,2,3\} \oplus 1,$ $C\{2,3\} = P\{12,14,23,34,1,2\} \oplus 1,$ $C\{12,14,23,34,3,4\} = P\{12,14,23,34,1,2\} \oplus 1,$ $C\{12,14,23,34,1,4\} = P\{12,14,23,34,2,3\} \oplus 1,$
S^{15}	$C\{1,2,3\} = P\{12,14,23,34,1,2\} \oplus 1,$ $C\{12,13,24,34,1,3\} = P\{2,4\},$ $C\{12,13,24,34,2,4\} = P\{1,2,4\},$ $C\{13,14,23,24,2,4\} = P\{2,4\} \oplus 1,$ $C\{13,14,23,24,1,3\} = P\{1,2,4\} \oplus 1,$ $C\{12,14,23,34,1,4\} = P\{12,13,24,34,2,4\},$ $C\{12,13,24,34,1,3\} = P\{12,13,24,34,2,4\},$
S^{16}	$C\{12,13,24,34,1,2\} = P\{12,13,24,34,1,2\},$ $C\{12,13,24,34,1,2\} = P\{13,14,23,24,2,3\},$ $C\{12,14,23,34,1,2\} = P\{12,14,23,34,2,3\},$ $C\{12,14,23,34,1,4\} = P\{12,14,23,34,1,2\},$ $C\{12,14,23,34,1,4\} = P\{13,14,23,24,1,3\},$ $C\{13,14,23,24,2,4\} = P\{12,13,24,34,1,3\},$ $C\{13,14,23,24,1,4\} = P\{12,14,23,34,1,2\},$ $C\{13,14,23,24,2,4\} = P\{12,14,23,34,2,3\},$
S^{17}	$C\{2,3\} = P\{12,13,24,34,1,3\},$ $C\{1,3,4\} = P\{13,14,23,24,2,3\} \oplus 1,$ $C\{13,14,23,24,2,3\} = P\{2\} \oplus 1,$ $C\{12,13,24,34,3,4\} = P\{2\} \oplus 1,$ $C\{13,14,23,24,1,4\} = P\{1,2\} \oplus 1,$ $C\{12,13,24,34,1,2\} = P\{1,2\} \oplus 1,$ $C\{13,14,23,24,1,4\} = P\{12,13,24,34,1,3\} \oplus 1,$
S^{18}	отсутствуют

Приведены наиболее вероятные соотношения для подстановок $S^1, \ldots, S^{18}$.

Заключение

Изложенные в книге результаты опубликованы в следующих статьях автора. Обзор, приведенный в Главе 1, опубликован в [32]. Обобщения бент-функций, представленные в Главе 2, опубликованы в [33]. Результат о группе автоморфизмов множества бент-функций, представленный в Главе 3, можно найти в [34]. Результатам Глав 4, 5 посвящены статьи [29, 30, 31, 199]. Статьи и электронный вариант данной книги доступны на web-странице `www.math.nsc.ru/~tokareva`. Ваши замечания и пожелания присылайте, пожалуйста, по адресу `tokareva@math.nsc.ru`.

В заключение я хотела бы выразить свою благодарность А. А. Нечаеву (МГУ), С. В. Агиевичу (Минск, Белоруссия), Лилии Будагян (Берген, Норвегия), Патрику Солé (Париж, Франция) и Франсуа Родье (Марсель, Франция) за ценные замечания и обсуждения по теме данной работы, а также пожелать удачи каждому исследователю, у которого возник интерес к задачам о бент-функциях.

* * *

Исследование выполнено при поддержке гранта Президента РФ для молодых российских ученых (грант МК-1250.2009.1), Российского фонда фундаментальных исследований (проекты 08-01-00671, 09-01-00528, 10-01-00424) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг. (гос. контракт 02.740.11.0429).

Литература

[1] *Августинович С. В.* Об одном свойстве совершенных двоичных кодов // Дискрет. анализ и исслед. операций. 1995. Т. 2, N 1. С. 4–6.

[2] *Агеев Д. В.* Основы теории линейной селекции. Кодовое разделение каналов // Сборник научных трудов Ленинградского экспериментального института связи, 1935.

[3] *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями // Дискретная математика. 1994. Т. 6, N 3. С. 50–60.

[4] *Буряков М. Л., Логачев О. А.* Об уровне аффинности булевых функций // Дискретная математика. 2005. Т. 17, N 4. С. 98–107.

[5] *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. 1962. Вып. 8. С. 337–339.

[6] *Иванов А. В.* Использование приведенного представления булевых функций при построении их нелинейных аппроксимаций // Вестник Томского госуниверситета. Приложение. 2007. N 23. С. 31–35.

[7] *Иванов А. В.* Мономиальные приближения платовидных функций // Прикладная дискретная математика. 2008. Т. 1, N 1. С. 10–14.

[8] *Иванов А. В.* Близость к классу мономиальных аппроксимаций приведенного представления булевой функции в зависимости от выбора базиса, в котором оно задано // Прикладная дискретная математика. 2009. Приложение. N 1. С. 7–9.

[9] *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная Дискретная Математика, 2009, N 4, С. 5–20.

[10] *Кротов Д. С.* $\mathbb{Z}_4$-линейные совершенные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, N 4. С. 78–90 (translated at `http://arxiv.org/abs/0710.0198`).

[11] *Кузнецов Ю. В., Шкарин С. А.* Коды Рида—Маллера (обзор публикаций) // Математические вопросы кибернетики. 1996. Вып. 6. С. 5–50.

[12] *Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б.* Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18, N 1. С. 9–29.

[13] *Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишкин В. А., Шишков А. Б.* Бент-функции и гипербент-функции над полем из 2^l элементов // Проблемы передачи информ. 2008. Т. 44, Вып. 1. С. 15–37.

[14] *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. Т. 10. М.: Физматлит. С. 97–122.

[15] *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Параметры (гипер-) бент-функций над полем из 2^l элементов // Труды по дискретной математике. 2008. Т. 11. М.: Физматлит. С. 47–59.

[16] *Логачев О. А., Сальников А. А., Ященко В. В.* Бент-функции на конечной абелевой группе // Дискретная математика. 1997. Т. 9, N 4. С. 3–20.

[17] *Логачев О. А., Сальников А. А., Ященко В. В.* Некоторые характеристики «нелинейности» групповых отображений // Дискрет. анализ и исслед. операций. Сер. 1. 2001. Т. 8. № 1. С. 40–54.

[18] *Логачев О. А., Сальников А. А., Ященко В. В.* Криптографические свойства дискретных функций // Материалы конференции «Московский университет и развитие криптографии в России», МГУ, 2002. М.: МЦНМО, 2003. С. 174–199.

[19] *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004.

[20] *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М: Связь, 1979. 745 с.

[21] *Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В.* Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002.

[22] *Молдовян А. А., Молдовян Н. А., Еремеев М. А.* Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004.

[23] *Нигматуллин Р. Г.* Сложность булевых функций. М.: Наука, 1991. 240 с.

[24] *Ростовцев А., Маховенко Е.* Введение в теорию итерированных шифров // СПб.: НПО «Мир и Семья», 2003.

[25] *Рязанов Б. В., Чечета С. И.* О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. 1995. Т. 7, N 3. С. 129–145.

[26] *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Т. 24. С. 15–42.

[27] *Сидельников В. М.* Об экстремальных многочленах, используемых при оценках мощности кода // Проблемы передачи информ. 1980. Т. 14, Вып. 3. С. 17–30.

[28] *Солодовников В. И.* Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискретная математика. 2002. Т. 14. N 1. С. 99–113.

[29] *Токарева Н. Н.* Бент-функции с более сильными свойствами нелинейности: k-бент-функции // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14, N 4. С. 76–102.

[30] *Токарева Н. Н.* О квадратичных аппроксимациях в блочных шифрах // Пробл. передачи информ. 2008. Т. 44, Вып. 3. С. 105–127.

[31] *Токарева Н. Н.* Описание k-бент-функций от четырех переменных // Дискр. анализ и исслед. операций. 2008. Т. 15, N 4. С. 74–83.

[32] *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная Дискретная Математика. 2009. Т. 2, N 1. С. 15–37.

[33] *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретный анализ и исследование операций. 2010. Т. 17, N 1. С. 34–64.

[34] *Токарева Н. Н.* Группа автоморфизмов множества бент-функций // Дискретная математика. 2010. Т. 22, N 4.

[35] *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная Дискретная Математика. 2009. N 3. С. 14–20.

[36] *Холл М.* Комбинаторика. М.: Мир, 1970. 424 с.

[37] *Черемушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.

[38] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си // М.: Триумф, 2002.

[39] *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Пробл. передачи информации. 1997. Т. 33. Вып. 1. С. 75–86.

[40] *Ященко В. В.* О двух характеристиках нелинейности булевых отображений // Дискрет. анализ и исслед. операций. Сер. 1. 1998. Т. 5. № 2. С. 90–96.

[41] *Adams C.* On immunity against Biham and Shamir's «differential cryptanalysis» // Information Processing Letters. 1992. V. 41. P. 77–80.

[42] *Adams C., Tavares S.* The structured design of cryptographically good S-boxes // J. Cryptology. 1990. V. 3. N 1. P. 27–43.

[43] *Agievich S. V.* On the representation of bent functions by bent rectangles // Fifth Int. Petrozavodsk conf. on probabilistic methods in discrete mathematics (Petrozavodsk, Russia, June 1–6, 2000). Proc. Boston: VSP, 2000. P. 121–135. Available at `http://arxiv.org/abs/math/0502087`.

[44] *Agievich S. V.* On the affine classification of cubic bent functions // Cryptology ePrint Archive, Report 2005/044, available at `http://eprint.iacr.org/`.

[45] *Agievich S. V.* Bent rectangles // NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Zvenigorod, Russia. September 8–18, 2007). Proc: Netherlands, IOS Press, 2008. P. 3–22. Available at `http://arxiv.org/abs/0804.0209`.

[46] `http://www.math.cornell.edu/News/AnnRep/AR01-02.pdf` — Cornell University. Department of Mathematics. Annual Report 2001–2002.

[47] `http://www.math.cornell.edu/News/AnnRep/AR2002-2003.pdf` — Cornell University. Department of Mathematics. Annual Report 2002–2003.

[48] *Baignères T., Junod P., Vaudenay S.* How Far Can We Go Beyond Linear Cryptanalysis? // Advances in Cryptology — ASIACRYPT '04, 10th International Conference on the Theory and Applications of Cryptology and Information Security (Jeju Island, Korea. December 5–9, 2004). Proc. Springer. 2004. P. 432–450 (Lecture Notes in Comput. Sci. V. 3329).

[49] *Bending T. D., Fon-Der-Flaass D. G.* Crooked Functions, Bent Functions and Distance Regular Graphs // Electronic Journal of Combinatorics. 1998. N 5 (R34).

[50] *Bernasconi A., Codenotti B.* Spectral analysis of Boolean functions as a graph eigenvalue problem // IEEE Trans. Computers. 1999. V. 48. No. 3. P. 345–351.

[51] *Bernasconi A., Codenotti B., VanderKam J. M.* A characterization of bent functions in terms of strongly regular graphs // IEEE Trans. Computers. 2001. V. 50. No. 9. P. 984–985.

[52] *Bey Ch., Kyureghyan G.* An Association Scheme of a Family of Cubic Bent Functions // Proc. of the Int. Workshop on Coding and Cryptography (Versailles, France. April 16–20, 2007). P. 13–19.

[53] *Biham E., Biryukov A.* How to strengthen DES using existing hardware // Advances in Cryptology — ASIACRYPT '94, 4th International Conference on the Theory and Applications of Cryptology. (Wollongong, Australia. November 28 – December 1, 1994) Proc. Springer. 1995. P. 398–412 (Lecture Notes in Comput. Sci. V. 917).

[54] *Biham E., Dunkelman O., Keller N.* Differential-Linear Cryptanalysis of Serpent // Fast Software Encryption — FSE'2003 (Proc. 10th International Workshop. Lund, Sweden. February 24–26, 2003). Berlin: Springer, 2003. P. 9–21 (Lecture Notes in Comput. Sci. V. 2887).

[55] *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4, N 1. P. 3–72.

[56] *Biryukov A., De Canniere C., Quisquater M.* On Multiple Linear Approximations // Advances in Cryptology — CRYPTO 2004, 24th Annual International Cryptology Conference. (Santa Barbara, California, USA. August 15-19, 2004) Proc. Springer–Verlag. 2004. P. 1–22 (Lecture Notes in Comput. Sci. V. 3152).

[57] *Borges J., Phelps K. T., Rifa J., Zinoviev V. A.* On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes // IEEE Trans. Inform. Theory. 2003. V. 49, N 11. P. 2834–2843.

[58] *Borst J., Preneel B., Vandewalle J.* Linear cryptanalysis of RC5 and RC6 // Fast Software Encryption, 6th International Workshop — FSE'99. (Rome, Italy. March 24–26, 1999) Proc. Berlin: Springer, 1999. P. 16–30 (Lecture Notes in Comput. Sci. V. 1636).

[59] *Braeken A.* Cryptographic properties of Boolean functions and S-boxes // Ph. D. Thesis, Katholieke Univ. Leuven, 2006. Available at `http://www.cosic.esat.kuleuven.be/publications/thesis-129.pdf`.

[60] *Bracken C., Leander G.* New families of functions with differential uniformity of 4 // Proc. Fourth International Conference BFCA — Boolean Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). P. 190–194.

[61] *Budaghyan L.* Private communication, 2008.

[62] *Budaghyan L., Carlet C., Leander G.* On inequivalence between known power APN functions // Proc. Fourth International Conference BFCA — Boolean Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). P. 3–15.

[63] *Budaghyan L., Pott A.* On differential uniformity and nonlinearity of functions // Discrete Mathematics. 2009. V. 309. No. 1. P. 371–384.

[64] *Buttyan L., Vajda I.* Searching for the best linear approximation of DES-like cryptosystems // Electronics Letters. 1995. V. 31, N 11. P. 873–874.

[65] *Byrne E., McGuire G.* On the non-existence of crooked functions on finite fields // Proc. of the Int. Workshop on Coding and Cryptography (Bergen, Norway. March 14–18, 2005). P. 316–324.

[66] *Canteaut A., Carlet C., Charpin P., Fontaine C.* On Cryptographic Properties of the Cosets of $R(1, m)$ // IEEE Trans. Inform. Theory. 2001. V. 47, N 4. P. 1494–1513.

[67] *Canteaut A., Charpin P., Kuyreghyan G.* A new class of monomial bent functions // Finite Fields and Applications. 2008. V. 14, N 1. P. 221–241.

[68] *Canteaut A., Daum M., Dobbertin H., Leander G.* Finding nonnormal bent functions // Discrete Appl. Math. 2006. V. 154, N 2. P. 202–218.

[69] *Carlet C.* Partially-bent functions // Designs, Codes and Cryptography. 1993. V. 3, N 2. P. 135–145.

[70] *Carlet C.* Generalized Partial Spreads // IEEE Trans. Inform. Theory. 1995. V. 41, N 5. P. 1482–1487.

[71] *Carlet C.* A construction of bent functions // Finite Fields and Applications, London mathematical society. 1996. Lecture series 233. P. 47–58.

[72] *Carlet C.* Hyper-bent functions // Int. Conference on the Theory and Applications of Cryptology — PRAGOCRYPT'96. Prague, Czech Technical University Publishing House, 1996. P. 149–155.

[73] *Carlet C.* $\mathbb{Z}_{2^k}$-linear codes // IEEE Trans. Inform. Theory. 1998. V. 44, N 4. P. 1543–1547.

[74] *Carlet C.* On cryptographic complexity of Boolean functions // Proc. of the Sixth Conference on Finite Fields with Applications to Coding Theory,

Cryptography and Related Areas. Springer, G. L. Mullen, H. Stichtenoth and H. Tapia-Recillas Eds. 2002. P. 53–69.

[75] *Carlet C.* On the confusion and diffusion properties of Maiorana—McFarland's and extended Maiorana—McFarland's functions // Special Issue «Complexity Issues in Coding Theory and Cryptography» dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, J. Complexity. 2004. V. 20. P. 182–204.

[76] *Carlet C.* Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications // IEEE Trans. Inform. Theory. 2008. V. 54, N 3. P. 1262–1272.

[77] *Carlet C.* On the higher order nonlinearities of Boolean functions and S-boxes, and their generalizations // The Fifth Int. Conf. on Sequences and Their Applications — SETA'2008 Proc. (Lexington, Kentucky, USA. September 14–18, 2008). Berlin: Springer, 2008. P. 345–367 (Lecture Notes in Comput. Sci. V. 5203).

[78] *Carlet C.* Boolean Functions for Cryptography and Error Correcting Codes // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at `www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`.

[79] *Carlet C.* Vectorial Boolean Functions for Cryptography // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at `www-rocq.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf`.

[80] *Carlet C., Charpin P., Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. V. 15, N 2. P. 125–156.

[81] *Carlet C., Danielsen L.-E., Parker M. G., Solé P.* Self Dual Bent Functions // Proc. Fourth International Conference BFCA — Boolean

Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). P. 39–52.

[82] *Carlet C., Ding C.* Highly nonlinear mappings // J. Complexity. 2004. V. 20, N 2–3. P. 205–244.

[83] *Carlet C., Ding C.* Nonlinearities of S-boxes // Finite Fields and Applications. 2007. V. 13, N 1. P. 121–135.

[84] *Carlet C., Ding C., Niederreiter H.* Authentication schemes from highly nonlinear functions // Designs, Codes and Cryptography. 2006. V. 40, N 1. P. 71–79.

[85] *Carlet C., Gaborit P.* Hyper-bent functions and cyclic codes // J. Combin. Theory. Ser. A. 2006. V. 113, N 3. P. 466–482.

[86] *Carlet C., Guillot P.* A characterization of binary bent functions // J. Combin. Theory. Ser. A. 1996. V. 76. No. 2. P. 328–335.

[87] *Carlet C., Guillot P.* An alternate characterization of the bentness of binary functions, with uniqueness // Designs, Codes and Cryptography. 1998. V. 14. P. 133–140.

[88] *Carlet C., Klapper A.* Upper bounds on the numbers of resilient functions and of bent functions // 23rd Symposium on Information Theory (Benelux, Belgium. May, 2002). Proc. 2002. P. 307–314. The full version will appear in Lecture Notes dedicated to Philippe Delsarte. Available at `http://www.cs.engr.uky.edu/~klapper/ps/bent.ps`.

[89] *Carlet C., Prouff E.* On Plateaued Functions and Their Constructions // Fast Software Encryption — FSE'2003 (Proc. 10th International Workshop. Lund, Sweden. February 24–26, 2003). Berlin: Springer, 2003. P. 54–73 (Lecture Notes in Comput. Sci. V. 2887).

[90] `http://www.faqs.org/rfcs/rfc2144.html` — CAST-128. Rfc 2144 — the cast-128 encryption algorithm— 1997.

[91] *Chabaud F., Vaudenay S.* Links between Differential and Linear Cryptanalysis // Advances in Cryptology — EUROCRYPT '94, International Conference on the Theory and Application of Cryptographic Techniques. (Perugia, Italy. May 9–12, 1994) Proc. Springer. 1995. P. 356–365 (Lecture Notes in Comput. Sci. V. 950).

[92] *Charnes C., Rotteler M., Beth T.* Homogeneous bent functions, invariants, and designs // Designs, Codes and Cryptography. 2002. V. 26, N 1–3. P. 139–154.

[93] *Charpin P., Pasalic E., Tavernier C.* On bent and semi-bent quadratic Boolean functions // IEEE Trans. Inform. Theory. 2005. V. 51. No. 12. P. 4286–4298.

[94] *Chase P. J., Dillon J. F., Lerche K. D.* Bent functions and difference sets // NSA R41 Technical Paper. September, 1970.

[95] *Chee S., Lee S., Kim K.* Semi-bent Functions // Advances in Cryptology — ASIACRYPT '94 — 4th International Conference on the Theory and Applications of Cryptology. (Wollongong, Australia. November 28 – December 1, 1994). Proc. Berlin: Springer. 1995. P. 107–118 (Lecture Notes in Comput. Sci. V. 917).

[96] *Clark J. A., Jacob J. L.* Two-stage optimisation in the design of Boolean functions // 5th Australian Conference on Information Security and Privacy. (Brisbane, Australia, July 10-12, 2000). Proc. Springer-Verlag, 2000. P. 242–254 (Lecture Notes in Comput. Sci. V. 1841).

[97] *Clark J. A., Jacob J. L., Maitra S., Stanica P.* Almost Boolean Functions: the Design of Boolean Functions by Spectral Inversion. // Computational Intelligence. Special Issue on Evolutionary Computing in Cryptography and Security. 2004. V. 20. No. 3. P. 450–462.

[98] *Climent J.-J., Garcia F. J., Requena V.* On the construction of bent functions of $n+2$ variables from bent functions of n variables. // Advances in Math. of Communications. 2008. V. 2. No. 4. P. 421–431.

[99] *Daemen J., Govaerts R., Vandevalle J.* Correlation Matrices // Fast Software Encryption, Second International Workshop — FSE'95. (Leuven, Belgium. December 14-16, 1994) Proc. Berlin: Springer, 1995. P. 275–285 (Lecture Notes in Comput. Sci. V. 1008).

[100] *Van Dam E. R., Fon-Der-Flaass D. G.* Uniformly Packed Codes and More Distance Regular Graphs from Crooked Functions // J. Algebraic Combinatorics. 2000. V. 12, N 2. P. 115–121.

[101] *Van Dam E. R., Fon-Der-Flaass D. G.* Codes, graphs, and schemes from nonlinear functions // European J. Combinatorics, 2003. V. 24, N 1. P. 85–98.

[102] *Delsarte P.* An algebraic approach to the association schemes of coding theory // Ph. D. Thesis, Univ. Catholique de Louvain, 1973.

[103] *Dempwolff U.* Automorphisms and equivalence of bent functions and of difference sets in elementary Abelian 2-groups // Communications in Algebra. 2006. V. 34. No. 3. P. 1077–1131.

[104] `http://www.mathematik.uni-kl.de/~dempw/` — Homepage of U. Dempwolff. See the section «Bent Functions in Dimensions 8,10,12». 2009.

[105] *Detombe J., Tavares S.* Constructing large cryptographically strong S-boxes // Advances in Cryptology — AUSCRYPT'92. (Gold Coast, Queensland, Australia. December 13–16, 1992) Proc. Berlin: Springer, 1993. P. 165–181 (Lecture Notes in Comput. Sci. V. 718).

[106] *Dillon J. F.* A survey of bent functions // The NSA Technical J. 1972. Special Issue. P. 191–215.

[107] *Dillon J. F.* Elementary Hadamard Difference sets // Ph. D. Thesis, Univ. of Maryland, 1974.

[108] *Dillon J. F., McGuire G.* Near bent functions on a hyperplane // Finite Fields and Applications. 2008. V. 14. P. 715–720.

[109] *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption, Second International Workshop — FSE'95. (Leuven, Belgium. December 14-16, 1994) Proc. Berlin: Springer, 1995. P. 61–74 (Lecture Notes in Comput. Sci. V. 1008).

[110] *Dobbertin H.* Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case // Inform. and Comput. 1999. V. 151, N 1–2. P. 57–72.

[111] *Dobbertin H.* Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5 // Finite Fields and Applications FQ5 (Augsburg, Germany, 2000). Proc. Springer. Eds: D. Jungnickel, H. Niederreiter. P. 113–121.

[112] *Dobbertin H., Leander G., Canteaut A. et al.* Construction of Bent Functions via Niho Power Functions // J. Combin. Theory. Ser. A. 2006. V. 113. No. 5. P. 779–798. Available at `http://www-rocq.inria.fr/secret/Anne.Canteaut/Publications/index-pub.html`.

[113] *Dobbertin H., Leander G.* A survey of some recent results on bent functions // Sequences and their applications. – SETA 2004. Third Int. conference (Seul, Korea. October 24–28, 2004). Revised selected papers. Berlin: Springer, 2005. P. 1–29 (Lecture Notes in Comput. Sci. V. 3486).

[114] *Dobbertin H., Leander G.* Cryptographer's Toolkit for Construction of 8-Bit Bent Functions // Cryptology ePrint Archive, Report 2005/089, available at `http://eprint.iacr.org/`.

[115] *Fuller J. E.* Analysis of affine equivalent Boolean functions for cryptography // Ph. D. thesis, Queensland University of Technology. Brisbane, Australia. 2003. Available at http://eprints.qut.edu.au/15828/.

[116] *Fuller J. E., Dawson E., Millan W.* Evolutionary generation of bent functions for cryptography // The 2003 Congress on Evolutionary Computation. 2003. CEC apos;03. V. 3. P. 1655–1661.

[117] *Gangopadhyay S., Sharma D., Sarkar S., Maitra S.* On Affine (Non) Equivalence of Bent Functions // CECC'08 — Central European Conference on Cryptography (Graz, Austria, July 2–4, 2008). Proc. 2008. Available at http://www.math.tugraz.at/∼cecc08/abstracts/cecc08_abstract_25.pdf.

[118] *Gong G., Golomb S. W.* Transform Domain Analysis of DES // IEEE Trans. Inform. Theory. 1999. V. 45, N 6. P. 2065–2073.

[119] *Grocholewska-Czuryło A.* A study of differences between bent functions constructed using Rothaus method and randomly generated bent functions // J. Telecommunications and Information Technology. 2003. No. 4. P. 19–24. Available at http://www.itl.waw.pl/czasopisma/JTIT/2003/4/19.pdf.

[120] *Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P.* The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. V. 40, N 2. P. 301–319.

[121] *Harpers C., Kramer G.G., Massey J.L.* A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma // Advances in Cryptology — EUROCRYPT '95 — International Conference on the Theory and Application of Cryptographic Techniques. (Saint-Malo, France. May 21-25, 1995) Proc. Springer. 1995. P. 24–38 (Lecture Notes in Comput. Sci. V. 921).

[122] *Hawkes P., O'Connor L.* On Applying Linear Cryptanalysis to IDEA // Advances in Cryptology — ASIACRYPT '96 — International Conference on the Theory and Applications of Cryptology and Information Security. (Kyongju, Korea. November 3–7, 1996) Proc. Berlin: Springer. 1996. P. 105–115 (Lecture Notes in Comput. Sci. V. 1163).

[123] *Helleseth T., Kalosha A.* Monomial and quadratic bent functions over the finite fields of odd characteristic // Reports in Informatics, 2005. University of Bergen, Norway. Report 310.

[124] *Heys H. M., Tavares S. E.* Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis // J. Cryptology. 1996. V. 9, N 1. P. 1–19.

[125] *Hou X.-D.* Cubic bent functions // Discrete Mathematics. 1998. V. 189. P. 149–161.

[126] *Hou X. D.* q-Ary bent functions constructed from chain rings // Finite Fields and Applications. 1998. V. 4, N 1. P. 55–61.

[127] *Hou X. D.* p-Ary and q-ary versions of certain results about bent functions and resilient functions // Finite Fields and Applications. 2004. V. 10, N 4. P. 566–582.

[128] *Hou X.-D., Langevin P.* Results on bent functions // J. Comb. Theory, Series A. 1997. V. 80. P. 232–246.

[129] *Hu H., Feng D.* On quadratic bent functions in polynomial forms // IEEE Trans. Inform. Theory 2007. V. 53. No. 7. P. 2610–2615.

[130] *Kaliski B., Robshaw M.* Linear Cryptanalysis Using Multiple Approximations // Advances in Cryptology — CRYPTO'94, 14th Annual International Cryptology Conference. (Santa Barbara, California, USA. August 21-25, 1994) Proc. Springer. 1994. P. 26–39 (Lecture Notes in Comput. Sci. V. 839).

[131] *Kantor W. M.* Codes, Quadratic Forms and Finite Geometries // Proceedings of Symposia in Applied Math. 1995. V. 50. P. 153–177. Available at `http://darkwing.uoregon.edu/~kantor/`.

[132] *Kavut S., Maitra S., Yucel M. D.* Search for Boolean functions with excellent profiles in the rotation symmetric class // IEEE Trans. Inform. Theory. 2007. V. 53, N 5. P. 1743–1751.

[133] *Kerdock A. M.* A class of low-rate non-linear binary codes // Inform. Control. 1972. V. 20, N 2. P. 182–187.

[134] *Khoo K., Gong G., Stinson D. R.* A new family of Gold-like sequences // ISIT — IEEE Int. Symposium on Information Theory (Lausanne, Switzerland, June 30-July 5, 2002). Proc. 2002. P. 181.

[135] *Khoo K., Gong G., Stinson D. R.* A new characterization of semi-bent and bent functions on finite fields // Designs, Codes and Cryptography. 2006. V. 38. No. 2. P. 279–295.

[136] *Kim K., Park S., Lee S.* Reconstruction of s2DES S-Boxes and their Immunity to Differential Cryptanalysis // Korea — Japan Workshop on Information Security and Cryptography. (Seoul, Korea. October 24–26, 1993) Proc. 1993. P. 282–291.

[137] *Knudsen L.* Practically secure Feistel ciphers // Fast Software Encryption — FSE, The Cambridge Security Workshop. (Cambridge, U.K. December 9–11, 1993) Proc. Springer-Verlag. 1994. P. 211–221 (Lecture Notes in Comput. Sci. V. 809).

[138] *Knudsen L. R., Robshaw M. J. B.* Non-linear approximation in linear cryptanalysis // Advances in Cryptology – EUROCRYPT'96. Workshop on the theory and application of cryptographic techniques (Saragossa, Spain. May 12–16, 1996). Proc. Springer-Verlag. 1996. P. 224–236 (Lecture Notes in Comput. Sci. V. 1070).

[139] *Krotov D. S.* $\mathbb{Z}_4$-linear Hadamard and extended perfect codes // Proc. of the Int. Workshop on Coding and Cryptography (Paris, France. January 8–12, 2001). P. 329–334.

[140] *Krotov D. S., Avgustinovich S. V.* On the Number of 1-Perfect Binary Codes: A Lower Bound // IEEE Trans. Inform. Theory. 2008. V. 54, N 4. P. 1760–1765.

[141] *Kumar P. V., Scholtz R. A., Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory. Ser. A. 1985. V. 40, N 1. P. 90–107.

[142] *Kuzmin A. S., Markov V. T., Nechaev A. A., Shishkin V. A., Shishkov A. B.* Bent- and hyperbent-functions over a field of 2^ℓ elements // Tenth Int. Workshop «Algebraic and Combinatorial Coding Theory» (Zvenigorod, Russia. September 3–9, 2006). Proc. 2006. P. 178–181.

[143] `http://langevin.univ-tln.fr/project/quartics/` — Classification of Boolean Quartics Forms in eight Variables (Langevin P.). 2008.

[144] *Langevin P., Leander G.* Monomial bent functions and Stickelberger's theorem // Finite Fields and Applications. 2008. V. 14. P. 727–742.

[145] *Langevin P., Leander G., McGuire G.* Kasami Bent Functions are Not Equivalent to Their Duals // submitted, 2007.

[146] *Langevin P., Rabizzoni P., Véron P., Zanotti J.-P.* On the number of bent functions with 8 variables // Second International Conference BFCA — Boolean Functions: Cryptography and Applications (Rouen, France, March 13-15, 2006). Proc. 2006. P. 125–135.

[147] *Leander N. G.* Monomial bent functions // IEEE Trans. Inform. Theory. 2006. V. 52, N 2. P. 738–743.

[148] *Leander N. G., Langevin P.* On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin // Algebraic Geometry and its applications (France, May 7–11, 2007) Proc. 2008. P. 410–418.

[149] *Leander N. G., McGuire G.* Construction of bent functions from near-bent functions // J. Comb. Theory, Series A. 2009. V. 116. N 4. P. 960–970.

[150] *Leveiller S., Zemor G., Guillot P. and Boutros J.* A new cryptanalytic attack for PN-generators filtered by a Boolean function // Selected Areas of Cryptography — SAC 2002. Proc. P. 232–249 (Lecture Notes in Comput. Sci. V. 2595).

[151] *Maitra S., Sarkar P.* Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables // IEEE Trans. Inform. Theory. 2002. V. 48, N 9. P. 2626–2630.

[152] *Mansoori S. D., Bizaki H. K.* On the vulnerability of simplified AES algorithm against linear cryptanalysis // Internat. J. of Computer Science and Network Security. 2007. V. 7, N 7. P. 257–263.

[153] *Matsufuji S., Imamura K.* Real-valued bent functions and its application to the design of balanced quadriphase sequences with optimal correlation properties // Int. Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes — AAECC-8 (Tokyo, Japan. August 20–24, 1990). Proc. 1990. P. 106–112 (Lecture Notes in Comput. Sci. V. 508).

[154] *Matsui M.* Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT'93. Workshop on the theory and application of cryptographic techniques (Lofthus, Norway. May 23–27, 1993). Proc. Berlin: Springer, 1994. P. 386–397 (Lecture Notes in Comput. Sci. V. 765).

[155] *Matsui M.* New structure of Block Ciphers with Provable Security Against Differential and Linear Cryptanalysis // Advances in Cryptology – EUROCRYPT'96. Workshop on the theory and application of cryptographic techniques (Saragossa, Spain. May 12–16, 1996). Proc. Springer-Verlag. P. 205–218 (Lecture Notes in Comput. Sci. V. 1070).

[156] *Matsui M., Yamagishi A.* A new method for known plaintext attack of FEAL cipher // Advances in Cryptology – EUROCRYPT'92. Workshop

on the theory and application of cryptographic techniques (Balatonfured, Hungary. May 24–28, 1992). Proc. Berlin: Springer, 1993. P. 81–91 (Lecture Notes in Comput. Sci. V. 658).

[157] *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15, N 1. P. 1–10.

[158] *Meng Q., Yang M. C., Zhang H., Cui J.-S.* A novel algorithm enumerating bent functions // Cryptology ePrint Archive, Report 2004/274, available at `http://eprint.iacr.org/`.

[159] *Meng Q., Zhang H., Wang Z.* Designing bent functions using evolving computing // Acta Electronica Sinica. 2004. No. 11. P. 1901–1903.

[160] *Meng Q., Zhang H., Yang M. C., Cui J.* On the degree of homogeneous bent functions // Available at `http://eprint.iacr.org`, 2004/284.

[161] *Meng Q., Zhang H., Yang M. C., Cui J.* On the degree of homogeneous bent functions // Discrete Applied Mathematics, 2007. V. 155, N 5. P. 665–669.

[162] *Millan W., Clark A., Dawson E.* An effective genetic algorithm for finding highly nonlinear Boolean functions // First Int. conference on Information and Communications Security — ICICS'97. (Beijing, China, November 11–14, 1997). Proc. Springer-Verlag, 1997. P. 149–158 (Lecture Notes in Comput. Sci. V. 1334).

[163] *Millan W., Clark A., Dawson E.* Smart hill climbing finds better Boolean functions // Workshop on Selected Areas in Cryptology. 1997. Workshop record. P. 50–63.

[164] *Nakahara J. Jr.* A Linear Analysis of Blowfish and Khufu // Information Security Practice and Experience — ISPEC 2007. Third International Conference (Hong Kong, China. May 7–9, 2007). Proc. 2007. P. 20–32 (Lecture Notes in Comput. Sci. V. 4464).

[165] *Nakahara J., Preneel B., Vandewalle J.* Experimental Non-Linear Cryptanalysis // COSIC Internal Report. Katholieke Universiteit Leuven. 2003. 17 p.

[166] *Nyberg K.* Perfect nonlinear S-boxes // Advances in cryptology — EUROCRYPT'1991. Int. conference on the theory and application of cryptographic techniques (Brighton, UK. April 8–11, 1991). Proc. Berlin: Springer, 1991. P. 378–386 (Lecture Notes in Comput. Sci. V. 547).

[167] *Nyberg K.* Differentially uniform mappings for cryptography // Advances in cryptology — EUROCRYPT'1993. Int. conference on the theory and application of cryptographic techniques (Lofthus, Norway. May 23–27, 1993). Proc. Berlin: Springer, 1994. P. 55–64 (Lecture Notes in Comput. Sci. V. 765).

[168] *Nyberg K.* New bent mappings suitable for fast implementation // Fast software encryption'93 (Cambridge, December 9–11, 1993). Proc. Berlin: Springer, 1994. P. 179–184 (Lecture Notes in Comput. Sci. V. 809).

[169] *Olejár D., Stanek M.* On cryptographic properties of random Boolean functions // J. Universal Computer Science. 1998. V. 4. No. 8. P. 705–717.

[170] *Olsen J. D., Scholtz R. A., Welch L. R.* Bent-function sequences // IEEE Trans. Inform. Theory. 1982. V. 28, N 6. P. 858–864.

[171] *Parker M. G.* The constabent properties of Golay-Davis-Jedwab sequences // IEEE International Symposium on Information Theory — ISIT'2000. (Sorrento, Italy. June 25-30, 2000). Proc. 2000. P. 302.

[172] *Parker M. G., Pott A.* On Boolean Functions Which Are Bent and Negabent // Sequences, Subsequences, and Consequences — SSC 2007 — International Workshop. (Los Angeles, CA, USA. May 31 – June 2, 2007). Proc. Berlin: Springer. 2007. P. 9–23 (Lecture Notes in Comput. Sci. V. 4893).

[173] *Paterson K. G.* Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. – Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. P. 46–71.

[174] *Paterson K. G.* On codes with low Peak-to-Average Power Ratio for Multicode CDMA // IEEE Trans. Inform. Theory. 2004. V. 50, N 3. P. 550–558.

[175] *Poinsot L.* Multidimensional bent functions // GESTS International Transactions on Computer Science and Engeneering. 2005. V. 18. N 1 P. 185–195.

[176] *Poinsot L., Harari S.* Nonabelian bent functions // IEEE Trans. Inform. Theory., to appear. See for details `http://poinsot.univ-tln.fr/publi.html`

[177] *Poinsot L., Harari S.* Generalized Boolean bent functions // Progress in Cryptology — Indocrypt 2004 (Chennai (Madras), India. December 20 – 22, 2004). Proc. Springer. P. 107–119 (Lecture Notes in Comput. Sci. V. 3348).

[178] *Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandevalle J.* Propogation characteristics of Boolean functions // Advances in cryptology — EUROCRYPT'1990. Int. conference on the theory and application of cryptographic techniques (Aarhus, Denmark. May 21–24, 1990). Proc. Berlin: Springer, 1991. P. 161–173 (Lecture Notes in Comput. Sci. V. 473).

[179] *Preneel B.* Analysis and design of cryptographic hash functions // Ph. D. thesis, Katholieke Universiteit Leuven, 3001 Leuven, Belgium. 1993.

[180] *Qu C., Seberry J., Pieprzyk J.* Homogeneous bent functions // Discrete Appl. Math. 2000. V. 102, N 1-2. P. 133–139.

[181] *Riera C., Parker M.G.* Generalised Bent Criteria for Boolean Functions (I) // IEEE Trans. Inform. Theory 2006. V. 52, N 9. P. 4142–4159.

[182] *Rodier F.* Asymptotic nonlinearity of Boolean functions // Designs, Codes and Cryptography. 2006. V. 40. No. 1. P. 59–70. Preprint is available at `http://iml.univ-mrs.fr/editions/preprint2003/files/RodierFoncBool.pdf`

[183] *Rodier F.* Private Communication. 2008.

[184] *Rothaus O.* On bent functions // IDA CRD W.P. No. 169. 1966.

[185] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20, N 3. P. 300–305.

[186] *Sakurai K., Furuya S.* Improving linear cryptanalysis of LOKI91 by probabilistic counting method // Fast Software Encryption, 4th International Workshop — FSE'97. (Haifa, Israel. January 20-22, 1997) Proc. Berlin: Springer, 1997. P. 114–133 (Lecture Notes in Comput. Sci. V. 1267).

[187] *Savicky P.* On the bent Boolean functions that are symmetric // Eur. J. Combinatorics. 1994. V. 15, N 4. P. 407–410.

[188] *Schmidt K-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // IEEE International Symposium on Information Theory — ISIT'2007. (Nice, France. June 24–29, 2007). Proc. 2007. P. 2781–2785. Available at `http://arxiv.org/abs/cs.IT/0611162`.

[189] *Selçuk A. A.* On Probability of Success in Linear and Differential Cryptanalysis // J. Cryptology. 2008. V. 21. N. 1. P. 131–147.

[190] *Shimoyama T., Kaneko T.* Quadratic relation of S-box and its application to the linear attack of full round DES // Advances in Cryptology — CRYPTO'98, 18th Annual International Cryptology Conference. (Santa Barbara, California, USA. August 23-27, 1998) Proc. Springer. 1998. P. 200–211 (Lecture Notes in Comput. Sci. V. 1462).

[191] *Shorin V.V., Jelezniakov V.V. Gabidulin E.M.* Linear and Differential Cryptanalysis of Russian GOST // Proc. of the Int. Workshop on Coding and Cryptography (Paris, France. January 8–12, 2001). P. 467–476.

[192] *Shorin V.V., Jelezniakov V.V. Gabidulin E.M.* Linear and Differential Cryptanalysis of Russian GOST // Electronic Notes in Discrete Mathematics, V. 6. April 2001. P. 538–547.

[193] *Siegentaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. V. IT-30, N 5. P. 776–780.

[194] *Solé P.* A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties // Third International Colloquium «Coding Theory and Applications» (Toulon, France. November 2–4, 1988). Proc. Springer. 1989. P. 193–201 (Lecture Notes in Comput. Sci. V. 388).

[195] *Solé P., Tokareva N.* Connections between quaternary and binary bent functions // Cryptology ePrint Archive, Report 2009/544, available at `http://eprint.iacr.org/`.

[196] *Tarannikov Yu.* On Resilient Boolean Functions with Maximal Possible Nonlinearity // INDOCRYPT 2000 — First International Conference in Cryptology in India (Calcutta, India. December 10–13, 2000). Proc. Springer. 2000. P. 19–30 (Lecture Notes in Comput. Sci. V. 1977).

[197] *Tarannikov Yu.* On some connections between codes and cryptographic properties of Boolean functions // Seventh Int. Workshop «Algebraic and Combinatorial Coding Theory» (Bansko, Bulgaria. June 18–24, 2000). Proc. 2000. P. 299–304.

[198] *Tapiador J. M. E., Clark J. A., Hernandez-Castro J. C.* Non-linear Cryptanalysis Revisited: Heuristic Search for Approximations to S-Boxes // Proc. 11th IMA International Conference. Cirencester, UK. December

18–20, 2007. Berlin: Springer, 2007. P. 99–117 (Lecture Notes in Comput. Sci. V. 4887).

[199] *Tokareva N. N.* k-Bent functions and quadratic approximations in block ciphers // Proc. Fourth International Conference BFCA — Boolean Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). P. 132–148.

[200] *Wada T.* Characteristic of bit sequences applicable to constant amplitude orthogonal multicode systems // IEICE Trans. Fundamentals. 2000. V. E83-A, N 11. P. 2160–2164.

[201] *Wang X., Zhou J.* Generalized partially bent functions // Future generation communication and networking (Jeju-Island, Korea. December 6–8, 2007) Proc. 2007. P. 16–21.

[202] *Wang L., Zhang J.* A best possible computable upper bound on bent functions // J. West of China. 2004. V. 33. No. 2. P. 113–115.

[203] *Xia T., Seberry J., Pieprzyk J., Charnes C.* Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$ // Discrete Applied Mathematics. 2004. V. 142, N 1–3. P. 127–132.

[204] *Yang M., Meng Q., Zhang H.* Evolutionary design of trace form bent functions // Cryptology ePrint Archive, Report 2005/322, available at `http://eprint.iacr.org/`.

[205] *Youssef A. and Gong G.* Hyper-bent functions // Advances in cryptology — EUROCRYPT'2001. Int. conference on the theory and application of cryptographic techniques (Innsbruk, Austria. May 6–10, 2001). Proc. Berlin: Springer, 2001. P. 406–419 (Lecture Notes in Comput. Sci. V. 2045).

[206] *Youssef A. M.* Generalized hyper-bent functions over $GF(p)$ // Discrete Applied Math. 2007. V. 155, N 8. P. 1066–1070.

[207] *Yu N. Y., Gong G.* Constructions of quadratic bent functions in polynomial forms // IEEE Trans. Inform. Theory 2006. V. 52. No. 7. P. 3291–3299.

[208] *Zhang B., Lü S.* I/O correlation properties of bent functions // Science in China Series E: Technological Sciences. 2000. V. 43, N 3. P. 282–286.

[209] *Zhe-Xian Wan.* Quaternary codes. Singapore: World Scientific Publishing Co. Pte. Ltd, 1997.

[210] *Zheng Y., Zhang X.-M.* Relationships between Bent Functions and Complementary Plateaued Functions // ICISC'99 — International Conference on Information Security and Cryptology (Seoul, Korea. December 9–10, 1999). Proc. Berlin: Springer. 2000. P. 60–75 (Lecture Notes in Comput. Sci. V. 1787).

[211] *Zheng Y., Zhang X.-M.* On Plateaued Functions // IEEE Trans. Inform. Theory. 2001. V. 47, N 3. P. 1215–1223.