

РОССИЙСКАЯ АКАДЕМИЯ НАУК
СИБИРСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТ МАТЕМАТИКИ им. С. Л. СОБОЛЕВА

На правах рукописи
УДК 519.1, 519.7

Токарева Наталья Николаевна

**Сильно нелинейные булевы функции:
бент-функции и их обобщения**

01.01.09 — дискретная математика и математическая кибернетика

Диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
к.ф.-м.н.
Ю.Л. Васильев

Новосибирск — 2008

Оглавление

Введение	4
1 Бент-функции и их обобщения	19
1.1 Определения и обозначения	19
1.2 Конструкции и свойства	21
1.3 О числе бент-функций и двоичных кодов	24
1.4 Обобщения бент-функций	25
1.4.1 Платовидные функции	25
1.4.2 Частично бент-функции	26
1.4.3 Частично определенные бент-функции	26
1.4.4 q -Значные бент-функции	26
1.4.5 Обобщенные булевы бент-функции	27
1.4.6 Полу-бент-функции (semi-bent functions)	27
1.4.7 Ненормальные бент-функции (nonnormal bent functions)	28
1.4.8 Бент-функции на конечной абелевой группе	29
1.4.9 Однородные бент-функции (homogeneous bent functions)	29
1.4.10 Гипер-бент-функции (hyper-bent functions)	30
1.4.11 \mathbb{Z} -бент-функции	30
1.4.12 Нега-бент-функции, бент ₄ -функции, I-бент-функции .	31
1.5 Векторные бент-функции	32
1.6 Другие направления	35
2 Понятие k-бент-функции	36
2.1 Определения и обозначения	36
2.2 Коды с параметрами кодов Адамара	37
2.3 Бинарная операция $\langle \mathbf{u}, \mathbf{v} \rangle_k$	43
2.4 Понятие k -аффинной функции	48

2.5	Понятие k -бент-функции	50
3	Построение k-бент-функций и их свойства	53
3.1	k -Бент-функции от малого числа переменных	54
3.1.1	Описание	54
3.1.2	Замечания	59
3.2	Индуктивный способ построения k -бент-функций	60
3.3	Взаимосвязь k -бент-функций с бент-функциями	64
4	Квадратичные аппроксимации в блочных шифрах	67
4.1	Линейный криптоанализ и его модификации	67
4.1.1	Линейный криптоанализ	67
4.1.2	Проблемы нелинейного криптоанализа	69
4.1.3	Квадратичный криптоанализ	70
4.2	Класс аппроксимирующих функций Δ_m	71
4.3	Квадратичные аппроксимации в блочных шифрах	75
4.4	Анализ четырехразрядных подстановок в S-блоках алгоритмов ГОСТ, DES, s^3 DES	81
4.5	Замечания и дополнения	87
4.6	Приложение	89
5	Приложение. Доказательство Теоремы 1	91
5.1	Равномерно упакованные коды	91
5.2	Три леммы	92
5.3	Верхняя оценка	96
	Заключение	99
	Благодарности	101
	Список литературы	102
	Предметный указатель	118

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 важный класс булевых функций, обладающих сильными свойствами нелинейности: бент-функции и их обобщения.

Мера нелинейности является важной характеристикой булевой функции. 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 (что является типичной ситуацией в математике) наибольший интерес вызывают те функции, для которых эти свойства экстремальны. Такие булевы функции называются *максимально-нелинейными* (или *бент-*) *функциями*².

Приведем ряд определений.

Пусть $\mathbf{u} = (u_1, \dots, u_m)$, $\mathbf{v} = (v_1, \dots, v_m)$ — двоичные векторы длины m . Обозначим через $\langle \mathbf{u}, \mathbf{v} \rangle$ их скалярное произведение по модулю 2,

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 \oplus \dots \oplus u_m v_m,$$

где \oplus означает сложение над \mathbb{Z}_2 . *Булевой функцией* от m переменных называется произвольная функция из \mathbb{Z}_2^m в \mathbb{Z}_2 . Булева функция f от переменных v_1, \dots, v_m называется *аффинной*, если она имеет вид

$$f(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle \oplus a$$

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

²В литературе встречается также термин *совершенно нелинейные функции*.

для некоторого вектора $\mathbf{u} \in \mathbb{Z}_2^m$ и константы $a \in \mathbb{Z}_2$. *Расстоянием Хэмминга* между векторами \mathbf{u} , \mathbf{v} называется число координат, в которых они различаются. Под расстоянием между двумя булевыми функциями от m переменных понимается расстояние Хэмминга между их векторами значений длины 2^m .

Максимально нелинейной называется булева функция от m переменных (m — любое натуральное число) такая, что расстояние Хэмминга от данной функции до множества всех аффинных функций является максимально возможным. В случае четного m это максимально возможное расстояние равно $2^{m-1} - 2^{(m/2)-1}$. В случае нечетного m точное значение максимального расстояния неизвестно (поиск этого значения или его оценок представляет весьма любопытную и сложную комбинаторную задачу [99, 86]). Термин «максимально нелинейная функция» принят в русскоязычной литературе, тогда как в англоязычной широкое распространение получил термин «бент-функция» (от англ. слова bent³ — изогнутый, наклоненный). Аналогия между терминами не полная. При четном числе переменных m бент-функции и максимально нелинейные функции совпадают, а при нечетном m бент-функции (в отличие от максимально нелинейных) не существуют.

Преобразование Уолша—Адамара булевой функции f от m переменных называется целочисленная функция W_f , заданная на множестве \mathbb{Z}_2^m двоичных векторов длины m равенством

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

В литературе функцию W_f также называют *дискретным преобразованием Фурье* или *преобразованием Адамара* функции f . Значения $W_f(\mathbf{v})$, $\mathbf{v} \in \mathbb{Z}_2^m$, называются *коэффициентами Уолша—Адамара* функции f . Для них справедливо равенство Парсеваля:

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

Поскольку число всех коэффициентов равно 2^m , из равенства следует, что максимум модуля коэффициента Уолша—Адамара не может быть меньше

³Английское слово bent очень многозначно; среди его значений: «изогнутый», «кривой», «натяжение», «напряженное состояние», «призвание», а еще и «соцветие подорожника».

величины $2^{m/2}$. Заметим, что расстояние Хэмминга от произвольной булевой функции f до множества всех аффинных функций тесно связано с коэффициентами Уолша—Адамара этой функции. А именно, это расстояние равно величине $2^{m-1} - \frac{1}{2} \max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f(\mathbf{v})|$. Очевидно, что чем меньше максимум модуля коэффициента Уолша—Адамара функции f , тем больше это расстояние.

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

В геометрической (кодовой) интерпретации векторы значений всех аффинных булевых функций от m переменных образуют двоичный линейный код Адамара (или иначе его называют код Рида—Маллера первого порядка) длины 2^m , а векторы значений бент-функций удалены от этого кода на максимально возможное расстояние Хэмминга $2^{m-1} - 2^{(m/2)-1}$ (при четном m).

Бент-функции были введены О. Ротхаусом еще в 60-х годах XX века, хотя его работа [121] на эту тему была опубликована лишь в 1976 году. Дж. Диллон [70] и Р. Л. МакФарланд [104] рассматривали бент-функции в связи с разностными множествами. В настоящее время известно большое число конструкций бент-функций, см. обзоры [15, 76, 52]. Тем не менее класс всех бент-функций от m переменных до сих пор не описан, для мощности этого класса не найдена асимптотика и не установлено даже приемлемых нижних и верхних оценок (некоторые продвижения в этом направлении можно найти в работе [60]).

Масштабы исследования бент-функций и их приложений поистине впечатляют. В настоящее время несколько сотен математиков и инженеров по всему миру регулярно публикуют свои статьи по этой тематике. Результаты обсуждаются на таких международных конференциях как EUROCRYPT,

CRYPTO, ASIACRYPT, INDOCRYPT, SETA, FSE, AAECSS, ISIT, ITW, BFCA, ACST, SIBECRYPT, МаБИТ и многих других. А счет общего числа публикаций о бент-функциях (и близких вопросах) уже идет на тысячи. К сожалению, публикаций на русском языке (по крайней мере, в открытой печати) известно не так уж много — всего несколько десятков. Своей работой мне хотелось бы привлечь внимание, прежде всего, российских исследователей к этой активно развивающейся области.

Так почему же бент-функции столь популярны? В качестве ответа приведем (далеко не полную) серию примеров теоретических и практических приложений бент-функций в комбинаторике, алгебре, теории кодирования, теории информации, теории символьных последовательностей, криптографии и криптоанализе.

Классическая комбинаторная задача построения *матриц Адамара* порядка n , известная с 1893 года, в случае $n = 2^m$ (m чётно) при некоторых ограничениях сводится к задаче построения бент-функций от m переменных [121]. В теории конечных групп построение *элементарных адамаровых разностных множеств* специального вида эквивалентно построению максимально нелинейных булевых функций, см. [15]. 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 [99, 86]. В теории оптимальных кодов специальные семейства квадратичных бент-функций определяют класс *кодов Кердока* [87], обладающих исключительным свойством: вместе с растущим кодовым расстоянием (при увеличении длины кода) каждый код Кердока имеет максимально возможную мощность, см. [69, 25]. 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 разветвлений* (orthogonal spreads) в конечном векторном пространстве [85], 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 [52]. В принципе тем же способом можно строить

линейные коды из любых булевых функций, но только бент-коды будут иметь всего два ненулевых значения для весов кодовых слов и при этом максимально возможные кодовые размерности.

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) [112]. Поэтому такие семейства успешно применяются в коммуникационных системах коллективного доступа. Генераторы бент-последовательностей легко инициализируются случайным образом и могут быстро перестраиваться с одной последовательности на другую. Этот факт используется в работе со стандартом CDMA — Code Division Multiple Access (множественный доступ с кодовым разделением каналов) — одним из двух стандартов для цифровых сетей сотовой связи в США. Отметим здесь же, что в системах CDMA для предельного снижения отношения пиковой и средней мощностей сигнала (peak-to-average power ratio) используются, так называемые, коды постоянной амплитуды (constant-amplitude codes). И например, четверичные такие коды можно построить с помощью обобщенных булевых бент-функций [123]. Не обходится без бент-функций или их аналогов и в квантовой теории информации, см. например, [118].

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 основным методам криптоанализа — линейному [102] и дифференциальному [36], см. подробнее [17]. Стойкость достигается за счет использования сильно нелинейных булевых функций в S-блоках (важнейших компонентах современных шифров) [110, 28], см., например, шифр CAST. Бент-функции и их обобщения находят свое применение также в схемах аутентификации [58], хэш-функциях и псевдослучайных генераторах [18].

Широко исследуются различные обобщения, подклассы и надклассы бент-функций, такие как *платовидные функции* [15], *частично бент-функции* [15], *частично определенные бент-функции* [15], *q-значные бент-функции* [93, 2], *обобщенные булевы бент-функции* [123], *полу-бент-функции*

[64], *ненормальные бент-функции* [48], *бент-функции на конечной абелевой группе* [13], *однородные бент-функции* [117], *гипер-бент-функции* [135], *\mathbb{Z} -бент-функции* [77], *нега-бент-функции* [114] и др. 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.

Обзоры некоторых результатов о бент-функциях можно найти в замечательной российской монографии 2004 года О. А. Логачева, А. А. Сальникова и В. В. Яценко [15], статье немецких криптографов Х. Доббертина и Г. Леандера [76] 2004 года, главах [52] и [53] французского математика и криптографа К. Карле, написанных для готовящейся к печати книги «Boolean Methods and Models» (2008 год). Однако, любой обзор в этой области очень быстро устаревает и а priori неполон.

В данной диссертации в рамках теоретико-кодowego подхода вводится новое обобщение бент-функций — *k -бент-функции*, — отражающее возможность поэтапного усиления (с ростом целого параметра k) нелинейных свойств булевой функции. Основная идея обобщения заключается в том, что принадлежность функции f классу бент-функций не исключает того, что f может оказаться достаточно хорошо аппроксимируемой функциями, являющимися нелинейными, но обладающими свойством «линейности в другом смысле». Опираясь на недавние результаты теории кодирования, связанные с исследованием альтернативной «линейности» кодов, мы выделяем $m/2$ различных типов «линейности» булевой функции от m переменных, схожих с обычной линейностью. Для этого строится специальная серия из $m/2$ кодов типа Адамара, на каждом из которых возможно определение групповой операции, согласованной с метрикой Хэмминга. Кодовые слова этих кодов есть векторы значений булевых функций вида $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$, где операция $\langle \cdot, \cdot \rangle_k$ для каждого k , $1 \leq k \leq m/2$, является аналогом скалярного произведения векторов. Булеву функцию назовем *k -бент-функцией*, $1 \leq k \leq m/2$, если она максимально нелинейна при k различных типах «линейности» одновременно. В таком определении 1-бент-функции совпадают с обычными бент-функциями, — т. е. «линейность» номер 1 есть

линейность в обычном смысле, — а $(m/2)$ -бент-функции могут считаться «наиболее нелинейными» в данной иерархии. В работе исследуются свойства k -бент-функций, приводятся способы их построения, классификация таких функций от малого числа переменных и возможные приложения k -бент-функций в криптографии. А именно, рассматривается возможность квадратичного криптоанализа блочных шифров на основе квадратичных аппроксимаций специального вида. Показано, что использование k -бент-функций в качестве функций шифрования предельно повышает стойкость шифра к данным квадратичным аппроксимациям.

Отметим, что наш подход предполагает дальнейшие обобщения: в частности, появление новых типов «линейности» приведет к вопросам существования соответствующих «бент»-функций и т. п. Возникает естественный вопрос: существует ли «самая нелинейная» булева функция? Полагаю, что задача в такой общей постановке лишена смысла. Во-первых, из-за невозможности дать строгое определение понятию «линейности». А во-вторых — из-за противоречивости тех свойств, которыми должна обладать искомая функция (в этом можно убедиться на простых примерах). Считаю, что исследовать «нелинейные» свойства функций имеет смысл лишь при конкретном понимании «линейности», представляющем интерес для теоретических или практических приложений.

В **первой главе** диссертации приводятся основные понятия и обзор известных результатов о бент-функциях. Особое внимание уделяется известным обобщениям бент-функций, пока еще очень слабо освещенным в обзорной литературе. Отдельный раздел главы посвящен векторным бент-функциям. Отмечается аналогия между проблемами нижних—верхних оценок для числа бент-функций и числа двоичных кодов, таких как совершенные и равномерно упакованные. Для числа равномерно упакованных двоичных кодов в **Теореме 1** устанавливается новая (лучшая на данный момент) верхняя оценка (доказательство теоремы приведено в главе 5).

Во **второй главе** вводится специальная серия двоичных кодов типа Адамара, с помощью которой определяются бинарные операции $\langle \cdot, \cdot \rangle_k$ на множестве двоичных векторов и изучаются их свойства; определяются k -преобразование Уолша—Адамара, k -нелинейность булевой функции, и вводится понятие k -бент-функции.

С 90-х годов в теории кодирования активно стали исследоваться нелинейные коды, образы которых под действием подходящих (как правило, взаимно-однозначных и изометричных) отображений в другие метрические пространства линейны. Так, ярким примером служат \mathbb{Z}_4 -линейные коды — двоичные коды, прообразы которых относительно отображения Грея

$$\varphi : 0 \rightarrow 00, 1 \rightarrow 01, 2 \rightarrow 11, 3 \rightarrow 10,$$

являются линейными кодами над кольцом \mathbb{Z}_4 . Интересно, что многие нелинейные в обычном смысле двоичные коды (среди них коды Кердока, Препараты, Геталса и др.) оказались \mathbb{Z}_4 -линейными, см. работы 1989 года А. А. Нечаева [19] и П. Солé [129], работу 1994 года А. Р. Хэммонса и др. [80]. Можно сказать, что это явление *альтернативной линейности*, которое удалось обнаружить, послужило ключом к структуре таких кодов и впервые позволило перенести богатый аппарат линейных методов теории кодирования в нелинейную область, см. [65, 20, 9, 91, 50, 39, 38], обзор [138] и другие работы. В данной диссертации альтернативный подход к линейности используется для изучения булевых функций.

Рассмотрим \mathbb{Z}_2 - и \mathbb{Z}_4 -линейные коды с параметрами кодов Адамара (далее кратко — *коды типа Адамара*). Известно, что \mathbb{Z}_2 -линейный (т. е. линейный в обычном смысле) двоичный код Адамара длины 2^m единствен с точностью до эквивалентности. Д. С. Кротовым [91] было показано, что существуют в точности $\lfloor m/2 \rfloor$ попарно неэквивалентных \mathbb{Z}_4 -линейных кодов типа Адамара длины 2^{m+1} при $m > 2$. Опираясь на классификацию [91] всех таких кодов, рассмотрим специальную серию двоичных кодов типа Адамара A_m^k , $1 \leq k \leq m/2$, длины 2^m (m четно). В этой серии каждый код A_m^k получается из линейного над \mathbb{Z}_4 кода \mathcal{A}_m^k заменой элементов 0, 1 на 0 и элементов 2, 3 на 1 в каждой координате, где \mathcal{A}_m^k — подкод соответствующего линейного четверичного кода Адамара типа $4^k 2^{m-2k}$ (см. [91]), состоящий из всех кодовых векторов, имеющих в первой координате только 0 или 2. Каждый код A_m^k образует абелеву группу относительно операции \bullet , индуцированной операцией $+$ покоординатного сложения над \mathbb{Z}_4 , определенной на векторах кода \mathcal{A}_m^k .

Теорема 2. *При четном m , целом k , $1 \leq k \leq m/2$, выполняются*

(i) *код A_m^k является кодом с параметрами кода Адамара;*

- (ii) код A_m^1 линеен, коды $A_m^1, \dots, A_m^{m/2}$ попарно неэквивалентны;
- (iii) операция \bullet , заданная на A_m^k , согласована с метрикой Хэмминга.

Множество \mathfrak{A}_m^k булевых функций, векторами значений которых являются кодовые векторы кода A_m^k , представляет собой аналог множества аффинных функций — это функции вида $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$, где $a \in \mathbb{Z}_2$ и операция $\langle \cdot, \cdot \rangle_k$ играет роль скалярного произведения. Такие функции далее названы *k-аффинными*⁴. Коды A_m^k выбраны таким образом, чтобы операции $\langle \cdot, \cdot \rangle_k$ обладали многими свойствами обычного скалярного произведения и на их основе оказались возможными конструктивные построения. Отметим, что каждая операция $\langle \cdot, \cdot \rangle_k$ при $k \geq 2$ не является билинейной формой. Явный вид операции $\langle \mathbf{u}, \mathbf{v} \rangle_k$ следующий.

Теорема 3. Пусть m, k — целые, $1 \leq k \leq m/2$. Для любого целого i , $1 \leq i \leq m/2$, 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

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \left(\bigoplus_{i=1}^k \bigoplus_{j=i}^k Y_i Y_j \right) \oplus \langle \mathbf{u}, \mathbf{v} \rangle.$$

Каждый класс функций \mathfrak{A}_m^k состоит из $2^{m-k+1}(k+1)$ аффинных функций и $2^{m-k+1}(2^k - k - 1)$ квадратичных функций.

С помощью операции $\langle \cdot, \cdot \rangle_k$ определяются *k-преобразование Уолша* — Адамара $W_f^{(k)}$ и *k-нелинейность* $N_f^{(k)}$ булевой функции f . Справедлива

Теорема 4 (равенство Парсеваля для $W_f^{(k)}$). Для любой булевой функции f от m переменных выполняется

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

Булеву функцию от четного числа переменных m назовем *максимально k-нелинейной (k-бент-)* функцией, $1 \leq k \leq m/2$, если вектор значений этой функции удален на максимально возможное расстояние $2^{m-1} - 2^{(m/2)-1}$ от каждого кода типа Адамара A_m^j , $j = 1, \dots, k$ (или, что эквивалентно,

⁴Необходимо отметить, что термин «*k-аффинная функция*» в другом значении уже использовался ранее М. Л. Буряковым и О. А. Логачевым [4]. Параметр k в их работе играет роль *уровня аффинности* булевой функции и не имеет ничего общего с параметром, определяемым здесь. К сожалению, такое совпадение терминов было замечено уже достаточно поздно.

$W_f^{(j)}(\mathbf{v}) = \pm 2^{m/2}$ для любого $\mathbf{v} \in \mathbb{Z}_2^m$ и каждого $j = 1, \dots, k$). Другими словами, каждая k -бент-функция одинаково плохо аппроксимируется булевыми функциями из каждого класса \mathfrak{A}_m^j , $j = 1, \dots, k$. Обычные бент-функции представляют собой класс 1-бент-функций. Через \mathfrak{B}_m^k обозначим класс всех k -бент-функций от m переменных.

Результаты второй главы опубликованы в работах [141, 145, 146, 147].

В **третьей главе** изучаются способы построения k -бент-функций и их свойства. Известно, что задача описания бент-функций для произвольного числа переменных m , или хотя бы нахождения хороших нижних и верхних оценок числа таких функций является очень сложной. Об этом свидетельствует, например, тот факт, что число 6 является максимальным значением для m , при котором еще известно точное значение числа бент-функций (равное $5\,425\,430\,528 \simeq 2^{32,3}$, см. описание в [29, 105], и более раннюю работу [116]), несмотря на длительный срок их исследования и большой интерес к этим объектам. В первой части третьей главы дается простое описание класса 2-бент-функций от четырех переменных.

Теорема 5. Пусть параметры i_1, i_2, i_3 и i_4 принимают различные целые значения от 1 до 4. Тогда множество функций \mathfrak{B}_4^2 состоит из всех функций степени 2 с квадратичными частями вида:

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

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

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

$$v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4 \quad (1 \text{ тип}).$$

Тем самым, параметр $m = 6$ становится наименьшим, при котором k -бент-функции пока не описаны.

Во второй части главы приводится итеративная конструкция k -бент-функций. Пусть \mathfrak{F}_m — множество всех булевых функций от m переменных, \mathfrak{F}_2^1 — множество симметрических функций от двух переменных.

Теорема 6. Пусть числа $m, r \geq 0$ четны, $j \geq 0$ — любое, k такое, что $1 \leq k \leq m/2$, и пусть функция $f \in \mathfrak{F}_{2j+m+r}$ представима в виде

$$f(a_1, a'_1, \dots, a_j, a'_j, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^j s_i(a_i, a'_i) \right) \oplus p(\mathbf{u}') \oplus q(\mathbf{u}''),$$

где $s_1, \dots, s_j \in \mathfrak{F}_2^1, p \in \mathfrak{F}_m$ и $q \in \mathfrak{F}_r$ — функции с непересекающимися множествами переменных. Тогда f принадлежит классу $\mathfrak{B}_{2j+m+r}^{j+k}$, если и только если $s_1, \dots, s_j \in \mathfrak{B}_2^1, p \in \mathfrak{B}_m^k$ и $q \in \mathfrak{B}_r^1$.

В качестве следствия устанавливается, что для $k > \ell \geq 1$ класс k -бент-функций \mathfrak{B}_m^k является собственным подклассом класса ℓ -бент-функций \mathfrak{B}_m^ℓ . Показывается, что существуют k -бент-функции с любой степенью нелинейности d , где $2 \leq d \leq \max\{2, \frac{m}{2} - k + 1\}$.

Пусть $S_{m,k}$ — подгруппа группы S_m подстановок на m элементах, порожденная k транспозициями: $(1, 2), (3, 4), \dots, (2k-1, 2k)$. Пусть \mathfrak{F}_m^k обозначает множество всех функций $f \in \mathfrak{F}_m$, постоянных на каждой орбите множества \mathbb{Z}_2^m под действием группы $S_{m,k}$; справедливо $|\mathfrak{F}_m^k| = 2^{2^{m-k} \log_2 \frac{4}{3}}$. Доказана следующая теорема о связи k -бент-функций и бент-функций.

Теорема 7. При любом четном $m \geq 2$, целом $k, 1 \leq k \leq m/2$, справедливо равенство $\mathfrak{F}_m^k \cap \mathfrak{B}_m^k = \mathfrak{F}_m^k \cap \mathfrak{B}_m^1$.

Результаты третьей главы опубликованы в работах [147, 148, 152].

В **четвертой 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 [101, 102] в 1993 году для шифров FEAL и DES и являющегося в настоящее время одним из наиболее эффективных.

Идея метода линейного криптоанализа заключается 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 $|\varepsilon|^{-2}$.

Общий подход к использованию в линейном криптоанализе нелинейных аппроксимаций предложили в 1996 году Л. Кнудсен и М. Робшау [90]. Основная его идея: 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?* В целом метод нелинейного криптоанализа не получил пока должного развития.

В данной работе предлагается аппроксимировать булевы функции от m переменных v_1, \dots, v_m функциями вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, где π — любая перестановка на m переменных, параметры $\mathbf{u} \in \mathbb{Z}_2^m$, k ($1 \leq k \leq m/2$) произвольны. Класс Δ_m всех таких аппроксимирующих функций может быть описан следующим образом. Пусть $\text{АНФ}(f)$ — алгебраическая нормальная форма функции f ; пусть $\text{Act}(f)$ — подмножество максимальной мощности множества $\{1, 2, \dots, m/2\}$ такое, что для любых различных элементов i, j из $\text{Act}(f)$ одночлены $v_{2i-1}v_{2j-1}$, $v_{2i-1}v_{2j}$, $v_{2i}v_{2j-1}$, $v_{2i}v_{2j}$ принадлежат множеству $\text{АНФ}(f)$. Через $\rho = \rho(f)$ обозначим любую перестановку m переменных такую, что $|\text{Act}(f^\rho)| = \max_{\pi \in S_m} |\text{Act}(f^\pi)|$, где по определению $f^\pi(\cdot) = f(\pi(\cdot))$. Справедлива

Теорема 8. *Булева функция $f \in \mathfrak{F}_m$, 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 ($1 \leq i, j \leq m/2$) 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 $\text{АНФ}(f^\rho)$;

- 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 $i \in \text{Act}(f^\rho)$.

Из теоремы 8 следует, что множество аппроксимирующих 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 для аппроксимации обусловлен наличием простых формул для вычисления расстояния Хэмминга от произвольной булевой функции f до класса $\mathfrak{A}_{m,0}^k(\pi)$ функций $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$ при фиксированных параметрах π и k :

$$\text{dist}(f, \mathfrak{A}_{m,0}^k(\pi)) = 2^{m-1} - \frac{1}{2} \max_{\mathbf{v} \in \mathbb{Z}_2^m} W_f^{(k)}(\mathbf{v}),$$

а также свойствами таких функций, близкими к линейным.

Исследования носят теоретический характер. Предложены модификации алгоритмов 1 и 2 линейного криптоанализа Мацуи [102] 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.

Пусть $F : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m_{\text{key}}} \rightarrow \mathbb{Z}_2^m$ — функция шифрования блочного шифра; P , C и K — открытый текст, шифротекст и ключ соответственно. Пусть вещественное число $\varepsilon(K)$ — преобладание (при фиксированном ключе K) равенства

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = \langle \mathbf{d}, \tau(K) \rangle_k,$$

где $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^m$, $\mathbf{d} \in \mathbb{Z}_2^{m_{\text{key}}}$, перестановки $\pi, \sigma \in S_m$, $\tau \in S_{m_{\text{key}}}$, целые числа i, j, k — некоторым образом выбранные параметры. Упомянутую выше роль k -бент-функций в блочном шифре отражает следующее утверждение.

Теорема 9. Пусть фиксирован ключ K . Если вектор \mathbf{b} , перестановки π, σ и параметр j , таковы что функция

$$\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$$

является $(m/2)$ -бент-функцией, то справедливо равенство

$$\max_{i,k,\mathbf{a},\mathbf{d},\tau} |\varepsilon(K)| = \min_{i,k,\mathbf{a},\mathbf{d},\tau} |\varepsilon(K)| = 2^{-(m/2)-1}.$$

Приведены свойства аппроксимирующих функций $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, которые могут быть использованы при согласовании нелинейных раундовых аппроксимаций в квадратичном криптоанализе. В заключение рассмотрены примеры четырехразрядных подстановок, рекомендованных для применения в узлах замены (S-блоках) алгоритмов ГОСТ 28147-89, DES, s^3 DES; 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.

Результаты четвертой главы опубликованы в работах [150, 151, 153].

В **пятой главе** диссертации приводится доказательство Теоремы 1, формулировка которой дана в первой главе. Результаты главы опубликованы в работах [142, 143, 144].

По теме диссертации опубликовано 13 работ: 4 статьи в журналах, 9 работ в трудах и тезисах международных конференций; см. [141–153]. На web-странице www.math.nsc.ru/~tokareva все они доступны в электронном виде.

Результаты докладывались на российских и международных конференциях: Шестой молодежной научной школе по дискретной математике и ее приложениям в 2007 году в Москве, ISIT'2007 — IEEE Международном Симпозиуме по Теории Информации в Ницце (Франция), Шестой школе-семинаре SIBECRYPT'2007 — «Компьютерная безопасность и криптография» в Горно-Алтайске, международной конференции «Математика в современном мире» в Новосибирске в 2007 году, Четвертой международной конференции BFCA'2008 — «Булевы функции: криптография и приложения» в Копенгагене (Дания), Пятнадцатой международной конференции «Проблемы теоретической кибернетики» в Казани в 2008 году, SIBIRCON-2008 — IEEE Международной Конференции «Вычислительные Технологии в Электрической и Электронной Инженерии» в Новосибирске, Седьмой школе-семинаре SIBECRYPT'2008 — «Компьютерная безопасность и криптография» в Красноярске.

Результаты докладывались на семинарах «Дискретный анализ», «Теория кодирования», «Геометрия, топология и их приложения» и общеинститутском семинаре Института Математики СО РАН; научных семинарах

Института проблем передачи информации им. А. А. Харкевича в Москве; лаборатории информатики, сигналов и систем национального центра научных исследований (I3S CNRS) в Софии Антиполисе (Франция); кафедры защиты информации и криптографии Томского государственного университета. Результаты кандидатской диссертации отмечены премией школы «Компьютерная безопасность и криптография» — SIBECRYPT'2007 — в 2007 году. Работа выполнена при поддержке интеграционного проекта СО РАН N 35 «Древовидный каталог математических Интернет-ресурсов mathtree.ru», Российского фонда фундаментальных исследований (проекты 07-01-00248, 08-01-00671), гранта «Лучшие аспиранты РАН» за 2008 год Фонда содействия отечественной науке, гранта «NUGET» (Agence Nationale de la Recherche, France), совета научной молодежи ИМ СО РАН и Новосибирского государственного университета.

Глава 1

Бент-функции и их обобщения

В данной главе приводятся основные определения — преобразования Уолша—Адамара булевой функции, нелинейности функции, бент-функции и др. Рассматриваются известные конструкции, свойства и обобщения бент-функций. Отмечается аналогия между проблемами нижних—верхних оценок для числа бент-функций и числа двоичных кодов, таких как совершенные и равномерно упакованные. Для числа равномерно упакованных двоичных кодов устанавливается новая (лучшая на данный момент) верхняя оценка.

1.1 Определения и обозначения

Пусть m — натуральное число, всюду далее пусть $n = 2^m$. Через \mathbb{N} обозначим множество натуральных чисел. Пусть $\langle \mathbf{u}, \mathbf{v} \rangle$ — обычное скалярное произведение двоичных векторов $\mathbf{u} = (u_1, \dots, u_m)$, $\mathbf{v} = (v_1, \dots, v_m)$ длины m , т. е. $\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 \oplus \dots \oplus u_m v_m$, где \oplus обозначает сложение по модулю 2. Множество всех булевых функций от m переменных обозначим через \mathfrak{F}_m . Через \mathfrak{A}_m обозначим класс всех аффинных булевых функций $\langle \mathbf{u}, \mathbf{v} \rangle \oplus a$ от m переменных v_1, \dots, v_m . Каждой булевой функции $f \in \mathfrak{F}_m$ соответствует двоичный вектор \mathbf{f} ее значений длины 2^m . Всюду далее векторы, в отличие от функций, будем выделять полужирным шрифтом. Число ненулевых координат двоичного вектора \mathbf{v} называется его *весом Хэмминга* и обозначается через $wt_H(\mathbf{v})$. *Расстояние Хэмминга* $d_H(\mathbf{u}, \mathbf{v})$ между двоичными векторами \mathbf{u}, \mathbf{v} равно числу координат, в которых векторы различаются. Под расстоянием $\text{dist}(f, g)$ между булевыми функциями f и g будем понимать расстояние Хэмминга между соответствующими векторами значений.

Напомним, что для функции $f \in \mathfrak{F}_m$ целочисленная функция W_f , заданная на множестве \mathbb{Z}_2^m двоичных векторов длины m равенством

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

называется *преобразованием Уолша—Адамара* функции f , а значения $W_f(\mathbf{v})$ — *коэффициентами Уолша—Адамара* этой функции.

Для коэффициентов $W_f(\mathbf{v})$ имеет место равенство Парсевала:

$$\sum_{\mathbf{v} \in \mathbb{Z}_2^m} (W_f(\mathbf{v}))^2 = 2^{2m}, \quad (1.1)$$

из которого следует, что $\max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f(\mathbf{v})| \geq 2^{m/2}$. Под *нелинейностью* N_f булевой функции f понимается расстояние от данной функции до множества всех аффинных функций, т. е.

$$N_f = \text{dist}(f, \mathfrak{A}_m) = 2^{m-1} - \frac{1}{2} \max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f(\mathbf{v})|$$

(см. подробнее, например, [15]). Функция $f \in \mathfrak{F}_m$ называется *максимально нелинейной* (m любое), если параметр N_f принимает максимальное возможное значение, и *бент-функцией* (m четное), если все ее коэффициенты Уолша—Адамара равны $\pm 2^{m/2}$. При четном m эти определения совпадают. Класс бент-функций от m переменных обозначим через \mathfrak{B}_m .

Приведем несколько основных понятий теории кодирования. Обозначим через $\langle \mathbb{Z}_2^n, d_H \rangle$ метрическое пространство на множестве двоичных векторов длины n с метрикой Хэмминга. Непустое множество $C \subseteq \mathbb{Z}_2^n$ мощности $|C| = M$ с минимальным расстоянием d между его различными элементами называется *двоичным* (n, M, d)*-кодом* (или *двоичным кодом с параметрами* n , M и d), а его элементы — *кодowymi словами*. Числа n и d называются соответственно *длиной* и *кодovым расстоянием* кода. Код называется *линейным*, если он образует линейное подпространство в \mathbb{Z}_2^n .

В геометрической интерпретации векторы значений всех аффинных булевых функций $\langle \mathbf{u}, \mathbf{v} \rangle \oplus a$ от m переменных образуют двоичный линейный код Адамара длины 2^m , а векторы значений бент-функций удалены от этого кода на максимально возможное расстояние $2^{m-1} - 2^{(m/2)-1}$ (m четно).

1.2 Конструкции и свойства

Бент-функции, как уже упоминалось выше, были введены О. Ротхаусом еще в 60-х годах XX века, хотя работа [121] опубликована лишь в 1976 году. В этой работе были установлены базовые свойства таких функций и предложены их простейшие конструкции.

Напомним, что *матрицей Адамара* A_n называется квадратная $n \times n$ матрица с элементами 1 и -1 , такая что $A_n A_n^T = nE$, где E — единичная матрица. Тесную связь бент-функций от m переменных с матрицами Адамара размера $2^m \times 2^m$ отражают следующие утверждения.

Теорема (Ротхаус, 1976, [121]). *Функция $f \in \mathfrak{F}_m$ является бент-функцией тогда и только тогда, когда матрица $A = (a_{\mathbf{u}, \mathbf{v}})$, где*

$$a_{\mathbf{u}, \mathbf{v}} = \frac{1}{2^{m/2}} W_f(\mathbf{u} \oplus \mathbf{v}),$$

$\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, является $2^m \times 2^m$ матрицей Адамара.

Теорема (Критерий Ротхауса). *Функция $f \in \mathfrak{F}_m$ является бент-функцией тогда и только тогда, когда матрица $D = (d_{\mathbf{u}, \mathbf{v}})$, где*

$$d_{\mathbf{u}, \mathbf{v}} = (-1)^{f(\mathbf{u} \oplus \mathbf{v})},$$

$\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, является матрицей Адамара.

Немного иначе этот критерий звучит так: f — бент-функция тогда и только тогда, когда для любого ненулевого $\mathbf{v} \in \mathbb{Z}_2^m$ функция $f(\mathbf{u}) \oplus f(\mathbf{u} \oplus \mathbf{v})$ сбалансирована (т. е. принимает значения 0 и 1 одинаково часто).

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

Теорема (Ротхаус, 1976, [121]). *Степень нелинейности любой бент-функции f от m переменных не превосходит числа $m/2$.*

В качестве свойства бент-функций можно отметить следующий факт.

Теорема. *Класс \mathfrak{B}_m бент-функций замкнут относительно*

- 1) *любой невырожденной аффинной замены переменных;*
- 2) *прибавления любой аффинной функции.*

Задача описания всех бент-функций от m переменных не решена. Очень сложно не только описать бент-функции полностью, но и предложить отдельные конструкции для них. Приведем несколько известных способов построения бент-функций.

Бент-функции можно построить итеративно.

Теорема (Ротхаус, 1976, [121]). *Функция $f \in \mathfrak{F}_{m'+m''}$ такая, что $f(\mathbf{u}', \mathbf{u}'') = g(\mathbf{u}') \oplus h(\mathbf{u}'')$, где $\mathbf{u}' \in \mathbb{Z}_2^{m'}$, $\mathbf{u}'' \in \mathbb{Z}_2^{m''}$, является бент-функцией тогда и только тогда, когда функции g, h — бент-функции.*

Например, бент-функцией от любого четного числа переменных m является функция $f(v_1, \dots, v_m) = v_1 v_2 \oplus v_3 v_4 \oplus \dots \oplus v_{m-1} v_m$. Отметим, что любая квадратичная бент-функция получается из нее аффинным преобразованием, см. [16].

Приведем простую и богатую конструкцию бент-функций Мэйорана—МакФарланда 1973 года. Именно эта конструкция (не смотря на многочисленные новые исследования) дает наилучшую в настоящий момент нижнюю оценку числа всех бент-функций.

Теорема (Мэйоран—МакФарланд, 1973, [104, 71]). *Пусть $T : \mathbb{Z}_2^{m/2} \rightarrow \mathbb{Z}_2^{m/2}$ — любое взаимно однозначное отображение, $h \in \mathfrak{F}_{m/2}$ — произвольная функция. Тогда функция $f \in \mathfrak{F}_m$ такая, что $f(\mathbf{u}', \mathbf{u}'') = \langle \mathbf{u}', T(\mathbf{u}'') \rangle \oplus h(\mathbf{u}'')$ является бент-функцией.*

Из теоремы легко следует, что существуют бент-функции с любой степенью нелинейности d , такой что $2 \leq d \leq m/2$.

Следующая конструкция опирается на специальные семейства подпространств m -мерного пространства и носит название Partial Spreads (частичные разветвления/распространения). Пусть $\text{Ind}_S : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$ — характеристическая функция подмножества $S \subseteq \mathbb{Z}_2^m$ (принимает значение 1 на элементах из S и значение 0 на остальных элементах).

Теорема (Диллон, 1974, [71]). *Пусть число q равно $2^{(m/2)-1}$ или $2^{(m/2)-1} + 1$. Пусть L_1, \dots, L_q — линейные подпространства размерности $(m/2)$ пространства \mathbb{Z}_2^m такие, что любые два из них пересекаются лишь по нулевому вектору. Тогда функция $f(\mathbf{v}) = \bigoplus_{i=1}^q \text{Ind}_{L_i}(\mathbf{v})$ является бент-функцией.*

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

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

Более общие конструкции в духе класса \mathcal{PS} см., например, в работе [49].

Другая серия конструкций объединяется названием *степенные* (или *мономиальные*) *бент-функции* (power bent functions, monomial bent functions). Пусть векторное пространство \mathbb{Z}_2^m отождествляется с полем Галуа $GF(2^m)$. Булевы функции от m переменных можно рассматривать как функции из $GF(2^m)$ в $GF(2)$, сопоставляя каждому вектору \mathbf{v} соответствующий элемент поля $GF(2^m)$, который будем обозначать тем же символом. Пусть $tr : GF(2^m) \rightarrow GF(2)$ — *функция следа*, т. е. $tr(\mathbf{v}) = \mathbf{v} + \mathbf{v}^2 + \dots + \mathbf{v}^{2^{m-1}}$, где $\mathbf{v} \in GF(2^m)$. Бент-функции, имеющие вид $f(\mathbf{v}) = tr(a\mathbf{v}^d)$, где $a \in GF^*(2^m)$ — некоторый параметр, называются *степенными* (или *мономиальными*), а целое число d называется *бент-показателем*. 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 [52].

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

Теорема. *Следующие значения d являются бент-показателями:*

- $d = 2^{m/2} - 1$ (Диллон \diamond , 1974, [71]);
- $d = 2^i + 1$, где $\frac{m}{\gcd(m,i)}$ чётно (показатель Голда \dagger);
- $d = 2^{2k} - 2^k + 1$, где $\gcd(k, m) = 1$ (показатель Касами);
- $d = (2^k + 1)^2$, где $m = 4k$, k нечётно (Канто–Леандер \dagger , 2004, [97]);
- $d = 2^{2k} + 2^k + 1$, где $m = 6k$ (Канто–Шарпин–Карегян \dagger , 2006, [47]).

Известно, что три типа степенных бент-функций (в теореме их показатели помечены знаком \dagger) 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. И по-прежнему остается актуальной задача поиска любых других конструкций для бент-функций. Хорошие обзоры на затронутые темы можно найти в [15, 76] и [52], см. также отдельные статьи, посвященные свойствам таких функций, например [95].

1.3 О числе бент-функций и двоичных кодов

В данном разделе число переменных булевой функции удобно обозначить через n . Наилучшую нижнюю оценку числа бент-функций от n переменных дает конструкция Мэйорана—МакФарланда (см. выше).

Теорема (Нижняя оценка, 1973, [104, 71]). *Справедливо*

$$|\mathfrak{B}_n| \geq 2^{2^{n/2}} (2^{n/2})!$$

Асимптотически, эта оценка имеет вид $(\frac{2^{(n/2)+1}}{e})^{2^{n/2}} \sqrt{2^{(n/2)+1}\pi}$, или если совсем грубо, $2^{2^{n/2}}$. Тривиальная верхняя оценка следует из того факта, что степень бент-функции не превышает $n/2$. Имеем

$$|\mathfrak{B}_n| \leq 2^{1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n/2}} = 2^{2^{n-1} + \frac{1}{2} \binom{n}{n/2}}.$$

К. Карле и А. Клаппер в 2002 году немного улучшили эту оценку.

Теорема (Верхняя оценка, 2002, [60]). *Выполняется*

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

Хотя по-прежнему верхняя оценка близка к тривиальной 2^{2^n} .

Мне показалось интересным, что аналогичная проблема сильного разрыва между нижней и верхней оценками наблюдается и для числа N_n совершенных двоичных кодов длины $n = 2^s - 1$ с расстоянием 3, см. определение в [16]. Нижнюю оценку вида $2^{2^{n/2}}$ дает конструкция Ю. Л. Васильева 1962 года [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.

Теорема (Васильев, 1962, [5]). *Справедливо $N_n \geq 2^{2^{(n+1)/2}}$.*

Последнее улучшение нижней оценки числа N_n (не меняющее, однако, коэффициент при n в «третьем этаже») можно найти в работе Д. С. Кротова и С. В. Августиновича [92]. А тип верхней оценки числа совершенных кодов по-прежнему остается тривиальным: 2^{2^n} . Небольшое улучшение дает

Теорема (Августинович, 1995, [1]). *Верно $N_n \leq 2^{2^{n - \frac{3}{2} \log_2 n + o(\log_2 n)}}$.*

В данной работе верхняя оценка [1] числа совершенных кодов обобщается на случай произвольных равномерно упакованных кодов. К этому классу относятся коды Препараты, коды БЧХ с расстояниями 5 и 7, коды Геталса и др. Согласно работе Л. А. Бассальго, Г. В. Зайцева и В. А. Зиновьева [3] двоичный код C длины n с кодовым расстоянием d и радиусом покрытия ρ называется *равномерно упакованным в широком смысле*, если существуют действительные числа $\alpha_0, \alpha_1, \dots, \alpha_\rho$ такие, что для любого двоичного вектора x длины n выполняется равенство $\sum_{i=0}^{\rho} \alpha_i f_i(x) = 1$, где $f_i(x)$ — число кодовых слов кода C , находящихся на расстоянии i от вектора x , $i = 0, 1, \dots, \rho$. Класс таких кодов обозначим через $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$, а число различных кодов в нем через $L_{n,d}$. Справедлива

Теорема 1. *При нечетном d выполняется $L_{n,d} < 2^{2^{n-\frac{d}{2} \log_2 n + o(\log_2 n)}}$.*

Доказательство этой теоремы приведено в главе 5.

1.4 Обобщения бент-функций

Кратко рассмотрим различные обобщения и подклассы бент-функций.

1.4.1 Платовидные функции

Функция $f \in \mathfrak{F}_m$ относится к этому классу, если существует положительное целое число M такое, что любой ее коэффициент Уолша—Адамара $W_f(\mathbf{v})$ равен 0 или $\pm M$, см. например [15, 52]. Из равенства Парсеваля (1.1) следует, что число M является степенью двойки, $M = 2^\beta$, и показатель β может принимать целые значения от $m/2$ до m . Число $2(m - \beta)$ часто называют *порядком*, а величину M *амплитудой* платовидной функции f (plateaued function). Бент-функции и аффинные функции являются крайними частными случаями платовидных функций. А именно:

бент-функция — это платовидная функция порядка m ($\beta = m/2$);

аффинная функция — платовидная функция порядка 0 ($\beta = m$).

Результаты о таких функциях можно найти в указанных выше обзорах, а также в работах [139, 140, 61].

1.4.2 Частично бент-функции

Это определение возникает естественным образом при рассмотрении сужений булевой функции на подпространства. Булева функция f от m переменных называется *частично бент-функцией*, если существует разложение пространства \mathbb{Z}_2^m в прямую сумму подпространств U и V четных размерностей такое, что

1) $f(\mathbf{u}, \mathbf{v}) = \langle \mathbf{u}, \mathbf{w} \rangle \oplus f|_V(\mathbf{v})$ для некоторого вектора $\mathbf{w} \in \mathbb{Z}_2^m$ и любых векторов $\mathbf{u} \in U$, $\mathbf{v} \in V$;

2) $f|_V$ — бент-функция.

О свойствах таких функций можно прочитать в монографии [15, гл. 6].

1.4.3 Частично определенные бент-функции

Еще одно определение из серии весьма естественных. Пусть $S \subseteq \mathbb{Z}_2^m$ — произвольное подмножество, $f : S \rightarrow \mathbb{Z}_2$ — *частично определенная булева функция*. Ее *неполным преобразованием Уолша—Адамара* называется отображение

$$W_{f,S}(\mathbf{v}) = \sum_{\mathbf{u} \in S} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle \oplus f(\mathbf{u})}, \text{ для любого } \mathbf{v} \in \mathbb{Z}_2^m.$$

Функция f — *частично определенная бент-функция*, если $W_{f,S}(\mathbf{v}) = \pm \sqrt{S}$ для любого $\mathbf{v} \in \mathbb{Z}_2^m$, см. подробнее [15, гл. 6].

1.4.4 q -Значные бент-функции

Три автора, П. В. Кумар, Р. А. Шольц и Л. Р. Велч [93], ввели в 1985 году такое обобщение бент-функций. Пусть $q \geq 2$ — 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 $f : \mathbb{Z}_q^m \rightarrow \mathbb{Z}_q$. *Преобразованием Уолша—Адамара* функции f называется следующая комплексная функция:

$$W_f(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_q^m} \omega^{\langle \mathbf{u}, \mathbf{v} \rangle + f(\mathbf{u})}, \text{ для любого } \mathbf{v} \in \mathbb{Z}_q^m,$$

где скалярное произведение q -значных векторов и сложение $+$ рассматриваются по модулю q . Функция f называется *бент-функцией*, если для

каждого $\mathbf{v} \in \mathbb{Z}_q^m$ выполняется $|W_f(\mathbf{v})| = q^{m/2}$. Для каждого q , такого что $q \not\equiv 2 \pmod{4}$, и любого четного m в работе [93] предложены конструкции q -значных бент-функций. Во многих других случаях доказано несуществование таких функций. А. С. Амбросимовым [2] в 1994 году изучались свойства q -значных бент-функций над конечными полями. В частности им были описаны и посчитаны все бент-функции степени 2 над произвольным конечным полем.

1.4.5 Обобщенные булевы бент-функции

Другое обобщение бент-функций стал рассматривать в 2006 году К. Шмидт [123]. Для некоторых задач в области циклических кодов оно представляется [130] более естественным, чем определение q -значной бент-функции Кумара, Шольца и Велча, см. 1.4.4. Пусть $q \geq 2$ — натуральное число, $i = \sqrt{-1}$ — мнимая единица. Пусть снова ω — примитивный комплексный корень степени q из единицы, $\omega = e^{2\pi i/q}$. Функция $f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_q$ называется *обобщенной булевой функцией*. Преобразование Уолша—Адамара такой функции называется комплексная функция

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

Если для каждого $\mathbf{v} \in \mathbb{Z}_2^m$ выполняется $|W_f(\mathbf{v})| = 2^{m/2}$, то функция f называется *обобщенной булевой бент-функцией*. В случае $q = 4$ такие бент-функции используются [123] для построения четверичных кодов постоянной амплитуды (quaternary constant-amplitude codes), позволяющих предельно понижать отношение пиковой и средней мощностей сигнала (peak-to-average power ratio) в мультикодовых системах множественного доступа с кодовым разделением каналов (multicode CDMA systems). Системы CDMA, как уже отмечалось выше, используются в цифровых сетях сотовой связи.

1.4.6 Полу-бент-функции (semi-bent functions)

С точки зрения криптографии к важным критериям, которым должна удовлетворять булева функция $f \in \mathfrak{F}_m$, относятся следующие [14, 52]:

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

✓ *критерий распространения* $PC(k)$ *порядка k (Propagation Criterion)* — для любого ненулевого вектора $\mathbf{u} \in \mathbb{Z}_2^m$ веса Хэмминга не более k , где $1 \leq k \leq m$, функция $f(\mathbf{v}) \oplus f(\mathbf{u} \oplus \mathbf{v})$ является сбалансированной [115];

✓ *максимальная нелинейность* — функция f такова, что значение ее нелинейности $N_f = \text{dist}(f, \mathcal{A}_m)$ максимально;

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

Проблема в том, что криптографические критерии противоречат друг другу. Бент-функции являются максимально-нелинейными, удовлетворяют критерию $PC(m)$ и обладают равномерной корреляцией с линейными функциями (значение равно $\pm 2^{-m/2}$). Но бент-функции никогда не сбалансированы. В 1994 году С. Чи, С. Ли и К. Ким [64] предложили понятие *полу-бент-функции* — сбалансированной булевой функции, обладающей при этом лучшей возможной нелинейностью, почти равномерной корреляцией с линейными функциями и удовлетворяющей критерию $PC(k)$ для достаточно большого k . Ясно, что полу-бент-функции и их аналоги — объединяющие противоречивые криптографические свойства — имеют очень важные криптографические приложения.

1.4.7 Ненормальные бент-функции (nonnormal bent functions)

Булева функция f от m переменных называется *нормальной (слабо нормальной)*, если существует $(m/2)$ -мерное подпространство пространства \mathbb{Z}_2^m , такое что f на нем является константой (аффинной функцией). Впервые такие функции стал рассматривать Х. Доббертин [73] в 1995 году для построения сбалансированных булевых функций с высокой нелинейностью. Десять лет вопрос о существовании бент-функций, не являющихся нормальными и слабо нормальными, был открыт. В 2005 году авторам [48] удалось построить такие функции.

1.4.8 Бент-функции на конечной абелевой группе

В 1997 году О. А. Логачев, А. А. Сальников и В. В. Яценко [13] дали следующее определение. Пусть G — конечная абелева группа порядка n и максимальный порядок ее элементов равен m . Пусть $T = \{e^{2\pi i x} \mid 0 \leq x < 1\}$ — группа вращений окружности, T_m — ее подгруппа, состоящая из корней степени m из единицы, T^G — множество функций вида $G \rightarrow T$. Через \hat{G} обозначим группу гомоморфизмов $\chi : G \rightarrow T_m$. Она называется *группой характеров* и изоморфна G (пусть $\mathbf{v} \rightarrow \chi_{\mathbf{v}}$ — соответствующий изоморфизм). *Преобразование Фурье* комплекснозначной функции $f : G \rightarrow \mathbb{C}$ задается равенством $\hat{f}_G(\mathbf{v}) = \sum_{\mathbf{u} \in G} f(\mathbf{u}) \bar{\chi}_{\mathbf{v}}(\mathbf{u})$. *Бент-функцией на группе G* авторы [13] называют функцию $f \in T^G$, для которой выполняется $|\hat{f}_G(\mathbf{v})|^2 = n$ при любом $\mathbf{v} \in G$, где $|\cdot|$ обозначает модуль комплексного числа. Если G является элементарной абелевой 2-группой, то данное понятие совпадает с понятием обычной бент-функции. В [13] приводятся способы построения бент-функций на группах и исследуются их свойства.

Нелинейные свойства функций из одной произвольной конечной абелевой группы $(A, +)$ в другую конечную абелеву группу $(B, +)$ изучали К. Карле и К. Динг [56, 57].

1.4.9 Однородные бент-функции (homogeneous bent functions)

Бент-функция относится к этому классу, если все одночлены ее алгебраической нормальной формы имеют одинаковые степени. Комбинаторная структура функций такого вида заинтересовала в 2000 году авторов статьи [117] Ч. Ку, Дж. Себерри и Й. Пипджика. В своей работе они 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 [63] доказали, что существуют однородные бент-функции степени 3 от любого числа переменных $m > 2$. В работе [134] Т. Кси, Дж. Себерри, Й. Пипджик и К. Чарнес установили, что однородных бент-функций максимальной степени $m/2$ не существует при $m > 3$. Исследователи из Китая К. Менг, Х. Жанг, М. Янг и Дж. Цуи [106, 107] показали, что не существует также однородных бент-функций степени $(m/2) - 1$ при $m > 4$. Но какова же

точная верхняя оценка степени нелинейности однородной бент-функции? На этот вопрос нет ответа. Есть только предположение авторов [106] о том, что для любого $k > 1$ найдется такое $N \geq 2$, что однородная бент-функция степени k от m переменных существует при каждом $m > N$.

1.4.10 Гипер-бент-функции (hyper-bent functions)

В 2001 году А. М. Йоссеф и Г. Гонг [135] предложили приближать булевы функции *собственными мономиальными функциями* (термин был введен позднее в работе [10]). Авторы [135] рассматривали булевы функции от m переменных как функции из $GF(2^m)$ в $GF(2)$, сопоставляя каждому вектору \mathbf{v} соответствующий элемент поля $GF(2^m)$. Известно, что любая линейная функция $\langle \mathbf{u}, \mathbf{v} \rangle$ может быть представлена как $tr(a_{\mathbf{u}}\mathbf{v})$ для подходящего элемента $a_{\mathbf{u}} \in GF(2^m)$. Собственными мономиальными функциями называются функции вида $tr(a_{\mathbf{u}}\mathbf{v}^s)$, где целое число s такое, что $1 \leq s \leq 2^m - 1$ и $\gcd(s, 2^m - 1) = 1$. Булевы функции, одинаково плохо приближающиеся всеми такими функциями, авторы [135] называли *гипер-бент-функциями*, и для каждого четного m доказали их существование. К. Карле и П. Габори [59] и независимо А. С. Кузьмин, В. Т. Марков, А. А. Нечаев и А. Б. Шишков [10] показали, что степень нелинейности любой гипер-бент-функции от m переменных равна $m/2$. Далее мономиальные приближения булевых функций изучались А. В. Ивановым [7, 8].

1.4.11 \mathbb{Z} -бент-функции

В 2005 году Х. Доббертин, см. [77], предложил исследовать бент-функции в контексте более общего подхода, который можно назвать рекурсивным. Не будем различать обычную булеву функцию $f(\mathbf{v})$, где $\mathbf{v} \in \mathbb{Z}_2^m$, и целочисленную функцию $F(\mathbf{v}) = (-1)^{f(\mathbf{v})}$. Добавим нормировочный множитель к преобразованию Уолша — Адамара (Фурье), пусть

$$\widehat{F}(\mathbf{v}) = \frac{1}{2^{m/2}} \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle} F(\mathbf{u}).$$

Тогда ± 1 -значная функция F является бент-функцией, если и только если \widehat{F} также ± 1 -значная. Обобщение Х. Доббертина состоит в следующем. Пусть $T \subseteq \mathbb{Z}$. Функция $F : \mathbb{Z}_2^m \rightarrow T$ называется *T-бент-функцией*, если

все значения функции \hat{F} принадлежат множеству T . Доббертин выделил естественную цепочку вложенных друг в друга множеств:

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

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

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 [77] исследуются возможности рекурсивного построения (разложения) \mathbb{Z} -бент-функций с повышением или понижением их уровня и числа переменных.

1.4.12 Нега-бент-функции, бент₄-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 [118] стали исследовать булевы функции, имеющие плоские спектры относительно множества унитарных преобразований. Напомним, что преобразование пространства, заданное квадратной матрицей A , *унитарно*, если $A\bar{A}^T = E$, где E — единичная матрица. Выбор этого множества не случаен и связан со специальным вида локальными унитарными преобразованиями, которые важны в квантовой теории информации с точки зрения структурного анализа стабилизаторов квантовых состояний n -кубитов. Пусть

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

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

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

✓ $\{N\}^m$ — состоящее из преобразования $U = \prod_{j=0}^{m-1} N_j$. Булева функция, обладающая плоским спектром относительно U , называется *нега-бент-функцией*. Отметим, что поскольку U — комплексная матрица, при определении спектра функции здесь возникают свои особенности, см. [114]. Любая аффинная булева функция является нега-бент. М. Паркер (2000, 2007) и А. Потт (2007) изучали нега-бент-функции в работах [113] и [114]. В последней работе исследовался вопрос о пересечении классов бент- и нега-бент-функций, полностью разрешенный для квадратичных функций.

✓ $\{H, N\}^m$ — состоящее из 2^m преобразований вида $\prod_{j \in R_H} H_j \prod_{j \in R_N} N_j$, где R_H и R_N разбивают множество $\{0, 1, \dots, m-1\}$. Булева функция f от m переменных является *бент₄-функцией*, если существует хотя бы одно разбиение R_H, R_N , относительно которого f имеет плоский спектр.

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

✓ $\{I, H, N\}^m$ — состоящее из 3^m преобразований $\prod_{j \in R_I} I_j \prod_{j \in R_H} H_j \prod_{j \in R_N} N_j$, где R_I, R_H и R_N разбивают $\{0, 1, \dots, m-1\}$. В этом случае определяются так называемые *I-бент₄-функции*, не представляющие, однако, особого интереса, так как этому классу принадлежит любая булева функция.

В [118] авторы развивают квантовый мотив своих исследований, изучают свойства бент-функций нового типа и их связь с графами.

1.5 Векторные бент-функции

С 90-х годов XX века стали исследоваться функции из \mathbb{Z}_2^m в \mathbb{Z}_2^n , которые получили название *векторных булевых функций*, или *(m, n)-функций*. Интерес к ним вызван в первую очередь тем, что нелинейные такие функции имеют непосредственные криптографические приложения. Например, они используются в качестве S-блоков при конструировании шифров.

Рассмотрим нелинейные свойства векторных функций.

Преобразованием Уолша—Адамара (m, n) -функции F называется отображение $W_F^{\text{vect}} : \mathbb{Z}_2^m \times \mathbb{Z}_2^n \rightarrow \mathbb{Z}$, заданное равенством

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

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

$$N_F = \min_{\mathbf{b} \in (\mathbb{Z}_2^n)^*} \text{dist}(f_{\mathbf{b}}, \mathfrak{A}_m) = 2^{m-1} - \frac{1}{2} \max_{\mathbf{a} \in \mathbb{Z}_2^m, \mathbf{b} \in (\mathbb{Z}_2^n)^*} |W_F^{\text{vect}}(\mathbf{a}, \mathbf{b})|.$$

Для нелинейности векторной булевой функции имеется та же самая верхняя оценка, что и в случае обычной булевой функции:

$$N_F \leq 2^{m-1} - 2^{(m/2)-1}. \quad (1.2)$$

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

Теорема (Ньюберг, 1991, [110]). *Бент (m, n) -функции существуют тогда и только тогда, когда m четно и $n \leq m/2$.*

Существование таких функций легко доказать, применяя конструкцию Мэйорана—МакФарланда в новой, векторной, форме. отождествим пространство $\mathbb{Z}_2^{m/2}$ с полем Галуа $GF(2^{m/2})$, а пространство \mathbb{Z}_2^m — с прямым произведением $GF(2^{m/2}) \times GF(2^{m/2})$. Пусть m четно, $n \leq m/2$.

Теорема (Ньюберг, 1991, [110]). *Пусть $T : GF(2^{m/2}) \rightarrow GF(2^{m/2})$ — любое взаимно однозначное отображение, H — любая $(m/2, n)$ -функция, $L : GF(2^{m/2}) \rightarrow \mathbb{Z}_2^{m/2}$ — любое линейное или аффинное отображение "на". Тогда векторная (m, n) -функция $F(\mathbf{u}', \mathbf{u}'') = L(\mathbf{u}' T(\mathbf{u}'')) \oplus H(\mathbf{u}'')$ является бент-функцией.*

Конструкция Мэйорана—МакФарланда является не единственной, которая переносится на векторный случай, см. подробнее [53].

Поскольку бент (m, n) -функций не существует при $n > m/2$, то оценка (1.2) в этом случае не точна. В 1971 году В. М. Сидельников и независимо в 1994 году авторы [62] установили следующий факт.

Теорема (Сидельников, 1971, [24], Шабат, Ваденай, 1994 [62]).
Пусть $n \geq m - 1$. Для любой (m, n) -функции выполняется

$$N_F \leq 2^{m-1} - \frac{1}{2} \sqrt{3(2^m) - 2 - 2 \frac{(2^m - 1)(2^{m-1} - 1)}{2^n - 1}}.$$

При $m/2 < n < m - 1$ оценки, улучшающей (1.2), пока не известно.

Случай $m = n$ выделяется особо.

Векторная (m, m) -функция F называется *почти бенг-функцией* (AB function — almost bent function), если параметр N_F достигает своего максимального возможного значения $N_F = 2^{m-1} - 2^{(m-1)/2}$. Такие функции существуют только если m нечетно. К. Карле, П. Шарпин и В. Зиновьев [54] доказали, что степень нелинейности любой такой функции не превышает величины $(m + 1)/2$. Более широким является класс APN функций.

Почти совершенно нелинейной функцией (APN function — almost perfect nonlinear function) называется (m, m) -функция F такая, что для любых элементов $\mathbf{a} \in (\mathbb{Z}_2^m)^*$, $\mathbf{b} \in \mathbb{Z}_2^m$ уравнение $F(\mathbf{v}) \oplus F(\mathbf{v} \oplus \mathbf{a}) = \mathbf{b}$ имеет не более двух решений. К. Ньюберг ввела в 1993 году этот термин при исследовании устойчивости шифров к дифференциальному криптоанализу. Эквивалентно, APN функция может быть определена как функция, сужение которой на любое двумерное аффинное подпространство пространства \mathbb{Z}_2^m является неаффинной функцией. При нечетном m APN функции существуют. А вот существуют ли они при четном m ? — пока открытый вопрос.

AB и APN функции тесно связаны (см. обзор результатов в [53]):

Теорема. Каждая AB функция является APN функцией.

Теорема. Квадратичная APN функция является AB функцией.

Теорема. Функция F является AB функцией тогда и только тогда, когда она APN функция и все булевы функции $f_{\mathbf{b}}$ при $\mathbf{b} \neq \mathbf{0}$ являются платовидными, причем одного порядка.

Более общим понятием по отношению к понятию APN функции является следующее. Векторная (m, m) -функция F называется *дифференциально δ -равномерной* (differential δ -uniform), δ — целое число, если уравнение $F(\mathbf{v}) \oplus F(\mathbf{v} \oplus \mathbf{a}) = \mathbf{b}$ при любых $\mathbf{a} \in (\mathbb{Z}_2^m)^*$, $\mathbf{b} \in \mathbb{Z}_2^m$ имеет не более δ решений. Наименьшее значение δ , при котором такие функции существу-

ют, равно двум¹, и это — APN функции. Дифференциально 4-равномерные функции (см., например [41]) используются в S-блоках симметричного алгоритма блочного шифрования AES (или Rijndael), являющегося с 26 мая 2002 года американским стандартом шифрования.

AB, APN, δ -равномерные функции и вопросы их эквивалентности широко исследуются. В частности [43], уже выдвинута гипотеза, что все степенные AB и APN функции найдены (Х. Доббертин, 1999, [74]) и обозначена проблема существования новых комбинаторных конструкций таких функций, см. подробнее [53, 42]. При $m \leq 25$ для APN функций и при $m \leq 33$ для AB функций гипотеза Доббертина уже подтвердилась [75, 98].

За пределами данного обзора, к сожалению, остались *скрюченные функции* (crooked functions) — специальный подкласс APN функций, введенный в 1998 году Т. Бендингом и Д. Г. Фон-дер-Флаассом [32]. С помощью таких функций оказалось возможно строить новые дистанционно регулярные графы, симметричные схемы отношений, и равномерно упакованные коды типа БЧХ и Препараты, [67, 68], см. также на эту тему работу [45].

1.6 Другие направления

В настоящем обзоре мы не коснулись очень многих тем, прямо или косвенно относящихся к теории бент-функций. Среди них:

- ✓ группы автоморфизмов бент-функций;
- ✓ представления бент-функций с помощью строго регулярных графов;
- ✓ криптографические свойства смежных классов кода Риды—Маллера первого порядка и их связь с нелинейными булевыми функциями [46];
- ✓ бент-функции, дуальные к данным (а также вопросы самодуальности [55] и эквивалентности бент-функций [96]);
- ✓ корреляционно-иммунные (correlation-immune), устойчивые (resilient) и др. функции, см. на эти темы работы [128, 131, 78, 12] и др.;
- ✓ обобщение: *профиль нелинейности* булевой функции [51];
- ✓ асимптотическая нелинейность булевых функций [120];
- ✓ корреляционные свойства бент-функций [137];
- ✓ почти бент-функции (near bent) и их сужения на гиперплоскости [72].

¹Интересно, что при рассмотрении q -значных векторных функций, $q \neq 2$, возможно и $\delta = 1$.

Глава 2

Понятие k -бент-функции

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.

2.1 Определения и обозначения

Введем понятия и обозначения, которые потребуются далее. Вектор длины m с компонентами из кольца \mathbb{Z}_4 будем называть *четверичным*. Весом $Li\ wt_L(\cdot)$ 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 $Li\ d_L(\mathbf{x}, \mathbf{y})$ 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 **0**, **1**, **2** и **3** обозначим векторы со всеми компонентами, равными 0, 1, 2 и 3 соответственно. Пусть $\beta, \gamma : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$ — следующие отображения:

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

Пусть $\varphi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ — 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 $\beta, \gamma : \mathbb{Z}_4^i \rightarrow \mathbb{Z}_2^i$ и $\varphi : \mathbb{Z}_4^i \rightarrow \mathbb{Z}_2^{2i}$ для любого целого i . Напомним, что φ согласно [80] 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 $\varphi^{-1}(C)$ линейен.

2.2 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 $0 \leq k \leq m/2$. 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,

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

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

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

Матрицы такого вида впервые рассматривались Д. С. Кротовым в работах [9] и [91] для построения \mathbb{Z}_4 -линейных кодов типа Адамара длины $2n$ и получения их полной классификации.

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

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

Аналогично тому, как это сделано в [39], определим бинарную операцию

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

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

$$\mathbf{h}^{\mathbf{u}} = \varphi_k^{-1}(\mathbf{u}) \cdot \mathbf{G}_m^k. \quad (2.1)$$

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

$$\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u} \star \mathbf{v}}. \quad (2.2)$$

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,

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

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

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 $\tilde{u} = 8u_1 + 4u_2 + 2u_3 + u_4$.

\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

\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 1. Векторы для \mathbf{C}_4^1 . **Таблица 2.** Векторы для \mathbf{C}_4^2 .

$c_{\mathbf{u},\mathbf{v}}^1$	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

$c_{\mathbf{u},\mathbf{v}}^2$	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 3. Матрица \mathbf{C}_4^1 .

Таблица 4. Матрица \mathbf{C}_4^2 .

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

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

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

Утверждение 1. При любых целых m, k таких, что $0 \leq k \leq m/2$, справедливы равенства

- (i) $\mathbf{C}_{m+1}^k = (\mathbf{C}_m^k \otimes J_2) + (J_n \otimes \mathbf{C}_1^0)$;
- (ii) $\mathbf{C}_{m+2}^{k+1} = (J_4 \otimes \mathbf{C}_m^k) + (\mathbf{C}_2^1 \otimes J_n)$;
- (iii) $(\mathbf{C}_m^k)^T = \mathbf{C}_m^k$.

Доказательство. Пусть $\mathbf{G}_m^k = (\mathbf{z}_1^T, \dots, \mathbf{z}_n^T)$. Тогда матрица \mathbf{G}_{m+1}^k имеет вид

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

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

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

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

следует, что $\mathbf{h}^{(a, b, \mathbf{u})} = (\delta, \varphi_k^{-1}(\mathbf{u})) \cdot \mathbf{G}_{m+1}^{k+1} = (\mathbf{h}^{\mathbf{u}}, \mathbf{h}^{\mathbf{u}} + \delta \mathbf{1}, \mathbf{h}^{\mathbf{u}} + \delta \mathbf{2}, \mathbf{h}^{\mathbf{u}} + \delta \mathbf{3})$, 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}_m^k состоит из всех векторов \mathbf{h}^u и $\mathbf{h}^u + \mathbf{2}$.

Утверждение 2 [91]. Код \mathcal{A}_m^k линейен и имеет параметры $(n, 2n, n)_4$.

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

$$A_m^k = \beta(\mathcal{A}_m^k), \quad H_m^k = \varphi(\mathcal{A}_m^k).$$

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 [91] любой \mathbb{Z}_4 -линейный код типа Адамара длины $2n$ эквивалентен одному из кодов $\varphi(\mathcal{A}_m^k \cup (\mathcal{A}_m^k + \mathbf{1}))$, где k пробегает значения $1, \dots, \lfloor m/2 \rfloor$.

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

Утверждение 3 [91]. Коды H_m^0 и H_m^1 линейны. При $k > 1$ справедливо равенство $|\text{Ker}(H_m^k)| = 2^{m-k+1}$.

Нетрудно установить следующий факт.

Утверждение 4. При любом целом k , $0 \leq k \leq m/2$, справедливо равенство $\text{Ker}(A_m^k) = \beta(\varphi^{-1}(\text{Ker}(H_m^k)))$.

Доказательство. Пусть $\varphi(\mathbf{x}) \in \text{Ker}(H_m^k)$ 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 $\text{Ker}(A_m^k) \supseteq \beta(\varphi^{-1}(\text{Ker}(H_m^k)))$.

Обратно, пусть $\beta(\mathbf{x}) \in \text{Ker}(A_m^k)$ для некоторого $\mathbf{x} \in \mathcal{A}_m^k$. Сначала покажем, что вектор $\gamma(\mathbf{x})$ также принадлежит $\text{Ker}(A_m^k)$. 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 $\beta(2\mathbf{x}) \in \text{Ker}(A_m^k)$. В силу линейности двоичного подкода $\text{Ker}(A_m^k)$ получаем $\gamma(\mathbf{x}) = \beta(\mathbf{x}) \oplus \beta(2\mathbf{x}) \in \text{Ker}(A_m^k)$. 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 $\text{Ker}(A_m^k)$, следует $\varphi(\mathbf{x}) \in \text{Ker}(H_m^k)$ (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, $\text{Ker}(A_m^k) \subseteq \beta(\varphi^{-1}(\text{Ker}(H_m^k)))$.

Утверждение 4 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 3 и 4 следует, что коды $A_m^1, \dots, A_m^{\lfloor m/2 \rfloor}$ попарно неэквивалентны.

На кодовых словах кода A_m^k определим бинарную операцию

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

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

$$\mathbf{x} \bullet \mathbf{y} = \beta(\beta^{-1}(\mathbf{x}) + \beta^{-1}(\mathbf{y})) \text{ для любых векторов } \mathbf{x}, \mathbf{y} \in A_m^k. \quad (2.3)$$

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 5. Для любых $\mathbf{x}, \mathbf{y}, \mathbf{z} \in A_m^k$ выполняются 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 $\text{supp}(\mathbf{v})$. 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 (2.3) имеем

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

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

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

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). \square

Согласно утверждениям 2 и 5 код A_m^k имеет кодовое расстояние $n/2$. Таким образом, из утверждений 2, 3, 4 и 5 следует

Теорема 2. При целых m, k , таких что $1 \leq k \leq m/2$, выполняется

- (i) код A_m^k является $(n, 2n, n/2)_2$ -кодом типа Адамара;
- (ii) код A_m^1 линейен, при $k \geq 2$ справедливо $|\text{Ker}(A_m^k)| = 2^{m-k+1}$, где через $\text{Ker}(A_m^k)$ 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 $\mathbf{y} \bullet \mathbf{y}^{-1} = \mathbf{0}$.

2.3 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 , $0 \leq k \leq m/2$, определим бинарную операцию

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

следующим образом:

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(c_{\mathbf{u}, \mathbf{v}}^k) \text{ для любых } \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m. \quad (2.4)$$

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 $(1, 2)(3, 4) \dots (2k-1, 2k)$ 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 6. Пусть $m \in \mathbb{N}$, k — целое, $0 \leq k \leq m/2$. 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) $\sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus \langle \mathbf{w}, \mathbf{v} \rangle_k} = \begin{cases} 2^m, & \text{если } \mathbf{u} = \mathbf{w}, \\ 0 & \text{в противном случае;} \end{cases}$
- (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) $\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k = \langle \mathbf{u} \star \mathbf{v}, \mathbf{w} \rangle_k \oplus \left(\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{w} \rangle_k \right) \left(\langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \langle \pi_k(\mathbf{v}), \mathbf{w} \rangle_k \right).$

Доказательство. Соотношение (i) следует из утверждения 1, 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 2 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 1, см. (i), справедливо равенство $c_{(\mathbf{u},\mathbf{a}),(\mathbf{v},\mathbf{b})}^k = c_{\mathbf{u},\mathbf{v}}^k + 2ab$, из которого следует (iv).

(v) Следует из определения, согласно которому

$\langle \cdot, \cdot \rangle_0$	00011011	$\langle \cdot, \cdot \rangle_1$	00011011
00	0 0 0 0	00	0 0 0 0
01	0 1 0 1	01	0 0 1 1
10	0 0 1 1	10	0 1 0 1
11	0 1 1 0	11	0 1 1 0

(vi) Из утверждения 1, см. (ii), следует, что $c_{(a,a',\mathbf{u}),(\mathbf{b},\mathbf{b}',\mathbf{v})}^{k+1} = \varphi^{-1}(a, a') \cdot \varphi^{-1}(b, b') + c_{\mathbf{u},\mathbf{v}}^k$. 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

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

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

$$c_{\pi_k(\mathbf{u}),\mathbf{v}}^k = 3c_{\mathbf{u},\mathbf{v}}^k,$$

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

(vii) Поскольку выполняется $\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u} \star \mathbf{v}}$ (см. (2.2)), имеем $c_{\mathbf{u},\mathbf{w}}^k + c_{\mathbf{v},\mathbf{w}}^k = c_{\mathbf{u} \star \mathbf{v},\mathbf{w}}^k$. 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 $c_{\mathbf{u}, \mathbf{w}}^k$ 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 $\beta(c_{\mathbf{u}, \mathbf{w}}^k) \oplus \beta(c_{\mathbf{v}, \mathbf{w}}^k) = \beta(c_{\mathbf{u} \star \mathbf{v}, \mathbf{w}}^k) \oplus \left(\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{w} \rangle_k \right) \left(\langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \langle \pi_k(\mathbf{v}), \mathbf{w} \rangle_k \right)$, что и требовалось показать. Утверждение 6 доказано. \square

Замечание. Операция $\langle \mathbf{u}, \mathbf{v} \rangle_k$ не является билинейной формой при $k \geq 2$. Это следует из Утверждения 14, которое будет приведено в разделе 4.5.

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

Теорема 3. Пусть m, k — целые, $1 \leq k \leq m/2$. Для любого целого i , $1 \leq i \leq m/2$, 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

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \left(\bigoplus_{i=1}^k \bigoplus_{j=i}^k Y_i Y_j \right) \oplus \langle \mathbf{u}, \mathbf{v} \rangle.$$

Доказательство. Докажем теорему индукцией по k .

При $k = 1$ согласно пунктам (iv) и (v) утверждения 6 имеем

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

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

Пусть теорема справедлива для некоторого k , $1 \leq k \leq (m-2)/2$. Покажем, что она имеет место и для $k+1$. По утверждению 6, см. пункт (vi), выполняется

$$\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \langle (u_1, u_2), (v_1, v_2) \rangle_\varepsilon \oplus \langle (u_3, \dots, u_m), (v_3, \dots, v_m) \rangle_k, \quad (2.5)$$

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

По предположению индукции имеем

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

и, как нетрудно видеть,

$$\begin{aligned} \langle \pi_k(u_3, \dots, u_m), (v_3, \dots, v_m) \rangle_k = \\ \left(\bigoplus_{i=2}^{k+1} \bigoplus_{j=i}^{k+1} Y_i Y_j \right) \oplus \bigoplus_{j=2}^{k+1} (u_{2j} v_{2j-1} \oplus u_{2j-1} v_{2j}) \oplus \bigoplus_{s=2k+3}^m u_s v_s. \end{aligned}$$

Отсюда следует, что $\varepsilon = \left(\bigoplus_{j=2}^{k+1} Y_j \right) \oplus 1$. Тогда первое слагаемое в правой части равенства (2.5) согласно пункту (v) утверждения 6 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

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

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

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

и следовательно,

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

Теорема 3 доказана. □

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

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

Как нетрудно заметить, координаты u_1, \dots, u_m (также как и v_1, \dots, 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 3 легко следует, что

$$\langle \mathbf{u}, \mathbf{v} \rangle_1 = \langle \mathbf{u}, \hat{\mathbf{v}} \rangle, \quad (2.6)$$

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 $m = 4$:

$$\langle \mathbf{u}, \mathbf{v} \rangle_2 = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1 \oplus v_2)(v_3 \oplus v_4) \oplus u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4 \quad (2.7)$$

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

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle_3 = & (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \\ & \oplus (u_1 \oplus u_2)(u_5 \oplus u_6)(v_1v_5 \oplus v_1v_6 \oplus v_2v_5 \oplus v_2v_6) \\ & \oplus (u_3 \oplus u_4)(u_5 \oplus u_6)(v_3v_5 \oplus v_3v_6 \oplus v_4v_5 \oplus v_4v_6) \\ & \oplus u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4 \oplus u_6v_5 \oplus u_5v_6. \end{aligned}$$

2.4 Понятие k -аффинной функции

Пусть каждому вектору кода A_m^k , где $m \in \mathbb{N}$, k — целое, $0 \leq k \leq m/2$, отвечает булева функция $g \in \mathfrak{F}_m$, 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 функций¹ и обозначим через \mathfrak{A}_m^k . Ясно, что $|\mathfrak{A}_m^k| = 2^{m+1}$. Из теоремы 3 следует

Утверждение 7. При любом $m \in \mathbb{N}$, целом k , $0 \leq k \leq m/2$, класс \mathfrak{A}_m^k состоит из функций вида

$$g(\mathbf{v}) = \left(\bigoplus_{i=1}^k \bigoplus_{j=i}^k (u_{2i-1} \oplus u_{2i})(u_{2j-1} \oplus u_{2j})(v_{2i-1} \oplus v_{2i})(v_{2j-1} \oplus v_{2j}) \right) \oplus \left(\bigoplus_{s=1}^m u_s v_s \right) \oplus a, \quad (2.8)$$

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

¹Как уже было отмечено ранее, 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.

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

$$g(v_1, v_2, v_3, v_4) = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus \\ u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4 \oplus a.$$

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 алгебраической нормальной формы (или многочлена Жегалкина). Из утверждения 7 следует, что степень булевой функции из произвольного класса \mathfrak{A}_m^k не превышает 2. Справедливо

Утверждение 8. Для любого $m \in \mathbb{N}$ и целого k , $0 \leq k \leq m/2$, 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 7 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 , $1 \leq j \leq k$, справедливо $u_{2j-1} = u_{2j}$;
- 2) найдется единственный номер j , $1 \leq j \leq k$, 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 .

2.5 Понятие k -бент-функции

Для любого $m \in \mathbb{N}$ и целого k , $0 \leq k \leq m/2$, 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 $f \in \mathfrak{F}_m$.

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 2), для $W_f^{(k)}$ имеет место аналог равенства Парсеваля, см. например, [15, гл. 6]. Для полноты изложения приведем доказательство этого факта.

Теорема 4 (равенство Парсеваля для $W_f^{(k)}$). При любом $m \in \mathbb{N}$ и целом k , $0 \leq k \leq m/2$, для любой функции $f \in \mathfrak{F}_m$ выполняется

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

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

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

(меняя порядок суммирования и используя пункт (iii) утверждения 6, получаем)

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

Теорема 4 доказана. □

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

Утверждение 9. Справедливо равенство $N_f^{(k)} = 2^{m-1} - \frac{1}{2} \max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f^{(k)}(\mathbf{v})|$.

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

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

Из определения $W_f^{(k)}$ и пункта (i) утверждения 6 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

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

Утверждение 9 доказано. \square

Из теоремы 4 следует неравенство

$$\max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f^{(k)}(\mathbf{v})| \geq 2^{m/2}. \quad (2.9)$$

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

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

Определение 2. Для четного m , целого k , $1 \leq k \leq m/2$, булеву функцию $f \in \mathfrak{F}_m$ назовем *k -бент-функцией*, если все коэффициенты $W_f^{(j)}(\mathbf{v})$, $j = 1, \dots, k$, 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 \mathfrak{B}_m^k . Из пунктов (iv) и (v) утверждения 6 следует, что

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

Поэтому класс \mathfrak{B}_m^1 представляет собой класс обычных бент-функций \mathfrak{B}_m .
Таким образом,

$$\mathfrak{B}_m = \mathfrak{B}_m^1 \supseteq \dots \supseteq \mathfrak{B}_m^{m/2},$$

и, как будет показано далее, каждое включение является строгим и

$$\mathfrak{B}_m^{m/2} \neq \emptyset.$$

Глава 3

Построение k -бент-функций и их свойства

Известно, что задача описания бент-функций для произвольного числа переменных m , или хотя бы нахождения хороших нижних и верхних оценок числа таких функций является очень сложной. Об этом свидетельствует, например, тот факт, что число 6 является максимальным значением для m , при котором еще известно точное значение числа бент-функций (равное $5\,425\,430\,528 \simeq 2^{32,3}$, см. описание в [29, 105], и более раннюю работу [116]), несмотря на длительный срок их исследования и большой интерес к этим объектам.

В первой части главы приводится простое описание класса 2-бент-функций от четырех переменных. Этот класс состоит из 384-х квадратичных функций с 12-ю различными типами квадратичной части. Тем самым, параметр $m = 6$ становится наименьшим, при котором k -бент-функции пока не описаны.

Во второй части главы предлагается итеративная конструкция k -бент-функций. В качестве следствия устанавливается, что для $k > \ell \geq 1$ класс k -бент-функций \mathfrak{B}_m^k является собственным подклассом класса ℓ -бент-функций \mathfrak{B}_m^ℓ . Показывается, что существуют k -бент-функции с любой степенью нелинейности d , где $2 \leq d \leq \max\{2, \frac{m}{2} - k + 1\}$. Для каждого k определяется подмножество \mathfrak{F}_m^k множества булевых функций \mathfrak{F}_m , на котором понятия k -бент-функции и 1-бент-функции совпадают.

3.1 k -Бент-функции от малого числа переменных

3.1.1 Описание

Рассмотрим малые значения параметра m .

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

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

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

Используя утверждение 6 и теорему 3, 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

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

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

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

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

Согласно теореме 3 имеем

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

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

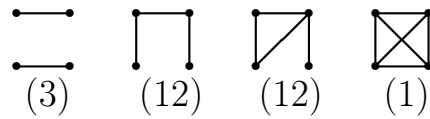
Поэтому

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

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

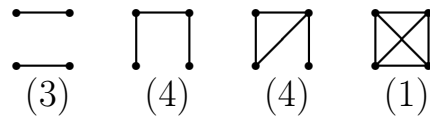
Из данного примера легко заключаем, что множество $\mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$ непусто. Рассмотрим теперь каждый класс \mathfrak{B}_4^1 и \mathfrak{B}_4^2 в отдельности.

Известно [16], что множество \mathfrak{B}_4^1 состоит из 896-ти булевых функций, причем каждая функция является квадратичной, т. е. степени нелинейности 2. Множество \mathfrak{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:

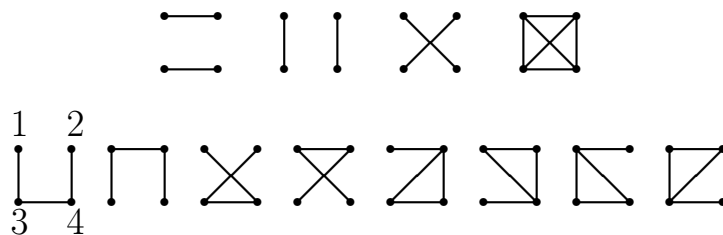


Под каждым графом указано число типов, которые он определяет. Например, имеется 12 типов квадратичной части, состоящей из трех слагаемых, и только один тип из шести слагаемых.

Приведем простое описание класса \mathfrak{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 \mathfrak{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, $|\mathfrak{B}_4^2| = 384$.

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

Теорема 5. Пусть параметры i_1, i_2, i_3 и i_4 принимают различные значения от 1 до 4. Тогда множество функций \mathfrak{B}_4^2 состоит из всех функций степени 2 с квадратичными частями вида:

$$\begin{aligned} v_{i_1}v_{i_2} \oplus v_{i_3}v_{i_4} & \quad (3 \text{ типа}); \\ v_{i_1}v_{i_2} \oplus v_{i_1}v_{i_3} \oplus v_{i_2}v_{i_4} \text{ при } \{i_1, i_2\} = \{1, 2\} \text{ или } \{3, 4\} & \quad (4 \text{ типа}); \\ v_{i_1}v_{i_2} \oplus v_{i_2}v_{i_3} \oplus v_{i_3}v_{i_4} \oplus v_{i_1}v_{i_3} \text{ при } \{i_1, i_2\} = \{1, 2\} \text{ или } \{3, 4\} & \quad (4 \text{ типа}); \\ v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4 & \quad (1 \text{ тип}). \end{aligned}$$

Доказательство. Очевидно, что \mathfrak{B}_4^2 содержит только функции степени 2. Заметим, что если функция f принадлежит \mathfrak{B}_4^2 , то функция $f \oplus 1$ также содержится в этом классе. Рассмотрим произвольную функцию $f_{\mathbf{w}} \in \mathfrak{B}_4^1$ 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

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

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

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

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

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

$$W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{v} \rangle \oplus g_{\mathbf{w}}(\mathbf{v})} = W_{g_{\mathbf{w}}}(\tilde{\mathbf{u}}), \quad (3.1)$$

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

$$g(\mathbf{v}) = (v_1 v_3 \oplus v_1 v_4 \oplus v_2 v_3 \oplus v_2 v_4) \oplus f(\mathbf{v}).$$

Выясним при каких условиях данные четыре коэффициента

$$W_{f_{\mathbf{w}}}^{(2)}(1010), W_{f_{\mathbf{w}}}^{(2)}(1001), W_{f_{\mathbf{w}}}^{(2)}(0110), W_{f_{\mathbf{w}}}^{(2)}(0101), \quad (3.2)$$

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:

$f(\mathbf{v})$	$g(\mathbf{v})$
$\dashv \vdash$ $v_1 v_2 \oplus v_3 v_4$	\boxtimes $v_1 v_2 \oplus \dots \oplus v_3 v_4$
\updownarrow $v_1 v_3 \oplus v_2 v_4$	\times $v_1 v_4 \oplus v_2 v_3$
\times $v_1 v_4 \oplus v_2 v_3$	\updownarrow $v_1 v_3 \oplus v_2 v_4$
\boxtimes $v_1 v_2 \oplus \dots \oplus v_3 v_4$	$\dashv \vdash$ $v_1 v_2 \oplus v_3 v_4$
\sqcup $v_1 v_3 \oplus v_2 v_4 \oplus v_3 v_4$	\times $v_1 v_4 \oplus v_2 v_3 \oplus v_3 v_4$
\sqcap $v_1 v_2 \oplus v_1 v_3 \oplus v_2 v_4$	\times $v_1 v_2 \oplus v_1 v_4 \oplus v_2 v_3$
\times $v_1 v_4 \oplus v_2 v_3 \oplus v_3 v_4$	\sqcup $v_1 v_3 \oplus v_2 v_4 \oplus v_3 v_4$
\times $v_1 v_2 \oplus v_1 v_4 \oplus v_2 v_3$	\sqcap $v_1 v_2 \oplus v_1 v_3 \oplus v_2 v_4$
\nearrow $v_1 v_2 \oplus v_2 v_3 \oplus v_2 v_4 \oplus v_3 v_4$	\nwarrow $v_1 v_2 \oplus v_1 v_3 \oplus v_1 v_4 \oplus v_3 v_4$
\searrow $v_1 v_2 \oplus v_1 v_4 \oplus v_2 v_4 \oplus v_3 v_4$	\nearrow $v_1 v_2 \oplus v_1 v_3 \oplus v_2 v_3 \oplus v_3 v_4$
\nwarrow $v_1 v_2 \oplus v_1 v_3 \oplus v_1 v_4 \oplus v_3 v_4$	\nearrow $v_1 v_2 \oplus v_2 v_3 \oplus v_2 v_4 \oplus v_3 v_4$
\nearrow $v_1 v_2 \oplus v_1 v_3 \oplus v_2 v_3 \oplus v_3 v_4$	\searrow $v_1 v_2 \oplus v_1 v_4 \oplus v_2 v_4 \oplus v_3 v_4$

В каждом из этих 12-ти случаев, так как g есть 1-бент-функция, имеем $W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u}) = W_{g_{\mathbf{w}}}(\tilde{\mathbf{u}}) = \pm 4$, и следовательно $f_{\mathbf{w}}$ принадлежит классу 2-бент-функций при любом векторе \mathbf{w} . Таким образом, мы показали, что класс

\mathfrak{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 (3.2) 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 $W_{f_{\mathbf{w}}}^{(2)}(1010)$ согласно (3.1) можно представить в виде

$$W_{f_{\mathbf{w}}}^{(2)}(1010) = W_{g_{\mathbf{w}}}(0101) = S_0 - S_1,$$

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

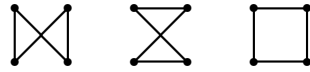
$$\{v_1v_3, v_1v_4, v_2v_3, v_2v_4\},$$

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 $W_{f_{\mathbf{w}}}^{(2)}(1010) = \pm 4$ не выполнено, и следовательно в этом случае функция $f_{\mathbf{w}}$ не является 2-бент-функцией ни при каком векторе \mathbf{w} . Теорема 5 доказана. \square

3.1.2 Замечания

Интересным следствием из теоремы 5 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 4), 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 5 следует, что функция $f \in \mathfrak{B}_4^1$ 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. 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 [15] и [52].

m	k	Информация о классах \mathfrak{B}_m^k
2	1	$ \mathfrak{B}_2^1 = 8$
4	1, 2	$ \mathfrak{B}_4^1 = 896$, см. описание в [16]; $ \mathfrak{B}_4^2 = 384$, описание в [152]; число в [147];
6	1, 2, 3	$ \mathfrak{B}_6^1 = 5\,425\,430\,528 \simeq 2^{32,3}$, см. [29, 105, 116]; $ \mathfrak{B}_6^2 \geq 4 \cdot 896 = 3\,584$, следует из [147]; $ \mathfrak{B}_6^3 \geq 4 \cdot 384 = 1\,536$, следует из [147];
8	1, 2, 3, 4	$ \mathfrak{B}_8^1 \geq 1\,559\,994\,535\,674\,013\,286\,400 \simeq 2^{70,4}$, см. [29]; $ \mathfrak{B}_8^2 > 2^{34,3}$, следует из [29, 105, 116] и [147]; $ \mathfrak{B}_8^3 \geq 16 \cdot 896 = 14\,336$, следует из [147]; $ \mathfrak{B}_8^4 \geq 16 \cdot 384 = 6\,144$, следует из [147];

Таблица 5. Оценки числа k -бент-функций от малого числа переменных.

3.2 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 10 и 11.

Утверждение 10. Пусть $m, r \in \mathbb{N}$ четны, $k \in \mathbb{N}$ такое, что $1 \leq k \leq m/2$, и пусть функция $f \in \mathfrak{F}_{m+r}$ 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 $p \in \mathfrak{F}_m$, $q \in \mathfrak{F}_r$ — функции с непересекающимися множествами переменных. Тогда функция f принадлежит классу \mathfrak{B}_{m+r}^k , если и только если $p \in \mathfrak{B}_m^k$, $q \in \mathfrak{B}_r^1$.

Доказательство. Для произвольных $\mathbf{v}' \in \mathbb{Z}_2^m$, $\mathbf{v}'' \in \mathbb{Z}_2^r$ и любого $\ell = 1, \dots, k$ рассмотрим коэффициент $W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'')$. Используя пункт (iv) утвер-

ждения 6, 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 $p \in \mathfrak{B}_m^k$, $q \in \mathfrak{B}_r^1 = \mathfrak{B}_r$, то, очевидно, $|W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'')| = 2^{m/2} \cdot 2^{r/2} = 2^{(m+r)/2}$ для любого ℓ , $1 \leq \ell \leq k$, и следовательно, функция f принадлежит классу \mathfrak{B}_{m+r}^k . С другой стороны, пусть $f \in \mathfrak{B}_{m+r}^k$. Для каждого ℓ , $1 \leq \ell \leq k$, 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

$$|W_p^{(\ell)}(\mathbf{v}'_\ell)| \geq 2^{m/2}, \quad |W_q(\mathbf{v}'')| \geq 2^{r/2}.$$

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 , $1 \leq \ell \leq k$, что выполняется тогда и только тогда, когда $p \in \mathfrak{B}_m^k$ и $q \in \mathfrak{B}_r = \mathfrak{B}_r^1$. Утверждение 10 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 \mathfrak{F}_2^1 (смысл этого обозначения будет раскрыт в разделе 3.3).

Утверждение 11. Пусть $t \in \mathbb{N}$ четно, $k \in \mathbb{N}$ такое, что $1 \leq k \leq t/2$, и пусть функция $f \in \mathfrak{F}_{m+2}$ 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 $s \in \mathfrak{F}_2^1$, $p \in \mathfrak{F}_m$ — функции с непересекающимися множествами переменных. Тогда функция f принадлежит классу \mathfrak{B}_{m+2}^{k+1} , если и только если $s \in \mathfrak{B}_2^1$, $p \in \mathfrak{B}_m^k$.

Доказательство. Рассмотрим коэффициент $W_f^{(\ell+1)}(b, b', \mathbf{v})$, где $\ell \in \mathbb{N}$, $1 \leq \ell \leq k$, 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 6 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 , $1 \leq \ell \leq k$, 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 10, получаем требуемое. Утверждение 11 доказано. \square

Непосредственно из утверждений 10 и 11 вытекает

Теорема 6. Пусть числа $m, r \geq 0$ четны, $j \geq 0$ — любое, k такое, что $1 \leq k \leq m/2$, и пусть функция $f \in \mathfrak{F}_{2j+m+r}$ представима в виде

$$f(a_1, a'_1, \dots, a_j, a'_j, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^j s_i(a_i, a'_i) \right) \oplus p(\mathbf{u}') \oplus q(\mathbf{u}''),$$

где $s_1, \dots, s_j \in \mathfrak{F}_2^1$, $p \in \mathfrak{F}_m$ и $q \in \mathfrak{F}_r$ — функции с непересекающимися множествами переменных. Тогда f принадлежит классу $\mathfrak{B}_{2j+m+r}^{j+k}$, если и только если $s_1, \dots, s_j \in \mathfrak{B}_2^1$, $p \in \mathfrak{B}_m^k$ и $q \in \mathfrak{B}_r^1$.

Следствие 4. Множество \mathfrak{B}_m^k непусто при любом четном m и любом целом k , $1 \leq k \leq m/2$.

Доказательство. Рассмотрим любые функции $s_1, \dots, s_{m/2}$ из $\mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$. Нетрудно видеть, что класс $\mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$ 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 $f \in \mathfrak{F}_m$ такая, что $f(a_1, a'_1, \dots, a_{m/2}, a'_{m/2}) = \bigoplus_{i=1}^{m/2} s_i(a_i, a'_i)$, согласно теореме 6 принадлежит классу $\mathfrak{B}_m^{m/2}$, и следовательно, каждому классу \mathfrak{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 [15] и работе [86]. 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 $m \geq 4$ имеют место строгие включения*

$$\mathfrak{B}_m^1 \supset \mathfrak{B}_m^2 \supset \dots \supset \mathfrak{B}_m^{m/2}.$$

Доказательство. При любом k , $1 \leq k \leq (m-2)/2$, покажем, что множество $\mathfrak{B}_m^k \setminus \mathfrak{B}_m^{k+1}$ непусто. Выберем произвольно функцию $\psi \in \mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$ (такие функции согласно 3.1.1 существуют). Пусть $k = 1$. Тогда для любой функции $q \in \mathfrak{B}_{m-4}^1$ функция $f \in \mathfrak{F}_m$ такая, что $f(\mathbf{u}', \mathbf{u}'') = \psi(\mathbf{u}') \oplus q(\mathbf{u}'')$, по теореме 6 принадлежит множеству $\mathfrak{B}_m^1 \setminus \mathfrak{B}_m^2$. Пусть далее $k > 1$. Выберем произвольные функции s_1, \dots, s_{k-1} из множества $\mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$ и функцию q из множества \mathfrak{B}_{m-2k-2}^1 . Тогда функция $f \in \mathfrak{F}_m$, заданная равенством $f(a_1, a'_1, \dots, a_{k-1}, a'_{k-1}, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^{k-1} s_i(a_i, a'_i) \right) \oplus \psi(\mathbf{u}') \oplus q(\mathbf{u}'')$, является k -бент-функцией, но не принадлежит классу \mathfrak{B}_m^{k+1} . Следствие 5 доказано. \square

Пусть $m \geq 4$. Известно (см. например, [15]), что степень нелинейности произвольной бент-функции от m переменных не превышает $m/2$, и для любого d , $2 \leq d \leq m/2$, существует бент-функция $f \in \mathfrak{B}_m$ такая, что $\deg f = d$. Для k -бент-функций имеет место

Следствие 6. *При любом четном m , $m \geq 4$, и произвольном $k \in \mathbb{N}$, $1 \leq k \leq m/2$, существуют k -бент-функции с любой степенью нелинейности d такой, что $2 \leq d \leq \max\{2, \frac{m}{2} - k + 1\}$.*

Доказательство. Случай $k = 1$ совпадает со случаем обычных бент-функций и не рассматривается. Пусть $2 \leq k \leq (m - 2)/2$. Для любого d , $2 \leq d \leq \frac{m}{2} - k + 1$, существует функция $p \in \mathfrak{B}_{m-2k+2}^1$ такая, что $\deg p = d$. Тогда по теореме 6 для произвольных функций s_1, \dots, s_{k-1} из множества $\mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$ функция $f \in \mathfrak{F}_m$, заданная равенством $f(a_1, a'_1, \dots, a_{k-1}, a'_{k-1}, \mathbf{u}) = \left(\bigoplus_{i=1}^{k-1} s_i(a_i, a'_i) \right) \oplus p(\mathbf{u})$, 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 $s_i \in \mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$, $i = 1, \dots, m/2$, является примером $m/2$ -бент-функции степени 2. Следствие 6 доказано. \square

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 [135] не совпадает ни с одним из классов \mathfrak{B}_m^k , $1 \leq k \leq m/2$ (это вытекает из того, что степень нелинейности произвольной гипер-бент-функции от m переменных равна $m/2$, см. [10, 59]).

Как уже отмечалось ранее, мощность класса \mathfrak{B}_m^1 всех бент-функций от m переменных не известна. Для k -бент-функций непосредственно из теоремы 6 получаем

Следствие 7. При четном m и любом k , $1 \leq k \leq m/2$, справедливо неравенство $|\mathfrak{B}_m^k| \geq 4|\mathfrak{B}_{m-2}^{k-1}|$.

Например для $m = 8$ имеем:

$$|\mathfrak{B}_8^1| > 2^{70,4} \text{ (согласно [29])},$$

$$|\mathfrak{B}_8^2| > 2^{34,3} \text{ (как следует из [116], где установлено, что } |\mathfrak{B}_6^1| > 2^{32,3}),$$

$$|\mathfrak{B}_8^3| \geq 7 \cdot 2^{11} \text{ (в начале раздела было отмечено, что } |\mathfrak{B}_4^1| = 896),$$

$$|\mathfrak{B}_8^4| \geq 2^9 \text{ (поскольку } |\mathfrak{B}_2^1| = 8).$$

Однако даже для $m = 4$ оценка следствия 7 является весьма грубой: имеем $|\mathfrak{B}_4^2| \geq 32$, хотя точное значение $|\mathfrak{B}_4^2|$ равно 384.

3.3 Взаимосвязь k -бент-функций с бент-функциями

Обозначим через $S_{m,k}$ подгруппу группы S_m подстановок на m координатах, порожденную k транспозициями: $(1, 2), (3, 4), \dots, (2k-1, 2k)$. Очевид-

но, 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

$$\sigma_k^{\mathbf{w}} = (1, 2)^{w_1} \cdot (3, 4)^{w_2} \cdot \dots \cdot (2k-1, 2k)^{w_k},$$

где $(i, j)^0$ обозначает тождественную подстановку. Заметим, что $\pi_k \equiv \sigma_k^1$. Пусть \mathfrak{F}_m^k обозначает множество всех функций $f \in \mathfrak{F}_m$, 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 $|\mathfrak{F}_m^k| = 2^{3^k 2^{m-2k}} = 2^{2^{m-k} \log_2 \frac{4}{3}}$. Покажем, что на каждом множестве функций \mathfrak{F}_m^k понятия k -бент-функции и бент-функции совпадают. А именно верна следующая теорема.

Теорема 7. При любом четном $m \geq 2$ и любом целом k , $1 \leq k \leq m/2$, справедливо равенство $\mathfrak{F}_m^k \cap \mathfrak{B}_m^k = \mathfrak{F}_m^k \cap \mathfrak{B}_m^1$.

Доказательство. С помощью утверждения 6 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 $1 \leq \ell \leq k$. Определим вектор $\mathbf{w} \in \mathbb{Z}_2^\ell$, зависящий от выбранных векторов \mathbf{u}, \mathbf{v} , следующим образом: для каждого $i = 1, \dots, \ell$ положим

$$w_i = \langle (u_{2i+1}, \dots, u_m), (v_{2i+1}, \dots, v_m) \rangle_{\ell-i} \oplus \langle \pi_{\ell-i}((u_{2i+1}, \dots, u_m)), (v_{2i+1}, \dots, v_m) \rangle_{\ell-i} \oplus 1,$$

если $i < \ell$, и пусть $w_\ell = 1$. Тогда в силу пункта (vi) утверждения 6 справедливо равенство

$$\langle \mathbf{u}, \mathbf{v} \rangle_\ell = \left(\bigoplus_{i=1}^{\ell} \langle (u_{2i-1}, u_{2i}), (v_{2i-1}, v_{2i}) \rangle_{w_i} \right) \oplus \langle (u_{2\ell+1}, \dots, u_m), (v_{2\ell+1}, \dots, v_m) \rangle$$

(здесь мы считаем, что в случае $\ell = m/2$ последнее слагаемое отсутствует). Отсюда, используя пункты (iv) и (v) утверждения 6, 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^ℓ , 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 , $1 \leq j \leq \ell$, 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 $u_{2j+1} = u'_{2j+1}, \dots, u_m = u'_m$. 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 $f \in \mathfrak{F}_m^k \cap \mathfrak{B}_m^1$. 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 $\ell = 1, \dots, k$. Теорема 7 доказана. \square

Несложно, однако, показать, что функциями из $\mathfrak{F}_m^k \cap \mathfrak{B}_m^1$ весь класс \mathfrak{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 4

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 [102] в 1993 году и являющегося в настоящее время одним из наиболее эффективных.

4.1 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.

4.1.1 Линейный криптоанализ

Метод линейного криптоанализа для блочного шифра FEAL был предложен М. Мацуи и А. Ямагиши [101] в 1992 году, для шифра DES — М. Мацуи [102] в 1993 году; в настоящее время этот метод наряду с методом дифференциального криптоанализа [36] считается одним из наиболее эффективных.

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 [111]; см. также работы [81, 44, 103]. В 1995 году авторы [66] 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 [84] было предложено для одной комбинации битов ключа рассматривать одновременно несколько линейных аппроксимаций; эту тему продолжает работа [37]. Авторы [122] 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 [31] и [124].

Серия работ посвящена вопросам стойкости различных алгоритмов шифрования к методу линейного криптоанализа. Л. Кнудсен [89] рассматривал вопросы построения схем шифрования типа Фейстеля, стойких к методам линейного и дифференциального криптоанализа. В. В. Шорин, В. В. Железняков, Э. М. Габидулин [126] 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 [40, 82, 35, 100, 108].

4.1.2 Проблемы нелинейного криптоанализа

Общий подход к использованию в линейном криптоанализе нелинейных аппроксимаций предложили в 1996 году Л. Кнудсен и М. Робшау [90]. 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 участвовать 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 [125], связанные с поиском квадратичных соотношений для конкретных подстановок, использующихся в S-блоках DES; экспериментальные исследования Дж. Накахары и др. [109]; работу Ж. Тапиадора и др. [133] 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 [22]. Вопросы нелинейных аппроксимаций булевых

функций (с использованием их приведенного представления) рассматривались А. В. Ивановым [7, 8]. Работы, направленные на решение второй проблемы, автору не известны. В целом метод нелинейного криптоанализа не получил пока должного развития.

4.1.3 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, \dots, v_m , где π — любая перестановка на m координатах, параметры $\mathbf{u} \in \mathbb{Z}_2^m, k$ ($1 \leq k \leq m/2$) 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 модификации алгоритмов 1 и 2 линейного криптоанализа Мацуи [102] 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^3 DES; 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.

4.2 Класс аппроксимирующих функций Δ_m

Рассмотрим следующий класс булевых функций от переменных v_1, \dots, v_m , где m четно. Для любого k , $1 \leq k \leq m/2$, и произвольной перестановки $\pi \in S_m$ на m переменных пусть

$$\mathfrak{A}_{m,0}^k(\pi) = \{\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k \mid \mathbf{u} \in \mathbb{Z}_2^m\}.$$

Заметим, что для любой перестановки $\pi \in S_m$ множество $\mathfrak{A}_{m,0}^1(\pi)$ состоит из всех линейных функций. Булевы функции от переменных v_1, \dots, v_m , используемые при шифровании, будем аппроксимировать функциями из множества

$$\Delta_m = \bigcup_{1 \leq k \leq m/2} \bigcup_{\pi \in S_m} \mathfrak{A}_{m,0}^k(\pi),$$

которое всюду далее называем *классом аппроксимирующих функций*. Говоря неформально, за счет произвольных перестановок π на переменных v_1, \dots, 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 $\mathfrak{A}_{m,0}^{k'}(\pi')$ и $\mathfrak{A}_{m,0}^{k''}(\pi'')$, вообще говоря, имеют непустое пересечение.

Для булевой функции $f \in \mathfrak{F}_m$ пусть множество $\text{АНФ}(f)$ 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 $\text{АНФ}(g) = \{v_1v_2, v_1v_3, v_1v_4, v_2v_3, v_3v_4, v_2, v_3, 1\}$. 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 $f \in \mathfrak{F}_m$ разобьем на пары; паре $\{v_{2i-1}, v_{2i}\}$ сопоставим номер i . Через $\text{Act}(f)$ обозначим подмножество максимальной мощности множества $\{1, 2, \dots, m/2\}$ такое, что для любых различных элементов i, j из $\text{Act}(f)$ одночлены

$$v_{2i-1}v_{2j-1}, v_{2i-1}v_{2j}, v_{2i}v_{2j-1}, v_{2i}v_{2j}$$

принадлежат множеству $\text{АНФ}(f)$. Будем говорить, что пара переменных с номером i *активна* для f , если $i \in \text{Act}(f)$. Заметим, что мощность $\text{Act}(f)$ для любой функции f либо нулевая, либо не меньше двух. Через $\rho = \rho(f)$ обозначим любую перестановку из S_m такую, что $|\text{Act}(f^\rho)| =$

$\max_{\pi \in S_m} |\text{Act}(f^\pi)|$. Рассмотрим, например, множество $\text{Act}(g)$ для функции g , заданной выше. Поскольку одночлены v_1v_3 , v_1v_4 , v_2v_3 принадлежат $\text{АНФ}(g)$, а одночлен v_2v_4 — нет, имеем $\text{Act}(g) = \emptyset$. Однако, при $\rho = (1, 3, 2, 4)$ имеем $\text{Act}(g^\rho) = \{1, 2\}$.

Теорема 8. *Булева функция $f \in \mathfrak{F}_m$, 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 ($1 \leq i, j \leq m/2$) 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 $\text{АНФ}(f^\rho)$;

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. (\Leftarrow) 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

$$\text{Act}(f^\rho) = \{i_1, \dots, i_k\},$$

где $2 \leq k \leq m/2$. Пусть $j_1, \dots, j_{(m/2)-k}$ — номера неактивных пар переменных функции f^ρ . Рассмотрим перестановку $\tau \in S_m$ такую, что $\tau(i_s) = s$ для любого $s = 1, \dots, k$ и $\tau(j_s) = k + s$ для любого $s = 1, \dots, (m/2) - k$. 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 $s = 1, \dots, m/2$. 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 $\text{Act}(f^{\rho \circ \pi}) = \{1, \dots, k\}$ также как и $\text{Act}(f^\rho)$ имеет мощность k . Поэтому далее, без ограничения общности, считаем, что $\text{Act}(f^\rho) = \{1, \dots, k\}$.

Заметим, что число k согласно условиям 1) и 2) однозначно определяет квадратичную часть функции f^ρ , которая имеет вид

$$\bigoplus_{i=1}^{k-1} \bigoplus_{j=i+1}^k (v_{2i-1}v_{2j-1} \oplus v_{2i-1}v_{2j} \oplus v_{2i}v_{2j-1} \oplus v_{2i}v_{2j}). \quad (4.1)$$

Покажем, что функция f^ρ принадлежит множеству $\mathfrak{A}_{m,0}^k$. Рассмотрим вектор $\mathbf{u} \in \mathbb{Z}_2^m$ такой, что

$$u_t = 1 \iff \begin{cases} v_t \notin \text{АНФ}(f^\rho), & \text{при } t = 1, \dots, 2k; \\ v_t \in \text{АНФ}(f^\rho), & \text{при } t = 2k+1, \dots, m. \end{cases}$$

Тогда $f^\rho(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k$. Действительно, по теореме 3 имеем

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle_k = & \left(\bigoplus_{i=1}^{k-1} \bigoplus_{j=i+1}^k Y_i Y_j \right) \oplus \left(\bigoplus_{i=1}^k (u_{2i}v_{2i-1} \oplus u_{2i-1}v_{2i}) \right) \\ & \oplus \left(\bigoplus_{i=k+1}^{m/2} (u_{2i-1}v_{2i-1} \oplus u_{2i}v_{2i}) \right), \end{aligned} \quad (4.2)$$

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 $i = 1, \dots, k$, 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 $1 \leq i < j \leq k$. Таким образом, квадратичная часть функции $\langle \mathbf{u}, \mathbf{v} \rangle_k$ совпадает с (4.1). Непосредственно из (4.2) 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 $\mathfrak{A}_{m,0}^k(\text{id})$, где id обозначает тождественную перестановку. Осталось заметить, что справедливо

$$f^\sigma \in \mathfrak{A}_{m,0}^k(\text{id}) \iff f \in \mathfrak{A}_{m,0}^k(\sigma^{-1}), \text{ для любой перестановки } \sigma \in S_m,$$

что вытекает из следующей эквивалентности:

$$\exists \mathbf{u} : f^\sigma(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k \iff \exists \mathbf{u} : f(\mathbf{v}) = \langle \mathbf{u}, \sigma^{-1}(\mathbf{v}) \rangle_k.$$

Отсюда, наконец, заключаем, что функция f принадлежит классу $\mathfrak{A}_{m,0}^k(\rho^{-1})$, а следовательно и классу Δ_m .

(\implies) Если функция f линейна, то выполнение условий 1), 2), 3) очевидно. Пусть f имеет нетривиальную квадратичную часть. Тогда, поскольку f принадлежит некоторому классу $\mathfrak{A}_{m,0}^k(\pi)$, мощность квадратичной части f равна $4 \cdot \binom{s}{2}$ для подходящего s , $2 \leq s \leq k$, что непосредственно следует из теоремы 3. Так как f^ρ также содержится в классе Δ_m , то $|\text{Act}(f^\rho)| = s$ (например, в качестве ρ можно взять перестановку π^{-1}). Тогда квадратичная часть $\text{АНФ}(f^\rho)$ 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 $i, j \in \text{Act}(f^\rho)$, и следовательно выполнены условия 1) и 2). Справедливость 3) вытекает из теоремы 3. Теорема доказана. \square

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 8 для каждого фиксированного k , $2 \leq k \leq m/2$, определим число квадратичных функций f из Δ_m таких, что $|\text{Act}(f^\rho)| = k$. 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 $\text{АНФ}(f)$ согласно условию 3) теоремы 8. Переменные, не содержащиеся в выбранных парах, входят или не входят в $\text{АНФ}(f)$ свободно. Таким образом, число функций $f \in \Delta_m$, $|\text{Act}(f^\rho)| = k$, 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 , $2 \leq k \leq m/2$, и учитывая линейные функции, получаем требуемое выражение для мощности класса Δ_m . \square

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 $m \rightarrow \infty$.

Теорема 8 и следствие 8 предлагают способ перечисления всех элементов множества Δ_m без повторений.

4.3 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 [15].

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, $K \in \mathbb{Z}_2^{m_{\text{key}}}$;

$F : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m_{\text{key}}} \rightarrow \mathbb{Z}_2^m$ — 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, $K^{(i)} \in \mathbb{Z}_2^{m'_{\text{key}}}$, $1 \leq i \leq r$, определяемый по ключу K ;

$F_i : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m'_{\text{key}}} \rightarrow \mathbb{Z}_2^m$ — преобразование i -го раунда шифрования, $1 \leq i \leq r$, взаимно однозначное, если второй аргумент фиксирован;

$$C^{(0)} = P;$$

$C^{(i)} = F_i(C^{(i-1)}, K^{(i)})$ — промежуточный шифротекст, $C^{(i)} \in \mathbb{Z}_2^m$, $1 \leq i \leq r$;

$C = C^{(r)}$ — 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

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = \langle \mathbf{d}, \tau(K) \rangle_k, \quad (4.3)$$

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 $1 \leq i, j \leq m/2$, $1 \leq k \leq m_{\text{key}}/2$.

Считаем, что равенство (4.3) выполняется с вероятностью $p = 1/2 + \varepsilon$, такой, что $0 < |\varepsilon| \leq 1/2$. Число ε назовем *преобладанием* равенства (4.3). 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 (4.3) 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 (4.3) 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

$$\{(P_t, C_t) \mid t = 1, \dots, N\}$$

известных пар открытого и зашифрованного текстов, $C_t = F(P_t, K)$. Следующий алгоритм является модификацией алгоритма Мацуи [102] 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 [15]). 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, \dots, 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 (4.3) 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 [102, 15]) с помощью функции нормального распределения, а именно

$$\xi_0 \simeq \Phi_{0,1}(-2|\varepsilon|\sqrt{N}) = \int_{-2|\varepsilon|\sqrt{N}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy. \quad (4.4)$$

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 $1 \leq i, j \leq m/2$, для произвольных перестановок $\pi, \sigma \in S_m$ обозначим через $\varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0)$ действительное число из отрезка $[-1/2, 1/2]$ такое, что вероятность выполнения равенства

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(P, K)) \rangle_j = 0 \quad (4.5)$$

равна $1/2 + \varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0)$.

Утверждение 12. Для любого отображения $F(\cdot, K) : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ и любых перестановок $\pi, \sigma \in S_m$ выполняется равенство

$$2^{m+1} \cdot \varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0) = W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a}).$$

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 $W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a})$ следует, что

$$W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{a}, \pi(\mathbf{u}) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(\mathbf{u}, K)) \rangle_j} = |M_0| - |M_1|.$$

С помощью (4.5) получаем $|M_0| = 2^m(1/2 + \varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0))$, и следовательно

$$|M_0| - |M_1| = 2^{m+1} \cdot \varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0).$$

Утверждение доказано. □

Напомним, что $\varepsilon(K)$ обозначает преобладание, с которым выполняется равенство (4.3) при фиксированном ключе K . Заметим, что для любых k , \mathbf{d} и τ справедливо

$$|\varepsilon(K)| = |\varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0)|. \quad (4.6)$$

Теорема 9. 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 , $1 \leq j \leq m/2$, таковы что функция

$$\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$$

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 $\mathfrak{B}_m^{m/2}$, имеем $|W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a})| = \pm 2^{m/2}$ для любого $\mathbf{a} \in \mathbb{Z}_2^m$ и каждого i , $1 \leq i \leq m/2$. Тогда из утверждения 12 и равенства (4.6) сразу следует, что для любых параметров k , \mathbf{d} и τ все значения $|\varepsilon(K)|$ равны $2^{-(m/2)-1}$, откуда и вытекает требуемое. \square

Из неравенства (2.9) следует, что $2^{-(m/2)-1}$ является минимальным возможным значением для $\max_{\mathbf{a} \in \mathbb{Z}_2^m} |\varepsilon(K)|$ при любых фиксированных $i, j, k, \mathbf{b}, \mathbf{d}, \pi, \sigma$ и τ . Согласно теореме 9 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 [102], основанную на исследовании промежуточных шифротекстов. Пусть выбраны целые числа s_1, s_2 , такие, что $0 \leq s_1 < s_2 \leq r$.

Рассмотрим равенство

$$\langle \mathbf{a}, \pi(C^{(s_1)}) \rangle_i \oplus \langle \mathbf{b}, \sigma(C^{(s_2)}) \rangle_j = \langle \tau(\mathbf{d}), K \rangle_k, \quad (4.7)$$

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 $1 \leq i, j \leq m/2$, $1 \leq k \leq m_{\text{key}}/2$. Будем считать, что (4.7) выполняется с вероятностью $\tilde{p} = 1/2 + \tilde{\varepsilon}$, такой, что $0 < |\tilde{\varepsilon}| \leq 1/2$.

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 $\mathbb{Z}_2^{m_{s_1, s_2}}$: $\tilde{K}_1, \dots, \tilde{K}_{2^{m_{s_1, s_2}}}$, так, что

$$\left| \frac{N}{2} - N_0(\tilde{K}_1) \right| \geq \dots \geq \left| \frac{N}{2} - N_0(\tilde{K}_{2^{m_{s_1, s_2}}}) \right|;$$

- для каждого q от 1 до $2^{m_{s_1, s_2}}$

$$\triangleright \text{ полагаем } \langle \mathbf{d}, \tau(K) \rangle_k = \begin{cases} 0, & \text{если } (N_0(\tilde{K}_q) - \frac{N}{2}) \cdot \tilde{\varepsilon} > 0; \\ 1, & \text{в другом случае;} \end{cases}$$

\triangleright с учетом полученного соотношения подбираем ключ.

Конец алгоритма

Надежность алгоритма 2 может быть оценена так же как в случае линейного криптоанализа (см. [102, 15]). 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 $K^{(s_1+1)}, \dots, K^{(s_2)}$ обозначим через $K^{(s_1+1, \dots, s_2)}$. Пусть отображение $F_{s_1+1, s_2} : \mathbb{Z}_2^m \times (\mathbb{Z}_2^{m'_{\text{key}}})^{s_2-s_1} \rightarrow \mathbb{Z}_2^m$ задано суперпозицией функций $F_{s_1+1}, \dots, F_{s_2}$:

$$F_{s_1+1, s_2}(C^{(s_1)}, K^{(s_1+1, \dots, s_2)}) = F_{s_2}(F_{s_2-1}(\dots (F_{s_1+1}(C^{(s_1)}, K^{(s_1+1)}), K^{(s_1+2)}) \dots), K^{(s_2)}).$$

Тогда выполняется

$$C^{(s_2)} = F_{s_1+1, s_2}(C^{(s_1)}, K^{(s_1+1, \dots, s_2)}).$$

Аналогично тому, как это было сделано для первого алгоритма, рассмотрим равенство

$$\langle \mathbf{a}, \pi(C^{(s_1)}) \rangle_i \oplus \langle \mathbf{b}, \sigma(F_{s_1+1, s_2}(C^{(s_1)}, K^{(s_1+1, \dots, s_2)})) \rangle_j = 0 \quad (4.8)$$

при фиксированном наборе подключей $K^{(s_1+1, \dots, s_2)}$. Пусть оно выполняется с вероятностью $1/2 + \tilde{\varepsilon}_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K^{(s_1+1, \dots, s_2)}; 0)$, где $-1/2 \leq \tilde{\varepsilon}_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K^{(s_1+1, \dots, s_2)}; 0) \leq 1/2$.

Аналогично утверждению 12 несложно доказать

Утверждение 13. Для любого отображения $F_{s_1+1, s_2}(\cdot, K^{(s_1+1, \dots, s_2)}) : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ имеем

$$2^{m+1} \cdot \tilde{\varepsilon}_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K^{(s_1+1, \dots, s_2)}; 0) = W_{\langle \mathbf{b}, \sigma(F_{s_1+1, s_2}(\pi^{-1}(\cdot), K^{(s_1+1, \dots, s_2)})) \rangle_j}^{(i)}(\mathbf{a}).$$

Через $\tilde{\varepsilon}(K)$ обозначим преобладание в равенстве (4.7) при фиксированном K . Тогда при любых параметрах k , \mathbf{d} и τ справедливо

$$|\tilde{\varepsilon}(K)| = |\tilde{\varepsilon}_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K^{(s_1+1, \dots, s_2)}; 0)|, \quad (4.9)$$

если $K^{(s_1+1, \dots, s_2)}$ является набором подключей ключа K .

Теорема 10. Пусть фиксирован ключ $K \in \mathbb{Z}_2^{m_{\text{key}}}$ и целые числа s_1, s_2 , где $0 \leq s_1 < s_2 \leq r$. Пусть $K^{(s_1+1, \dots, s_2)}$ — набор подключей ключа K . Пусть вектор $\mathbf{b} \in \mathbb{Z}_2^m$, перестановки $\pi, \sigma \in S_m$ и параметр j , $1 \leq j \leq m/2$, таковы, что функция

$$\langle \mathbf{b}, \sigma(F_{s_1+1, s_2}(\pi^{-1}(\cdot), K^{(s_1+1, \dots, s_2)})) \rangle_j : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$$

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 10 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.

4.4 Анализ четырехразрядных подстановок в S-блоках алгоритмов ГОСТ, DES, $s^3\text{DES}$

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^3 DES. 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 [21] приведена серия экстремальных четырехразрядных подстановок, рекомендованных для S-блоков стандарта ГОСТ 28147-89 (см. подстановки S^1, \dots, 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 линейные 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:

$$\begin{aligned} &\langle 0101, v_1 v_2 v_3 v_4 \rangle_2, \quad \langle 0110, v_1 v_2 v_3 v_4 \rangle_2, \quad \langle 1001, v_1 v_2 v_3 v_4 \rangle_2, \quad \langle 1010, v_1 v_2 v_3 v_4 \rangle_2, \\ &\langle 0101, v_1 v_3 v_2 v_4 \rangle_2, \quad \langle 0110, v_1 v_3 v_2 v_4 \rangle_2, \quad \langle 1001, v_1 v_3 v_2 v_4 \rangle_2, \quad \langle 1010, v_1 v_3 v_2 v_4 \rangle_2, \\ &\langle 0101, v_1 v_4 v_2 v_3 \rangle_2, \quad \langle 0110, v_1 v_4 v_2 v_3 \rangle_2, \quad \langle 1001, v_1 v_4 v_2 v_3 \rangle_2, \quad \langle 1010, v_1 v_4 v_2 v_3 \rangle_2. \end{aligned}$$

Для этого мы выбрали все различные множества из двух неупорядоченных пар переменных: $\left\{ \{v_1, v_2\}, \{v_3, v_4\} \right\}, \left\{ \{v_1, v_3\}, \{v_2, v_4\} \right\}, \left\{ \{v_1, v_4\}, \{v_2, v_3\} \right\}$; затем для каждого множества составили четыре квадратичные функции, различающиеся только линейной частью.

$S^1 = (0, 13, 11, 8, 3, 6, 4, 1, 15, 2, 5, 14, 10, 12, 9, 7)$
 $S^2 = (0, 1, 9, 14, 13, 11, 7, 6, 15, 2, 12, 5, 10, 4, 3, 8)$
 $S^3 = (0, 1, 11, 13, 9, 14, 6, 7, 12, 5, 8, 3, 15, 2, 4, 10)$
 $S^4 = (0, 1, 2, 4, 3, 5, 8, 10, 7, 9, 6, 13, 11, 14, 12, 15)$
 $S^5 = (0, 1, 11, 2, 8, 6, 15, 3, 14, 10, 4, 9, 13, 5, 7, 12)$
 $S^6 = (0, 1, 11, 2, 8, 3, 15, 6, 14, 10, 4, 9, 13, 5, 7, 12)$
 $S^7 = (0, 4, 11, 2, 8, 6, 10, 1, 14, 15, 3, 9, 13, 5, 7, 12)$
 $S^8 = (0, 4, 11, 2, 8, 3, 15, 1, 14, 10, 6, 9, 13, 5, 7, 12)$
 $S^9 = (0, 11, 15, 9, 1, 5, 6, 8, 3, 10, 4, 12, 14, 13, 7, 2)$
 $S^{10} = (0, 7, 10, 14, 9, 1, 13, 8, 12, 2, 11, 15, 3, 5, 4, 6)$
 $S^{11} = (4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3)$
 $S^{12} = (8, 2, 11, 13, 4, 1, 14, 7, 5, 15, 0, 3, 10, 6, 9, 12)$
 $S^{13} = (10, 5, 3, 15, 12, 9, 0, 6, 1, 2, 8, 4, 11, 14, 7, 13)$
 $S^{14} = (5, 10, 12, 6, 0, 15, 3, 9, 8, 13, 11, 1, 7, 2, 14, 4)$
 $S^{15} = (3, 9, 15, 0, 6, 10, 5, 12, 14, 2, 1, 7, 13, 4, 8, 11)$
 $S^{16} = (15, 0, 10, 9, 3, 5, 4, 14, 8, 11, 1, 7, 6, 12, 13, 2)$
 $S^{17} = (12, 6, 3, 9, 0, 5, 10, 15, 2, 13, 4, 14, 7, 11, 1, 8)$
 $S^{18} = (13, 10, 0, 7, 3, 9, 14, 4, 2, 15, 12, 1, 5, 6, 11, 8)$

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

Таблица 6. 4-Разрядные подстановки,
с предельно высокой нелинейностью $NL = 4$.

Таблица 7.
Подстановка S^2 .

Рассмотрим соотношения

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = 0, \quad (4.10)$$

где при $i = 1$ вектору \mathbf{a} соответствуют числа $0, \dots, 15$ и тождественная перестановка π ; при $i = 2$ вектору \mathbf{a} отвечают числа $5, 6, 9, 10$ и перестановки $\pi = \text{id}, (1, 3, 2, 4), (1, 3, 4, 2)$ (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}, π) , а столбцы — тройками (j, \tilde{b}, σ) , такую что на пересечении строки и столбца находится преобразование $\varepsilon_{j, \tilde{b}, \sigma}^{i, \mathbf{a}, \pi}$ соответствующего равенства (4.10), умноженное на 16 (т. е. отклонение числа выполнений равенства (4.10) 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 $P \rightarrow C$, 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 $NQ(S) \leq NL(S)$. Согласно [83] справедливо $NL(S) \leq 4$ для любой четырехразрядной подстановки S .

Для подстановки S^2 имеем $NL(S^2) = 4$, $NQ(S^2) = 2$ (см. таблицу 8). 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 $i = 2$, $\tilde{a} = 6$, $\pi = \text{id}$, $j = 1$, $\tilde{b} = 2$, $\sigma = \text{id}$, 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 (2.6) и (2.7), 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 .

$16 \cdot \varepsilon_{j,b,\sigma}^{i,a,\pi}$		$j = 1$ 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	6	2	2	0	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. Преобразования для подстановки S^2 .

Аналогично, если выбрать соотношение при $i = 1$, $\tilde{a} = 9$, $\pi = \text{id}$, $j = 2$, $\tilde{b} = 10$, $\sigma = (1, 3, 2, 4)$, 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 (2.6) и (2.7) 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 таблице 9 приведены наиболее вероятные соотношения на P и C для подстановок S^1, \dots, 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 удастся 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 $t = 1, \dots, 10$.

На данном примере можно убедиться в том, что использование соотношений вида (4.10) 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 [27] 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, [27]), 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, [27]) в S-блоках модифицированного алгоритма $s^3\text{DES}$ [88, 34], которые считаются устойчивыми к методам дифференциального и линейного криптоанализа. Среди них только 7 подстановок (это подстановки S^{12}, \dots, 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}, \dots, S^{18} приведены в таблице 10.

4.5 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 $\mathbf{u} = (u_1, \dots, u_m)$ пусть $\bar{\mathbf{u}}^k = (u_1 \oplus u_2, \dots, u_{2k-1} \oplus u_{2k})$ — вектор длины k . Через $*$ обозначим обычное покомпонентное умножение векторов. Пусть $|\mathbf{u}| = \langle \mathbf{u}, \mathbf{u} \rangle$. Справедливо

Утверждение 14. Для любых векторов $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$, для любого k , $1 \leq k \leq m/2$, 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 3 имеем

$$\begin{aligned} \langle \mathbf{u} \oplus \mathbf{v}, \mathbf{w} \rangle_k &= \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \left(\bigoplus_{i=1}^k \bigoplus_{j=i}^k (\bar{u}_i^k \oplus \bar{v}_i^k)(\bar{u}_j^k \oplus \bar{v}_j^k) \bar{w}_i^k \bar{w}_j^k \right) = \\ &= \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \left(\bigoplus_{i=1}^k \bigoplus_{j=i}^k \bar{u}_i^k \bar{v}_j^k \bar{w}_i^k \bar{w}_j^k \right) \oplus \left(\bigoplus_{i=1}^k \bigoplus_{j=i}^k \bar{u}_j^k \bar{v}_i^k \bar{w}_i^k \bar{w}_j^k \right) = \\ &= \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \left(\bigoplus_{i=1}^k \bigoplus_{j=1}^k \bar{u}_i^k \bar{v}_j^k \bar{w}_i^k \bar{w}_j^k \right) \oplus \left(\bigoplus_{i=1}^k \bar{u}_i^k \bar{v}_i^k \bar{w}_i^k \right). \end{aligned}$$

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. \square

Из утверждения 14 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 4.1.2) такая добавка может быть оценена с некоторой вероятностью по частичной информации о неизвестных битах.

Аналог линейности. Напомним, что в 2.2 была определена бинарная операция $\star : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ 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 (2.2) вытекает

Утверждение 15. При любых целых m, k , любых $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$ справедливо $c_{\mathbf{u}, \mathbf{w}}^k + c_{\mathbf{v}, \mathbf{w}}^k = c_{\mathbf{u} \star \mathbf{v}, \mathbf{w}}^k$, где $+$ обозначает сложение над \mathbb{Z}_4 .

Напомним, что по определению (2.4) выполняется $\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(c_{\mathbf{u}, \mathbf{v}}^k)$. Из этого следует, что вектор значений булевой функции $\langle \mathbf{u}, \cdot \rangle_k : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$ является образом (под действием отображения β) вектора значений функции $\langle \langle \mathbf{u}, \cdot \rangle \rangle_k : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_4$, такой что $\langle \langle \mathbf{u}, \mathbf{v} \rangle \rangle_k = c_{\mathbf{u}, \mathbf{v}}^k$. Другими словами, $\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(\langle \langle \mathbf{u}, \mathbf{v} \rangle \rangle_k)$. Заметим, что $\langle \langle \mathbf{u}, \mathbf{v} \rangle \rangle_k = \langle \langle \mathbf{v}, \mathbf{u} \rangle \rangle_k$. Согласно утверждению 15 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).

4.6 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}	$C\{1, 4\} = P\{13, 14, 23, 24, 1, 3\},$ $C\{1, 2, 3, 4\} = P\{12, 14, 23, 34, 1, 4\},$ $C\{13, 14, 23, 24, 1, 3\} = P\{1, 3\},$ $C\{12, 14, 23, 34, 3, 4\} = P\{1, 3\},$ $C\{13, 14, 23, 24, 2, 4\} = P\{12, 14, 23, 34, 3, 4\},$ $C\{13, 14, 23, 24, 2, 4\} = P\{13, 14, 23, 24, 1, 3\},$

Таблица 9. Наиболее вероятные квадратичные соотношения для входных и выходных битов подстановок S^1, \dots, S^{10} .

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

Таблица 10. Наиболее вероятные квадратичные соотношения для входных и выходных битов подстановок S^{11}, \dots, S^{18} .

Глава 5

Приложение.

Доказательство Теоремы 1

В данной главе рассматриваются равномерно упакованные (в широком смысле) двоичные коды длины n с кодовым расстоянием d и радиусом покрытия ρ , и приводится доказательство Теоремы 1. Будет показано, что любой такой код однозначно определяется множеством своих кодовых слов весов $\lceil n/2 \rceil - \rho, \dots, \lceil n/2 \rceil + \rho$, и в случае нечетного d число различных таких кодов не превышает числа $2^{2^{n-\frac{d}{2} \log_2 n + o(\log_2 n)}}$.

5.1 Равномерно упакованные коды

Двоичный код C длины n с кодовым расстоянием d для краткости будем называть (n, d) -кодом. Радиусом покрытия ρ кода C называется максимальное расстояние, на которое может быть удален от кода C двоичный вектор длины n , т. е.

$$\rho = \max_{x \in \mathbb{Z}_2^n} d_H(x, C).$$

Согласно работе Л. А. Бассалыго, Г. В. Зайцева и В. А. Зиновьева [3] двоичный (n, d) -код C с радиусом покрытия ρ называется *равномерно упакованным в широком смысле*, если существуют действительные числа $\alpha_0, \alpha_1, \dots, \alpha_\rho$ такие, что для любого двоичного вектора x длины n выполняется равенство

$$\sum_{i=0}^{\rho} \alpha_i f_i(x) = 1,$$

где $f_i(x)$ — число кодовых слов кода C , находящихся на расстоянии i от вектора x , $i = 0, 1, \dots, \rho$. Пусть $d = 2t + 1$. Известно другое определение равномерно упакованных двоичных кодов j -го порядка ($j = 1, \dots, t$), введенное Дж. М. Геталсом и Х. ван Тилборгом [79], которое при $j = \rho - t$ является частным случаем определения из [3]. При $j = \rho - t = 1$ оба определения [3] и [79] совпадают; при этом соответствующие коды называются *строго равномерно упакованными* или *равномерно упакованными в узком смысле*. Такие коды впервые были рассмотрены Н. В. Семаковым, В. А. Зиновьевым и Г. В. Зайцевым [23]. Далее под термином «равномерно упакованный» будем понимать «равномерно упакованный в широком смысле».

С. В. Августиневич [1] показал, что каждый двоичный совершенный код длины n с кодовым расстоянием $d = 3$ однозначно определяется множеством своих кодовых слов веса $(n - 1)/2$. Используя это свойство, в [1] было показано, что число различных совершенных двоичных кодов не превосходит $2^{2^{n - \frac{3}{2} \log n + o(\log n)}}$ (здесь и далее \log обозначает логарифм по основанию 2).

Рассмотрим произвольный класс $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$ двоичных равномерно упакованных (в широком смысле) (n, d) -кодов с радиусом покрытия ρ и параметрами равномерной упаковки $\alpha_0, \dots, \alpha_\rho$. Считаем, что d и ρ — константы. Число различных кодов в классе $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$ обозначим через $L_{n,d}$. Используя границу сферической упаковки для мощности (n, d) -кода, несложно получить следующую тривиальную оценку: $L_{n,d} \leq 2^{2^{n - \frac{d-1}{2} \log n + o(\log n)}}$. Обобщая метод работы [1], покажем, что любой код из класса $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$ однозначно определяется множеством своих кодовых слов весов $\lceil n/2 \rceil - \rho, \dots, \lceil n/2 \rceil + \rho$, и в случае нечетного d имеет место оценка:

$$L_{n,d} < 2^{2^{n - \frac{d}{2} \log n + \log \log n + \delta}},$$

где константа δ равна $d \log d + \log(\rho + 1)$.

5.2 Три леммы

Пусть x, y — любые двоичные векторы длины n , и пусть $d_H(x, y) = k$. Известно (см., например, [16, гл. 21]), что число векторов $z \in \mathbb{Z}_2^n$ таких, что

$d_H(x, z) = i$ и $d_H(y, z) = j$, не зависит от выбора векторов x и y , а зависит лишь от чисел i, j, k, n . Обозначим это число через p_{ijk} (подразумевая также зависимость этого параметра от n). Ясно, что

$$p_{ijk} = \binom{k}{(i-j+k)/2} \binom{n-k}{(i+j-k)/2},$$

если $i + j - k$ четно; $p_{ijk} = 0$, если $i + j - k$ нечетно. Будем считать, что параметр p_{ijk} определен для любых значений i, j и k , $0 \leq i, j, k \leq n$, и равен нулю, если соответствующее множество векторов z пусто.

Пусть C — произвольный код из класса равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$. Обозначим через C_i и E_i множества векторов веса i кода C и пространства \mathbb{Z}_2^n соответственно, где $i = 0, 1, \dots, n$. Пусть μ_C^i — мощность множества C_i . Набор $\mu(C) = \{\mu_C^0, \mu_C^1, \dots, \mu_C^n\}$ называется *весовым спектром* кода C , а числа μ_C^i , $i = 0, 1, \dots, n$, — *спектральными значениями* кода. В работе [3] приведена формула для вычисления весового спектра (более точно: весовой функции) произвольного равномерно упакованного кода, содержащая ρ неизвестных констант. Для определения этих констант требуется знать любые ρ спектральных значений кода, при которых возможно решение соответствующей системы линейных уравнений (см. подробнее [3]).

Убедимся в справедливости следующего утверждения.

Лемма 1. *Весовой спектр произвольного кода C из класса равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$ однозначно определяется значениями $\mu_C^0, \dots, \mu_C^{\rho-1}$.*

Доказательство. Покажем как с помощью известных значений $\mu_C^0, \dots, \mu_C^{j+\rho-1}$ при любом $j = 0, 1, \dots, n - \rho$ восстановить значение $\mu_C^{j+\rho}$. При любом $i = 0, 1, \dots, \rho$ имеет место следующее равенство

$$\sum_{x \in E_j} f_i(x) = \sum_{k=\max\{0, j-i\}}^{j+i} p_{ijk} \mu_C^k. \quad (5.1)$$

Действительно, каждый кодовый вектор веса k находится на расстоянии i в точности от p_{ijk} двоичных векторов веса j . Заметим, что в каждом соотношении (5.1) при $i = 0, 1, \dots, \rho - 1$ участвуют лишь известные спектральные

значения $\mu_C^{\max\{0, j-\rho+1\}}, \dots, \mu_C^{j+\rho-1}$, а при $i = \rho$ единственным неизвестным спектральным значением является $\mu_C^{j+\rho}$, причем оно входит в это равенство с ненулевым коэффициентом. В силу равномерной упакованности кода C справедливо равенство

$$\sum_{x \in E_j} \sum_{i=0}^{\rho} \alpha_i f_i(x) = \binom{n}{j}.$$

Меняя местами знаки суммирования в этом равенстве и пользуясь (5.1), получаем

$$\sum_{i=0}^{\rho} \alpha_i \sum_{k=\max\{0, j-i\}}^{j+i} p_{ijk} \mu_C^k = \binom{n}{j}.$$

Отсюда однозначно определяется значение $\mu_C^{j+\rho}$. Таким образом последовательно восстанавливаются значения $\mu_C^{\rho}, \dots, \mu_C^n$. \square

Следующая лемма является обобщением одного свойства совершенных двоичных кодов, приведенного в работе [1].

Лемма 2. *Множество $X = C_{\lceil n/2 \rceil - \rho} \cup \dots \cup C_{\lceil n/2 \rceil + \rho}$ однозначно определяет код C из класса равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_{\rho})$.*

Доказательство. Обозначим через A и B следующие множества:

$$A = C_0 \cup \dots \cup C_{\lceil n/2 \rceil - \rho - 1} \text{ и } B = C_{\lceil n/2 \rceil + \rho + 1} \cup \dots \cup C_n.$$

Имеем

$$C = A \cup X \cup B.$$

Несложно заметить, что расстояние между множествами A и B не меньше $2\rho+1$ и, следовательно, не меньше d . Предположим, что существует другой код

$$C' = A' \cup X \cup B'$$

из класса $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_{\rho})$, и пусть $B \neq B'$. Тогда код C'' , полученный из C заменой множества B на B' , также имеет кодовое расстояние d . Покажем, что C'' принадлежит классу $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_{\rho})$, т. е. является

равномерно упакованным кодом с параметрами $\alpha_0, \dots, \alpha_\rho$. Для произвольного вектора $x \in \mathbb{Z}_2^n$ рассмотрим сумму

$$\sum_{i=0}^{\rho} \alpha_i f_i(x), \quad (5.2)$$

где $f_i(x)$ — число кодовых слов кода C'' , находящихся на расстоянии i от вектора x . Обозначим через $T_\rho^D(x)$ множество всех кодовых слов произвольного кода D длины n , содержащихся в шаре радиуса ρ с центром в вершине x , т. е. $T_\rho^D(x) = \{ y \in D \mid d_H(x, y) \leq \rho \}$. По построению кода C'' имеем

$$T_\rho^{C''}(x) = \begin{cases} T_\rho^C(x), & \text{если } wt(x) \leq \lfloor n/2 \rfloor, \\ T_\rho^{C'}(x), & \text{если } wt(x) \geq \lceil n/2 \rceil. \end{cases}$$

Так как коды C и C' являются равномерно упакованными с параметрами $\alpha_0, \dots, \alpha_\rho$, то для любого вектора $x \in \mathbb{Z}_2^n$ сумма (5.2) равна 1. Таким образом, код C'' принадлежит классу равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$.

Поскольку $B \neq B'$, без ограничения общности можно считать, что найдется вектор $y \in \mathbb{Z}_2^n$ такой, что $y \in B$ и $y \notin B'$. Пусть $z = y \oplus \mathbf{1}$, где $\mathbf{1}$ — вектор со всеми координатами, равными 1, и \oplus обозначает покомпонентное сложение векторов по модулю 2. Тогда, как нетрудно заметить, выполняется неравенство $wt(z) \leq \lceil n/2 \rceil - \rho - 1$, поэтому

$$T_\rho^C(z) = T_\rho^{C''}(z).$$

Отсюда следует, что для равномерно упакованных кодов $z \oplus C$ и $z \oplus C''$ (сдвигов кодов C и C'' соответственно на вектор z) первые $\rho + 1$ спектральных значений одинаковы, т. е.

$$\mu_{z \oplus C}^0 = \mu_{z \oplus C''}^0, \dots, \mu_{z \oplus C}^\rho = \mu_{z \oplus C''}^\rho.$$

Тогда согласно лемме 1 коды $z \oplus C$ и $z \oplus C''$ имеют одинаковые весовые спектры. Но поскольку $\mathbf{1} \in z \oplus C$ и $\mathbf{1} \notin z \oplus C''$, имеем $\mu_{z \oplus C}^n \neq \mu_{z \oplus C''}^n$. Полученное противоречие доказывает лемму 2. \square

Далее докажем одну простую оценку для числа кодовых слов веса i произвольного двоичного кода C . Этой оценки достаточно для доказательства

основного результата работы, хотя следует отметить, что известны существенно более сильные оценки для числа $|C_i|$ (см., например, [16, гл. 17]).

Лемма 3. *Для любого двоичного кода C длины n с кодовым расстоянием $d = 2t + 1$ при любом $i = t, \dots, n - t$ справедливо $|C_i| \leq \frac{2^{it}}{n^t} \binom{n}{i}$.*

Доказательство. Пусть $i \leq \lfloor n/2 \rfloor$. Для каждого вектора x веса i определим множество V_x , состоящее из векторов веса $i - t$, все ненулевые координаты которых лежат среди ненулевых координат вектора x . Заметим, что $|V_x| = \binom{i}{t}$. Поскольку для любых кодовых векторов x и y из C_i множества V_x и V_y не пересекаются (иначе $d_H(x, y) < d$), имеем

$$|C_i| \leq \frac{|E_{i-t}|}{|V_x|} = \frac{\binom{n}{i-t}}{\binom{i}{t}},$$

откуда следует искомая оценка. Рассуждения легко переносятся на случай $i \geq \lceil n/2 \rceil$. \square

5.3 Верхняя оценка

Теорема 1. *Для числа $L_{n,d}$ различных кодов из класса равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \dots, \alpha_\rho)$ при $n \geq 3$ и нечетном $d \geq 3$ справедлива оценка*

$$L_{n,d} < 2^{2^{n-\frac{d}{2} \log n + \log \log n + \delta}},$$

где константа δ равна $d \log d + \log(\rho + 1)$.

Доказательство. Из леммы 2 следует, что

$$L_{n,d} \leq \left(\frac{|E_{\lceil n/2 \rceil - \rho}| + \dots + |E_{\lfloor n/2 \rfloor + \rho}|}{|C_{\lceil n/2 \rceil - \rho}| + \dots + |C_{\lfloor n/2 \rfloor + \rho}|} \right). \quad (5.3)$$

Имеем $|E_{\lceil n/2 \rceil - \rho}| + \dots + |E_{\lfloor n/2 \rfloor + \rho}| \leq (2\rho + 1) \binom{n}{\lfloor n/2 \rfloor}$. По лемме 3 для произвольного двоичного кода C длины n с кодовым расстоянием d выполняется

неравенство $|C_{\lfloor n/2 \rfloor - \rho}| + \dots + |C_{\lfloor n/2 \rfloor + \rho}| \leq \frac{\lambda}{n^t} \binom{n}{\lfloor n/2 \rfloor}$, где $\lambda = (2\rho + 1) \cdot 2^t \cdot t!$ и $t = (d - 1)/2$. Применяя формулу Стирлинга

$$n^n e^{-n} \sqrt{2\pi n} \leq n! \leq n^n e^{1-n} \sqrt{2\pi n},$$

получаем $\binom{n}{\lfloor n/2 \rfloor} \leq 2^{n - \frac{1}{2} \log n + 2}$. Тогда в силу (5.3) имеем

$$L_{n,d} < \binom{2^{n - \frac{1}{2} \log n + (2 + \log(2\rho + 1))}}{2^{n - \frac{d}{2} \log n + (2 + \log \lambda)}}.$$

Отсюда и из неравенства $\binom{a}{b} < \left(\frac{3a}{b}\right)^b$ для любых $a > b > 1$ вытекает

$$L_{n,d} < 2^{2^{n - \frac{d}{2} \log n + \log \log n + (\log \lambda + \log d + 1)}}.$$

Тогда, используя неравенство $c! \leq \left(\frac{c+1}{2}\right)^c$ для любого $c \geq 1$, несложно получить

$$\log \lambda + \log d + 1 \leq d \log d + \log(\rho + 1),$$

и следовательно,

$$L_{n,d} < 2^{2^{n - \frac{d}{2} \log n + \log \log n + \delta}}.$$

Теорема доказана. □

Приведем примеры классов кодов, к которым применима Теорема 1.

1) Двоичные *совершенные коды* длины $n = 2^m - 1$ ($m \geq 2$), мощности $2^{n - \log(n+1)}$ с кодовым расстоянием $d = 3$ и параметрами равномерной упаковки $\alpha_0 = \alpha_1 = 1$ (см. [23]). Этот частный случай был доказан в [1].

Замечание. Отметим, что для мощностей отдельных подклассов совершенных кодов известны лучшие оценки или даже точные значения. Например, посчитаны и полностью описаны \mathbb{Z}_4 -линейные совершенные коды [9]; классифицированы некоторые классы совершенных кодов одного ранга [30].

Другие примеры равномерно упакованных кодов с $d = 3$ можно найти в [79] (см. также [3] и [119]).

2) Двоичные коды Препараты длины $n = 2^m - 1$ ($m \geq 4$ четно), мощности $2^{n-2\log(n+1)+1}$ с кодовым расстоянием $d = 5$ и параметрами упаковки $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = 3/n$ (см. [23, 3]).

Следствие 9. Число различных двоичных кодов Препараты длины n с кодовым расстоянием 5 не превосходит величины $2^{2^{n-\frac{5}{2}\log n + o(\log n)}}$.

Замечание. Отметим, что для числа кодов одного специального подкласса кодов Препараты имеет место более точная оценка. А именно, согласно [26, следствие 2], число неэквивалентных четверичных линейных кодов Препараты длины n с расстоянием 6 не превосходит величины $2^{n\log n}$.

3) Двоичные примитивные коды типа БЧХ длины $n = 2^m - 1$ ($m \geq 5$ нечетно), мощности $2^{n-2\log(n+1)}$ с кодовым расстоянием $d = 5$, радиусом покрытия $\rho = 3$ и параметрами $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = \frac{6}{n-1}$ (см. [3]).

4) Двоичные коды Геталса (или коды типа Геталса) длины $n = 2^m - 1$ ($m \geq 4$ четно), мощности $2^{n-3\log(n+1)+2}$ с кодовым расстоянием $d = 7$, радиусом покрытия $\rho = 5$ и параметрами упаковки $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = \frac{15}{2n}, \alpha_4 = \alpha_5 = \frac{30}{n(n-3)}$ (см. [79] и [6]).

Следствие 10. Число различных двоичных кодов Геталса длины n с кодовым расстоянием 7 не превосходит величины $2^{2^{n-\frac{7}{2}\log n + o(\log n)}}$.

5) Двоичные примитивные коды типа БЧХ длины $n = 2^m - 1$ ($m \geq 5$ нечетно) мощности $2^{n-3\log(n+1)}$ с кодовым расстоянием $d = 7$, радиусом покрытия $\rho = 5$ и параметрами упаковки $\alpha_0 = \alpha_1 = 1, -\alpha_2 = -\alpha_3 = \alpha_4 = \alpha_5 = \frac{120}{(n-1)(n-7)}$ (см. [79]).

Заключение

В работе получены следующие результаты.

1. На множестве двоичных векторов длины m введены новые бинарные операции $\langle \mathbf{u}, \mathbf{v} \rangle_k$, являющиеся аналогами скалярного произведения. Исследованы их свойства. Определены новые понятия *k -нелинейности* и *k -преобразования Уолша—Адамара* булевой функции.

2. Введено новое обобщение понятия бент-функции — *k -бент-функция*, — отражающее возможность поэтапного усиления нелинейности булевой функции с ростом целого параметра k . Бент-функции и 1-бент-функции совпадают. Доказано, что класс k -бент-функций строго вложен в класс ℓ -бент-функций при $k > \ell$.

3. Предложены способы построения k -бент-функций и исследованы их свойства. Доказано существование k -бент-функций от m переменных любой степени нелинейности d , где $2 \leq d \leq \max\{2, \frac{m}{2} - k + 1\}$.

4. Классифицированы k -бент-функции от малого числа переменных.

5. Исследованы квадратичные аппроксимации вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, где \mathbf{v} — вектор переменных; перестановка π , целое k и вектор \mathbf{u} — параметры. Показано, что использование k -бент-функций в качестве функций шифрования максимально повышает стойкость блочного шифра к таким аппроксимациям.

6. Рассмотрены четырехразрядные подстановки, рекомендованные для S-блоков алгоритмов ГОСТ 28147-89, DES, s^3 DES; с помощью компьютера показано, что для всех этих подстановок (кроме одной) существуют более вероятные (по сравнению с линейными) квадратичные приближения функциями вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$.

7. Отмечена аналогия между проблемами нижних—верхних оценок числа бент-функций и двоичных кодов, таких как совершенные и равномерно

упакованные. Для числа равномерно упакованных двоичных кодов установлена новая (лучшая на данный момент) верхняя оценка.

Благодарности

*Their eyes were bent on this work...*¹

Я искренне признательна своему научному руководителю Юрию Леонидовичу Васильеву (Институт математики им. С. Л. Соболева) за неизменную поддержку и постоянное внимание к данной работе.

Моя самая глубокая благодарность Александру Александровичу Нечаеву (Московский государственный университет) и Леониду Александровичу Бассальго (Институт проблем передачи информации им. А. А. Харкевича, Москва), проявившим неподдельный интерес к моей работе и высказавшим немало ценных замечаний и критики.

Я очень благодарна сотрудникам института математики им. С. Л. Соболева: Денису Станиславовичу Кротову — за ценные замечания, позволившие существенно расширить множество кодов, для которых справедлива Теорема 1, и Владимиру Николаевичу Потапову, взявшему на себя труд прочесть рукопись и указавшему на целый ряд неточностей.

Мне очень приятно выразить признательность профессору Патрику Солé (Национальный Центр Научных Исследований — CNRS, — София Антиполис, Франция) за гостеприимство и увлекательную совместную работу в области бент-функций, благодаря которой удалось узнать много нового.

С большим удовольствием я благодарю Лилию Будагян (Университет Бергена, Норвегия) за консультации по векторным бент-функциям, внимательное прочтение текста и замечания, которые трудно переоценить.

Отдельную благодарность я приношу всем рецензентам печатных работ, обратившим мое внимание на многие существенные вопросы.

¹Игра слов: «Их взор был обращен к этой работе...» (англ.)

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] *Амбросимов А. С.* Свойства бент-функций q -значной логики над конечными полями // Дискретная математика. 1994. Т. 6, N 3. С. 50–60.
- [3] *Бассалыго Л. А., Зиновьев В. А., Зайцев Г. В.* О равномерно упакованных кодах // Проблемы передачи информации. 1974. Т. 10, Вып. 1. С. 9–14.
- [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] *Зиновьев В. А., Хеллесет Т.* О весовых спектрах сдвигов кодов типа Геталса // Проблемы передачи информации. 2004. Т. 40, Вып. 2. С. 19–36.
- [7] *Иванов А. В.* Использование приведенного представления булевых функций при построении их нелинейных аппроксимаций // Вестник Томского государственного университета. Приложение. 2007. N 23. С. 31–35.
- [8] *Иванов А. В.* Мономиальные приближения платовидных функций // Прикладная дискретная математика. 2008. Т. 1, N 1. С. 10–14.
- [9] *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>).

- [10] 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.
- [11] 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.
- [12] Лобанов М. С. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. Т. 18, N 3. С. 152–159.
- [13] Логачев О. А., Сальников А. А., Яценко В. В. Бент-функции на конечной абелевой группе // Дискретная математика. 1997. Т. 9, N 4. С. 3–20.
- [14] Логачев О. А., Сальников А. А., Яценко В. В. Криптографические свойства дискретных функций // Материалы конференции «Московский университет и развитие криптографии в России», МГУ, 2002. М.: МЦНМО, 2003. С. 174–199.
- [15] Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004.
- [16] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М: Связь, 1979.
- [17] Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002.
- [18] Молдовян А. А., Молдовян Н. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004.
- [19] Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. 1989. Т. 1, N 4. С. 123–139.
- [20] Нечаев А. А., Хонольд Т. Полновесные модули и представления кодов // Проблемы передачи информ. 1999. Т. 35, Вып. 3. С. 18–39.

- [21] *Ростовцев А., Маховенко Е.* Введение в теорию итерированных шифров // СПб.: НПО «Мир и Семья», 2003.
- [22] *Рязанов Б. В., Чечета С. И.* О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. 1995. Т. 7, N 3. С. 129–145.
- [23] *Семаков Н. В., Зиновьев В. А., Зайцев Г. В.* Равномерно упакованные коды // Проблемы передачи информации. 1971. Т. 7, Вып. 1. С. 38–50.
- [24] *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Т. 24. С. 15–42.
- [25] *Сидельников В. М.* Об экстремальных многочленах, используемых при оценках мощности кода // Проблемы передачи информ. 1980. Т. 14, Вып. 3. С. 17–30.
- [26] *Токарева Н. Н.* Представление \mathbb{Z}_4 -линейных кодов Препараты с помощью векторных полей // Проблемы передачи информации. 2005. Т. 41, Вып. 2. С. 50–62.
- [27] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си // М.: Триумф, 2002.
- [28] *Adams C.* On immunity against Biham and Shamir's «differential cryptanalysis» // Information Processing Letters. 1992. V. 41. P. 77–80.
- [29] *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.
- [30] *Avustinovich S. V., Heden O., Solov'eva F. I.* The classification of some perfect codes // Designs, Codes and Cryptography. 2004. V. 31, N 3. P. 313–318.
- [31] *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).

- [32] *Bending T. D., Fon-Der-Flaass D. G.* Crooked Functions, Bent Functions and Distance Regular Graphs // Electronic Journal of Combinatorics. 1998. N 5 (R34).
- [33] *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.
- [34] *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).
- [35] *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).
- [36] *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4, N 1. P. 3–72.
- [37] *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).
- [38] *Borges J., Fernandez C., Phelps K. T.* Quaternary Reed-Muller codes // IEEE Trans. Inform. Theory. 2005. V. 51, N 7. P. 2686–2691.
- [39] *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.

- [40] *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).
- [41] *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.
- [42] *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.
- [43] *Budaghyan L.* Private communication, 2008.
- [44] *Buttyan L., Vajda I.* Searching for the best linear approximation of DES-like cryptosystems // Electronics Letters. 1995. V. 31, N 11. P. 873–874.
- [45] *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.
- [46] *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.
- [47] *Canteaut A., Charpin P., Kuyreglyan G.* A new class of monomial bent functions // Finite Fields and Applications. 2008. V. 14, N 1. P. 221–241.
- [48] *Canteaut A., Daum M., Dobbertin H., Leander G.* Finding nonnormal bent functions // Discrete Appl. Math. 2006. V. 154, N 2. P. 202–218.
- [49] *Carlet C.* Generalized Partial Spreads // IEEE Trans. Inform. Theory. 1995. V. 41, N 5. P. 1482–1487.
- [50] *Carlet C.* \mathbb{Z}_{2^k} -linear codes // IEEE Trans. Inform. Theory. 1998. V. 44, N 4. P. 1543–1547.

- [51] *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.
- [52] *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.
- [53] *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.
- [54] *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.
- [55] *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.
- [56] *Carlet C., Ding C.* Highly nonlinear mappings // J. Complexity. 2004. V. 20, N 2–3. P. 205–244.
- [57] *Carlet C., Ding C.* Nonlinearities of S-boxes // Finite Fields and Applications. 2007. V. 13, N 1. P. 121–135.
- [58] *Carlet C., Ding C., Niederreiter H.* Authentication schemes from highly nonlinear functions // Designs, Codes and Cryptography. 2006. V. 40, N 1. P. 71–79.
- [59] *Carlet C., Gaborit P.* Hyper-bent functions and cyclic codes // J. Combin. Theory. Ser. A. 2006. V. 113, N 3. P. 466–482.
- [60] *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.

- [61] *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).
- [62] *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).
- [63] *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.
- [64] *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).
- [65] *Constantinescu I., Heise W., Honold T.* Monomial extensions of isometries between codes over \mathbb{Z}_m // Proc. of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory — ACCT 1996 (Sozopol, Bulgaria. June 1–7, 1996) P. 98–104.
- [66] *Daemen J., Govaerts R., Vandevale 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).
- [67] *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.
- [68] *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.

- [69] *Delsarte P.* An algebraic approach to the association schemes of coding theory // Ph. D. Thesis, Univ. Catholique de Louvain, 1973.
- [70] *Dillon J. F.* A survey of bent functions // The NSA Technical J. 1972. Special Issue. P. 191–215.
- [71] *Dillon J. F.* Elementary Hadamard Difference sets // Ph. D. Thesis, Univ. of Maryland, 1974.
- [72] *Dillon J. F., McGuire G.* Near bent functions on a hyperplane // Finite Fields and Applications. 2008. V. 14. P. 715–720.
- [73] *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).
- [74] *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.
- [75] *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.
- [76] *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).
- [77] *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/>.
- [78] *Fedorova M., Tarannikov Yu.* On the Constructing of Highly Nonlinear Resilient Boolean Functions by Means of Spectral Matrices // INDOCRYPT 2001. P. 254–266 (Lecture Notes in Comput. Sci. V. 2247).

- [79] *Goethals J. M., Van Tilborg H. C. A.* Uniformly packed codes // Philips Res. Repts. 1975. V. 30. P. 9–36.
- [80] *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.
- [81] *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).
- [82] *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).
- [83] *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.
- [84] *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).
- [85] *Kantor W. M.* Codes, Quadratic Forms and Finite Geometries // Proceedings of Symposia in Applied Math. 1995. V. 50. P. 153–177.
- [86] *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.
- [87] *Kerdock A. M.* A class of low-rate non-linear binary codes // Inform. Control. 1972. V. 20, N 2. P. 182–187.

- [88] *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.
- [89] *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).
- [90] *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).
- [91] *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.
- [92] *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.
- [93] *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.
- [94] *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.
- [95] *Langevin P., Leander G.* Monomial bent functions and Stickelberger’s theorem // Finite Fields and Applications. 2008. V. 14. P. 727–742.
- [96] *Langevin P., Leander G., McGuire G.* Kasami Bent Functions are Not Equivalent to Their Duals // submitted, 2007.
- [97] *Leander N. G.* Monomial bent functions // IEEE Trans. Inform. Theory. 2006. V. 52, N 2. P. 738–743.

- [98] *Leander N. G., Langevin P.* On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin // to appear. 2008.
- [99] *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.
- [100] *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.
- [101] *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).
- [102] *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).
- [103] *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).
- [104] *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.
- [105] *Meng Q., Yang M. C., Zhang H.* A novel algorithm enumerating bent functions // Available at <http://eprint.iacr.org>, 2004/274.
- [106] *Meng Q., Zhang H., Yang M. C., Cui J.* On the degree of homogeneous bent functions // Available at <http://eprint.iacr.org>, 2004/284.
- [107] *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.

- [108] *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).
- [109] *Nakahara J., Preneel B., Vandewalle J.* Experimental Non-Linear Cryptanalysis // COSIC Internal Report. Katholieke Universiteit Leuven. 2003. 17 p.
- [110] *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).
- [111] *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).
- [112] *Olsen J. D., Scholtz R. A., Welch L. R.* Bent-function sequences // IEEE Trans. Inform. Theory. 1982. V. 28, N 6. P. 858–864.
- [113] *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.
- [114] *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).
- [115] *Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandevall J.* Propagation 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).
- [116] *Preneel B.* Analysis and design of cryptographic hash functions // Ph. D. thesis, Katholieke Universiteit Leuven, 3001 Leuven, Belgium. 1993.

- [117] *Qu C., Seberry J., Pieprzyk J.* Homogeneous bent functions // Discrete Appl. Math. 2000. V. 102, N 1-2. P. 133–139.
- [118] *Riera C., Parker M.G.* Generalised Bent Criteria for Boolean Functions (I) // IEEE Trans. Inform. Theory 2006. V. 52, N 9. P. 4142–4159.
- [119] *Rifa J., Zinoviev V. A.* On completely regular codes from perfect codes // ACCT 2006 — Tenth Int. Workshop «Algebraic and Combinatorial Coding Theory» (Zvenigorod, Russia. September, 3–9, 2006). Proc. 2006. P. 225–229.
- [120] *Rodier F.* Asymptotic nonlinearity of Boolean functions // Designs, Codes and Cryptography. 2006. V. 40, N 1. P. 59–70.
- [121] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20, N 3. P. 300–305.
- [122] *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).
- [123] *Schmidt K-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // Available at <http://arxiv.org/abs/cs.IT/0611162>.
- [124] *Selçuk A. A.* On Probability of Success in Linear and Differential Cryptanalysis // J. Cryptology. 2008. V. 21. N. 1. P. 131–147.
- [125] *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).
- [126] *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.

- [127] *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.
- [128] *Siegentaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. V. IT-30, N 5. P. 776–780.
- [129] *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).
- [130] *Solé P.* Private communication, 2008.
- [131] *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).
- [132] *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.
- [133] *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).
- [134] *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.
- [135] *Youssef A. and Gong G.* Hyper-bent functions // Advances in cryptology — EUROCRYPT’2001. Int. conference on the theory and application of cryptographic techniques (Innsbruck, Austria. May 6–10, 2001). Proc. Berlin: Springer, 2001. P. 406–419 (Lecture Notes in Comput. Sci. V. 2045).

- [136] *Youssef A. M.* Generalized hyper-bent functions over $GF(p)$ // Discrete Applied Math. 2007. V. 155, N 8. P. 1066–1070.
- [137] *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.
- [138] *Zhe-Xian Wan.* Quaternary codes. Singapore: World Scientific Publishing Co. Pte. Ltd, 1997.
- [139] *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).
- [140] *Zheng Y., Zhang X.-M.* On Plateaued Functions // IEEE Trans. Inform. Theory. 2001. V. 47, N 3. P. 1215–1223.

Публикации автора по теме диссертации
(доступны по адресу www.math.nsc.ru/~tokareva)

- [141] *Токарева Н. Н.* Иерархия классов бент-функций кратной нелинейности // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, Россия. 16–21 апреля, 2007) Часть III, 2007. С. 5–11.
- [142] *Токарева Н. Н.* О верхней оценке числа равномерно упакованных двоичных кодов // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, Россия. 16–21 апреля, 2007) Часть III, 2007. С. 11–16.
- [143] *Tokareva N. N.* An Upper Bound for the Number of Uniformly Packed Codes // IEEE International Symposium on Information Theory — ISIT'2007. (Nice, France. June 24–29, 2007). Proc. 2007. P. 346–350.
- [144] *Токарева Н. Н.* О верхней оценке числа равномерно упакованных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14, N 3. С. 90–97.

- [145] *Tokareva N. N.* On k -bent functions // Вестник Томского госуниверситета. Приложение. 2007. N 23. С. 74–76.
- [146] *Токарева Н. Н.* Бент-функции кратной нелинейности: k -бент-функции // Материалы российской конференции «Математика в современном мире» (Новосибирск, Россия. 17–21 сентября, 2007). С. 288–289.
- [147] *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.
- [148] *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.
- [149] *Токарева Н. Н.* k -Преобразование Уолша-Адамара в теории кодирования и криптографии // Материалы XV Международной конференции «Проблемы теоретической кибернетики» (Казань, Россия, 2–7 июня, 2008). С. 113–114.
- [150] *Tokareva N. N.* k -Bent Functions: from Coding Theory to Cryptology // Proc. First IEEE International Conference SIBIRCON — Computational Technologies in Electrical and Electronics Engineering (Novosibirsk, Russia, July 21–25, 2008). P. 36–40.
- [151] *Токарева Н. Н.* О квадратичных аппроксимациях в блочных шифрах // Пробл. передачи информ. 2008. Т. 44, Вып. 3. С. 105–127.
- [152] *Токарева Н. Н.* Описание k -бент-функций от четырех переменных // Дискр. анализ и исслед. операций. 2008. Т. 15, N 4. С. 74–83.
- [153] *Токарева Н. Н.* Квадратичные аппроксимации специального вида для четырехразрядных подстановок в S-блоках // Прикладная дискретная математика. 2008. Т. 1, N 1. С. 50–54.

Предметный указатель

- (m, n) -функция, 32
- I -бент₄-функция, 32
- I -бент-функция, 32
- $NL(S)$, 84
- $NQ(S)$, 84
- \mathbb{Z} -бент-функция, 30
- k -аффинная функция, 12, 48
- k -бент-функция, 9, 12, 51, 79
- k -нелинейность, 50
- k -преобразование Уолша—Адамара, 50
- $s^3\text{DES}$, 86
- AB function, 34
- APN function, 34
- CDMA standard, 8, 27
- crooked function, 35
- DES, 86
- Partial Spreads, 22
- $\text{PC}(k)$, 28
- S-блок, 17, 81
- ГОСТ 28147-89, 82
- Кротов Д.С., 11, 38
- аффинная функция, 4
- бент₄-функция, 32
- бент-код, 7
- бент-показатель, 23
- бент-последовательность, 8
- бент-функция, 6, 20, 31
 - q -значная, 26
 - векторная, 33
 - мономиальная, 23
 - на конечной абелевой группе, 29
 - ненормальная, 28
 - обобщенная булева, 27
 - однородная, 29
 - самодуальная, 35
 - степенная, 23
- булева функция, 4
- векторная функция, 32
- вес
 - Ли, 36
 - Хэмминга, 19
- весовой спектр кода, 93
- гипер-бент-функция, 30
- гипотеза Доббертина, 35
- дифференциально δ -равномерная функция, 34
- класс аппроксимирующих функций, 71
- код
 - \mathbb{Z}_4 -линейный, 11, 37
 - Адамара, 6
 - БЧХ, 35, 98

Геталса, 98
 Кердока, 7
 Препараты, 35, 98
 Рида—Маллера, 6, 7
 равномерно упакованный, 25, 91
 совершенный, 24, 97
 типа Адамара, 11
 конструкция
 Мэйорана—МакФарланда, 22
 степенная, 23
 частичных разветвлений, 22
 корреляционно-иммунная функция, 35
 коэффициенты Уолша—Адамара, 20
 криптоанализ
 дифференциальный, 8
 квадратичный, 70
 линейный, 8, 67
 нелинейный, 69
 критерий
 Ротхауса, 21
 распространения, 28
 максимально k -нелинейная функция, 12, 51
 максимально нелинейная функция, 5, 20
 матрица Адамара, 7, 21
 мономиальная функция, 30
 нега-бент-функция, 32
 нелинейность подстановки, 84
 нормальная функция, 28
 операция
 \bullet , 42
 $\langle \mathbf{u}, \mathbf{v} \rangle_k$, 44
 \star , 38
 ортогональное разветвление, 7
 отображение
 β , 36
 γ , 36
 φ_k , 38
 Грея, φ , 11, 37
 оценки числа бент-функций, 24
 оценки числа совершенных кодов, 24
 параметр неквадратичности, 84
 платовидная функция, 25
 полу-бент-функция, 27
 почти бент-функция, 34, 35
 почти совершенно нелинейная функция, 34
 преобразование Уолша—Адамара, 5, 20
 профиль нелинейности, 35
 равенство Парсеваля, 20, 50
 радиус покрытия кода, 91
 разностное множество, 7
 расстояние
 Ли, 36
 Хэмминга, 19
 сбалансированная функция, 28
 скрюченная функция, 35
 слабо нормальная функция, 28
 спектр плоский, 31
 степень нелинейности функции, 21, 49
 уравновешенная функция, 28
 устойчивая функция, 35

функция равномерно коррелирующая
с линейными функциями, 28

частично бент-функция, 26

ядро кода, 41