

УДК 519.7; 519.1

БЕНТ-ФУНКЦИИ С БОЛЕЕ СИЛЬНЫМИ СВОЙСТВАМИ НЕЛИНЕЙНОСТИ: k -БЕНТ-ФУНКЦИИ^{*)}

Н. Н. Токарева

Вводится понятие k -бент-функции — булевой функции от чётно-го числа переменных m , одинаково плохо аппроксимируемой всеми функциями вида $\langle \mathbf{u}, \mathbf{v} \rangle_j \oplus a$, где $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, $a \in \mathbb{Z}_2$, при всех целых j , $1 \leq j \leq k$, где $\langle \cdot, \cdot \rangle_j$ является аналогом скалярного произведения векторов и k меняется от 1 до $m/2$. Произведения $\langle \cdot, \cdot \rangle_k$, $1 \leq k \leq m/2$, определяются с помощью специальной серии двоичных кодов типа Адамара A_m^k длины 2^m , а именно векторы значений функций $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$, где $a \in \mathbb{Z}_2$, являются кодовыми словами кода A_m^k . Коды A_m^k строятся с помощью подкодов \mathbb{Z}_4 -линейных кодов типа Адамара длины 2^{m+1} , классификация которых была дана Д. С. Кротовым (2001). При этом код A_m^1 линейен и коды $A_m^1, \dots, A_m^{m/2}$ попарно неэквивалентны. На каждом коде A_m^k определяется своя групповая операция \bullet . Поэтому можно считать, что k -бент-функции — это функции максимально нелинейные при k различных смыслах линейности одновременно. Обычные бент-функции представляют собой класс 1-бент-функций. Для $1 \leq \ell < k$ класс k -бент-функций является собственным подклассом класса ℓ -бент-функций. В статье приводятся способы построения k -бент-функций и рассматриваются их свойства. Показано, 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 определено подмножество \mathfrak{F}_m^k множества булевых функций \mathfrak{F}_m , на котором понятия k -бент-функции и 1-бент-функции совпадают.

Введение

Одной из важных характеристик булевой функции в криптографии является мера её нелинейности. Линейность и близкие к ней свойства булевой функции, как правило, представляют собой богатый источник

^{*)}Исследование выполнено при финансовой поддержке интеграционного проекта СО РАН № 35 «Древовидный каталог математических Интернет-ресурсов» и Российского фонда фундаментальных исследований (проект 07-01-00248).

информации о многих других её свойствах, что в криптографии, безусловно, является нежелательным. С целью максимизации меры нелинейности булевой функции в криптографии выделяют класс *максимально нелинейных* (или *бент-*) функций — функций, удалённых от множества всех аффинных функций на наибольшее возможное расстояние. Отметим, что понятия максимально нелинейной функции и бент-функции совпадают только в случае чётного числа переменных. Бент-функции были введены О. Ротхаусом ещё в 60-х годах XX века, хотя работа [37] была опубликована лишь в 1976 году. Дж. Диллон [23] и Р. Л. МакФарланд [32] рассматривали бент-функции в связи с разностными множествами. В настоящее время известно большое число конструкций бент-функций (см. обзоры [6] и [24]). Тем не менее класс всех бент-функций от m переменных до сих пор не описан, для мощности этого класса не найдена асимптотика и не установлены приемлемые нижние и верхние оценки (некоторые продвижения в этом направлении смотри в [20]). Известны различные обобщения понятия бент-функции (см., например, [29], [1], [5], [36], [30]). Широко изучаются связанные с бент-функциями такие объекты как бент-последовательности (см., например, [33] и [34]). Большую роль бент-функции играют в теории кодирования: для построения кодов Кердока, кодов Препараты, кодов БЧХ; в связи с изучением подкодов кода Рида–Маллера второго порядка, циклических и оптимальных кодов (см., например, [7], а также [18], [21], [22], [38]). К числу последних работ, в которых изучаются свойства бент-функций, можно отнести работу [16].

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 $2^{m-1} - 2^{(m/2)-1}$ (при чётном m). Говоря неформально, каждая функция f из класса бент-функций крайне плохо аппроксимируется аффинными функциями. Именно это свойство булевых функций, использующихся, например, в блочных шифрах, способствует предельному повышению стойкости этих шифров к методам линейного [31] и дифференциального [13] криптоанализа (см. подробнее [8]).

В литературе рассматривались различные классы аппроксимирующих функций, отличные от класса аффинных функций. В [39] А. М. Йоссеф и Г. Гонг предложили приближать булевы функции *собственными мономиальными функциями* (термин был введён позднее в [4]) и булевы функции от m переменных рассматривали как функции из $GF(2^m)$ в

$GF(2)$, сопоставляя каждому вектору \mathbf{v} соответствующий элемент поля $GF(2^m)$. 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 $\mathbf{v} \in GF(2^m)$. Тогда 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 мономияльными 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 $\text{нод}(s, 2^m - 1) = 1$. Булевы функции, одинаково плохо приближающиеся всеми такими функциями, названы *гипер-бент-функциями*, и для каждого чётного m доказано их существование. К. Карле и П. Габори [19] и независимо А. С. Кузьмин, В. Т. Марков, А. А. Нечаев и А. Б. Шишков [4] показали, что степень нелинейности произвольной гипер-бент-функции от m переменных равна $m/2$. Подходы, связанные с аппроксимацией булевых функций различными нелинейными функциями, можно найти в [27] и [2].

Основная идея настоящей статьи 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 «скрытой линейности» — линейности в некотором другом смысле. Тогда при использовании таких бент-функций, например, в блочном шифре может обнаружиться его слабость к соответствующим модификациям вышеупомянутых методов криптоанализа. С целью избежать подобные ситуации мы рассмотрим бент-функции с более сильными свойствами нелинейности, а именно бент-функции от m переменных, максимально нелинейные при k различных смыслах линейности одновременно, где k меняется от 1 до $m/2$.

С 90-х годов в теории кодирования активно исследуются нелинейные коды, образы которых под действием подходящих (как правило, взаимно-однозначных и изометричных) отображений в другие метрические пространства линейны (см. [9], [25], [3], [28], [17], [15], [14]). 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 [28] было показано, что существуют в точности $\lfloor m/2 \rfloor$ попарно неэквивалентных \mathbb{Z}_4 -линейных кодов типа Адамара длины 2^{m+1} при $m \geq 3$. Опираясь на данную Д. С. Кротовым [28] классификацию всех таких кодов, рассмотрим серию некоторых «скрыто линейных» двоичных кодов типа Адамара A_m^k , $1 \leq k \leq \lfloor m/2 \rfloor$, длины 2^m . В этой серии каждый код A_m^k получается из линейного четверичного кода \mathcal{A}_m^k заменой в каждой координате элементов 0, 1 на 0 и

элементов 2, 3 на 1, где \mathcal{A}_m^k — подкод соответствующего линейного четверичного кода Адамара типа $4^k 2^{m-2k}$ (см. [28]), состоящий из всех кодовых векторов, имеющих в первой координате только 0 или 2. При этом код A_m^1 линейен и коды $A_m^1, \dots, A_m^{\lfloor m/2 \rfloor}$ попарно неэквивалентны. Каждый код A_m^k образует абелеву группу относительно операции \bullet , индуцированной операцией $+$ покоординатного сложения над \mathbb{Z}_4 , определённой на множестве векторов кода \mathcal{A}_m^k . В этом смысле код A_m^k является «скрыто линейным».

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*. Коды A_m^k выбраны таким образом, чтобы возникающие новые скалярные произведения $\langle \cdot, \cdot \rangle_k$ обладали многими свойствами обычного скалярного произведения, и на их основе оказались возможными конструктивные построения. Пусть $\mathbf{u} = (u_1, \dots, u_m)$, $\mathbf{v} = (v_1, \dots, v_m)$. Тогда явный вид произведения $\langle \mathbf{u}, \mathbf{v} \rangle_k$ следующий:

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

где $Y_i = (u_{2i-1} \oplus u_{2i})(v_{2i-1} \oplus v_{2i})$ при любом целом i , $1 \leq i \leq \lfloor m/2 \rfloor$. Таким образом, 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 скалярного произведения $\langle \cdot, \cdot \rangle_k$ определяются *k-преобразование Уолша — Адамара* $W_f^k(\cdot)$ и *k-нелинейность* N_f^k булевой функции f . Булеву функцию от чётного числа переменных m назовём *максимально k-нелинейной (k-бент)* функцией, $1 \leq k \leq m/2$, если вектор значений этой функции удалён на максимальное возможное расстояние $2^{m-1} - 2^{(m/2)-1}$ от каждого кода типа Адамара A_m^j , $j = 1, \dots, k$ (или, что эквивалентно, $W_f^j(\mathbf{v}) = \pm 2^{m/2}$ 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 \mathfrak{B}_m^1 . Для $k > \ell \geq 1$ класс *k-бент-функций* \mathfrak{B}_m^k является собственным подклассом класса ℓ -бент-функций \mathfrak{B}_m^ℓ . Для каждого k , $1 \leq k \leq m/2$, в статье приводятся способы построения *k-бент-функций* и рассматриваются некоторые их свойства. В частности показано, 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 определено подмноже-

ство \mathfrak{F}_m^k множества булевых функций \mathfrak{F}_m , на котором понятия k -бент-функции и 1-бент-функции совпадают.

Необходимые определения и обозначения даны в § 1. Далее в § 2 определяются двоичные коды A_m^k с параметрами кодов Адамара. В § 3 вводятся соответствующие кодам A_m^k скалярные произведения $\langle \cdot, \cdot \rangle_k$. Классы k -аффинных булевых функций $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ и представление таких функций с помощью алгебраических нормальных форм (многочленов Жегалкина) рассматриваются в § 4. Понятие k -бент-функции и способы построения таких функций приводятся соответственно в § 5 и § 6. Взаимосвязь k -бент-функций с обычными бент-функциями рассматривается в § 7.

§ 1. Необходимые определения и обозначения

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. $\langle \mathbf{u}, \mathbf{v} \rangle = \bigoplus_{j=1}^m u_j v_j$, 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} её значений длины 2^m . Далее векторы в отличие от функций будем выделять полужирным шрифтом. Число ненулевых координат двоичного вектора \mathbf{v} называется его *весом Хемминга* и обозначается через $wt_H(\mathbf{v})$. *Расстояние Хемминга* $d_H(\mathbf{u}, \mathbf{v})$ 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 Хемминга 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* (или *дискретным преобразованием Фурье*) функции f , а значения $W_f(\mathbf{v})$ — *коэффициентами Уолша–Адамара* этой функции. Имеет место равенство Парсеваля

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

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, [6]). Функция $f \in \mathfrak{F}_m$ называется *максимально нелинейной* (m любое), если параметр N_f принимает максимально возможное значение, и *бент-функцией* (m чётное), если все её коэффициенты Уолша–Адамара равны $\pm 2^{m/2}$. При чётном m эти определения совпадают. Класс бент-функций от m переменных обозначим через \mathfrak{B}_m .

Напомним несколько основных понятий теории кодирования. Пусть $\langle \mathbb{Z}_2^n, d_H \rangle$ обозначает метрическое пространство на множестве двоичных векторов длины n с метрикой Хемминга. Непустое множество $C \subseteq \mathbb{Z}_2^n$ мощности $|C| = M$ с минимальным расстоянием d между его различными элементами называется *двоичным* $(n, M, d)_2$ -*кодом* (или *двоичным кодом с параметрами* n, M и d), а его элементы — *кодowymi словами*. Числа n и d называются соответственно *длиной* и *кодowym расстоянием* кода. Код называется *линейным*, если он образует линейное подпространство в \mathbb{Z}_2^n . *Весом* Li $wt_L(\cdot)$ четверичного вектора называется обычная сумма весов его компонент, где $wt_L(0) = 0, wt_L(1) = wt_L(3) = 1, wt_L(2) = 2$. *Расстоянием* 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. Символом $+$ будем обозначать операцию сложения по модулю 4. Параметры четверичного кода обозначим через $(n, M, d)_4$. Через $\mathbf{0}, \mathbf{1}, \mathbf{2}$ и $\mathbf{3}$ обозначим векторы со всеми компонентами, равными 0, 1, 2 и 3 соответственно. Пусть $\beta, \gamma : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$ — 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 $c \in \mathbb{Z}_4$. Отображения β, γ и φ покомпонентно продолжаются до отображений $\beta, \gamma : \mathbb{Z}_4^i \rightarrow \mathbb{Z}_2^i$ и $\varphi : \mathbb{Z}_4^i \rightarrow \mathbb{Z}_2^{2i}$ при любом целом i . Напомним,

что согласно [25] φ 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. Коды A_m^k с параметрами кодов Адамара

В этом параграфе будут определены двоичные коды A_m^k типа Адамара с заданной на них групповой операцией.

Пусть $m \in \mathbb{N}$, k — фиксированное целое такое, что $0 \leq k \leq m/2$. Всюду далее пусть $n = 2^m$. 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,

$$\begin{aligned} \mathbf{G}_1^0 = (02), \mathbf{G}_2^0 = \begin{pmatrix} 0022 \\ 0202 \end{pmatrix}, \mathbf{G}_2^1 = (0123), \mathbf{G}_3^0 = \begin{pmatrix} 00002222 \\ 00220022 \\ 02020202 \end{pmatrix}, \\ \mathbf{G}_3^1 = \begin{pmatrix} 00112233 \\ 02020202 \end{pmatrix}, \mathbf{G}_4^2 = \begin{pmatrix} 0000111122223333 \\ 0123012301230123 \end{pmatrix}. \end{aligned}$$

Матрицы такого вида впервые рассматривались Д. С. Кротовым в [3] и [28] при построении \mathbb{Z}_4 -линейных кодов типа Адамара длины $2n$ и получении 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 было сделано в [15], определим бинарную операцию $\star : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ следующим образом:

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

где $+$ 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

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

Нетрудно заметить, что для любых векторов $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ справедливо равенство $\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u} \star \mathbf{v}}$. 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 все возможные векторы $\mathbf{h}^{\mathbf{u}}$, расположенные в порядке лексикографического возрастания векторов $\varphi_k^{-1}(\mathbf{u})$. Будем считать, что нумерация столбцов матрицы \mathbf{C}_m^k также производится в порядке лексикографического возрастания векторов $\varphi_k^{-1}(\mathbf{v})$. Например,

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

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

Пусть J_s — квадратная матрица порядка s , 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} , при любом $a \in \mathbb{Z}_2$ получаем

$$\mathbf{h}^{(\mathbf{u}, a)} = (\varphi_k^{-1}(\mathbf{u}), a) \cdot \mathbf{G}_{m+1}^k = (h_1, h_1 + 2a, \dots, h_n, h_n + 2a).$$

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 $\delta = \varphi^{-1}(a, b)$, где $a, b \in \mathbb{Z}_2$. 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 пунктов (i), (ii) и равенства $(A \otimes B)^T = A^T \otimes B^T$. Утверждение 1 доказано.

Пусть четверичный код \mathcal{A}_m^k состоит из всевозможных векторов $\mathbf{h}^{\mathbf{u}}$ и $\mathbf{h}^{\mathbf{u}} + \mathbf{2}$ (см. (1)).

Утверждение 2 [28]. Четверичный код \mathcal{A}_m^k линеен 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 [28] 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 [28]. 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. Равенство $\text{Ker}(A_m^k) = \beta(\varphi^{-1}(\text{Ker}(H_m^k)))$ справедливо при любом целом k , $0 \leq k \leq m/2$.

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, $\beta(\mathbf{x}) \oplus A_m^k = A_m^k$. Поэтому $\text{Ker}(A_m^k) \supseteq \beta(\varphi^{-1}(\text{Ker}(H_m^k)))$.

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 ядру $\text{Ker}(A_m^k)$. 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, что $\varphi(\mathbf{x}) \in \text{Ker}(H_m^k)$ (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 называются *эквивалентными*, 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 $\tau(C') = \{ \tau(\mathbf{y}) \mid \mathbf{y} \in C' \}$. Из утверждений 3 и 4 следует, что коды $A_m^1, \dots, A_m^{\lfloor m/2 \rfloor}$ попарно неэквивалентны. Отметим, что на множестве A_m^k отображение β обратимо, что, вообще говоря, неверно для \mathbb{Z}_2^n . 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

$$\mathbf{x} \bullet \mathbf{y} = \beta(\beta^{-1}(\mathbf{x}) + \beta^{-1}(\mathbf{y})) \text{ для любых векторов } \mathbf{x}, \mathbf{y} \in A_m^k. \quad (2)$$

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 $\beta^{-1}(\mathbf{x}^{-1}) = -\beta^{-1}(\mathbf{x})$.

Приведём 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 $\mathbf{x}' = \beta^{-1}(\mathbf{x})$ — 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 её столбца \mathbf{z}_1^T найдётся 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) 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 \mathcal{A}_m^k . Опираясь на упомянутое в пункте (i) свойство матрицы \mathbf{G}_m^k (для любого её столбца \mathbf{z}_1^T найдётся 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). Утверждение 5 доказано.

Согласно утверждениям 2 и 5 код \mathcal{A}_m^k имеет кодовое расстояние $n/2$. Таким образом, из утверждений 2–5 следует

Теорема 1. При любом $m \in \mathbb{N}$ и любом целом k , $0 \leq k \leq m/2$, двоичный код \mathcal{A}_m^k с заданной на нём групповой операцией \bullet является $(n, 2n, n/2)_2$ -кодом типа Адамара. Коды \mathcal{A}_m^0 , \mathcal{A}_m^1 линейны, при $k \geq 2$ справедливо равенство $|\text{Ker}(\mathcal{A}_m^k)| = 2^{m-k+1}$.

Так как мощности ядер кодов $\mathcal{A}_m^1, \dots, \mathcal{A}_m^{\lfloor m/2 \rfloor}$ попарно различны, то коды $\mathcal{A}_m^1, \dots, \mathcal{A}_m^{\lfloor m/2 \rfloor}$ попарно неэквивалентны.

§ 3. Аналог скалярного произведения $\langle \mathbf{u}, \mathbf{v} \rangle_k$

Итак, пусть $\mathbf{C}_m^k = (c_{\mathbf{u}, \mathbf{v}}^k)$ — выше определённая четверичная квадратная матрица порядка n , где векторы \mathbf{u}, \mathbf{v} пробегает 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:

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

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 для обычного скалярного произведения оба 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 $h^{\mathbf{u}}$ и $h^{\pi_k(\mathbf{u})}$ матрицы \mathbf{C}_m^k , соответствующих векторам \mathbf{u} и $\pi_k(\mathbf{u})$, равна нулевому вектору.

Некоторые 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) $\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{k+1} = \langle (a, a'), (b, b') \rangle_\varepsilon \oplus \langle \mathbf{u}, \mathbf{v} \rangle_k$ при любых $a, a', b, b' \in \mathbb{Z}_2$, где $\varepsilon = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{v} \rangle_k \oplus 1 \in \mathbb{Z}_2$;
- (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 1 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 пункту (i) утверждения 1 справедливо равенство $c_{(\mathbf{u}, a), (\mathbf{v}, b)}^k = c_{\mathbf{u}, \mathbf{v}}^k + 2ab$, из которого следует (iv).

(v) следует из определения, согласно которому

$\langle \cdot, \cdot \rangle_0$	00	01	10	11	$\langle \cdot, \cdot \rangle_1$	00	01	10	11
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 пункта (ii) утверждения 1 следует, что

$$c_{(a,a',\mathbf{u}), (b,b',\mathbf{v})}^{k+1} = \varphi^{-1}(a, a') \cdot \varphi^{-1}(b, b') + c_{\mathbf{u}, \mathbf{v}}^k.$$

Сперва непосредственной проверкой установим, что

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

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

Действительно, эти равенства несложно получить, используя пункт (v).

Далее нетрудно видеть, что для любых $p, q \in \mathbb{Z}_4$

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

Отсюда следует, что $\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{k+1} = \beta(c_{(a,a',\mathbf{u}), (b,b',\mathbf{v})}^{k+1}) = \beta(c_{\mathbf{u}, \mathbf{v}}^k) \oplus \langle (a, a'), (b, b') \rangle_\varepsilon$, где $\varepsilon = 1$, если $c_{\mathbf{u}, \mathbf{v}}^k \in \{0, 2\}$, и $\varepsilon = 0$ в противном случае. Заметим, что $c_{\mathbf{u}, \mathbf{v}}^k$ принадлежит множеству $\{0, 2\}$ 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 $\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u} \star \mathbf{v}}$, 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.

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

Утверждение 7. Пусть $m, k \in \mathbb{N}$, причём $1 \leq k \leq m/2$. Далее для любого $i \in \mathbb{N}$, $1 \leq i \leq m/2$, и любых векторов $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ 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 утверждение индукцией по k .

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

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

Заметим, что $Y_j^2 = Y_j$ при любом j , откуда получаем требуемое.

Пусть утверждение справедливо при некотором k , $1 \leq k \leq (m-2)/2$. Покажем, что оно справедливо и при $k+1$. По пункту (vi) утверждения 6 выполняется равенство

$$\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \langle (u_1, u_2), (v_1, v_2) \rangle_\varepsilon \oplus \langle (u_3, \dots, u_m), (v_3, \dots, v_m) \rangle_k, \quad (3)$$

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 согласно пункту (v) утверждения 6 первое слагаемое в правой части равенства (3) имеет вид

$$\begin{aligned} \langle (u_1, u_2), (v_1, v_2) \rangle_\varepsilon &= (\varepsilon \oplus 1)(u_1 v_1 \oplus u_2 v_2) \oplus \varepsilon(u_2 v_1 \oplus u_1 v_2) \\ &= \varepsilon Y_1 \oplus u_1 v_1 \oplus u_2 v_2. \end{aligned}$$

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,

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

Следовательно, $\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \left(\bigoplus_{i=1}^{k+1} \bigoplus_{j=i}^{k+1} Y_i Y_j \right) \oplus \langle \mathbf{u}, \mathbf{v} \rangle$. Утверждение 7 доказано.

Следствие 1. Справедливо равенство $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{v} \rangle_k = \bigoplus_{i=1}^k Y_i$ для любых векторов $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ и любого k , $1 \leq k \leq m/2$.

Следствие 2. Верно равенство $\langle \mathbf{u}, \mathbf{v} \rangle_{k+1} = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus Y_{k+1} \left(\bigoplus_{i=1}^{k+1} Y_i \right)$ для любых $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ и произвольного k , $1 \leq k \leq (m-2)/2$.

§ 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, причём $g(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ 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 назовём множеством k -аффинных функций и обозначим через \mathfrak{A}_m^k . Ясно, что $|\mathfrak{A}_m^k| = 2^{m+1}$. Из утверждения 7 следует

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

$$\begin{aligned} g(\mathbf{v}) &= \left(\bigoplus_{i=1}^k \bigoplus_{j=i}^k (u_{2i-1} \oplus u_{2i})(u_{2j-1} \oplus u_{2j})(v_{2i-1} \oplus v_{2i})(v_{2j-1} \oplus v_{2j}) \right) \\ &\quad \oplus \left(\bigoplus_{s=1}^m u_s v_s \right) \oplus a, \quad (4) \end{aligned}$$

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

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

$$\begin{aligned} &g(v_1, v_2, v_3, v_4) \\ &= (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1 v_3 \oplus v_1 v_4 \oplus v_2 v_3 \oplus v_2 v_4) \oplus u_2 v_1 \oplus u_1 v_2 \oplus u_4 v_3 \oplus u_3 v_4 \oplus a. \end{aligned}$$

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 a .

Напомним, что *степенью нелинейности* $\deg f$ булевой функции f называется число переменных в самом длинном слагаемом её алгебраической нормальной формы (или многочлена Жегалкина). Из теоремы 2 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 точно $2^{m-k+1}(k+1)$ аффинных функций и $2^{m-k+1}(2^k - k - 1)$ квадратичных функций.

ДОКАЗАТЕЛЬСТВО. Согласно теореме 2 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) при любом j , $1 \leq j \leq k$, справедливо равенство $u_{2j-1} = u_{2j}$;
- 2) найдётся 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 — $k2^{m-k}$. Отсюда следует, что число аффинных функций в классе \mathfrak{A}_m^k равно $2^{m-k+1}(k+1)$. Поэтому число квадратичных функций равно $2^{m+1} - 2^{m-k+1}(k+1)$. Утверждение 8 доказано.

Несложно доказать

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

§ 5. Понятие k -бент-функции

При любом $m \in \mathbb{N}$ и целом k , $0 \leq k \leq m/2$, целочисленную функцию W_f^k , заданную на множестве \mathbb{Z}_2^m равенством

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

назовём 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 её элемента c на $(-1)^c$ является матрицей Адамара (это следует из теоремы 1), для W_f^k имеет место аналог равенства Парсеваля (см., например, [6, гл. 6]). Для полноты изложения приведём доказательство этого факта.

Теорема 3 (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 соотношение

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

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

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

Теорема 3 доказана.

Расстояние между функцией $f \in \mathfrak{F}_m$ и множеством функций \mathfrak{A}_m^k назовём 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 , соответствующая 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.

Из теоремы 3 следует неравенство $\max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f^k(\mathbf{v})| \geq 2^{m/2}$. 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 введём следующие понятия.

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

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

Определение 2. Для любых $m, k \in \mathbb{N}$ таких, что $1 \leq k \leq m/2$ и m чётно, функцию $f \in \mathfrak{F}_m$ назовём *k -бент-функцией*, если все коэффициенты $W_f^j(\mathbf{v})$, $j = 1, \dots, k$, равны $\pm 2^{m/2}$.

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

§ 6. Построение k -бент-функций

Сначала рассмотрим малые значения параметра $m \in \mathbb{N}$.

Пусть $m = 2$. Класс \mathfrak{B}_2^1 состоит из всех функций $f \in \mathfrak{F}_2$, векторы значений которых имеют нечётный вес. Ясно, что $|\mathfrak{B}_2^1| = 8$.

Случай $m = 4$. С помощью компьютера нами было проверено, что $|\mathfrak{B}_4^1| = 896$, $|\mathfrak{B}_4^2| = 384$. Приведём пример функции $\xi \in \mathfrak{F}_4$ такой, что $\xi \in \mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$:

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

Используя утверждения 6 и 7, 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

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

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

Приведём 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 утверждению 7 имеем $\langle \mathbf{u}, 0101 \rangle_1 = u_1 \oplus u_4$, $\langle \mathbf{u}, 0101 \rangle_2 = u_1 u_3 \oplus u_1 u_4 \oplus u_2 u_3 \oplus u_2 u_4 \oplus u_1 \oplus u_3$. Поэтому

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

$$\begin{aligned} W_\xi^2(0101) = & (1 + 1 - 1 + 1) + (1 - 1 - 1 - 1) + (-1 + 1 - 1 - 1) \\ & + (1 + 1 + 1 - 1) = 0. \end{aligned}$$

Таким образом, $\xi \in \mathfrak{B}_k^1 \setminus \mathfrak{B}_k^2$.

С помощью заданной k -бент-функции построим k -бент-функции и $(k+1)$ -бент-функции от большего числа переменных (см. утверждения 10 и 11).

Утверждение 10. Пусть $m, r \in \mathbb{N}$ и чётны, $k \in \mathbb{N}$ 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) утверждения 6, несложно убедиться в справедливости равенства

$$\langle (\mathbf{u}', \mathbf{u}''), (\mathbf{v}', \mathbf{v}'') \rangle_\ell = \langle \mathbf{u}', \mathbf{v}' \rangle_\ell \oplus \langle \mathbf{u}'', \mathbf{v}'' \rangle_\ell.$$

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}'_ℓ , \mathbf{v}'' такими, чтобы значения $|W_p^\ell(\mathbf{v}'_\ell)|$ и $|W_q(\mathbf{v}'')|$ были максимальны. Тогда из соответствующих равенств Парсеваля получаем $|W_p^\ell(\mathbf{v}'_\ell)| \geq 2^{m/2}$, $|W_q(\mathbf{v}'')| \geq 2^{r/2}$. С учётом того, что $|W_f^\ell(\mathbf{v}'_\ell, \mathbf{v}'')| = 2^{(m+r)/2}$, имеем $|W_q(\mathbf{v}'')| = 2^{r/2}$ и $|W_p^\ell(\mathbf{v}'_\ell)| = 2^{m/2}$ 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.

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 ниже).

Утверждение 11. Пусть $m \in \mathbb{N}$ чётно, $k \in \mathbb{N}$ такое, что $1 \leq k \leq m/2$, и пусть функция $f \in \mathfrak{F}_{m+2}^1$ 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

$$\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{\ell+1} = \langle \mathbf{u}, \mathbf{v} \rangle_\ell \oplus \langle (a, a'), (b, b') \rangle_\varepsilon.$$

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 при любых $b, b' \in \mathbb{Z}_2$ и любого ε имеет место равенство $W_s^\varepsilon(b, b') = W_s(b, b')$. Таким образом, при каждом 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.

Непосредственно из утверждений 10 и 11 вытекает

Теорема 4. Пусть числа $m, r \in \mathbb{N} \cup \{0\}$ и чётны, $j \in \mathbb{N} \cup \{0\}$ — любое, $k \in \mathbb{N}$ 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 чётном 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 четырёх 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 из \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 4 принадлежит классу $\mathfrak{B}_m^{m/2}$, и следовательно, каждому классу \mathfrak{B}_m^k . Следствие 4 доказано.

Радиусом покрытия двоичного кода называется максимальное расстояние, на которое может быть удалён 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 нечётном m) является открытой (см. некоторые результаты в этом направлении в [6], [26]). Заметим, что согласно следствию 4 радиус покрытия каждого кода A_m^k равен $2^{m-1} - 2^{(m/2)-1}$.

Следствие 5. При любом чётном $m \geq 4$ 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 произвольную функцию

$\psi \in \mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$ (такие функции существуют, см. приведённый выше пример). 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 4 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.

Пусть $m \geq 4$. Известно (см., например, [6]), 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 чётном 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 4 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, причём $\deg f = d$. 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.

Вопрос о существовании k -бент-функций со степенью нелинейности выше $\frac{m}{2} - k + 1$ остаётся открытым. Пользуясь следствием 6, можно убедиться в том, что известный класс \mathcal{HB}_m гипер-бент-функций [39] 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 $m/2$ [4], [19]).

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 4 получаем

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

Например, для $m = 8$ имеем:

$$|\mathfrak{B}_8^1| > 2^{70.4} \text{ (согласно [12])},$$

$$|\mathfrak{B}_8^2| \geq 2^{34} \text{ (как следует из [35], где установлено, что } |\mathfrak{B}_6^1| = 2^{32}),$$

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

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

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.

§ 7. Взаимосвязь k -бент-функций с бент-функциями

Обозначим через $S_{m,k}$ подгруппу группы S_m подстановок на m координатах, порождённую k транспозициями: $(1, 2), (3, 4), \dots, (2k-1, 2k)$. Очевидно, что группы $S_{m,k}$ и \mathbb{Z}_2^k изоморфны. Для произвольного вектора $\mathbf{w} \in \mathbb{Z}_2^k$ определим подстановку $\sigma_k^{\mathbf{w}}$ на m координатах равенством

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

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 число 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 — критерий для проверки принадлежности некоторых известных бент-функций классам k -бент-функций для различных k .

Теорема 5. При любом чётном $m \geq 2$ и любом $k \in \mathbb{N}$, $1 \leq k \leq m/2$, 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 найдём 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 учётом 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

$$W_f^\ell(\mathbf{v}) = \sum_{\mathbf{u}' \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}', \mathbf{v} \rangle \oplus f(\mathbf{u}')}, \text{ где } \mathbf{u}' = \sigma_\ell^{\mathbf{w}}(\mathbf{u}).$$

Следовательно, $W_f^\ell(\mathbf{v}) = W_f(\mathbf{v})$ для каждого $\ell = 1, \dots, k$. Теорема 5 доказана.

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?

Результаты статьи частично были анонсированы в [10] и [11].

ЛИТЕРАТУРА

1. Амбросимов А. С. Свойства бент-функций q -значной логики над конечными полями // Дискретная математика. 1994. Т. 6, вып. 3. С. 50–60.
2. Иванов А. В. Использование приведённого представления булевых функций при построении их нелинейных аппроксимаций // Вестник ТГУ. Приложение. 2007. № 23. С. 31–35.
3. Кротов Д. С. \mathbb{Z}_4 -линейные совершенные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 4. С. 78–90.
4. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б. Приближение булевых функций мономияльными // Дискретная математика. 2006. Т. 18, вып. 1. С. 9–29.
5. Логачёв О. А., Сальников А. А., Яценко В. В. Бент-функции на конечной абелевой группе // Дискретная математика. 1997. Т. 9, вып. 4. С. 3–20.
6. Логачёв О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004.
7. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М: Связь, 1979.
8. Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002.
9. Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. 1989. Т. 1, вып. 4. С. 123–139.
10. Токарева Н. Н. Иерархия классов бент-функций кратной нелинейности // Материалы VI молодежной научной школы по дискретной математике и её приложениям (Москва, 16–21 апреля 2007 г.) Часть III. 2007. С. 5–11.
11. Tokareva N. N. On k -bent functions // Вестник ТГУ. Приложение. 2007. № 23. С. 74–76.
12. 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.
13. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4, N 1. P. 3–72.
14. Borges J., Fernandez C., Phelps K. T. Quaternary Reed-Muller codes // IEEE Trans. Inform. Theory. 2005. V. 51, N 7. P. 2686–2691.
15. 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.
16. Canteaut A., Daum M., Dobbertin H., Leander G. Finding nonnormal bent functions // Discrete Appl. Math. 2006. V. 154, N 2. P. 202–218.

17. **Carlet C.** \mathbb{Z}_{2^k} -linear codes // IEEE Trans. Inform. Theory. 1998. V. 44, N 4. P. 1543–1547.
18. **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.
19. **Carlet C., Gaborit P.** Hyper-bent functions and cyclic codes // J. Combin. Theory. Ser. A. 2006. V. 113, N 3. P. 466–482.
20. **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.
21. **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.
22. **van Dam E. R., Fon-Der-Flaass D. G.** Codes, graphs, and schemes from nonlinear functions // European J. of Combinatorics, 2003. V. 24, N 1. P. 85–98.
23. **Dillon J. F.** A survey of bent functions // The NSA Technical J. 1972. Special Issue. P. 191–215.
24. **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).
25. **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.
26. **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.
27. **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. Berlin: Springer-Verlag, 1996. P. 224–236. (Lecture Notes in Comput. Sci.; V. 1070).
28. **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.
29. **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.

30. **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.
31. **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).
32. **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.
33. **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).
34. **Olsen J. D., Scholtz R. A., Welch L. R.** Bent-function sequences // IEEE Trans. Inform. Theory. 1982. V. 28, N 6. P. 858–864.
35. **Preneel B.** Analysis and design of cryptographic hash functions // Ph. D. thesis, Katholieke Universiteit Leuven, 3001 Leuven, Belgium. 1993.
36. **Qu C., Seberry J., Pieprzyk J.** Homogeneous bent functions // Discrete Appl. Math. 2000. V. 102, N 1–2. P. 133–139.
37. **Rothaus O.** On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20, N 3. P. 300–305.
38. **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.
39. **Youssef A., 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).

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
Новосибирский гос. университет,
ул. Пирогова, 2,
630090 Новосибирск,
Россия.
E-mail: tokareva@math.nsc.ru

Статья поступила
11 мая 2007 г.