

УДК 519.7

ОБОБЩЕНИЯ БЕНТ-ФУНКЦИЙ. ОБЗОР РАБОТ *)

Н. Н. Токарева

Аннотация. Бент-функции (булевы функции, обладающие экстремальными нелинейными свойствами) интенсивно изучаются в силу своих многочисленных приложений в криптографии, теории кодирования и других областях. Новые постановки задач приводят к большому числу обобщений бент-функций, многие из которых остаются мало известными специалистам в области булевых функций. Их систематический обзор предлагается в настоящей статье.

Ключевые слова: булева функция, преобразование Уолша — Адамара, нелинейность, бент-функция, CDMA.

Введение

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

В настоящей статье предлагается систематический обзор существующих обобщений бент-функций и сделана попытка установить (где это возможно) взаимосвязи между различными обобщениями. Статья может рассматриваться как продолжение обзора [17]. Предполагается, что читатель знаком с основными результатами в области бент-функций.

Обобщения бент-функций разделены на несколько групп. Сразу отметим, что разделение довольно условное, но оно показалось удобным для изложения материала. При описании каждого обобщения внимание, по возможности, обращается на то, когда, кем и почему было введено

*) Исследование выполнено при финансовой поддержке гранта Президента РФ для молодых российских ученых (грант МК-1250.2009.1), Российского фонда фундаментальных исследований (проекты 08-01-00671, 09-01-00528) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт 02.740.11.0429).

обобщение; какой вид имеют функции и преобразование Уолша — Адамара (или Фурье), как правило возникающее в каждом случае; какие известны результаты о данном обобщении; как рассматриваемое обобщение связано с другими и т. д. По каждому обобщению приводятся соответствующие ссылки.

Приведём структуру статьи по разделам.

Разд. 1. Алгебраические обобщения бент-функций (q -значные бент-функции; бент-функции над конечным полем; обобщённые булевы бент-функции; бент-функции из конечной абелевой группы в множество комплексных чисел единичной окружности; бент-функции из конечной абелевой группы в другую конечную абелеву группу; векторные G -бент-функции; многомерные бент-функции на конечной абелевой группе).

Разд. 2. Комбинаторные обобщения бент-функций (частично определённые бент-функции; платовидные функции; \mathbb{Z} -бент-функции; однородные бент-функции).

Разд. 3. Криптографические обобщения бент-функций (уравновешенные бент-функции; частично бент-функции; гипербент-функции; почти бент-функции; бент-функции порядка r ; k -бент-функции).

Разд. 4. Квантовые обобщения бент-функций (нега-бент-функции; бент₄-функции; I-бент-функции).

Приведём список обозначений и определений:

q, n — натуральные числа;

$+$ — сложение по модулю q ;

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

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

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

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

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

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

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

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

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

1. Алгебраические обобщения бент-функций

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

1.1. q -Значные бент-функции. Это естественное обобщение бент-функций предложили в 1985 г. Кумар, Шольц и Велч [37] с целью построения q -значных бент-последовательностей, применимых в системах CDMA (см. подробнее дальше).

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 $f : \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q$.

Преобразованием Уолша — Адамара функции f называется комплексная функция

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

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

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

При $q = 2$ это понятие совпадает с понятием булевой бент-функции. Множество всех q -значных бент-функций от n переменных обозначим через $\mathfrak{B}_{n,q}$. В [37] получены следующие результаты.

Теорема 1. Класс $\mathfrak{B}_{n,q}$ замкнут относительно

- (i) любого невырожденного аффинного преобразования переменных;
- (ii) прибавления любой q -значной аффинной функции.

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

Теорема 2. Следующие утверждения эквивалентны:

- (i) q -значная функция f является бент-функцией;
- (ii) матрица $A = (a_{x,y})$, где $a_{x,y} = \omega^{f(x+y)}$, является обобщённой матрицей Адамара.

Отметим, что при $q = 2$ теоремы 1 и 2 представляют собой хорошо известные факты о булевых бент-функциях (см., например, [17]). К особенностям q -значного случая относится тот факт [37], что функция f остаётся бент-функцией при замене ω в определении $W_f(y)$ на любой другой примитивный корень γ степени q из единицы. Отметим также, что q -значные бент-функции существуют как для чётных, так и для нечётных n .

Теорема 3. Пусть m, n, q — любые натуральные числа. Для произвольных функций $g \in \mathfrak{B}_{m,q}$, $h \in \mathfrak{B}_{n,q}$ функция $f(x', x'') = g(x') + h(x'')$ является q -значной бент-функцией.

Имеет место аналог теоремы Мэйорана — МакФарланда [40].

Теорема 4. Пусть n чётно, q — любое число. Тогда

$$f(x', x'') = \langle x', h(x'') \rangle + g(x'')$$

является q -значной бент-функцией, где g — произвольная q -значная функция от $n/2$ переменных, h — любая перестановка на множестве $\mathbb{Z}_q^{n/2}$.

Пусть n нечётно, $q = 2 \bmod 4$, $q > 2$. В [37] показано, что если существует целое число b такое, что $2^b + 1$ делится на $q/2$, то q -значных бент-функций от n переменных не существует.

Для каждого q такого, что $q \not\equiv 2 \bmod 4$, и любого n бент-функции существуют. Они могут быть построены, например, с помощью теоремы 3 из следующих одномерных ($n = 1$) функций.

Теорема 5. Следующие q -значные функции от одной переменной являются бент-функциями:

- (i) $f(x) = x^2 + cx$, где $c \in \mathbb{Z}_q$ — любая константа (если q нечётно);
- (ii) $f(x) = rx'h(x'') + g(x'')$, где $x = rx' + x'' \in \mathbb{Z}_q$, $0 \leq x', x'' \leq r - 1$, h — любая перестановка на \mathbb{Z}_r , g — любая функция вида $\mathbb{Z}_r \rightarrow \mathbb{Z}_q$ (если $q = r^2$ для некоторого r).

См. подробнее [37]. Конструкции q -значных бент-функций, полученные с помощью цепных колец, предложены Хоу [35].

Наиболее полно свойства булевых бент-функций сохраняются для *регулярных q -значных бент-функций*. Бент-функция $f : \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q$ называется *регулярной*, если любой её коэффициент Уолша — Адамара представляется в виде

$$W_f(y) = q^{n/2} \omega^{g(y)}$$

для некоторой q -значной функции g . Можно доказать [37], что g также является регулярной бент-функцией, её называют *дуальной* к функции f .

Приведём несколько примеров.

При $n = 1$, $q = 4$ $f(x) = x^3 + 3x^2$ является регулярной бент-функцией. Её спектр Уолша — Адамара (набор коэффициентов в порядке возрастания аргумента) имеет вид

$$(2, 2i, 2, -2i) = (2\omega^0, 2\omega^1, 2\omega^0, 2\omega^3),$$

где $\omega = e^{\pi i/2}$; дуальная функция $g(x)$ равна x^3 .

При $n = 1$, $q = 3$ бент-функция $f(x) = x^2$ не является регулярной, её спектр равен

$$\left(\sqrt{3}i, \frac{3}{2} - \frac{\sqrt{3}}{2}i, \frac{3}{2} - \frac{\sqrt{3}}{2}i \right)$$

или, представляя через степени примитивного корня,

$$(\sqrt{3}\omega^{3/4}, \sqrt{3}\omega^{11/4}, \sqrt{3}\omega^{11/4}),$$

где $\omega = e^{2\pi i/3}$. При этом все показатели степеней ω не целые.

Нетрудно заметить, что булева бент-функция ($q = 2$) всегда является регулярной. Бент-функции, построенные в теоремах 4, 5 (при $q = 1 \bmod 4$ в п. (i)) являются регулярными. При нечётном n и $q = 2, 3 \bmod 4$ регулярных бент-функций не существует [37]. С. В. Агиевичем [19] показано, что регулярные q -значные бент-функции могут быть описаны с помощью *бент-прямоугольников*; для двоичного случая такое описание приводилось в [17].

В [56] исследовались q -значные бент-функции при $q = 4$. Произвольную четверичную функцию f от n переменных можно представить в виде $f(x + 2y) = a(x, y) + 2b(x, y)$ для подходящих булевых функций a, b от $2n$ переменных, где $x, y \in \mathbb{Z}_2^n$.

Булевы функции c и d от $2n$ переменных назовём *бент-коррелирующими* (при заданном разбиении множества переменных на две равные части), если при любых $x, y \in \mathbb{Z}_2^n$ выполняются условия:

- (i) $W_c^2(x, y) + W_c^2(x + y, y) + W_d^2(x, y) + W_d^2(x + y, y) = 4^{n+1}$;
- (ii) $W_c(x, y) = W_d(x + y, y) = \pm 2^n \iff W_c(x + y, y) = W_d(x, y) = \pm 2^n$.

Если c и d — бент-функции, то условие (i) всегда выполняется. Условие (ii) задаёт некую согласованность знаков у коэффициентов Уолша — Адамара этих функций. Отметим, что бент-коррелирующие функции одновременно либо являются, либо не являются бент-функциями. В [56] доказана

Теорема 6. Функция $f : \mathbb{Z}_4^n \rightarrow \mathbb{Z}_4$ — бент-функция в смысле определения 1 тогда и только тогда, когда функции b , $a + b$ являются бент-коррелирующими.

Далее о q -значных бент-функциях см. [34, 36], о бент-последовательностях — [44].

1.2. Бент-функции над конечным полем. А. С. Амбросимов [2] в 1994 г. предложил другое — вероятностное — определение q -значных бент-функций. В отличие от предыдущего случая здесь рассматриваются только q -значные функции над конечным полем \mathbb{F}_{q^n} .

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

Пусть $f : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$ — q -значная функция. Предположим, что вектор $x \in \mathbb{F}_{q^n}$ выбирается случайно и равновероятно. Для случайной величины $\xi = f(x)$ определяется характеристическая функция $\varphi_\xi(z) = \mathbf{E} \omega^{\langle \xi, z \rangle}$, $z \in \mathbb{F}_q$, где элементы ξ и z рассматриваются как векторы длины ℓ над полем \mathbb{F}_p , и скалярное произведение $\langle \xi, z \rangle$ берётся по модулю p . При фиксированном $z \in \mathbb{F}_q$ преобразование Уолша — Адамара функции f определяется как

$$W_{f,z}(y) = q^n \varphi_{\langle x,y \rangle + f(x)}(z),$$

или, что то же самое,

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

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

$$W_{f,z}(y) = \sum_{x \in \mathbb{F}_{q^n}} \omega^{\langle \langle x,y \rangle + f(x), z \rangle} \text{ для } y \in \mathbb{F}_{q^n}. \quad (2)$$

Отметим, что в (1) и (2) используются примитивные корни из единицы разных степеней — степени q и p соответственно. Параметр z в (2) задаёт проекцию элемента $\langle x, y \rangle + f(x)$ из поля \mathbb{F}_q в простое поле \mathbb{F}_p .

Можно предложить и эквивалентное определение

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

заменяв скалярное произведение функцией следа $\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$. При таком определении $W_{f,z}(y)$ и $W'_{f,z}(y)$ отличаются лишь с точностью до перестановки на элементах z, y .

Согласно [2] для любой функции f и любого ненулевого z выполняется равенство Парсевала

$$\sum_{y \in \mathbb{F}_{q^n}} |W_{f,z}(y)|^2 = q^{2n},$$

из которого следует, что

$$\max_{y \in \mathbb{F}_{q^n}} |W_{f,z}(y)| \geq q^{n/2}.$$

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

$$|W_{f,z}(y)| = q^{n/2}.$$

Сделаем следующие замечания.

- При $q = p$, $\ell = 1$ определение 2 q -значной бент-функции совпадает с определением 1 Кумара, Шольца и Велча.
- В определении 2 коэффициенты Уолша — Адамара должны быть одинаковыми по модулю при любой ненулевой проекции показателя степени примитивного элемента в (2) из поля \mathbb{F}_q в поле \mathbb{F}_p . Тогда как в определении 1 они одинаковы по модулю без рассмотрения проекций (кроме того, \mathbb{Z}_q может не быть полем).

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

Для бент-функций над полем справедлив критерий Ротхауса [2].

Теорема 7. Функция $f : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$ является бент-функцией тогда и только тогда, когда при любом фиксированном $y \in \mathbb{F}_{q^n}$ функция $f(x+y) - f(x)$ имеет равномерное распределение на \mathbb{F}_q при равномерном распределении аргумента x на \mathbb{F}_{q^n} .

В [2] приводится описание всех квадратичных q -значных бент-функций от n переменных и подсчитывается их число, которое обозначим через $M_q(n)$.

Теорема 8. Пусть $q = p^\ell$. Справедливы утверждения

(i) если $p = 2$, $\ell \geq 2$, то

$$M_q(n) = \begin{cases} q^{\binom{n}{2} + 2n + 1} \prod_{j=1}^{n/2} (1 - q^{-2j+1}) & \text{при чётном } n, \\ 0 & \text{при нечётном } n; \end{cases}$$

(ii) если $p \neq 2$, то

$$M_q(n) = (q-1)q^n M_q(n-1) + q^{n+1}(q^{n-1} - 1)M_q(n-2)$$

при $n \geq 3$.

К сожалению, в [2] не прослеживается явно взаимосвязь между бент-функциями Амбросимова и бент-функциями Кумара, Шольца и Велча. При $q = p^\ell$ не ясно, например, является ли бент-функция в одном смысле бент-функцией в другом.

1.3. Обобщённые булевы бент-функции Шмидта. Другое обобщение бент-функций стал рассматривать в 2006 г. Шмидт [55] в связи с построением четверичных кодов постоянной амплитуды (quaternary constant-amplitude codes) для мультикодовых систем CDMA. Остановимся на этом подробнее.

Технология цифровой сотовой связи CDMA (Code Division Multiple Access — множественный доступ с кодовым разделением каналов) была стандартизована в 1993 г. американской телекоммуникационной промышленной ассоциацией (US TIA) в виде стандарта IS-95 (Mobile Station — Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System). В настоящее время технология активно используется большинством поставщиков беспроводного оборудования во всем мире согласно стандартам IMT-2000 мобильной связи третьего поколения (в России — стандарты IMT-МС 450 или CDMA-450). Отметим, что первая работа [1], посвящённая этой технологии, была опубликована в СССР ещё в 1935 г. Д. В. Агеевым. В системах CDMA применяются широкополосные сигналы, при этом вся полоса частот канала одновременно используется многими абонентами. Поскольку каждому абоненту присваивается свой уникальный код, он легко выделяется из общего «шума». В системах CDMA существенно повышается пропускная способность канала, кроме того, они являются весьма экономичными.

Связь между бент-функциями и кодами для CDMA установил Вада в 2000 г. [57], см. также работу Патерсона [47].

Рассмотрим простейшую модель передачи информации в мультикодовой системе CDMA. Пусть $N = 2^n$ — степень двойки, $A_N = (a_{jt})$ — матрица Адамара типа Сильвестра размера $N \times N$. Имеются N параллельных потоков данных. Передаваемую информацию можно представить двоичным вектором s длины N (по биту от каждого потока). Сигнал в MC-CDMA моделируется в виде

$$S_c(t) = \sum_{j=0}^{N-1} (-1)^{c_j} a_{jt},$$

где $t = 0, 1, \dots, N-1$ — дискретный параметр времени, т. е. j -я строка матрицы A домножается на $(-1)^{c_j}$, а передаваемый сигнал S_c является

суммой этих новых строк. В каждый момент времени передаётся один бит последовательности S_c . Важным параметром является *отношение пиковой и средней мощностей сигнала* (peak-to-average power ratio), которое определяется как

$$\text{PAPR}(c) = \frac{1}{N} \max_t |S_c(t)|^2.$$

Отметим, что $1 \leq \text{PAPR}(c) \leq N$. Величина $|S_c(t)|^2$ пропорциональна мощности, необходимой для передачи данного сигнала, поэтому наиболее подходящими для передачи являются такие векторы c , для которых $\text{PAPR}(c)$ минимальна. Можно считать, что векторы c выбираются из некоторого двоичного кода C длины N . Пусть $\text{PAPR}(C) = \max_{c \in C} \text{PAPR}(c)$. Если $\text{PAPR}(C) = 1$, то C называется *кодом постоянной амплитуды*. Задача построения таких кодов с большой мощностью и большим кодовым расстоянием весьма актуальна. Справедлива [47, 57]

Теорема 9. Код C длины 2^n является кодом постоянной амплитуды тогда и только тогда, когда каждое его кодовое слово — вектор значений некоторой бент-функции от n переменных.

Действительно, если c — вектор значений булевой функции f от n переменных, то

$$\text{PAPR}(c) = \frac{1}{2^n} \max_{x \in \mathbb{Z}_2^n} |W_f(x)|^2.$$

Таким образом, бент-функции играют существенную роль при построении кодов для CDMA систем.

Обобщение Шмидта [55] состоит в следующем. Пусть $q \geq 2$ — натуральное число, ω — примитивный комплексный корень степени q из единицы, $\omega = e^{2\pi i/q}$. Функция $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_q$ называется *обобщённой булевой функцией*. Её *преобразование Уолша — Адамара* называется комплексная функция

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

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

С помощью таких функций строятся коды постоянной амплитуды для q -значного варианта MC-CDMA, в котором двоичный вектор c дли-

ны N моделируется как

$$S_{c,q}(t) = \sum_{j=0}^{N-1} \omega^{c_j} a_{jt}.$$

Отметим также, что для некоторых задач в области циклических кодов определение Шмидта представляется более естественным, чем определение q -значной бент-функции Кумара, Шольца и Велча.

Шмидт [55] подробно разбирает случай $q = 4$, исследует взаимосвязи между обобщёнными бент-функциями, кодами постоянной амплитуды и известными \mathbb{Z}_4 -линейными кодами.

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

В [56] дан ответ на этот вопрос в одном частном случае. Пусть обобщённая булева функция $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_4$ ($q = 4$) представляется в виде $f(x) = a(x) + 2b(x)$, где a, b — булевы функции от n переменных. В [56] показано, что f — обобщённая бент-функция тогда и только тогда, когда функции b и $a + b$ являются обычными бент-функциями.

Отметим, что *действительнозначные бент-функции* (real-valued bent functions) вида $\mathbb{Z}_2^n \rightarrow \{0, 1/2, 1, 3/2\}$, рассмотренные в [41], совпадают с обобщёнными бент-функциями при $q = 4$.

1.4. Бент-функции из конечной абелевой группы в множество комплексных чисел единичной окружности. В 1997 г. О. А. Логачёв, А. А. Сальников и В. В. Яценко [10] ввели понятие бент-функции на произвольной конечной абелевой группе. В случае, если группа является элементарной абелевой 2-группой, это понятие совпадает с понятием булевой бент-функции.

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

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

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

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

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

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

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

Сделаем следующие замечания.

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

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

Функция $f : A \rightarrow S_1(\mathbb{C})$ называется *уравновешенной*, если

$$\sum_{x \in A} f(x) = 0.$$

Критерием Ротхауса для бент-функций на группе [10] является

Теорема 10. Функция f — бент-функция на группе A тогда и только тогда, когда функция $\overline{f(x)}f(x+y)$ уравновешена для каждого $y \in A$, $y \neq 0$.

В [10] можно найти и другие критерии.

Для бент-функции f на группе A так же, как в булевом случае, можно определить *дуальную* функцию $\widetilde{f} : A \rightarrow S_1(\mathbb{C})$. Она задаётся равенством

$$\widetilde{f}(x) = \frac{1}{\sqrt{n}} \widehat{f}(x)$$

и тоже является бент-функцией.

Если для некоторого разложения группы A в прямое произведение групп A_1 и A_2 функция $f : A \rightarrow S_1(\mathbb{C})$ может быть представлена в виде

$$f(x', x'') = f_1(x') f_2(x''),$$

где $f_1 : A_1 \rightarrow S_1(\mathbb{C})$, $f_2 : A_2 \rightarrow S_1(\mathbb{C})$, то функция f называется *разложимой*. Справедлива [10]

Теорема 11. Разложимая функция f является бент-функцией на группе A тогда и только тогда, когда f_1 и f_2 — бент-функции на группах A_1 и A_2 соответственно.

1.5. Бент-функции из конечной абелевой группы в другую конечную абелеву группу. В. И. Солодовников [13] в 2002 г. предложил наиболее общий подход к алгебраическому обобщению бент-функций. При изложении его результатов будем использовать как оригинальные обозначения, так и обозначения из [24], представляющиеся иногда более удобными. Отметим, что в 2004 г. Карле и Динг [24] повторили результаты В. И. Солодовникова, к сожалению, без ссылки на предшественника.

Пусть $(A, +)$ и $(B, +)$ — конечные абелевы группы порядков n и m соответственно, a и b — максимальные порядки элементов в этих группах. Пусть \hat{A} и \hat{B} — группы характеров групп A и B . Зафиксируем изоморфизмы $y \rightarrow \chi_y$ и $z \rightarrow \eta_z$ между A и \hat{A} , B и \hat{B} соответственно, где $\chi_y : A \rightarrow T_a$ и $\eta_z : B \rightarrow T_b$ — характеры. Пусть $f : A \rightarrow B$ — произвольная функция. Следующие определения из [13] приведём в несколько иной форме (введём нормировочные множители), не искажая при этом их смысл. *Преобразованием Фурье характера функции f* при фиксированном $z \in B$ называется функция

$$\hat{f}_z(y) = \sum_{x \in A} \eta_z(f(x)) \overline{\chi_y(x)}, \text{ где } y \in A. \quad (3)$$

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

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

Фиксируя элемент $z \in B$, от функции f можно перейти к комплекснозначной функции $\eta_z \circ f : A \rightarrow T_b$. Можно сказать, что (3) является разложением этой функции* по группе характеров \hat{A} . Функции вида $A \rightarrow S_1(\mathbb{C})$ уже рассматривались Логачёвым, Сальниковым и Яценко (см. определение 4). Имеет место [13, 24]

Теорема 12. Функция $f : A \rightarrow B$ является бент-функцией тогда и только тогда, когда при каждом $z \neq 0$ функция $\eta_z \circ f$ — бент-функция в смысле Логачёва, Сальникова и Яценко.

*Здесь и далее запись $g \circ f(x)$ означает функцию $g(f(x))$.

Производной функции f по направлению $y \in A$ называется функция

$$D_y f(x) = f(x + y) - f(x).$$

Справедлива [13, 24]

Теорема 13. Функция $f : A \rightarrow B$ является бент-функцией, если и только если функция $D_y f(x)$ уравновешена для каждого ненулевого $y \in A$, т. е. мощности всех её прообразов одинаковы.

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

В. И. Солодовниковым [13] определяется функция близости двух функций $f, g : A \rightarrow B$ как

$$\delta(f, g) = \left(\frac{1}{m} \sum_{y \in B} \left(\frac{|\{x : f(x) - g(x) = y\}|}{n} - \frac{1}{m} \right)^2 \right)^{1/2}. \quad (4)$$

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

Пусть $\text{Hom}(A, B)$ — множество всех гомоморфизмов группы A в группу B . По определению для каждого гомоморфизма h производная $D_y h(x)$ по любому ненулевому направлению $y \in A$ является постоянной функцией. Тогда функцию $f : A \rightarrow B$ такую, что для любого ненулевого $y \in A$ функция $D_y f(x)$ уравновешена, естественно называть [13] *абсолютно негомоморфной*. Согласно теореме 13 абсолютно негомоморфные функции и бент-функции совпадают.

Теорема 14. Для любой бент-функции f и произвольного гомоморфизма h выполняется

$$\delta(f, h) = \frac{\sqrt{m-1}}{m\sqrt{n}}.$$

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

значение $\delta_f = \delta(f, \text{Hom}(A, B))$ минимально. При $A = \mathbb{Z}_q^\ell$, $B = \mathbb{Z}_q^r$ показано [13], что функция f минимальна, если

$$\delta_f = \sqrt{m-1}/(m\sqrt{n}).$$

Функция называется *абсолютно минимальной*, если её свойство минимальности инвариантно относительно любых эпиморфизмов группы B .

Теорема 15. Пусть q простое, $A = \mathbb{Z}_q^\ell$, $B = \mathbb{Z}_q^r$ и бент-функции из A в B существуют. Тогда

- (i) любая бент-функция является абсолютно минимальной;
- (ii) при $q = 2$ класс всех бент-функций совпадает с классом всех абсолютно минимальных функций.

См. далее на эту тему [25]. Скоро, видимо, появятся работы о бент-функциях и на конечных неабелевых группах [49].

1.6. Векторные G -бент-функции. Идея этого обобщения для функций вида $f : A \rightarrow B$ впервые предложена В. И. Солодовниковым в [13]. Поинсо и Харари [50] в 2004 г. подробно её рассмотрели для случая $A = (\mathbb{Z}_2^k, +)$ и $B = (\mathbb{Z}_2^r, +)$, т. е. векторных булевых функций. Основу обобщения составляет возможность иначе определить производную функции $f : A \rightarrow B$.

А именно, пусть $S(A)$ — симметрическая группа A в мультипликативной записи. Перестановка $\sigma \in S(A)$ называется *инволюцией*, если $\sigma\sigma = e$, где e — тождественная перестановка. Перестановка σ без неподвижных точек, если для любого $x \in A$ справедливо $\sigma(x) \neq x$. Множество всех инволюций σ без неподвижных точек обозначим через $\text{Inv}(A)$. Подгруппа G группы $S(A)$ такая, что $G \subseteq \text{Inv}(A) \cup \{e\}$, называется *группой инволюций группы A* .

Пусть теперь $A = \mathbb{Z}_2^k$, $B = \mathbb{Z}_2^r$. Отметим, что

$$|\text{Inv}(\mathbb{Z}_2^k)| = \frac{2^k!}{2^{k-1}!2^{k-1}}.$$

В [50] показано, что любая группа инволюций G группы \mathbb{Z}_2^k является абелевой и $|G| \leq 2^k$. Будем рассматривать только группы G максимального порядка 2^k . Простым примером такой группы является *группа трансляций* $T(\mathbb{Z}_2^k)$, состоящая из всех перестановок σ_y , $y \in \mathbb{Z}_2^k$, таких, что $\sigma_y(x) = x + y$. Но существуют [50] и другие максимальные группы инволюций.

Пусть $f : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^r$, G — максимальная группа инволюций группы \mathbb{Z}_2^k . Обобщённой производной f по направлению $\sigma \in G$ называется функция

$$D_\sigma f(x) = f(\sigma(x)) - f(x).$$

Отметим, что, если G — группа трансляций $T(\mathbb{Z}_2^k)$, то обобщённая производная совпадает с обычной $D_y f(x) = f(x + y) - f(x)$.

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

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

В [50] предлагается перевод определения G -бент-функции на язык обобщённых коэффициентов Фурье, но пока, как представляется, он не вполне доработан и содержит неточности. Не ясно также в какой мере подход [50] применим, если A и B — произвольные абелевы группы.

1.7. Многомерные бент-функции на конечной абелевой группе. Это прямое обобщение бент-функций О. А. Логачёва, А. А. Сальникова и В. В. Яценко [10] предложил рассматривать Поинсо [48] в 2005 г.

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

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

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

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

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

При $m = 1$ данное определение полностью совпадает с определением 4. Аналогично, для многомерных бент-функций выполняется критерий Ротхауса, определяется дуальная многомерная бент-функция и т. п. [48]. Но пока не ясно, представляют ли многомерные бент-функции самостоятельный интерес, или же являются несколько формальным обобщением бент-функций из определения 4.

2. Комбинаторные обобщения бент-функций

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

2.1. Частично определённые бент-функции. Пусть $S \subseteq \mathbb{Z}_2^n$ — произвольное подмножество, $f : S \rightarrow \mathbb{Z}_2$ — *частично определённая булева функция*. Её *неполным преобразованием Уолша — Адамара* называется отображение

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

Для такого преобразования справедлив аналог равенства Парсеваля:

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

Определение 8. Булева функция f называется *частично определённой бент-функцией*, если

$$W_{f,S}(y) = \pm \sqrt{|S|}$$

для любого $y \in \mathbb{Z}_2^n$.

Подробнее такие функции разбираются в [12, гл. 6]. Здесь отметим лишь, что пока не известно, при каких условиях на множество S частично определённые бент-функции существуют.

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

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

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

Результаты о таких функциях можно найти в обзорах [12, 23], а также в [27, 62, 63].

2.3. \mathbb{Z} -бент-функции. В 2005 г. Доббертин [32] предложил исследовать бент-функции в контексте более общего подхода, который можно назвать рекурсивным. Не будем различать обычную булеву функцию $f(x)$, где $x \in \mathbb{Z}_2^n$, и целочисленную функцию $F(x) = (-1)^{f(x)}$. Преобразование Фурье функции $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}$ определяется как

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

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

Определение 10 (Доббертин, 2005). Пусть $T \subseteq \mathbb{Z}$. Функция $F : \mathbb{Z}_2^n \rightarrow T$ 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 [32] исследуются возможности рекурсивного построения (разложения) \mathbb{Z} -бент-функций с повышением или понижением их уровня и числа переменных.

2.4. Однородные бент-функции (homogeneous bent functions). Этот подкласс бент-функций выделен в [52] как состоящий из функций с относительно простыми алгебраическими нормальными формами.

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

В [52] Ку, Себерри и Пипджик перечислили все однородные бент-функции степени 3 от 6 переменных (их оказалось ровно 30) и поставили вопрос о классификации таких бент-функций от большего числа переменных. Чарнес, Роттелер и Бет [28] доказали, что существуют однородные бент-функции степени 3 от любого числа переменных $n > 2$. В [59] Кси, Себерри, Пипджик и Чарнес установили, что однородных бент-функций от n переменных максимально возможной степени $n/2$ не существует при $n > 3$. Исследователи из Китая Мэн, Чжан, Ян и Цоу [42, 43] показали, что не существует также однородных бент-функций степени

$(n/2) - 1$ при $n > 4$. Но какова же точная верхняя оценка степени нелинейности однородной бент-функции? На этот вопрос нет ответа. Есть только предположение [42] о том, что для любого $k > 1$ найдётся $N \geq 2$ такое, что однородная бент-функция степени k от n переменных существует при каждом $n > N$.

3. Криптографические обобщения бент-функций

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

3.1. Уравновешенные бент-функции. С точки зрения криптографии к важным критериям, которым должна удовлетворять булева функция f от n переменных, относятся следующие [11, 23]:

- *уравновешенность* (или *сбалансированность*) — функция f принимает значения 0 и 1 одинаково часто;
- *критерий распространения* $PC(k)$ порядка k (*Propagation Criterion*) — для любого ненулевого вектора $y \in \mathbb{Z}_2^n$ веса не более k , где $1 \leq k \leq n$, функция $f(x + y) + f(x)$ уравновешена [51];
- *максимальная нелинейность* — функция f такова, что значение её нелинейности N_f максимально;
- *равномерность корреляции с линейными функциями*; значение корреляции между функциями f и g определяется как

$$c(f, g) = 1 - \frac{\text{dist}(f, g)}{2^{n-1}};$$

для функции f равномерная корреляция означает, что значение $|c(f, g)|$ постоянно при любой линейной функции g .

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

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

В [18] установлено, что если n нечётно и f — уравновешенная функция, то $N_f \leq 2^{n-1} - 2^{(n-1)/2}$.

В 1994 г. Чи, Ли и Ким [29] предложили способ построения уравновешенных бент-функций от нечётного числа переменных, имеющих при этом почти равномерную корреляцию с линейными функциями и удовлетворяющих критерию $PC(k)$ для достаточно большого k . Приведём этот способ.

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

Теорема 16. Пусть f_0 — бент-функция от $n-1$ переменных, f_1 — эквивалентная ей бент-функция:

$$f_1(x) = f_0(Ax + b) + 1.$$

Тогда функция $g(x, z) = f_z(x)$ от n переменных, где $x \in \mathbb{Z}_2^{n-1}$, $z \in \mathbb{Z}_2$,

- (i) является уравновешенной бент-функцией;
- (ii) является почти бент-функцией (см. определение далее);
- (iii) имеет следующие возможные значения корреляции с любой линейной функцией: $0, \pm 2^{-(n-1)/2}$;
- (iv) удовлетворяет критерию PC для любого ненулевого вектора $(y, 0)$, где $y \in \mathbb{Z}_2^{n-1}$;
- (v) удовлетворяет критерию $PC(n-1)$, если $A = E$ и b — вектор из всех единиц.

3.2. Частично бент-функции (partially bent functions). Как уже было отмечено, бент-функции не являются ни уравновешенными, ни корреляционно-иммунными. Карле [20] предложил свой способ расширить класс \mathfrak{B}_n функциями, обладающими данными свойствами и имеющими при этом достаточно высокую нелинейность. Определение таких *частично бент-функций* даётся с помощью следующего экстремального свойства. Пусть

$$\Delta_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) + f(x+y)}$$

— автокорреляция булевой функции f по направлению y . Пусть NW_f и $N\Delta_f$ — количества ненулевых коэффициентов Уолша — Адамара и коэффициентов автокорреляции булевой функции f соответственно. Тогда [20] для любой булевой функции выполняется $NW_f \cdot N\Delta_f \geq 2^n$.

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

Теорема 17. Следующие утверждения эквивалентны:

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

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

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

Далее z обозначает вектор, определённый в теореме 17. Подпространство L для частично бент-функции f определяется как множество векторов x таких, что $\Delta_f(x) \neq 0$. Эквивалентно можно определить L как пространство линейных структур f , т. е. пространство, состоящее из всех векторов y таких, что $f(x + y) + f(x) = \text{const}$. Подпространство L' для разложения \mathbb{Z}_2^n в прямую сумму выбирается произвольно. Заметим, что размерность подпространства L' должна быть чётной, пусть она равна $2h$. Согласно [20] справедливы следующие результаты (необходимые определения см. в [12]).

Теорема 18. Частично бент-функция является

- (i) уравновешенной тогда и только тогда, когда $f|_L \neq \text{const}$;
- (ii) неуравновешенной веса w тогда и только тогда, когда $f|_L$ — константа, причём $w = 2^{n-1} \pm 2^{n-h-1}$, где $\dim L = n - 2h$;
- (iii) платовидной порядка $2h$;
- (iv) корреляционно-иммунной порядка k , если и только если смежный класс $z + L^\perp$ не содержит векторов веса w , $1 \leq w \leq k$;
- (v) уравновешенной корреляционно-иммунной порядка k , если и только если класс $z + L^\perp$ не содержит векторов веса не больше k ;
- (vi) удовлетворяет критерию распространения $PC(k)$ тогда и только тогда, когда L не содержит векторов веса w , $1 \leq w \leq k$.

Отметим, что частично бент-функциями являются все аффинные, квадратичные и бент-функции. Справедлива [20]

Теорема 19. Пусть f — частично бент-функция, $\dim L = n - 2h$. Тогда

$$N_f = 2^{n-1} - 2^{n-h-1},$$

$$W_f(x) = \begin{cases} \pm 2^{n-h} & \text{при } x \in z + L^\perp; \\ 0 & \text{в противном случае.} \end{cases}$$

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

См. далее на эту тему [23, 58].

3.3. Гипербент-функции (hyper-bent functions). Йоссеф и Гонг [60] в 2001 г. ввели понятие гипербент-функции*. Их работе предшествовала статья Голомба и Гонга [33] 1999 г., в которой алгоритм шифрования DES рассматривался как регистр сдвига с нелинейными обратными связями и проводился анализ его S-блоков. При таком подходе авторы [33] предложили использовать для приближения координатных функций S-блоков вместо линейных булевых функций собственные мономиальные функции. Эта идея и была развита в [60].

Булеву функцию от n переменных можно рассматривать как функцию из \mathbb{F}_{2^n} в \mathbb{F}_2 , сопоставляя каждому вектору x соответствующий элемент поля \mathbb{F}_{2^n} . Известно, что любая линейная функция $\langle x, y \rangle$ может быть представлена как $\text{Tr}(a_x y)$ для подходящего элемента $a_x \in \mathbb{F}_{2^n}$, где $\text{Tr} : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ — функция следа. Тогда преобразование Уолша — Адамара приобретает эквивалентный вид

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

Функция вида $\text{Tr}(a_x y^s)$, где целое число s такое, что $1 \leq s \leq 2^n - 1$ и $\gcd(s, 2^n - 1) = 1$, называется *собственной мономиальной функцией*. *Расширенное преобразование Уолша — Адамара* булевой функции f имеет вид

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

Определение 14 (Йоссеф, Гонг, 2001). Булева функция f называется *гипербент-функцией*, если для любого $y \in \mathbb{F}_{2^n}$ и любого целого s , $\gcd(s, 2^n - 1) = 1$, выполняется $|W_{f,s}(y)| = 2^{n/2}$.

Другими словами, гипербент-функция одинаково плохо приближается всеми собственными мономиальными функциями, её обобщённая нелинейность

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

максимальна, т. е. равна $2^{n-1} - 2^{(n/2)-1}$. Авторы [60] для каждого чётного n доказали существование гипербент-функций, предложили их векторный вариант, для малого числа переменных рассмотрели уравновешенные гипербент-функции. В 2006 г. Карле и Габори [26] и независимо

* До этого термин *гипербент-функция* однажды использовался в [21] для обозначения другого класса функций, но больше в этом значении он не употребляется.

А. С. Кузьмин, В. Т. Марков, А. А. Нечаев и А. Б. Шишков [6] показали, что степень нелинейности любой гипербент-функции от n переменных равна $n/2$.

А. С. Кузьмин и др. [7, 8] обобщили понятие гипербент-функции: от булевых функций они перешли к функциям над произвольным конечным полем характеристики 2.

А именно, пусть $q = 2^\ell$. В [8] рассматривается задача приближения произвольной функции из \mathbb{F}_q^n в \mathbb{F}_q (как и выше она отождествляется с функцией $f : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$) функциями из некоторого ограниченного класса \mathcal{A} . Для оценки эффективности приближения функции f функцией $g \in \mathcal{A}$ вводится параметр *согласие* $\nabla(f, g)$, связанный с функцией близости В. И. Солодовникова (4) соотношением

$$\nabla(f, g) = \frac{q}{\sqrt{q-1}} \delta(f, g),$$

если конечные группы выбирать как $A = (\mathbb{F}_{q^n}, +)$ и $B = (\mathbb{F}_q, +)$. Этот параметр представляется более естественным, поскольку $0 \leq \nabla(f, g) \leq 1$ и при крайних значениях 0 и 1 функции f и g отличаются на уравновешенную функцию и на константу соответственно. При $q = 2$ справедливо

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

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

- Если $\mathcal{A} = \text{Hom}(A, B)$ — класс всех гомоморфизмов из A в B , то функция $f : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$ такая, что параметр $\nabla(f, \text{Hom}(A, B))$ принимает минимально возможное значение $q^{-n/2}$, является бент-функцией в смысле определения 1.

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

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

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

В [7] проведено детальное исследование таких обобщённых гипербент-функций. Приведём здесь лишь одну конструкцию таких функций.

Мультипликативная группа поля \mathbb{F}_{q^n} есть прямое произведение $(\mathbb{F}_{q^{n/2}}, \cdot)$ на циклическую группу V порядка $q^{n/2} + 1$. Пусть $z_{a,d}$ равно единице (нулю) для $a, d \in \mathbb{F}_q$, если элементы a и d равны (не равны) соответственно.

Теорема 20. Пусть задана функция $g : V \rightarrow \mathbb{F}_q$ такая, что найдётся элемент $d \in \mathbb{F}_q$, при котором число решений уравнения $g(x) = a$ в множестве V равно $q^{(n/2)-1} + z_{a,d}$, где $a \in \mathbb{F}_q$. Тогда функция $f : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$ такая, что $f(0) = d$, $f(x) = g(x^{q^{n/2}-1})$ при $x \neq 0$, является гипербент-функцией.

См. далее на эту тему [9, 61]. Мономиальные приближения булевых функций также изучались А. В. Ивановым [3, 4]. Например, им было показано [5], что свойство бент-функции быть гипербент-функцией, вообще говоря, зависит от выбора базиса, при котором рассматривается её приведённое представление.

3.4. Почти бент-функции (near bent functions). Бент-функции существуют только для чётного числа переменных. При нечётном n одним из их аналогов можно считать почти бент-функции, обладающие достаточно высокой нелинейностью.

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

Почти бент-функции суть не что иное как платовидные функции максимального порядка $n - 1$ от нечётного числа переменных, см. определение 9. Не будем рассматривать их подробно. Отметим лишь, что булевы функции, имеющие три различных значения в спектре Уолша — Адамара, интересны для обеспечения защиты от так называемой soft output joint attack на генераторы псевдослучайных последовательностей (PN-generators) [39]. Такие генераторы используются в уже упоминавшемся выше стандарте IS-95 технологии CDMA. Почти бент-функции используются также для построения криптографически стойких S-блоков [30].

См. о почти бент-функциях [31, 38].

3.5. Бент-функции более высокого порядка нелинейности. Это довольно естественное направление, тесно связанное с нелинейными обобщениями различных методов криптоанализа.

Известно, что эффективность приближения бент-функции любой линейной функцией является самой низкой. Расширяя класс линейных функций, естественно рассматривать для приближения булевы функции степени не выше r , где $2 \leq r \leq n - 1$. При этом возникает понятие

нелинейности r -го порядка $N_r(f)$ булевой функции f как расстояния Хэмминга от f до всех таких функций.

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

Трудность заключается в определении этого максимально возможного значения для $N_r(f)$. При $r \geq 2$ это нерешённая задача, более известная в теории кодирования как определение радиуса покрытия кода Риды — Маллера порядка r . Известны пока некоторые оценки для $N_r(f)$, его асимптотическое значение, связь с другими криптографическими параметрами и т. п. Подробнее на эту тему см. обзор Карле [22] 2008 г.

3.6. k -Бент-функции. В 2007 г. автором было введено следующее понятие [14], основной идеей которого было рассмотрение аппроксимирующих функций, отличных от линейных, но являющихся в какой-то степени их аналогами.

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

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

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

Функция

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

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

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

Функция f называется *k -бент-функцией при фиксированном порядке переменных*, если все её коэффициенты $W_f^{(j)}(y)$, $j = 1, \dots, k$, равны $\pm 2^{n/2}$. Такие функции рассматривались в [14]. Однако их недостатком являлась

зависимость от порядка переменных функции. Приведём более общее определение, избавленное от этого недостатка.

Определение 18. Булева функция f от n переменных называется k -бент-функцией, если для произвольной подстановки $\pi \in S_n$, любого $j = 1, \dots, k$ и любого вектора y выполняется

$$W_{f \circ \pi}^{(j)}(y) = \pm 2^{n/2}.$$

Поясним смысл определения. Рассмотрим множества функций

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

от n переменных. Векторы значений функций из каждого класса $\mathfrak{A}_n^k(\pi)$ образуют двоичный код Адамара. Этот код является нелинейным (при $k > 1$), но у него существует линейный прообраз в пространстве \mathbb{Z}_4^n относительно некоторого простого отображения, см. подробнее [14]. Поэтому функции из $\mathfrak{A}_n^k(\pi)$ можно считать аналогами аффинных функций. Заметим, что они являются квадратичными. k -Нелинейностью булевой функции f называется минимальное расстояние Хэмминга $N_f^{(k)}$ от неё до множества всех функций вида $\langle \pi(x), y \rangle_k + a$, где π — любая перестановка. Справедливо равенство

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

Таким образом, k -бент-функция — это функция, для которой $N_f^{(j)}$ максимально, $N_f^{(j)} = 2^{n-1} - 2^{(n/2)-1}$ при любом $j = 1, \dots, k$, т. е. она одновременно максимально удалена от всех классов функций $\mathfrak{A}_n^j(\pi)$, $\pi \in S_n$, $j = 1, \dots, k$. Заметим, что 1-бент-функции совпадают с обычными бент-функциями. С ростом k нелинейные свойства функций усиливаются, поэтому наиболее интересной задачей представляется описание класса всех $(n/2)$ -бент-функций. Как следует из [14], этот класс не пуст, при любом чётном n ему принадлежат, например, все симметричные бент-функции: $f(x) = \sum_{i=1}^n \sum_{j=i+1}^n x_i x_j$, $f(x) + 1$, $f(x) + \sum_{i=1}^n x_i$, $f(x) + \sum_{i=1}^n x_i + 1$, характеристика которых приводится в [54].

При $n = 4$ все $(n/2)$ -бент-функции были описаны в [16]. Это 128 квадратичных функций с квадратичной частью одного из четырёх видов: $x_1 x_2 + x_3 x_4$, $x_1 x_3 + x_2 x_4$, $x_1 x_4 + x_2 x_3$, $x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4$ и произвольной линейной частью. См. также на эту тему [15].

4. Квантовые обобщения бент-функций

4.1. Нега-бент-функции, бент₄-функции, I-бент-функции.

Бент-функцию часто определяют как функцию, которая имеет *плоский* спектр относительно преобразования Уолша — Адамара. Плоский означает, что модули всех коэффициентов Уолша — Адамара равны. В 2006 г. Риера и Паркер [53] стали исследовать булевы функции, имеющие плоские спектры относительно множества унитарных преобразований специального вида. Напомним, что преобразование пространства \mathbb{C}^n , заданное квадратной матрицей A , *унитарно*, если $A\bar{A}^T = E$, где E — единичная матрица. Выбранные преобразования используются при анализе стабилизаторов квантовых состояний [53]. 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 (кронекерово) произведение n матриц, где A встречается на j -м месте. Рассмотрим следующие множества преобразований.

✓ $\{H\}^n$, состоящее из преобразования $U = \prod_{j=0}^{n-1} H_j$. Если $F = (-1)^f$ —

функция *знака* булевой функции f от n переменных, то вектор спектральных значений f относительно преобразования U определяется как $\hat{F} = UF$. Тогда f — *бент-функция* (в обычном смысле), если её спектр относительно U плоский, т. е. каждая компонента \hat{F} равна ± 1 .

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

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

Отметим, что поскольку U — комплексная матрица, при определении спектра функции здесь возникают свои особенности [46]. Любая аффинная булева функция является нега-бент-функцией. Паркер (2000, 2007) и Потт (2007) изучали нега-бент-функции в [45, 46]. В [46] исследовался вопрос о пересечении классов бент- и нега-бент-функций, полностью разрешённый для квадратичных функций.

✓ $\{H, N\}^n$, состоящее из 2^n преобразований вида $\prod_{j \in R_H} H_j \prod_{j \in R_N} N_j$,

где R_H и R_N разбивают множество $\{0, 1, \dots, n-1\}$. Булева функция f от n переменных является *бент₄-функцией*, если существует хотя бы одно разбиение R_H, R_N , относительно которого f имеет плоский спектр.

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

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

Риера и Паркер [53] развивают квантовый мотив своих исследований, изучают свойства бент-функций нового типа и их связь с графами.

Выражаю свою благодарность рецензенту за внимательное прочтение работы и полезные замечания.

ЛИТЕРАТУРА

1. Агеев Д. В. Основы теории линейной селекции. Кодовое разделение каналов // Сб. научн. тр. Ленинградского экспериментального ин-та связи. — Л.: Изд-во экспериментального ин-та связи, 1935. — С. 3–35.
2. Амбросимов А. С. Свойства бент-функций q -значной логики над конечными полями // Дискрет. математика. — 1994. — Т. 6, № 3. — С. 50–60.
3. Иванов А. В. Использование приведённого представления булевых функций при построении их нелинейных аппроксимаций // Вестн. Томского гос. университета. Приложение. — 2007. — № 23. — С. 31–35.
4. Иванов А. В. Мономиальные приближения платовидных функций // Прикл. дискрет. математика. — 2008. — Т. 1, № 1. — С. 10–14.
5. Иванов А. В. Близость к классу мономиальных аппроксимаций приведенного представления булевой функции в зависимости от выбора базиса, в котором оно задано // Прикл. дискрет. математика. Приложение. — 2009. — № 1. — С. 7–9.
6. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б. Приближение булевых функций мономиальными // Дискрет. математика. — 2006. — Т. 18, № 1. — С. 9–29.
7. Кузьмин А. С., Нечаев А. А., Шишкин В. А. Бент- и гипербент-функции над конечным полем // Тр. по дискрет. математике. — 2007. — Т. 10. — С. 97–122.
8. 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 // Пробл. передачи информ. — 2008. — Т. 44, вып. 1. — С. 15–37.

9. Кузьмин А. С., Нечаев А. А., Шишкин В. А. Параметры (гипер-) бент-функций над полем из 2^l элементов // Тр. по дискрет. математике. — 2008. — Т. 11. — С. 47–59.
10. Логачёв О. А., Сальников А. А., Яценко В. В. Бент-функции на конечной абелевой группе // Дискрет. математика. — 1997. — Т. 9, № 4. — С. 3–20.
11. Логачёв О. А., Сальников А. А., Яценко В. В. Криптографические свойства дискретных функций // Мат. конф. «Московский университет и развитие криптографии в России», МГУ, 2002. — М.: МЦНМО, 2003. — С. 174–199.
12. Логачёв О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.
13. Солодовников В. И. Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискрет. математика. — 2002. — Т. 14, № 1. — С. 99–113.
14. Токарева Н. Н. Бент-функции с более сильными свойствами нелинейности: k -бент-функции // Дискрет. анализ и исслед. операций. Сер. 1. — 2007. — Т. 14, № 4. — С. 76–102.
15. Токарева Н. Н. О квадратичных аппроксимациях в блочных шифрах // Пробл. передачи информ. — 2008. — Т. 44, вып. 3. — С. 105–127.
16. Токарева Н. Н. Описание k -бент-функций от четырёх переменных // Дискрет. анализ и исслед. операций. — 2008. — Т. 15, № 4. — С. 74–83.
17. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ // Прикл. дискрет. математика. — 2009. — Т. 2, № 1. — С. 15–37. <http://mi.mathnet.ru/pdm50>.
18. Adams C., Tavares S. The structured design of cryptographically good S-boxes // J. Cryptology. — 1990. — Vol. 3, N 1. — P. 27–43.
19. Agievich S. V. Bent rectangles // NATO advanced study institute on Boolean functions in cryptology and information security (Zvenigorod, Russia. September 8–18, 2007). Proc. — Netherlands: IOS Press, 2008. — P. 3–22. <http://arxiv.org/abs/0804.0209>.
20. Carlet C. Partially-bent functions // Des. Codes Cryptography. — 1993. — Vol. 3, N 2. — P. 135–145.
21. Carlet C. Hyper-bent functions // Intern. Conf. on the Theory and Applications of Cryptology — PRAGOCRYPT'96. — Prague: Czech Tech. Univ. Publ. House, 1996. — P. 149–155.
22. Carlet C. On the higher order nonlinearities of Boolean functions and S-boxes, and their generalizations // 5th Intern. Conf. on Sequences and their Applications — SETA'2008 (Lexington, Kentucky, USA. September 14–18, 2008). Proc. — Berlin: Springer-Verl., 2008. — P. 345–367 (Lect. Notes Comput. Sci.; Vol. 5203).
23. Carlet C. Boolean functions for cryptography and error correcting codes // Chapter of the monograph «Boolean Methods and Models». Cam-

- bridge: Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf.
24. **Carlet C., Ding C.** Highly nonlinear mappings // J. Complexity. — 2004. — Vol. 20, N 2–3. — P. 205–244.
 25. **Carlet C., Ding C.** Nonlinearities of S-boxes // Finite Fields Appl. — 2007. — Vol. 13, N 1. — P. 121–135.
 26. **Carlet C., Gaborit P.** Hyper-bent functions and cyclic codes // J. Comb. Theory. Ser. A. — 2006. — Vol. 113, N 3. — P. 466–482.
 27. **Carlet C., Prouff E.** On plateaued functions and their constructions // Fast software encryption — FSE'2003, 10th Int. Workshop (Lund, Sweden. February 24–26, 2003). Proc. — Berlin: Springer-Verl., 2003. — P. 54–73 (Lect. Notes Comput. Sci.; Vol. 2887).
 28. **Charnes C., Rotteler M., Beth T.** Homogeneous bent functions, invariants, and designs // Des. Codes Cryptography. — 2002. — Vol. 26, N 1–3. — P. 139–154.
 29. **Chee S., Lee S., Kim K.** Semi-bent functions // Advances in cryptology — ASIACRYPT '94 — 4th Int. Conf. on the Theory and Applications of Cryptology (Wollongong, Australia. November 28–december 1, 1994). Proc. — Berlin: Springer-Verl., 1995. — P. 107–118 (Lect. Notes Comput. Sci.; Vol. 917).
 30. **Detombe J., Tavares S.** Constructing large cryptographically strong S-boxes // Advances in cryptology — AUSCRYPT'92 (Gold Coast, Queensland, Australia. December 13–16, 1992) Proc. — Berlin: Springer-Verl., 1993. — P. 165–181 (Lect. Notes Comput. Sci.; Vol. 718).
 31. **Dillon J. F., McGuire G.** Near bent functions on a hyperplane // Finite Fields Appl. — 2008. Vol. 14. — P. 715–720.
 32. **Dobbertin H., Leander G.** Cryptographer's toolkit for construction of 8-bit bent functions // Cryptology ePrint Archive, Report 2005/089. <http://eprint.iacr.org/>
 33. **Gong G., Golomb S. W.** Transform domain analysis of DES // IEEE Trans. Inform. Theory. — 1999. — Vol. 45, N 6. — P. 2065–2073.
 34. **Helleseth T., Kalosha A.** Monomial and quadratic bent functions over the finite fields of odd characteristic // Reports in informatics, 2005. Report 310. Bergen: University of Bergen, 2005. — 34 p.
 35. **Hou X. D.** q -Ary bent functions constructed from chain rings // Finite Fields Appl. — 1998. — Vol. 4, N 1. — P. 55–61.
 36. **Hou X. D.** p -Ary and q -ary versions of certain results about bent functions and resilient functions // Finite Fields Appl. — 2004. — Vol. 10, N 4. — P. 566–582.
 37. **Kumar P. V., Scholtz R. A., Welch L. R.** Generalized bent functions and their properties // J. Comb. Theory. Ser. A. — 1985. — Vol. 40, N 1. — P. 90–107.
 38. **Leander N. G., McGuire G.** Construction of bent functions from near-bent

- functions // J. Comb. Theory, Ser. A. — 2009. — Vol. 116, N 4. — P. 960–970.
39. **Leveiller S., Zemor G., Guillot P., Boutros J.** A new cryptanalytic attack for PN-generators filtered by a Boolean function // Selected areas of cryptography — SAC'2002 (Newfoundland, Canada, August 15–16, 2002). Proc. — Berlin: Springer-Verl., 2003. — P. 232–249 (Lect. Notes Comput. Sci.; Vol. 2595).
40. **McFarland R. L.** A family of difference sets in non-cyclic groups // J. Comb. Theory, Ser. A. — 1973. — Vol. 15, N 1. — P. 1–10.
41. **Matsufuji S., Imamura K.** Real-valued bent functions and its application to the design of balanced quadriphase sequences with optimal correlation properties // Intern. Symposium on Applied Algebra, Algebraic Algorithms and Error-correcting Codes — AAEECC-8 (Tokyo, Japan, August 20–24, 1990). Proc. — Berlin: Springer-Verl., 1990. — P. 106–112 (Lect. Notes Comput. Sci.; Vol. 508).
42. **Meng Q., Zhang H., Yang M. C., Cui J.** On the degree of homogeneous bent functions // <http://eprint.iacr.org>, 2004/284.
43. **Meng Q., Zhang H., Yang M. C., Cui J.** On the degree of homogeneous bent functions // Discr. Appl. Math. — 2007. — Vol. 155, N 5. — P. 665–669.
44. **Olsen J. D., Scholtz R. A., Welch L. R.** Bent-function sequences // IEEE Trans. Inform. Theory. — 1982. — Vol. 28, N 6. — P. 858–864.
45. **Parker M. G.** The constabent properties of Golay–Davis–Jedwab sequences // IEEE Intern. Symp. on Information Theory — ISIT'2000 (Sorrento, Italy, June 25–30, 2000). Proc. — New York: Institute of Electrical and Electronics Engineers, 2000. — P. 302.
46. **Parker M. G., Pott A.** On Boolean functions which are bent and negabent // Sequences, Subsequences, and Consequences — SSC'2007 — Intern. Workshop (Los Angeles, CA, USA, May 3–June 2, 2007). Proc. — Berlin: Springer-Verl., 2007. — P. 9–23 (Lect. Notes Comput. Sci.; Vol. 4893).
47. **Paterson K. G.** On codes with low peak-to-average power ratio for Multi-code CDMA // IEEE Trans. Inform. Theory. — 2004. — Vol. 50, N 3. — P. 550–558.
48. **Poinsot L.** Multidimensional bent functions // GESTS Intern. Transactions on Comput. Sci. Eng. — 2005. — Vol. 18, N 1. — P. 185–195.
49. **Poinsot L., Harari S.** Nonabelian bent functions // IEEE Trans. Inform. Theory, to appear. <http://poinsot.univ-tln.fr/publi.html>
50. **Poinsot L., Harari S.** Generalized Boolean bent functions // Progress in cryptology — Indocrypt'2004 (Chennai (Madras), India, December 20–22, 2004). Proc. — Berlin: Springer-Verl., 2005. — P. 107–119 (Lect. Notes Comput. Sci.; Vol. 3348).
51. **Preneel B., van Leekwijck W., van Linden L., Govaerts R., Vandevale J.** Propagation characteristics of Boolean functions // Adv. Cryptology — EUROCRYPT'1990. Intern. Conf. on the Theory and Application of Cryptographic Techniques (Aarhus, Denmark, May 21–24, 1990). Proc. — Berlin:

- Springer-Verl., 1991. — P. 161–173 (Lect. Notes Comput. Sci. Vol. 473).
52. **Qu C., Seberry J., Pieprzyk J.** Homogeneous bent functions // Discrete Appl. Math. — 2000. — Vol. 102, N 1-2. — P. 133–139.
 53. **Riera C., Parker M. G.** Generalised bent criteria for Boolean functions (I) // IEEE Trans. Inform. Theory. — 2006. — Vol. 52, N 9. — P. 4142–4159.
 54. **Savicky P.** On the bent Boolean functions that are symmetric // Eur. J. Comb. — 1994. — Vol. 15, N 4. — P. 407–410.
 55. **Schmidt K.-U.** Quaternary constant-amplitude codes for multicode CDMA // IEEE Intern. Symp. on Information Theory — ISIT'2007 (Nice, France. June 24–29, 2007). Proc. — 2007. — P. 2781–2785. <http://arxiv.org/abs/cs.IT/0611162>.
 56. **Solé P., Tokareva N.** Connections between quaternary and binary bent functions // Cryptology ePrint Archive, Report 2009/544. — 13 p. <http://eprint.iacr.org>
 57. **Wada T.** Characteristic of bit sequences applicable to constant amplitude orthogonal multicode systems // IEICE Trans. Fundamentals. — 2000. — Vol. E83-A, N 11. — P. 2160–2164.
 58. **Wang X., Zhou J.** Generalized partially bent functions // Future generation communication and networking (Jeju-Island, Korea. December 6–8, 2007) Proc. — 2007. — P. 16–21.
 59. **Xia T., Seberry J., Pieprzyk J., Charney C.** Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$ // Discrete Appl. Math. — 2004. — Vol. 142, N 1–3. — P. 127–132.
 60. **Youssef A., Gong G.** Hyper-bent functions // Adv. Cryptology — EURO-CRYPT'2001. Intern. Conf. on the Theory and Application of Cryptographic Techniques (Innsbruck, Austria. May 6–10, 2001). Proc. — Berlin: Springer-Verl., 2001. — P. 406–419 (Lect. Notes Comput. Sci. Vol. 2045).
 61. **Youssef A. M.** Generalized hyper-bent functions over $GF(p)$ // Discrete Appl. Math. — 2007. — Vol. 155, N 8. — P. 1066–1070.
 62. **Zheng Y., Zhang X.-M.** Relationships between bent functions and complementary plateaued functions // ICISC'99 — Intern. Conf. on Information Security and Cryptology (Seoul, Korea. December 9–10, 1999). Proc. — Berlin: Springer-Verl., 2000. — P. 60–75 (Lect. Notes Comput. Sci. Vol. 1787).
 63. **Zheng Y., Zhang X.-M.** On plateaued functions // IEEE Trans. Inform. Theory. — 2001. — Vol. 47, N 3. — P. 1215–1223.

Токарева Наталья Николаевна,
e-mail: tokareva@math.nsc.ru

Статья поступила
22 сентября 2009 г.
Переработанный вариант —
21 октября 2009 г.