ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

БЕНТ-ФУНКЦИИ И ИХ ОБОБЩЕНИЯ[1]

Н. Н. Токарева

Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

E-mail: tokareva@math.nsc.ru

Лекция посвящена бент-функциям — булевым функциям, максимально удаленным в метрике Хэмминга от множества всех аффинных функций. Это экстремальное свойство определяет большое число приложений бент-функций в самых разных областях. Рассматриваются также обобщения бент-функций.

Ключевые слова: *бент-функция, обобщения бент-функций.*

Введение

Бент-функции впервые были введены О. Ротхаусом в 60-х годах XX века. Выпускник Принстонского университета Оскар Ротхаус (1927–2003) после службы во время Корейской войны в войсках связи поступил на работу математиком в Агентство Национальной Безопасности США. С 1960 по 1966 г. он работал в Институте оборонного анализа (IDA). Его криптографические работы того времени оценивались руководством IDA достаточно высоко. Как и его преподавательская деятельность: «he was one of the most important teachers of cryptology to mathematicians and mathematics to cryptologists» [8]. На это же время приходится и его первая работа о бент-функциях [36]. В открытой печати она появилась только в 1976 г. [37]. В ней были установлены базовые свойства бент-функций, предложены их простейшие конструкции и намечена классификация бент-функций от шести переменных.

В настоящее время бент-функции и их приложения изучаются очень активно.

Семейства бент-последовательностей из элементов $+1$ и -1, построенные на основе бент-функций, имеют предельно низкие значения как взаимной корреляции, так и автокорреляции (достигают нижней границы Велча). Такие семейства успешно применяются в коммуникационных системах коллективного доступа, а также в работе со стандартом CDMA. 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. В настоящее время технология используется большинством поставщиков беспроводного оборудования во всем мире согласно стандартам IMT–2000 мобильной связи третьего поколения (в России — стандарты IMT–MC 450 или CDMA–450). В системах CDMA для предельного снижения отношения пиковой и

[1]Работа выполнена при финансовой поддержке гранта Президента РФ для молодых российских ученых (МК-1250.2009.1), Российского фонда фундаментальных исследований (проекты 07-01-00248, 08-01-00671, 09-01-00528), Фонда содействия отечественной науке, ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг. (гос. контракт 02.740.11.0429).

средней мощностей сигнала (peak-to-average power ratio) используются коды постоянной амплитуды. Их построение напрямую связано с выбором специального подмножества бент-функций.

В блочных и поточных шифрах бент-функции и их векторные аналоги способствуют предельному повышению стойкости этих шифров к линейному и дифференциальному методам криптоанализа. Стойкость достигается за счет использования сильно нелинейных булевых функций в S-блоках (см., например, шифр CAST). Бент-функции и их обобщения находят свое применение также в схемах аутентификации, хэш-функциях (см. HAVAL) и псевдослучайных генераторах. См. также пример использования бент-функций в поточном шифре Grain.

Несмотря на высокий интерес к бент-функциям, прогресс в их изучении самый минимальный. Для мощности класса бент-функций не найдена асимптотика, не установлено приемлемых нижних и верхних оценок. Мало изучены и их обобщения, возникающие из новых постановок прикладных задач.

Данная лекция построена на основе двух обзоров автора [5, 6] и по сути является их кратким конспектом. Приводятся основные свойства, конструкции, эквивалентные представления бент-функций. Значительное внимание уделяется обобщениям бент-функций. В конце статьи приводятся открытые вопросы в этой области.

Нам потребуются следующие определения и обозначения:

q, n — натуральные числа;

$+$ — сложение по модулю q;

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

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

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

$\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n$ — скалярное произведение векторов;

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

$\boldsymbol{f}$ — вектор значений длины 2^n функции f. Будем считать, что аргументы функции (т. е. векторы длины n) перебираются в лексикографическом порядке;

$\mathrm{dist}(f, g)$ — *расстояние Хэмминга* между функциями f и g, т. е. число позиций, в которых различаются векторы $\boldsymbol{f}$ и $\boldsymbol{g}$;

АНФ — *алгебраическая нормальная форма* функции;

$\deg(f)$ — *степень нелинейности* булевой функции f, т. е. число переменных в самом длинном слагаемом ее АНФ;

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

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

максимально нелинейная функция — булева функция с максимально возможным значением N_f;

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;

аффинно эквивалентные функции f и g от n переменных: существуют невырожденная $n \times n$-матрица A, векторы b, c длины n и константа $\lambda \in \mathbb{Z}_2$, такие, что $g(x) = f(Ax + b) + \langle c, x\rangle + \lambda$.

1. Критерии и свойства

▶ Следующие утверждения эквивалентны:

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

(ii) матрица $A = (a_{x,y})$, где $a_{x,y} = 2^{-n/2} W_f(x+y)$, является матрицей Адамара;

(iii) матрица $D = (d_{x,y})$, где $d_{x,y} = (-1)^{f(x+y)}$, является матрицей Адамара;

(iv) для любого ненулевого вектора x функция $f(y) + f(x+y)$ *сбалансирована*, т. е. принимает значения 0 и 1 одинаково часто.

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

▶ Бент-функции любой степени $2 \leqslant \deg(f) \leqslant n/2$ существуют.

▶ Любая квадратичная бент-функция от n переменных аффинно эквивалентна функции $f(x_1, \ldots, x_n) = x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$.

▶ Класс бент-функций замкнут относительно

(i) любого невырожденного аффинного преобразования переменных;

(ii) прибавления любой аффинной функции.

2. Эквивалентные представления бент-функций

▶ Бент-функции могут быть описаны в терминах элементарных адамаровых разностных множеств и симметричных блок-схем [19].

▶ (Описание В. В. Ященко, 1997 [7].) Любая булева функция f от n переменных может быть представлена в виде *линейного разветвления* $f(x', x'') = \langle x', h(x'') \rangle + g(x'')$, где $x' \in \mathbb{Z}_2^r, x'' \in \mathbb{Z}_2^k$ для подходящих чисел r и k, таких, что $n = r + k$, отображения $h : \mathbb{Z}_2^k \to \mathbb{Z}_2^r$ и булевой функции g от k переменных. Максимально возможное значение r в таком представлении называется *индексом линейности* булевой функции f. Подмножество M пространства $\mathbb{Z}_2^n$ называется *бент-множеством*, если его мощность равна $2^{2\ell}$ при некотором ℓ и для любого ненулевого вектора $\boldsymbol{z} \in \mathbb{Z}_2^n$ множество $M \cap (\boldsymbol{z} + M)$ либо пусто, либо имеет четную мощность. Пара $(g; M)$, где g — булева функция от k переменных, M — бент-множество, называется *частичной бент-функцией*, если для любого $y' \in \mathbb{Z}_2^r$ и ненулевого $y'' \in \mathbb{Z}_2^k$ функция $g(x'') + g(x'' + y'')$ сбалансирована на множестве $M \cap ((y', y'') + M)$.

Функция f в виде линейного разветвления является бент-функцией тогда и только тогда, когда $n \geqslant 2r$ и для любого вектора $x' \in \mathbb{Z}_2^r$ выполняются условия:

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

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

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

▶ (Описание К. Карле и Ф. Гуилло, 1998 [15].) Пусть f — булева функция от n переменных. Пусть $\mathrm{Ind}_S : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — характеристическая функция подмножества $S \subseteq \mathbb{Z}_2^n$, т. е. Ind_S принимает значение 1 на элементах из S и значение 0 на остальных элементах.

Функция f является бент-функцией тогда и только тогда, когда существуют подпространства $E_1, \ldots, E_k$ размерности $n/2$ или $(n/2)+1$ пространства $\mathbb{Z}_2^n$ и ненулевые целые числа $m_1, \ldots, m_k$, такие, что $\sum_{i=1}^k m_i \mathrm{Ind}_{E_i}(y) = \pm 2^{(n/2)-1} \mathrm{Ind}_{\{\mathbf{0}\}}(y) + f(y)$ для любого $y \in \mathbb{Z}_2^n$. Можно ввести ограничения на способ выбора пространств $E_1, \ldots, E_k$, при которых можно говорить об однозначности такого представления.

▶ (Описание А. Бернаскони, Б. Коденотти и Дж. Ван-дер-Кама, 1999 [10, 11].) Пусть f — булева функция от n переменных. Через $\mathrm{supp}(f)$ обозначим ее *носитель*, т. е. множество всех двоичных векторов длины n, на которых функция f принимает значение 1. Рассмотрим *граф Кэли* $G_f = G(\mathbb{Z}_2^n, \mathrm{supp}(f))$ булевой функции f. Вершина-

ми графа являются все векторы длины n. Две вершины x, y соединяются ребром, если вектор $x+y$ принадлежит множеству $\mathrm{supp}(f)$. Граф G называется *сильно регулярным* (strongly regular), если существуют неотрицательные целые числа λ, μ, такие, что для любых двух вершин x, y общее число смежных им вершин равно λ или μ в зависимости от того, соединены вершины x, y ребром или нет.

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

► (Описание С. В. Агиевича, 2000 [9].) Пусть f — булева функция от n переменных, $n = r + k$. Вектор $\boldsymbol{W}_f$ коэффициентов Уолша—Адамара назовем *спектральным вектором* функции f. Представим двоичный вектор $\boldsymbol{f}$ в виде $\boldsymbol{f} = (\boldsymbol{f}_{(1)}, \ldots, \boldsymbol{f}_{(2^r)})$, где каждый вектор $\boldsymbol{f}_{(i)}$ имеет длину 2^k. Пусть $f_{(i)}$ — булева функция от k переменных, для которой $\boldsymbol{f}_{(i)}$ является вектором значений, $i = 1, \ldots, 2^r$. Свяжем с функцией f матрицу $\mathcal{M}_f$ размера $2^r \times 2^k$, строками которой являются спектральные векторы $\boldsymbol{W}_{f_{(1)}}, \ldots, \boldsymbol{W}_{f_{(2^r)}}$. Матрица размера $2^r \times 2^k$ называется *бент-прямоугольником*, если каждая ее строка и каждый столбец, домноженный на $2^{r-(n/2)}$, являются спектральными векторами для подходящих булевых функций. Согласно [9], выполняется следующая теорема.

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

3. Оценки числа бент-функций

Число бент-функций от n переменных неизвестно. Существует большой разрыв между нижней и верхней оценками этого числа. Асимптотически он имеет вид $C_1 \cdot 2^{2^{n/2}} \leqslant |\mathfrak{B}_n| \leqslant C_2 \cdot 2^{2^n}$. Нижняя оценка получается из конструкции Мэйорана—МакФарланда (некоторое ее улучшение см. в [9]). Верхняя оценка приводится в [16]. Сократить этот разрыв — серьезная задача.

4. Нелинейность произвольной булевой функции

В 1998 г. Д. Оледжар и М. Станек [32] исследовали криптографические свойства случайной булевой функции от n переменных. В частности, они показали, что существует константа c, такая, что при достаточно больших n почти для каждой булевой функции f от n переменных выполняется $N_f \geqslant 2^{n-1} - c\sqrt{n}\,2^{n/2}$. То есть с ростом n нелинейность случайной булевой функции от n переменных становится достаточно высокой и даже сопоставимой с нелинейностью бент-функции!

Для криптографических приложений булева функция кроме нелинейности должна обладать целым рядом других свойств. Приведенный факт позволяет сказать, что есть «гарантированная возможность» выбора функции с высокой нелинейностью не в ущерб этим свойствам. Но хотя нелинейность почти всех булевых функций высока, это не означает, что такие функции легко построить.

Задача описания всех бент-функций от n переменных решена лишь при малых значениях n. Приведем эти результаты (см. таблицу). Количество бент-функций при $n = 8$ равно $2^9 \times 193\,887\,869\,660\,028\,067\,003\,488\,010\,240 \simeq 2^{106{,}29}$

5. Конструкции бент-функций

► Функция $f(x', x'') = g(x') + h(x'')$, где векторы x', x'' имеют четные длины r, k соответственно, является бент-функцией тогда и только тогда, когда функции g, h — бент-функции.

Бент-функции от малого числа переменных

n	Число функций	Число кл. экв.	Представители классов эквивалентности
2	8	1	x_1x_2
4	896	1	$x_1x_2 + x_3x_4$
6	$5\,425\,430\,528 \simeq$ $\simeq 2^{32,3}$	4	Представители степени 2 $x_1x_2 + x_3x_4 + x_5x_6$, представители степени 3 $x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6$, $x_1x_2x_3 + x_2x_4x_5 + x_1x_2 + x_1x_4 + x_2x_6 + x_3x_5 + x_4x_5$, $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4 + x_2x_6 + x_3x_4 +$ $+x_3x_5 + x_3x_6 + x_4x_5 + x_4x_6$
8	$\simeq 2^{106,29}$	$\geqslant 536$	Представители степени 2 $x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$, представители степени 3 $x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6 + x_7x_8$, $x_1x_2x_3 + x_2x_4x_5 + x_3x_4 + x_2x_6 + x_1x_7 + x_5x_8$, $x_1x_2x_3 + x_2x_4x_5 + x_1x_3 + x_1x_5 + x_2x_6 + x_3x_4 + x_7x_8$, $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_3x_5 + x_2x_6 + x_2x_5 +$ $+x_1x_7 + x_4x_8$, $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_3x_5 + x_1x_3 + x_1x_4 +$ $+x_2x_7 + x_6x_8$, $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_3x_5 + x_2x_6 + x_2x_5 +$ $+x_1x_2 + x_1x_3 + x_1x_4 + x_7x_8$, $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_3x_5 + x_1x_6 + x_2x_7 + x_4x_8$, $x_1x_2x_7 + x_3x_4x_7 + x_5x_6x_7 + x_1x_4 + x_3x_6 + x_2x_5 +$ $+x_4x_5 + x_7x_8$, $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4x_7 + x_3x_5 + x_2x_7 +$ $+x_1x_5 + x_1x_6 + x_4x_8$, представителей степени 4 см. в [26, 27]
$\geqslant 10$	???	???	???

► Пусть $n = r+k$, где r и k четны, f — булева функция от n переменных. Пусть x', x'' пробегают $\mathbb{Z}_2^r$ и $\mathbb{Z}_2^k$ соответственно. Предположим, что функции $f_{x''}(x') = f(x', x'')$ являются бент-функциями при любых x''. Определим $g_{x'}(x'') = \widetilde{f_{x''}}(x')$. Тогда f — бент-функция, если и только если $g_{x'}$ — бент-функция для любого x'.

► (Конструкция Мэйорана—МакФарланда, 1973 [29].) Пусть h — любая перестановка на $\mathbb{Z}_2^{n/2}$, пусть g — произвольная булева функция от $n/2$ переменных. Тогда функция $f(x', x'') = \langle x', h(x'')\rangle + g(x'')$ является бент-функцией от n переменных.

► (Partial Spreads, Дж. Диллон, 1974 [20].) Пусть $\mathrm{Ind}_S : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — характеристическая функция подмножества $S \subseteq \mathbb{Z}_2^n$. Пусть число q равно $2^{(n/2)-1}$ или $2^{(n/2)-1}+1$. Пусть $L_1, \ldots, L_q$ — линейные подпространства размерности $n/2$ пространства $\mathbb{Z}_2^n$, такие, что любые два из них пересекаются лишь по нулевому вектору. Тогда функция $f(y) = \bigoplus_{i=1}^{q} \mathrm{Ind}_{L_i}(y)$ является бент-функцией. Различают классы бент-функций $\mathcal{PS}^+$ и $\mathcal{PS}^-$ (при $q = 2^{(n/2)-1}$ и $q = 2^{(n/2)-1}+1$ соответственно).

► (*Степенные* или *мономиальные бент-функции* — power/monomial bent functions.) Пусть векторное пространство $\mathbb{Z}_2^n$ отождествляется с полем Галуа $\mathbb{F}_{2^n}$. Булевы функ-

ции от n переменных можно рассматривать как функции из $\mathbb{F}_{2^n}$ в $\mathbb{F}_2$, сопоставляя каждому вектору y соответствующий элемент поля $\mathbb{F}_{2^n}$, который будем обозначать тем же символом. Пусть $\mathrm{tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ — *функция следа*, т. е. $\mathrm{tr}(y) = y + y^2 + \cdots + y^{2^{n-1}}$. Бент-функции, имеющие вид $f(y) = \mathrm{tr}(ay^d)$, где $a \in \mathbb{F}_{2^n}^*$ — некоторый параметр, называются *степенными* или *мономиальными*, а целое число d называется *бент-показателем*. Здесь $\mathbb{F}_{2^n}^*$ — множество ненулевых элементов поля. Пусть $\gcd(\cdot,\cdot)$ — наибольший общий делитель двух чисел. Известны следующие бент-показатели: $2^{n/2}-1$, 2^i+1 (если $n/\gcd(n,i)$ четно), $2^{2k}-2^k+1$ (при $\gcd(k,n)=1$), $(2^k+1)^2$ (если $n=4k$, k нечетно), $2^{2k}+2^k+1$ (при $n=6k$).

► Пусть булева функция представлена в виде $f(y) = \mathrm{tr}(a_1 y^{d_1} + a_2 y^{d_2})$ для подходящих элементов $a_1, a_2 \in \mathbb{F}_{2^n}$ и показателей d_1, d_2. Будем рассматривать специальные степенные показатели — *показатели Нихо* вида $d \equiv 2^i \bmod (2^{n/2}-1)$. Без ограничения общности [21] пусть первый показатель равен $d_1 = (2^{(n/2)}-1)\frac{1}{2}+1$. Тогда [23] если $d_2 = (2^{(n/2)}-1)\lambda + 1$, где λ равно $1/6$, $1/4$ или 3, то существуют элементы $a_1, a_2 \in \mathbb{F}_{2^n}$, такие, что f является бент-функцией.

► Общий алгебраический подход к описанию бент-функций мог бы основываться на том, что любая булева функция $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ может быть представлена *с помощью следа* (в так называемой trace form), т. е. в виде $f(y) = \mathrm{tr}\left(\sum\limits_{d \in CS} a_d y^d\right) = \sum\limits_{d \in CS} \mathrm{tr}(a_d y^d)$ для подходящих элементов $a_d \in \mathbb{F}_{2^n}$, где CS — множество представителей циклотомических классов по модулю 2^n-1. Эволюционный алгоритм на основе такого представления был предложен М. Янгом, К. Менгом и Х. Жангом [39]. На основе многочисленных компьютерных исследований авторы делают в этой работе некоторые предположения, например о том, что бент-функцию — представителя класса аффинной эквивалентности — можно представить в trace form с участием небольшого числа мономов. Причем более вероятными ненулевыми коэффициентами a_d считаются те, для которых d является бент-показателем.

6. Алгебраические обобщения бент-функций

Приведем обобщения, в которых рассматриваемые функции отличаются от булевых. Как правило, это отображения из одной алгебраической системы в другую. В этом и других пунктах обобщения приводятся на уровне определений. О том, в каких случаях доказано существование этих обобщений, см. подробнее в [6].

► (ВЕКТОРНЫЕ БЕНТ-ФУНКЦИИ.) С 90-х годов XX века стали исследоваться функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, получившие название *векторных булевых функций*, или (n,m)-*функций*. Нелинейные такие функции имеют непосредственные криптографические приложения. Например, в шифрах они используются в качестве S-блоков. *Преобразованием Уолша—Адамара* (n,m)-функции f называется отображение $W_f^{\mathrm{vect}} : \mathbb{Z}_2^n \times \mathbb{Z}_2^m \to \mathbb{Z}$, заданное равенством $W_f^{\mathrm{vect}}(x',x'') = \sum_{y \in \mathbb{Z}_2^n} (-1)^{\langle x',y\rangle + \langle x'', f(y)\rangle}$. Векторная (n,m)-функция называется *бент-функцией*, если $|W_f^{\mathrm{vect}}(x',x'')| = 2^{n/2}$ для каждых $x' \in \mathbb{Z}_2^n$, $x'' \in (\mathbb{Z}_2^m)^*$. Но векторные бент-функции существуют тогда и только тогда, когда n четно и $m \leqslant n/2$ [31]. При $m > n/2$ (в частности при $m = n$) рассматриваются аналоги бент-функций, такие, как APN- и AB-функции.

► (q-ЗНАЧНЫЕ БЕНТ-ФУНКЦИИ, q-ARY BENT FUNCTIONS, П. В. Кумар, Р. А. Шольц и Л. Р. Велч, 1985 [25].) Пусть $q \geqslant 2$ — натуральное число, $i = \sqrt{-1}$ — мнимая единица. Пусть ω — примитивный комплексный корень степени q из единицы, $\omega = e^{2\pi i/q}$. Рассмотрим q-значную функцию $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$. *Преобра-*

зованием Уолша—Адамара функции f называется комплексная функция $W_f(y) = \sum_{x\in\mathbb{Z}_q^n} \omega^{\langle x,y\rangle+f(x)}$, $y \in \mathbb{Z}_q^n$, где скалярное произведение и сложение + рассматриваются по модулю q. Пусть $|c|$ обозначает модуль комплексного числа c. Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *q-значной бент-функцией*, если $|W_f(y)| = q^{n/2}$ для каждого $y \in \mathbb{Z}_q^n$.

▶ (БЕНТ-ФУНКЦИИ НАД КОНЕЧНЫМ ПОЛЕМ, А. С. Амбросимов, 1994 [1].) Пусть $q = p^\ell$, где p — простое, ℓ — натуральное. Пусть ω — примитивный комплексный корень степени p из единицы, $\omega = e^{2\pi i/p}$. Пусть $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ — q-значная функция. При фиксированном $z \in \mathbb{F}_q$ *преобразование Уолша—Адамара* функции f определяется как $W_{f,z}(y) = \sum_{x\in\mathbb{F}_{q^n}} \omega^{\langle\langle x,y\rangle+f(x),z\rangle}$, где z рассматривается как вектор над $\mathbb{F}_p$ длины ℓ и внешнее скалярное произведение берется по модулю p (внутреннее — по модулю q). Для любой функции f и любого ненулевого z выполняется равенство Парсеваля $\sum_{y\in\mathbb{F}_{q^n}} |W_{f,z}(y)|^2 = q^{2n}$, из которого следует, что $\max\limits_{y\in\mathbb{F}_{q^n}} |W_{f,z}(y)| \geqslant q^{n/2}$. Функция $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ называется *бент-функцией*, если при любых векторах $z \in \mathbb{F}_q\backslash\{0\}$, $y \in \mathbb{F}_{q^n}$ выполняется $|W_{f,z}(y)| = q^{n/2}$. Заметим, что при $q = p$, $\ell = 1$ данное определение q-значной бент-функции совпадает с определением Кумара, Шольца и Велча.

▶ (ОБОБЩЕННЫЕ БУЛЕВЫ БЕНТ-ФУНКЦИИ, К. Шмидт, 2006 [38].) Они возникли в связи с построением обобщенных кодов постоянной амплитуды для систем CDMA. Пусть $q \geqslant 2$ — натуральное число, ω — примитивный комплексный корень степени q из единицы, $\omega = e^{2\pi i/q}$. Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ называется *обобщенной булевой функцией*. Ее *преобразованием Уолша—Адамара* называется комплексная функция $W_f(y) = \sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle}\omega^{f(x)}$, $y \in \mathbb{Z}_2^n$.

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

▶ (БЕНТ-ФУНКЦИИ ИЗ КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЫ В МНОЖЕСТВО КОМПЛЕКСНЫХ ЧИСЕЛ ЕДИНИЧНОЙ ОКРУЖНОСТИ, О. А. Логачев, А. А. Сальников и В. В. Ященко, 1997 [2].) Пусть $(A, +)$ — конечная абелева группа порядка n и максимальный порядок ее элементов (или *экспонента* группы) равен q. Пусть $T_q = \{e^{2\pi ik/q} \mid k = 0, 1, \ldots, q-1\}$ — группа корней степени q из единицы. Через $\widehat{A}$ обозначим группу гомоморфизмов $\chi : A \to T_q$. Она называется *группой характеров группы A* (или ее *дуальной группой*). Известно, что группы A и $\widehat{A}$ изоморфны; пусть $y \to \chi_y$ — некоторый фиксированный изоморфизм, $y \in A$. Вместо преобразования Уолша—Адамара удобно ввести *преобразование Фурье* комплекснозначной функции $f : A \to \mathbf{C}$. Оно определяется как $\widehat{f}(y) = \sum_{x\in A} f(x)\overline{\chi_y(x)}$. Далее рассматриваются только такие функции из A в $\mathbf{C}$, все значения которых лежат на единичной окружности $S_1(\mathbf{C})$ с центром в нуле.

Функция $f : A \to S_1(\mathbf{C})$ называется *бент-функцией*, если $|\widehat{f}(y)|^2 = n$ при любом $y \in A$. Заметим, что 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. Если q, m — целые числа, то q-значные бент-функции Кумара, Шольца и Велча от m переменных являются частным случаем данных бент-функций при $A = \mathbb{Z}_q^m$ и $n = q^m$. Для этого необходима лишь небольшая модификация: от функций вида $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ нужно перейти к функциям $f' : \mathbb{Z}_q^m \to T_q \subset \mathbf{C}$, где $f'(x) = \omega^{f(x)}$. А в качестве изоморфизма между A и ее группой характеров $\widehat{A}$ выбрать соответствие $y \to \chi_y(x) = \omega^{\langle x,y\rangle}$, где $\omega = e^{2\pi i/q}$.

В 2005 г. Л. Поинсо [33] предложил многомерное обобщение этих бент-функций. Пусть $\mathbf{C}^m$ — m-мерное унитарное пространство с обычным скалярным произведением

$\langle x, y\rangle = \sum_{j=1}^{m} x_j \overline{y}_j$, нормой $\|x\|^2 = \langle x, x\rangle$ и метрикой $d(x, y) = \|y - x\|$. Пусть $S_1(\mathbf{C}^m)$ — множество его точек, лежащих на сфере радиуса 1 с центром в нуле. *Преобразованием Фурье* функции $f : A \to \mathbf{C}^m$ называется следующая функция из A в $\mathbf{C}^m$: $\widehat{f}(y) = \sum_{x\in A} f(x)\overline{\chi_y(x)}$. Функция $f : A \to S_1(\mathbf{C}^m)$ называется *многомерной бент-функцией*, если $||\widehat{f}(y)||^2 = n$ для каждого $y \in A$. При $m = 1$ данное определение полностью совпадает с определением Логачева, Сальникова и Ященко.

▶ (БЕНТ-ФУНКЦИИ ИЗ КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЫ В ДРУГУЮ КОНЕЧНУЮ АБЕЛЕВУ ГРУППУ, В. И. Солодовников, 2002 [3].) Это наиболее общий подход к алгебраическому обобщению бент-функций. Следует отметить, что в 2004 г. К. Карле и К. Динг [14] повторили результаты В. И. Солодовникова, к сожалению, без ссылки на предшественника. Пусть $(A, +)$ и $(B, +)$ — конечные абелевы группы порядков n и m соответственно, a и b — максимальные порядки элементов в этих группах. Пусть $\widehat{A}$ и $\widehat{B}$ — группы характеров групп A и B. Зафиксируем изоморфизмы $y \to \chi_y$ и $z \to \eta_z$ между A и $\widehat{A}$, B и $\widehat{B}$ соответственно, где $\chi_y : A \to T_a$ и $\eta_z : B \to T_b$ — характеры. Пусть $f : A \to B$ — произвольная функция. Следующие определения из [3] приведем в несколько иной форме (введем нормировочные множители), не искажая при этом их смысл. *Преобразованием Фурье характера функции* f при фиксированном $z \in B$ называется функция $\widehat{f}_z(y) = \sum_{x\in A} \eta_z(f(x))\overline{\chi_y(x)}$, где $y \in A$. При любом z выполняется равенство Парсеваля $\sum_{y\in A} |\widehat{f}_z(y)|^2 = n^2$.

Функция $f : A \to B$ называется *бент-функцией*, если для любого $z \in B$, $z \neq 0$ и произвольного $y \in A$ справедливо $|\widehat{f}_z(y)|^2 = n$. Заметим, что функция $f : A \to B$ является бент-функцией тогда и только тогда, когда при каждом $z \neq 0$ функция $\eta_z \circ f$ — бент-функция в смысле Логачева, Сальникова и Ященко[2].

▶ (ВЕКТОРНЫЕ G-БЕНТ-ФУНКЦИИ, Л. Поинсо и С. Харари, 2004 [34].) Идея этого обобщения для функций вида $f : A \to B$ впервые была предложена В. И. Солодовниковым в работе [3] 2002 г. Л. Поинсо и С. Харари подробно ее рассмотрели для случая $A = (\mathbb{Z}_2^k, +)$ и $B = (\mathbb{Z}_2^r, +)$, т. е. векторных булевых функций. Основу обобщения составляет возможность иначе определить производную функции $f : A \to B$.

А именно, пусть $S(A)$ — симметрическая группа A в мультипликативной записи. Перестановка $\sigma \in S(A)$ называется *инволюцией*, если $\sigma\sigma = e$, где e — тождественная перестановка. Перестановка σ *без неподвижных точек*, если для любого $x \in A$ справедливо $\sigma(x) \neq x$. Множество всех инволюций σ без неподвижных точек обозначим через $Inv(A)$. Подгруппа G группы $S(A)$, такая, что $G \subseteq Inv(A) \cup \{e\}$, называется *группой инволюций группы* A. Пусть $A = \mathbb{Z}_2^k$, $B = \mathbb{Z}_2^r$. Любая группа инволюций G группы $\mathbb{Z}_2^k$ является абелевой и $|G| \leqslant 2^k$. Будем рассматривать только группы G максимального порядка 2^k. Пусть $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^r$, G — максимальная группа инволюций группы $\mathbb{Z}_2^k$. *Обобщенной производной* f *по направлению* $\sigma \in G$ называется функция $D_\sigma f(x) = f(\sigma(x)) - f(x)$. Отметим, что если G — группа трансляций (т. е. состоящая из всех перестановок σ_y, $y \in \mathbb{Z}_2^k$, таких, что $\sigma_y(x) = x + y$), то обобщенная производная совпадает с обычной, $D_y f(x) = f(x + y) - f(x)$.

Функция $f : A \to B$ называется G*-бент-функцией*, если обобщенная производная $D_\sigma f(x)$ по каждому направлению $\sigma \in G$ для $\sigma \neq e$ уравновешена.

[2]Здесь запись $g \circ f(x)$ означает функцию $g(f(x))$.

7. Комбинаторные обобщения бент-функций

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

▶ (ЧАСТИЧНО ОПРЕДЕЛЕННЫЕ БЕНТ-ФУНКЦИИ.) Пусть $S \subseteq \mathbb{Z}_2^n$ — произвольное подмножество, $f : S \to \mathbb{Z}_2$ — *частично определенная булева функция*. Ее *неполным преобразованием Уолша—Адамара* называется отображение $W_{f,S}(y) = \sum_{x \in S}(-1)^{\langle x,y\rangle + f(x)}$, $y \in \mathbb{Z}_2^n$. Справедлив аналог равенства Парсеваля: $\sum_{y \in \mathbb{Z}_2^n} W_{f,S}^2(y) = 2^n |S|$. Булева функция f называется *частично определенной бент-функцией*, если $W_{f,S}(y) = \pm\sqrt{|S|}$ для любого $y \in \mathbb{Z}_2^n$. Отметим, что условия на множество S, при которых частично определенные бент-функции существуют, пока не известны.

▶ (ПЛАТОВИДНЫЕ ФУНКЦИИ.) Булева функция называется *платовидной*, если все ее ненулевые коэффициенты Уолша—Адамара равны по модулю. Из равенства Парсеваля следует, что ненулевые коэффициенты должны иметь вид $\pm 2^{n-h}$ для некоторого целого h, где $0 \leqslant h \leqslant n$. Количество таких ненулевых коэффициентов должно быть равно 2^{2h}. Показатель $2h$ и величину 2^{n-h} называют соответственно *порядком* и *амплитудой* платовидной функции. Бент-функции и аффинные функции являются крайними частными случаями платовидных функций (порядков n и 0 соответственно).

Часто платовидные функции максимального порядка $n - 1$ от нечетного числа переменных называют *почти бент-функциями*. Такие функции интересны для обеспечения защиты от так называемой soft output joint attack на генераторы псевдошумовых последовательностей (PN-generators) [28]. Такие генераторы используются в уже упоминавшемся выше стандарте IS–95 технологии CDMA. Почти бент-функции используются также для построения криптографически стойких S-блоков [18].

▶ ($\mathbb{Z}$-БЕНТ-ФУНКЦИИ, Х. Доббертин, 2005 [22].) Не будем различать обычную булеву функцию $f(x)$, где $x \in \mathbb{Z}_2^n$, и целочисленную функцию $F(x) = (-1)^{f(x)}$. *Преобразование Фурье* функции $F : \mathbb{Z}_2^n \to \mathbb{Z}$ определяется как $\widehat{F}(y) = 2^{-n/2} \sum_{x \in \mathbb{Z}_2^n}(-1)^{\langle x,y\rangle} F(x)$. Тогда ± 1-значная функция F является бент-функцией, если и только если $\widehat{F}$ также ± 1-значная. Пусть $T \subseteq \mathbb{Z}$ — любое подмножество. Функция $F : \mathbb{Z}_2^n \to T$ называется *T-бент-функцией*, если все значения функции $\widehat{F}$ принадлежат множеству T. Доббертин выделил естественную цепочку вложенных друг в друга множеств: $T_0 = \{-1, +1\}$; $T_r = \{w \in \mathbb{Z} \mid -2^{r-1} \leqslant w \leqslant 2^{r-1}\}$ (при $r > 0$). T_r-бент-функция называется *$\mathbb{Z}$-бент-функцией уровня r*, а все такие бент-функции (при $r \in \mathbb{Z}$) составляют класс *$\mathbb{Z}$-бент-функций*.

▶ (ОДНОРОДНЫЕ БЕНТ-ФУНКЦИИ (HOMOGENEOUS BENT F.), Ч. Ку, Дж. Себерри и Й. Пипджик, 2000 [35].) Этот подкласс бент-функций был выделен как состоящий из функций с относительно простыми алгебраическими нормальными формами. Бент-функция называется *однородной*, если все одночлены ее алгебраической нормальной формы имеют одинаковые степени. Открытым вопросом является задача определения точной верхней оценки степени нелинейности однородной бент-функции. Пока есть только предположение [30] о том, что для любого $k > 1$ найдется такое $N \geqslant 2$, что однородная бент-функция степени k от n переменных существует при каждом $n > N$.

8. Криптографические обобщения бент-функций

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

▶ (УРАВНОВЕШЕННЫЕ БЕНТ-ФУНКЦИИ.) Известно, что криптографические критерии часто противоречат друг другу. Бент-функции являются максимально-нелинейными, удовлетворяют критерию $PC(n)$, но не являются уравновешенными. Довольно естественно возникает следующее определение.

Булева функция f от n переменных называется *уравновешенной бент-функцией*, если она уравновешена и имеет при этом максимально возможную нелинейность. В 1994 г. С. Чи, С. Ли и К. Ким [17] предложили способ построения уравновешенных бент-функций от нечетного числа переменных, имеющих при этом почти равномерную корреляцию с линейными функциями и удовлетворяющих критерию $PC(k)$ для достаточно большого k.

▶ (ЧАСТИЧНО БЕНТ-ФУНКЦИИ (PARTIALLY BENT F.), К. Карле, 1993 [12].) Бент-функции не являются ни уравновешенными, ни корреляционно-иммунными. К. Карле предложил свой способ расширить класс $\mathfrak{B}_n$ функциями, обладающими данными свойствами и имеющими при этом достаточно высокую нелинейность. Пусть $\Delta_f(y) = \sum\limits_{x\in\mathbb{Z}_2^n} (-1)^{f(x)+f(x+y)}$ — *автокорреляция* булевой функции f по направлению y. Пусть NW_f и $N\Delta_f$ — количества ненулевых коэффициентов Уолша—Адамара и коэффициентов автокорреляции булевой функции f соответственно. Известно, что $NW_f \cdot N\Delta_f \geqslant 2^n$ для любой булевой функции.

Булева функция f, для которой $NW_f \cdot N\Delta_f = 2^n$, называется *частично бент-функцией*.

▶ (ГИПЕРБЕНТ-ФУНКЦИИ (HYPER-BENT FUNCTIONS), А. М. Йоссеф и Г. Гонг, 2001 [40].) Их работе предшествовала статья С. В. Голомба и Г. Гонга [24] 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 [24] предложили использовать для приближения координатных функций S-блоков вместо линейных булевых функций собственные мономиальные функции. Эта идея и была развита в [40].

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 $\mathrm{tr}(a_x y)$ для подходящего элемента $a_x \in \mathbb{F}_{2^n}$, где $\mathrm{tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ — функция следа. Тогда преобразование Уолша—Адамара приобретает следующий, эквивалентный, вид: $W_f(y) = \sum\limits_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(yx)+f(x)}$. Функция вида $\mathrm{tr}(a_x y^s)$, где $1 \leqslant s \leqslant 2^n - 1$ и $\gcd(s, 2^n - 1) = 1$, называется *собственной мономиальной функцией. Расширенное преобразование Уолша—Адамара* булевой функции f имеет вид $W_{f,s}(y) = \sum\limits_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(yx^s)+f(x)}$.

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

▶ (БЕНТ-ФУНКЦИИ БОЛЕЕ ВЫСОКОГО ПОРЯДКА НЕЛИНЕЙНОСТИ.) Это довольно естественное направление, тесно связанное с нелинейными обобщениями различных методов криптоанализа. Известно, что эффективность приближения бент-функции любой линейной функцией является самой низкой. Расширяя класс линейных функций, естественно рассматривать для приближения булевы функции степени не выше r, где $2 \leqslant r \leqslant n - 1$. При этом возникает понятие *нелинейности r-го порядка* $N_r(f)$ булевой функции f как расстояния Хэмминга от f до всех таких функций. Булева функция, удаленная от всех функций степени не выше r на максимальное расстояние, называется *бент-функцией порядка r*. Но трудность заключается в определении

этого максимального возможного значения для $N_r(f)$. При $r \geqslant 2$ это нерешенная задача, более известная в теории кодирования как определение радиуса покрытия кода Рида—Маллера порядка r. Известны пока некоторые оценки для $N_r(f)$, его асимптотическое значение, связь с другими криптографическими параметрами и т. п. Подробнее на эту тему см. обзор К. Карле [13].

► (k-БЕНТ-ФУНКЦИИ, 2007 [4].) Основная идея обобщения — рассмотреть аппроксимирующие функции, отличные от линейных, но являющиеся в каком-то смысле их аналогами. Пусть x, y — двоичные векторы длины n. Пусть k — любое целое число, такое, что $1 \leqslant k \leqslant n/2$. Определим бинарную операцию

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

которая служит нелинейным аналогом скалярного произведения. 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: $\sum_{y\in\mathbb{Z}_2^n}\left(W_f^{(k)}(y)\right)^2 = 2^{2n}$. Булева функция f от n переменных называется *k-бент-функцией*, если для произвольной подстановки $\pi \in S_n$, любого $j = 1, \ldots, k$ и любого вектора y выполняется $W_{f\circ\pi}^{(j)}(y) = \pm 2^{n/2}$.

9. Открытые вопросы

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

Получить аффинную классификацию бент-функций (от 10, 12 и т. д. переменных).

Получить алгебраическую классификацию бент-функций (от 10, 12 и т. д. переменных).

Получить асимптотику числа бент-функций от n переменных.

Улучшить нижнюю и верхнюю оценки числа бент-функций.

Предложить новые конструкции бент-функций, в частности — векторных.

Разработать эффективные алгоритмы порождения бент-функций.

Исследовать взаимосвязи между нелинейностью и другими криптографическими характеристиками булевой функции.

Разработать эффективные методы построения уравновешенных булевых функций с высокой нелинейностью (и др. криптографическими свойствами) из бент-функций.

Исследовать максимально нелинейные функции от нечетного числа переменных.

Исследовать группы автоморфизмов бент-функций.

Исследовать метрическую структуру класса бент-функций.

Получить конструкции оптимальных кодов, кодовые слова которых являются векторами значений бент-функций.

Исследовать взаимосвязи между различными обобщениями бент-функций.

Получить новые конструкции обобщенных бент-функций, исследовать их свойства.

Получить новые эквивалентные представления бент-функций, полнее отражающие содержательную сторону этих объектов.

Предложить более общие подходы к исследованию бент-функций за счет установления взаимосвязей с другими дискретными (и не только) объектами.

Исследовать новые приложения бент-функций в криптографии, теории кодирования и т. д.

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

ЛИТЕРАТУРА

1. *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями // Дискретная математика. 1994. Т 6. № 3. С. 50–60.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Бент-функции на конечной абелевой группе // Дискретная математика. 1997. Т. 9. № 4. С. 3–20.
3. *Солодовников В. И.* Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискретная математика. 2002. Т. 14. № 1. С. 99–113.
4. *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.
5. *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. Т. 2. № 1. С. 15–37. Доступен на `http://mi.mathnet.ru/pdm50`.
6. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискрет. анализ и исслед. операций. 2009. Т. 16.
7. *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Пробл. передачи информации. 1997. Т. 33. Вып. 1. С. 75–86.
8. `http://www.math.cornell.edu/News/AnnRep/AR2002-2003.pdf` — Cornell University. Department of Mathematics. Annual Report 2002–2003.
9. *Agievich S. V.* On the representation of bent functions by bent rectangles // Fifth Int. Petrozavodsk conf. on probabilistic methods in discrete mathematics (Petrozavodsk, Russia, June 1–6, 2000). Proc. Boston: VSP, 2000. P. 121–135. Available at `http://arxiv.org/abs/math/0502087`.
10. *Bernasconi A., Codenotti B.* Spectral analysis of Boolean functions as a graph eigenvalue problem // IEEE Trans. Computers. 1999. V. 48. No. 3. P. 345–351.
11. *Bernasconi A., Codenotti B., VanderKam J. M.* A characterization of bent functions in terms of strongly regular graphs // IEEE Trans. Computers. 2001. V. 50. No. 9. P. 984–985.
12. *Carlet C.* Partially-bent functions // Designs, Codes and Cryptography. 1993. V. 3. No. 2. P. 135–145.
13. *Carlet C.* On the higher order nonlinearities of Boolean functions and S-boxes, and their generalizations // The Fifth Int. Conf. on Sequences and Their Applications — SETA'2008 Proc. (Lexington, Kentucky, USA. September 14–18, 2008). Berlin: Springer, 2008. P. 345–367 (Lecture Notes in Comput. Sci. V. 5203).
14. *Carlet C., Ding C.* Highly nonlinear mappings // J. Complexity. 2004. V. 20. No. 2–3. P. 205–244.
15. *Carlet C., Guillot P.* An alternate characterization of the bentness of binary functions, with uniqueness // Designs, Codes and Cryptography. 1998. V. 14. P. 133–140.
16. *Carlet C., Klapper A.* Upper bounds on the numbers of resilient functions and of bent functions // 23rd Symposium on Information Theory (Benelux, Belgium. May, 2002). Proc. 2002. P. 307–314. The full version will appear in Lecture Notes dedicated to Philippe Delsarte. Available at `http://www.cs.engr.uky.edu/~klapper/ps/bent.ps`.
17. *Chee S., Lee S., Kim K.* Semi-bent Functions // Advances in Cryptology — ASIACRYPT '94 — 4th International Conference on the Theory and Applications of Cryptology. (Wollongong, Australia. November 28 – December 1, 1994). Proc. Berlin: Springer, 1995. P. 107–118 (Lecture Notes in Comput. Sci. V. 917).
18. *Detombe J., Tavares S.* Constructing large cryptographically strong S-boxes // Advances in Cryptology — AUSCRYPT'92. (Gold Coast, Queensland, Australia. December 13–16, 1992) Proc. Berlin: Springer, 1993. P. 165–181 (Lecture Notes in Comput. Sci. V. 718).
19. *Dillon J. F.* A survey of bent functions // The NSA Technical J. 1972. Special Issue. P. 191–215.

20. *Dillon J. F.* Elementary Hadamard Difference sets // Ph. D. Thesis. Univ. of Maryland, 1974.
21. *Dobbertin H., Leander G.* A survey of some recent results on bent functions // Sequences and their applications. – SETA 2004. Third Int. conference (Seoul, Korea, October 24–28, 2004). Revised selected papers. Berlin: Springer, 2005. P. 1–29 (Lecture Notes in Comput. Sci. V. 3486).
22. *Dobbertin H., Leander G.* Cryptographer's Toolkit for Construction of 8-Bit Bent Functions // Cryptology ePrint Archive, Report 2005/089, available at `http://eprint.iacr.org/`.
23. *Dobbertin H., Leander G., Canteaut A., et al.* Construction of Bent Functions via Niho Power Functions // J. Combin. Theory. Ser. A. 2006. V. 113. No. 5. P. 779–798. Available at `http://www-rocq.inria.fr/secret/Anne.Canteaut/Publications/index-pub.html`.
24. *Gong G., Golomb S. W.* Transform Domain Analysis of DES // IEEE Trans. Inform. Theory. 1999. V. 45. No. 6. P. 2065–2073.
25. *Kumar P. V., Scholtz R. A., Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory. Ser. A. 1985. V. 40. No. 1. P. 90–107.
26. `http://langevin.univ-tln.fr/project/quartics/` — Classification of Boolean Quartics Forms in eight Variables (Langevin P.). 2008.
27. *Langevin P., Leander G.* Counting all bent functions in dimension 8 // Workshop on Coding and Cryptograpy. 2009. to appear.
28. *Leveiller S., Zemor G., Guillot P., and Boutros J.* A new cryptanalytic attack for PN-generators filtered by a Boolean function // Selected Areas of Cryptography — SAC 2002. Proc. P. 232–249 (Lecture Notes in Comput. Sci. V. 2595).
29. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
30. *Meng Q., Zhang H., Yang M. C., Cui J.* On the degree of homogeneous bent functions // Available at `http://eprint.iacr.org`, 2004/284.
31. *Nyberg K.* Perfect nonlinear S-boxes // Advances in cryptology — EUROCRYPT'1991. Int. conference on the theory and application of cryptographic techniques (Brighton, UK, April 8–11, 1991). Proc. Berlin: Springer, 1991. P. 378–386 (Lecture Notes in Comput. Sci. V. 547).
32. *Olejár D., Stanek M.* On cryptographic properties of random Boolean functions // J. Universal Computer Science. 1998. V. 4. No. 8. P. 705–717.
33. *Poinsot L.* Multidimensional bent functions // GESTS International Transactions on Computer Science and Engeneering. 2005. V. 18. No. 1 P. 185–195.
34. *Poinsot L., Harari S.* Generalized Boolean bent functions // Progress in Cryptology — Indocrypt 2004 (Chennai (Madras), India. December 20 – 22, 2004). Proc. Springer. P. 107–119 (Lecture Notes in Comput. Sci. V. 3348).
35. *Qu C., Seberry J., Pieprzyk J.* Homogeneous bent functions // Discrete Appl. Math. 2000. V. 102. No. 1–2. P. 133–139.
36. *Rothaus O.* On bent functions // IDA CRD W. P. 1966. No. 169.
37. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
38. *Schmidt K-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // IEEE International Symposium on Information Theory — ISIT'2007. (Nice, France. June 24–29, 2007). Proc. 2007. P. 2781–2785. Available at `http://arxiv.org/abs/cs.IT/0611162`.
39. *Yang M., Meng Q., Zhang H.* Evolutionary design of trace form bent functions // Cryptology ePrint Archive, Report 2005/322, available at `http://eprint.iacr.org/`.
40. *Youssef A., Gong G.* Hyper-bent functions // Advances in cryptology — EUROCRYPT'2001. Int. conference on the theory and application of cryptographic techniques (Innsbruk, Austria, May 6–10, 2001). Proc. Berlin: Springer, 2001. P. 406–419 (Lecture Notes in Comput. Sci. V. 2045).