2009 Теоретические основы прикладной дискретной математики №1(3)
DOI 10.17223/20710410/3/2
УДК 519.7

БЕНТ-ФУНКЦИИ: РЕЗУЛЬТАТЫ И ПРИЛОЖЕНИЯ. ОБЗОР РАБОТ[1]

Н. Н. Токарева

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

E-mail: tokareva@math.nsc.ru

Приводится краткий обзор основных результатов в области бент-функций. Рассматриваются их теоретические и практические приложения.

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

Введение

Данный обзор посвящен результатам в области бент-функций и их приложениям. Логическим продолжением этой работы следует считать обзор [16], в котором будут рассмотрены различные обобщения бент-функций и история их возникновения.

Мера нелинейности является важной характеристикой булевой функции. Линейность часто свидетельствует о простой (в определенном смысле) структуре этой функции и, как правило, представляет собой богатый источник информации о многих других ее свойствах. Задача построения булевых функций, обладающих нелинейными свойствами, естественным образом возникает во многих областях дискретной математики. И часто (что является типичной ситуацией в математике) наибольший интерес вызывают те функции, для которых эти свойства экстремальны. Такие булевы функции называются *максимально нелинейными* или *бент-функциями*.

Первой работой, посвященной бент-функциям, принято считать статью О. Ротхауса 1976 г. [110], хотя эти специальные булевы функции были введены им еще в 60-х годах XX века [109]. В настоящее время можно говорить уже о *теории бент-функций*.

Приведем ряд определений и обозначений. Пусть

$\oplus$ — сложение по модулю 2 (или XOR);

n — натуральное число;

$\boldsymbol{v} = (v_1, \ldots, v_n)$ — двоичный вектор;

$\mathbb{Z}_2^n$ — множество всех двоичных векторов длины n;

$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = u_1 v_1 \oplus \ldots \oplus u_n v_n$ — 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 $\boldsymbol{g}$.

Известно, что каждая булева функция однозначно может быть задана своей *алгебраической нормальной формой* (АНФ), а именно представлена в виде

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

[1]Исследование выполнено при финансовой поддержке интеграционного проекта СО РАН № 35 «Древовидный каталог математических интернет-ресурсов mathtree.ru», РФФИ (проекты 07-01-00248, 08-01-00671, 09-01-00528-а) и Фонда содействия отечественной науке.

где при каждом k индексы $i_1, \ldots, i_k$ различны и в совокупности пробегают все k-элементные подмножества множества $\{1, \ldots, n\}$. Коэффициенты $a_{i_1,\ldots,i_k}$, a_0 принимают значения 0 или 1. В русскоязычной литературе АНФ также называют *полиномом Жегалкина*. Напомним, что *степень нелинейности* $\deg(f)$ булевой функции f — это число переменных в самом длинном слагаемом ее АНФ. Функция называется *аффинной*, *квадратичной*, *кубической* и т. д., если ее степень равна соответственно 1, 2, 3 и т. д. Каждая аффинная функция от n переменных $v_1, \ldots, v_n$ имеет вид $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \oplus a$ для подходящих вектора $\boldsymbol{u}$ и константы a.

Максимально нелинейной называется булева функция от n переменных (n любое) такая, что расстояние Хэмминга N_f от данной функции до множества всех аффинных функций является максимально возможным. Величину N_f называют *нелинейностью* булевой функции. В случае четного n максимально возможное значение нелинейности равно $2^{n-1} - 2^{(n/2)-1}$. В случае нечетного n точное значение максимального расстояния неизвестно (поиск этого значения или его оценок представляет весьма любопытную и сложную комбинаторную задачу [89, 78]). Термин «максимально нелинейная функция» принят в русскоязычной литературе, тогда как в англоязычной широкое распространение получил термин «бент-функция» (от англ. bent — изогнутый, наклоненный). Аналогия между терминами не полная. При четном числе переменных n бент-функции и максимально нелинейные функции совпадают, а при нечетном n бент-функции (в отличие от максимально нелинейных) не существуют.

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

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

Справедливо равенство Парсеваля, $\sum\limits_{\boldsymbol{v} \in \mathbb{Z}_2^n} \left(W_f(\boldsymbol{v})\right)^2 = 2^{2n}$. Поскольку число всех коэффициентов $W_f(\boldsymbol{v})$ равно 2^n, из равенства следует, что максимум модуля коэффициента Уолша—Адамара не может быть меньше величины $2^{n/2}$.

Нелинейность N_f произвольной функции f тесно связана с ее коэффициентами Уолша—Адамара, а именно $N_f = 2^{n-1} - \frac{1}{2} \max\limits_{\boldsymbol{v} \in \mathbb{Z}_2^n} |W_f(\boldsymbol{v})|$. Очевидно, что чем меньше максимум модуля коэффициента $W_f(\boldsymbol{v})$, тем выше нелинейность функции f.

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

1. Приложения

Впечатляют масштабы исследования бент-функций. В настоящее время несколько сотен математиков и инженеров по всему миру регулярно публикуют свои статьи по этой тематике. Результаты обсуждаются на таких международных конференциях, как EUROCRYPT, CRYPTO, ASIACRYPT, INDOCRYPT, SETA, FSE, AAECC, ISIT, ITW, BFCA, ACCT, SIBECRYPT, МаБИТ и многих других. Счет общего числа публикаций о бент-функциях (и близких вопросах) идет на тысячи. К сожалению, публикаций на русском языке известно не так уж много — всего несколько десятков.

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

Классическая комбинаторная задача построения *матриц Адамара* порядка N, известная с 1893 г., в случае $N = 2^n$ (n четно) при некоторых ограничениях сводится к задаче построения бент-функций от n переменных [110] (см. далее теорему 1).

В теории конечных групп построение *элементарных адамаровых разностных множеств* специального вида эквивалентно построению максимально нелинейных булевых функций (см. [8] и теорему 5).

В теории кодирования широко известна задача определения радиуса покрытия произвольного *кода Рида—Маллера*, которая эквивалентна (в случае кодов первого порядка) поиску наиболее нелинейных булевых функций [78, 89]. В теории оптимальных кодов специальные семейства квадратичных бент-функций определяют класс *кодов Кердока* [79], обладающих исключительным свойством: вместе с растущим кодовым расстоянием (при увеличении длины кода) каждый код Кердока имеет максимально возможную мощность (см. [13, 59]). Этим свойством коды Кердока «обязаны» экстремальной нелинейности бент-функций. Отметим, что задача построения таких семейств бент-функций, задающих код Кердока, несложно переводится в задачу поиска *ортогональных расщеплений* (orthogonal spreads) в конечном векторном пространстве [77], что представляется элегантным примером связи бент-функций с экстремальными геометрическими объектами. Другим примером из теории кодирования служат так называемые *бент-коды* — линейные двоичные коды, каждый из которых определенным образом строится из некоторой бент-функции [40]. В принципе, тем же способом можно строить линейные коды из любых булевых функций, но только бент-коды имеют максимально возможные кодовые размерности.

Семейства *бент-последовательностей* из элементов $+1$ и -1, построенные на основе бент-функций, имеют предельно низкие значения как взаимной корреляции, так и автокорреляции (достигают нижней границы Велча) [99]. Поэтому такие семейства успешно применяются в коммуникационных системах коллективного доступа [102]. Генераторы бент-последовательностей легко инициализируются случайным образом и могут быстро перестраиваться с одной последовательности на другую. Этот факт используется в работе со стандартом CDMA — Code Division Multiple Access (множественный доступ с кодовым разделением каналов) — одним из двух стандартов для цифровых сетей сотовой связи в США. Отметим здесь же, что в системах CDMA для предельного снижения отношения пиковой и средней мощностей сигнала (peak-to-average power ratio) используются так называемые *коды постоянной амплитуды* (constant-amplitude codes). И например, четверичные такие коды можно построить с помощью обобщенных булевых бент-функций [111]. Не обходится без бент-функций или их аналогов и в квантовой теории информации (см., например, [106]).

Бент-функцию можно определить как функцию, которая крайне плохо аппроксимируется аффинными функциями. Это базовое свойство бент-функций используется в криптографии. В блочных и поточных шифрах бент-функции и их векторные аналоги способствуют предельному повышению стойкости этих шифров к линейному [90] и дифференциальному [28] методам криптоанализа. Стойкость достигается за счет использования сильно нелинейных булевых функций в S-блоках (важнейших компонентах современных шифров) [21, 96] (см., например, шифр CAST [49]). Бент-функции

и их обобщения находят свое применение также в схемах аутентификации [45], хэш-функциях и псевдослучайных генераторах [10].

Широко исследуются различные обобщения, подклассы и надклассы бент-функций, такие, как *платовидные функции* [8], *частично бент-функции* [8], *частично определенные бент-функции* [8], *q-значные бент-функции* [2, 83], *обобщенные булевы бент-функции* [111], *полу-бент-функции* [53], *бент-функции на конечной абелевой группе* [6, 14, 44], *однородные бент-функции* [105], *гипер-бент-функции* [114], *$\mathbb{Z}$-бент-функции* [68], *нега-бент-функции* [101], *k-бент-функции* [15] и др. С одной стороны, эти исследования мотивированы высокой сложностью задачи описания бент-функций и являются попытками перехода к более общим (или более частным) ее постановкам — в надежде на частичное решение основной проблемы. С другой стороны, интерес к обобщениям постоянно стимулируется новыми запросами со стороны приложений.

Обзоры некоторых результатов о бент-функциях можно найти в замечательной российской монографии 2004 г. О. А. Логачева, А. А. Сальникова и В. В. Ященко [8], статье немецких криптографов Х. Доббертина и Г. Леандера [67] 2004 г., главах [40, 41] французского математика и криптографа К. Карле, написанных для готовящейся к печати книги «Boolean Methods and Models» (2008 г.). См. также более ранние работы Ю. В. Кузнецова и С. А. Шкарина [4] 1996 г., Дж. Ф. Диллона [62] 1972 г. и др. Обобщениям бент-функций будет посвящен отдельный обзор автора [16].

Однако любой обзор в этой области очень быстро устаревает и a priori неполон.

2. Результаты

Бент-функции, как уже упоминалось выше, были введены О. Ротхаусом еще в 60-х годах XX века. В работе [110] были установлены базовые свойства таких функций и предложены их простейшие конструкции. Дж. Диллон [62] и Р. Л. МакФарланд [91] рассматривали бент-функции в связи с разностными множествами. В настоящее время известны серии конструкций бент-функций, но тем не менее класс всех бент-функций от n переменных (обозначим его через $\mathfrak{B}_n$) до сих пор не описан, для мощности этого класса не найдена асимптотика и не установлено даже приемлемых нижних и верхних оценок. Известным результатам и открытым вопросам в области бент-функций посвящен этот раздел.

2.1. Критерии и свойства

Всюду далее n предполагается четным числом.

Напомним, что *матрицей Адамара* называется квадратная $k \times k$-матрица A с элементами ± 1, такая, что $AA^T = kE$, где E — единичная матрица. Строки и столбцы матрицы размера $2^n \times 2^n$ занумеруем векторами $\boldsymbol{u}, \boldsymbol{v}$ длины n. Справедлива [110]

Теорема 1. Следующие утверждения эквивалентны:

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

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

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

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

Пункт (iv) теоремы носит название *критерия распространения* $\mathrm{PC}(n)$ *порядка* n. В качестве важного свойства бент-функций можно отметить следующий факт [110], согласно [5] полученный В. А. Елисеевым и О. П. Степченковым еще в 1962 г.

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

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

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

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

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

Согласно [52] (см. [9, 62]), выполняется

Теорема 3. Любая квадратичная бент-функция от n переменных аффинно эквивалентна функции (1).

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

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

В силу теоремы 4 имеет смысл вопрос об аффинной классификации бент-функций, который для функций степени $\geqslant 3$ пока остается открытым. Подробнее о методах аффинной и линейной классификации булевых функций можно прочитать в [18].

Часто с бент-функцией f связывают так называемую *дуальную булеву функцию* $\widetilde{f}$ от n переменных, которая определяется равенством $W_f(\boldsymbol{v}) = 2^{n/2}(-1)^{\widetilde{f}(\boldsymbol{v})}$. Определение корректно, поскольку $W_f(\boldsymbol{v}) = \pm 2^{n/2}$ для каждого вектора $\boldsymbol{v}$. Несложно доказать, что булева функция $\widetilde{f}$ является бент-функцией. Справедливо $\widetilde{\widetilde{f}} = f$. Отметим, что если $\deg(f) = n/2$, то степень $\widetilde{f}$ также максимальна: $\deg(\widetilde{f}) = n/2$. Самодуальные бент-функции, т. е. такие, что $f = \widetilde{f}$, изучались в [43].

Дуальные бент-функции потребуются далее в теореме 14.

2.2. Характеризации бент-функций

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

С самого начала бент-функции изучались в связи с разностными множествами [62]. Пусть конечная абелева группа G имеет порядок v и дана в аддитивной записи. Подмножество $D \subseteq G$ мощности k называется *разностным множеством* с параметрами (v, k, λ), если каждый ненулевой элемент $g \in G$ можно представить в виде $g = b - d$ ровно λ способами, где b, d — элементы множества D. Справедлива [62]

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

Разностные множества с приведенными в теореме 5 параметрами называются *элементарными адамаровыми*. Примеры таких множеств были известны еще до появления бент-функций [62].

Известно [17], что разностные множества тесно связаны с блок-схемами. Напомним, что *блок-схемой* с параметрами (v, k, λ) называется система k-элементных подмножеств (или *блоков*) v-элементного множества, такая, что каждая пара различных

элементов содержится ровно в λ блоках. Блок-схема *симметрична*, если число блоков равно числу элементов, т. е. равно v. Теорема 5 имеет следующий эквивалентный вид.

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

В. В. Ященко [19] в 1997 г. предложил следующее описание класса бент-функций. В его основе лежит тот факт, что любая булева функция f от n переменных может быть представлена в виде *линейного разветвления*

$$f(\boldsymbol{u'}, \boldsymbol{u''}) = \langle \boldsymbol{u'}, h(\boldsymbol{u''}) \rangle \oplus g(\boldsymbol{u''}), \text{ где } \boldsymbol{u'} \in \mathbb{Z}_2^r, \boldsymbol{u''} \in \mathbb{Z}_2^k \tag{2}$$

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

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

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

Теорема 7. Булева функция f вида (2) является бент-функцией тогда и только тогда, когда $n > 2r$ и для любого вектора $\boldsymbol{u'} \in \mathbb{Z}_2^r$ выполняются условия:
(i) мощность множества $h^{-1}(\boldsymbol{u'})$ равна 2^{n-2r};
(ii) множество $h^{-1}(\boldsymbol{u'})$ является бент-множеством;
(iii) пара $(g; h^{-1}(\boldsymbol{u'}))$ является частичной бент-функцией.

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

Приведем геометрическое описание класса бент-функций, которое предложили в 1998 г. К. Карле и Ф. Гуилло [47] (см. также более раннюю работу [46]).

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

Теорема 8. Функция f является бент-функцией тогда и только тогда, когда существуют подпространства $E_1, \ldots, E_k$ размерности $n/2$ или $(n/2)+1$ пространства $\mathbb{Z}_2^n$ и ненулевые целые числа $m_1, \ldots, m_k$, такие, что для любого $\boldsymbol{v} \in \mathbb{Z}_2^n$ выполняется

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

Авторы [47] вводят ограничения на способ выбора пространств $E_1, \ldots, E_k$, при которых такой выбор становится единственным для каждой бент-функции. Таким образом, можно говорить об однозначности такого представления.

Другой подход предложили в 1999 г. А. Бернаскони и Б. Коденотти [26], затем к ним присоединился и Дж. Ван-дер-Кам [27].

Пусть f — булева функция от n переменных. Через $\mathrm{supp}(f)$ обозначим ее *носитель*, т. е. множество всех двоичных векторов длины n, на которых функция f принимает

значение 1. Рассмотрим *граф Кэли* $G_f = G(\mathbb{Z}_2^n, \mathrm{supp}(f))$ булевой функции f. Вершинами графа являются все векторы длины n. Две вершины $\boldsymbol{u}$, $\boldsymbol{v}$ соединяются ребром, если вектор $\boldsymbol{u} \oplus \boldsymbol{v}$ принадлежит множеству $\mathrm{supp}(f)$.

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. В работе [27] доказана

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

С. В. Агиевич в 2000 г. [22] установил биекцию между множеством всех бент-функций от n переменных и множеством *бент-прямоугольников*.

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

Матрица размера $2^r \times 2^k$ называется *бент-прямоугольником*, если каждая ее строка и каждый столбец, домноженный на $2^{r-(n/2)}$, являются спектральными векторами для подходящих булевых функций. Согласно [22], выполняется

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

Данный подход позволил [22] дать описание всех бент-функций от шести переменных (см. далее) и получить алгоритм построения специального класса бент-функций от произвольного числа переменных n. В работе [24] С. В. Агиевич исследует соответствие между бент-прямоугольниками и регулярными q-значными бент-функциями [83], описывает аффинные трансформации первых и переводит на язык бент-прямоугольников основные конструкции бент-функций. Дальнейшее развитие этого подхода представляется весьма перспективным.

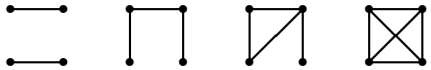
Здесь перечислены лишь некоторые возможные характеризации бент-функций.

2.3. Бент-функции от малого числа переменных

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

$n = 2$. Функция $v_1 v_2$ является представителем единственного класса аффинной эквивалентности. Класс $\mathfrak{B}_2$ состоит из восьми функций. Это все функции, векторы значений которых содержат нечетное число единиц.

$n = 4$. Множество $\mathfrak{B}_4$ состоит из 896 булевых функций, причем каждая функция является квадратичной. Все бент-функции от четырех переменных аффинно эквивалентны функции $v_1 v_2 \oplus v_3 v_4$. Множество $\mathfrak{B}_4$ можно разделить на 28 классов по 32 функции. Алгебраические нормальные формы функций из каждого класса обладают одинаковой квадратичной частью, произвольной линейной частью и любым свободным членом. Если рассмотреть граф на множестве переменных, а ребрами соединить те вершины, которые образуют слагаемое в квадратичной части АНФ функции, то эти 28 типов можно задать следующим образом:



(3) (12) (12) (1)

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

$n = 6$. Аффинная классификация бент-функций от 6 переменных была получена еще в работе О. Ротхауса [110]: множество $\mathfrak{B}_6$ состоит из четырех классов аффинной эквивалентности, представителями которых являются следующие функции:

$v_1v_2 \oplus v_3v_4 \oplus v_5v_6$,

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

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

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

В работе [113] приводится подобная алгебраическая классификация. Пусть $GF(2^6) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{62}\}$, где α — корень многочлена $x^6 + x + 1$. Пусть булева функция отождествляется с функцией $f(\boldsymbol{v}) : GF(2^6) \to GF(2)$, где $\boldsymbol{v}$ рассматривается как элемент поля $GF(2^6)$. Тогда в качестве представителей классов аффинной эквивалентности множества $\mathfrak{B}_6$ можно выбрать функции: $\mathrm{tr}(\boldsymbol{v}^3 + \alpha^5\boldsymbol{v}^5)$, $\mathrm{tr}(\alpha^3\boldsymbol{v}^7 + \boldsymbol{v}^9)$, $\mathrm{tr}(\alpha\boldsymbol{v}^3 + \alpha^6\boldsymbol{v}^7 + \alpha^{60}\boldsymbol{v}^{13})$, $\mathrm{tr}(\boldsymbol{v}^7 + \alpha\boldsymbol{v}^9 + \boldsymbol{v}^{21})$, где tr — функция следа из $GF(2^6)$ в $GF(2)$.

Дж. Диллоном [62] (см. также [30]) было показано, что любая бент-функция от шести переменных аффинно эквивалентна функции из класса Мэйорана—МакФарланда (см. далее теорему 16).

Класс $\mathfrak{B}_6$ содержит $5\,425\,430\,528 \simeq 2^{32,3}$ функций. Описание было дано С. В. Агиевичем [22] с использованием бент-квадратов, т. е. бент-прямоугольников при $r = k$ (см. теорему 10). Скажем, что две бент-функции *квадратно-эквивалентны*, если бент-квадрат одной из них может быть получен из бент-квадрата второй изменением знаков элементов и перестановкой строк и столбцов. Пусть $r = k = 3$. Все функции класса $\mathfrak{B}_6$ разбиваются на восемь классов квадратной эквивалентности. Ниже приводятся соответствующие бент-квадраты размера $2^3 \times 2^3$ и количество функций в каждом классе.

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

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

Отметим, что мощность $\mathfrak{B}_6$ была найдена раньше в диссертации Б. Пренела [104]. В 2004 г. авторы [92] перечислили функции класса $\mathfrak{B}_6$ способом, отличным от приведенного в [22].

$n = 8$. Аффинная классификация бент-функций от восьми переменных степени не выше 3 была получена в работах [30, 74] (см. также работу [23], посвященную кубическим бент-функциям специального вида). Бент-функции от восьми переменных степени не выше 3 делятся на 10 классов аффинной эквивалентности, представителями которых являются:

$v_1v_2 \oplus v_3v_4 \oplus v_5v_6 \oplus v_7v_8$,
$v_1v_2v_3 \oplus v_1v_4 \oplus v_2v_5 \oplus v_3v_6 \oplus v_7v_8$,
$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4 \oplus v_2v_6 \oplus v_1v_7 \oplus v_5v_8$,
$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_1v_3 \oplus v_1v_5 \oplus v_2v_6 \oplus v_3v_4 \oplus v_7v_8$,
$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_2v_6 \oplus v_2v_5 \oplus v_1v_7 \oplus v_4v_8$,
$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_7 \oplus v_6v_8$,
$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_2v_6 \oplus v_2v_5 \oplus v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_7v_8$,
$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_3v_5 \oplus v_1v_6 \oplus v_2v_7 \oplus v_4v_8$,
$v_1v_2v_7 \oplus v_3v_4v_7 \oplus v_5v_6v_7 \oplus v_1v_4 \oplus v_3v_6 \oplus v_2v_5 \oplus v_4v_5 \oplus v_7v_8$,
$v_1v_2v_3 \oplus v_2v_4v_5 \oplus v_3v_4v_6 \oplus v_1v_4v_7 \oplus v_3v_5 \oplus v_2v_7 \oplus v_1v_5 \oplus v_1v_6 \oplus v_4v_8$.

В диссертации [30] также показано, что все эти функции аффинно эквивалентны функциям из класса Мэйорана—МакФарланда.

Нижняя $2^{70,4}$ и верхняя $2^{129,2}$ оценки числа всех функций в классе $\mathfrak{B}_8$ были получены соответственно в [22] и [86]. Некоторые результаты по частичному описанию класса $\mathfrak{B}_8$ на основе исследования групп автоморфизмов бент-функций приводит У. Демпвольф в работах [60, 61]. М. Янг, К. Менг и Х. Жанг [113] показали, что множество $\mathfrak{B}_8$ состоит не менее чем из 129 классов аффинной эквивалентности. Представители всех найденных ими классов приводятся в их работе. Это 53 функции вида $\mathrm{tr}(\alpha^i \boldsymbol{v}^{d_1} + \alpha^j \boldsymbol{v}^{d_2} + \alpha^k \boldsymbol{v}^{d_3})$ и 76 функций вида $\mathrm{tr}(\alpha^i \boldsymbol{v}^{d_1} + \alpha^j \boldsymbol{v}^{d_2} + \alpha^k \boldsymbol{v}^{d_3} + \alpha^\ell \boldsymbol{v}^{d_4})$, где $\mathrm{tr} : GF(2^8) \to GF(2)$ — функция следа. Авторы [72] показали, что множество $\mathfrak{B}_8 \cap \mathcal{PS}$ содержит функции из не менее чем шести классов аффинной эквивалентности, где $\mathcal{PS}$ — класс бент-функций, полученных методом частичного расщепления (см. далее теорему 18).

По последним данным (2009) аффинная классификация бент-функций от восьми переменных четвертой степени завершена [84]. Описаны все 536 возможных вариантов для части четвертой степени[2] АНФ бент-функции от восьми переменных. Установлено точное число всех бент-функций от восьми переменных [84]. Оно равно
$2^9 \times 193\,887\,869\,660\,028\,067\,003\,488\,010\,240 \simeq 2^{106,29}$.

При $n \geqslant 10$ класс $\mathfrak{B}_n$ не описан, его мощность неизвестна. В работе [113] построено большое число бент-функций от десяти переменных; установлено, что среди них содержится как минимум несколько сотен попарно аффинно неэквивалентных функций. Некоторую информацию о классах $\mathfrak{B}_{10}$, $\mathfrak{B}_{12}$ можно найти на сайте [61].

2.4. Оценки числа бент-функций

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

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

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

Асимптотически, эта оценка имеет вид $(\frac{2^{(n/2)+1}}{e})^{2^{n/2}}\sqrt{2^{(n/2)+1}\pi}$, или, если совсем грубо, $2^{2^{n/2}}$. Следует отметить, что в работе [22] приводится уточнение оценки теоремы 11, являющееся на данный момент лучшим. Однако охарактеризовать асимптотическое поведение оценки [22] достаточно трудно.

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

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

К. Карле и А. Клаппер в 2002 г. [48] немного улучшили эту оценку:

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

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

Однако по-прежнему верхняя оценка близка к тривиальной 2^{2^n}. Верхняя оценка обсуждается также в работе [112].

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

Например, для совершенных двоичных кодов длины $n = 2^s - 1$ с расстоянием 3 (см. определение в [9]). Нижнюю оценку вида $2^{2^{n/2}}$ дает конструкция Ю. Л. Васильева 1962 г. [3], и с ней схожа, на мой взгляд, конструкция Мэйорана—МакФарланда для бент-функций; схожа по своей простоте и изяществу, и той роли основного, базового класса, которую играет в множестве бент-функций. А тип верхней оценки числа совершенных кодов по-прежнему остается тривиальным: 2^{2^n}. Небольшие улучшения нижней и верхней оценок приводятся соответственно в [82] и [1].

2.5. Конструкции бент-функций

Очень сложно не только классифицировать бент-функции, но и предложить отдельные способы их построения. В этом разделе мы следуем в основном работе [40] К. Карле, в которой всевозможные конструкции бент-функций представлены наиболее полно. Конструкции принято делить на *первичные* (primary) и *вторичные* (secondary). К первой группе относят те, с помощью которых бент-функции строятся напрямую, ко второй группе — конструкции, опирающиеся на уже известные бент-функции (например, от меньшего числа переменных).

Ко вторичным конструкциям относится простая *итеративная конструкция* [110].

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

Конструкция легко может быть описана в терминах бент-прямоугольников [24]. Приведем следующее обобщение этой простой конструкции, полученное в [37].

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

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

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

Заметим, что теорема 13 следует из теоремы 14. Итеративный способ построения бент-функций от $n+2$ переменных из бент-функций от n переменных приводится в [56]. В качестве упражнения можно доказать следующий факт (см. [75]).

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

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

К первичным конструкциям принадлежит простая и богатая *конструкция Мэйорана—МакФарланда* 1973 г. [63, 91].

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

Основной идеей конструкции служит, по выражению К. Карле [40], «конкатенация аффинных функций». Действительно, при каждом фиксированном значении переменных из второй половины функция f является аффинной от $n/2$ первых переменных. С другой стороны, аффинные функции возникают и при рассмотрении соответствующих бент-квадратов. А именно, бент-функция принадлежит классу Мэйорана—МакФарланда, если и только если строки и столбцы ее бент-квадрата являются спектральными векторами аффинных булевых функций [22].

Из теоремы легко следует, что существуют бент-функции с любой степенью нелинейности d, такой, что $2 \leqslant d \leqslant n/2$. Итак, в теореме 16 переменные функции f разбиваются пополам. В 2004 г. К. Карле [39] (см. также [40]) обобщил идею Мэйорана—МакФарланда, рассмотрев разбиение переменных на неравные части.

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

Отметим, что конструкция К. Карле имеет сильные сходства с методом описания бент-функций, предложенным В. В. Ященко [19] еще в 1997 г. (см. выше теорему 7).

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

Следующая первичная конструкция Дж. Диллона [63] 1974 г. опирается на специальные семейства подпространств n-мерного пространства и носит название *частичного расщепления* (Partial Spreads).

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

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

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

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

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

Более общие геометрические конструкции можно найти, например, в работе [36].

Приведем несколько алгебраических конструкций.

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

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

где $a \in GF^*(2^n)$ — некоторый параметр, называются *степенными* или *мономиальными*, а целое число d называется *бент-показателем*. Здесь $GF^*(2^n)$ — множество ненулевых элементов поля. Бент-функции такого вида интересны в первую очередь для криптографических приложений в силу своей простой вычислимости. Хотя криптографы до сих пор не определились: считать простоту вычислимости бент-функции ее достоинством или скорее недостатком [40].

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

Теорема 19. Следующие значения d являются бент-показателями:

$d = 2^{n/2} - 1$	(**Диллон ⋄, 1974, [63]**);
$d = 2^i + 1$, где $\frac{n}{\gcd(n,i)}$ четно	(**показатель Голда †**);
$d = 2^{2k} - 2^k + 1$, где $\gcd(k,n) = 1$	(**показатель Касами**);
$d = (2^k+1)^2$, где $n = 4k$, k нечетно	(**Канто–Леандер †, 2004, [87]**);
$d = 2^{2k} + 2^k + 1$, где $n = 6k$	(**Канто–Шарпин–Карегян †, 2006, [35]**).

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

Вторая серия бент-функций состоит из функций вида

$$f(\boldsymbol{v}) = \mathrm{tr}(a_1\boldsymbol{v}^{d_1} + a_2\boldsymbol{v}^{d_2}) \tag{3}$$

для подходящих элементов $a_1, a_2 \in GF(2^n)$ и показателей d_1, d_2. Известны примеры таких функций со специальными степенными показателями — так называемыми *показателями Нихо* вида $d \equiv 2^i \bmod (2^{n/2} - 1)$. Без ограничения общности [67] пусть первый показатель равен $d_1 = (2^{(n/2)} - 1)\frac{1}{2} + 1$. Справедлива [69]

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

Алгоритмические вопросы построения функций такого вида разбираются в [113].

Бент-функции вида $f(\boldsymbol{v}) = \sum\limits_{i=1}^{(n-1)/2} c_i\,\mathrm{tr}(\boldsymbol{v}^{1+2^i})$ изучались в [51, 76, 80, 81, 113, 115].

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

с помощью следа (в так называемой trace form), т. е. в виде

$$f(\boldsymbol{v}) = \mathrm{tr}\left(\sum_{d\in CS} a_d \boldsymbol{v}^d\right) = \sum_{d\in CS} \mathrm{tr}(a_d \boldsymbol{v}^d) \tag{4}$$

для подходящих элементов $a_d \in GF(2^n)$, где CS — множество представителей циклотомических классов по модулю $2^n - 1$. Эволюционный алгоритм на основе такого представления был предложен М. Янгом, К. Менгом и Х. Жангом [113]. Эта работа уже упоминалась нами в связи с классификацией бент-функций от 6 и 8 переменных. На основе многочисленных компьютерных исследований авторы делают в этой работе некоторые предположения относительно общего алгебраического вида бент-функций. В частности, они предполагают, что бент-функцию — представителя класса аффинной эквивалентности — можно представить в виде (4) с участием небольшого числа мономов. Причем более вероятными ненулевыми коэффициентами a_d в этом представлении авторы [113] считают те, для которых d является бент-показателем (см. теорему 19).

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

Более полно (с доказательствами) конструкции бент-функций представлены в обзорах [8, 40, 67], см. также другие конструкции в работах [37, 64].

2.6. Генерация бент-функций

Серия работ посвящена алгоритмическим методам построения бент-функций. Каждый метод основывается, как правило, на одном из возможных представлений булевой функции и использует те его особенности, которые проявляются в случае, когда булева функция оказывается бент-функцией. К таким базовым представлениям относятся: таблица истинности [92, 93], АНФ [70, 71], спектральный вектор булевой функции [55], представление с помощью следа [113] и др.

В диссертации Дж. Е. Фаллер [70] подробно разбираются эвристические методы построения бент-функций. Их основная идея заключается в постепенном изменении начальной булевой функции с улучшением тех или иных ее криптографических свойств, включающих нелинейность. Так, для построения бент-функций применяются: генетический алгоритм [94], алгоритмы случайного поиска [95, 70], алгоритм имитации отжига [54]. В диссертации [70] предлагается достаточно быстрый алгоритм построения псевдослучайных бент-функций степени не выше некоторой заданной: функции строятся из случайной квадратичной бент-функции g путем итеративного добавления к АНФ(g) слагаемых более высоких степеней. При этом основная трудность — «отбраковка» бóльшей части слагаемых — преодолевается за счет существенного использования комбинаторных свойств бент-функций.

В 2004 г. К. Менг с соавторами предложили алгоритм [92], позволяющий (теоретически) построить все бент-функции от любого числа переменных n. По сравнению с полным перебором сложность данного алгоритма ниже за счет использования соотношений между отдельными коэффициентами Уолша—Адамара произвольной булевой функции и спектральными векторами ее подфункций, а также за счет оперирования свойствами бент-функций, приведенными в теореме 4. Практически, данный алгоритм и его модификации оказались применимы пока только для генерации всех бент-функций от 6 переменных, всех однородных [105] бент-функций степени 3 от 8 переменных и доказательства несуществования однородных бент-функций степени 4 от 10 переменных.

С. В. Агиевичем [22] приводится алгоритм порождения достаточно большого числа бент-функций, основанный на использовании бент-прямоугольников (см. теорему 10). Данный алгоритм позволил установить лучшую на данный момент нижнюю оценку числа бент-функций от n переменных. Эволюционный алгоритм на основе представления булевых функций с помощью следа предложен в [113]. Подробнее о применении эволюционных вычислений для генерации бент-функций см. также в [55, 71, 93]. Отдельные аспекты порождения случайных бент-функций обсуждаются в работе [73].

2.7. Другие результаты

В 1998 г. Д. Оледжар и М. Станек [98] исследовали криптографические свойства случайной булевой функции от n переменных. В частности, ими была доказана

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

Позднее в 2002 г. этот факт был независимо получен К. Карле [38].

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

Пусть нелинейность произвольной булевой функции g от n переменных имеет вид $N_g = 2^{n-1} - S(g)$, где $S(g)$ — некоторая функция. В 2006 г. Ф. Родье [107] установил асимптотическое значение нелинейности булевой функции. Пусть V^∞ — множество бесконечных двоичных последовательностей, почти все элементы которых равны нулю. Пусть $f : V^\infty \to \mathbb{Z}_2$. Обозначим через f_n сужение функции f на множество $\mathbb{Z}_2^n$ (см. подробнее [107]).

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

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

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

Для криптографических приложений булева функция кроме нелинейности должна обладать целым рядом других свойств. Можно сказать, что теорема 22 «гарантирует» возможность выбора функции с высокой нелинейностью не в ущерб этим свойствам. Но хотя нелинейность почти всех булевых функций высока, это не означает, что такие функции легко построить. Подобные «парадоксы» уже возникали для булевых функций, например при исследовании их сложностных характеристик[3]. В данном случае асимптотическая оценка теоремы 22 задает некий *уровень* нелинейности, с которым имеет смысл сравнивать нелинейность той или иной криптографической булевой функции [108].

В 2006 г. У. Демпвольф [60] предпринял попытку исследования групп автоморфизмов бент-функций. Более точно — групп автоморфизмов соответствующих элементарных адамаровых разностных множеств (см. теорему 5). У. Демпвольф показал, что каждое такое разностное множество, при наличии определенного свойства у его группы автоморфизмов, относится к одному из пяти указанных им специальных классов.

В целом группы автоморфизмов бент-функций исследованы пока крайне мало.

[3] К. Шенноном было доказано, что почти все булевы функции имеют очень большую сложность реализации, асимптотически равную сложности «самой сложной» функции [11], но ни одну такую функцию построить пока не удалось.

2.8. Векторные бент-функции

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

Рассмотрим нелинейные свойства векторных функций.

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

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

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

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

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

$$N_f \leqslant 2^{n-1} - 2^{(n/2)-1}. \tag{5}$$

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

Теорема 23. Векторная (n, m)-функция f является бент-функцией тогда и только тогда, когда для любого ненулевого вектора $\boldsymbol{u}$ функция $f(\boldsymbol{v}) \oplus f(\boldsymbol{v} \oplus \boldsymbol{u})$ сбалансирована, т. е. принимает каждое из 2^m возможных значений ровно 2^{n-m} раз.

Следующий важный факт о существовании векторных бент-функций получила К. Ньюберг [96] в 1991 г.

Теорема 24. Бент (n, m)-функции существуют тогда и только тогда, когда n четно и $m \leqslant n/2$.

Легко построить примеры таких функций, например, применяя конструкцию Мэйорана—МакФарланда в новой, векторной, форме, предложенной К. Ньюберг [96]. Отождествим пространство $\mathbb{Z}_2^{n/2}$ с полем Галуа $GF(2^{n/2})$, а пространство $\mathbb{Z}_2^n$ — с прямым произведением $GF(2^{n/2}) \times GF(2^{n/2})$. Пусть n четно, $m \leqslant n/2$. Справедлива

Теорема 25. Пусть $h : GF(2^{n/2}) \to GF(2^{n/2})$ — любое взаимно однозначное отображение, g — произвольная $(n/2, m)$-функция. Пусть $L : GF(2^{n/2}) \to \mathbb{Z}_2^{n/2}$ — любое линейное или аффинное отображение «на». Тогда векторная (n, m)-функция $f(\boldsymbol{u'}, \boldsymbol{u''}) = L(\boldsymbol{u'} \cdot h(\boldsymbol{u''})) \oplus g(\boldsymbol{u''})$ является бент-функцией.

Конструкция Мэйорана—МакФарланда является не единственной, которая переносится на векторный случай (см. подробнее [41]).

Поскольку бент (n, m)-функций не существует при $m > n/2$, то оценка (5) в этом случае не точна. В 1971 г. В. М. Сидельников [12] и независимо в 1994 г. Ф. Шабат, С. Ваденай [50] установили следующий факт.

Теорема 26. Пусть $m \geqslant n-1$. Для любой (n,m)-функции f выполняется

$$N_f \leqslant 2^{n-1} - \frac{1}{2}\sqrt{3(2^n) - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}. \tag{6}$$

При $n/2 < m < n-1$ оценки, улучшающей (5), пока не известно.

Случай $n = m$ выделяется особо. В этом случае оценка (6) имеет вид

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

Векторная (n,n)-функция f называется *почти бент-функцией* (AB function — almost bent function), если параметр N_f достигает своего максимального возможного значения, $N_f = 2^{n-1} - 2^{(n-1)/2}$. Следует отметить, что по смыслу слово «почти» здесь совершенно лишнее, поскольку речь идет о максимальном значении N_f. Но термин в таком виде уже устоялся. AB-функции существуют, только если n нечетно. К. Карле, П. Шарпин и В. Зиновьев [42] доказали, что степень нелинейности любой такой функции не превышает величины $(n+1)/2$.

Более широким является класс APN-функций.

Эти векторные (n,n)-функции стала рассматривать в 1993 г. К. Ньюберг [97] при исследовании устойчивости шифров к дифференциальному криптоанализу [28]. Стойкость S-блока, заданного векторной функцией f, к дифференциальному криптоанализу тем выше, чем меньше значение $\delta_f = \max\limits_{\boldsymbol{a}\in(\mathbb{Z}_2^n)^*, \boldsymbol{b}\in\mathbb{Z}_2^n} \delta_{f,\boldsymbol{a},\boldsymbol{b}}$, где через $\delta_{f,\boldsymbol{a},\boldsymbol{b}}$ обозначено число решений уравнения $f(\boldsymbol{v}) \oplus f(\boldsymbol{v} \oplus \boldsymbol{a}) = \boldsymbol{b}$. Параметр δ_f и его связи с другими нелинейными характеристиками исследовались в работах [7, 20, 33]. Наименьшее возможное значение параметра δ_f равно двум[4]. Векторная (n,n)-функция, для которой этот минимум достигается, называется *почти совершенно нелинейной* (APN function — almost perfectly nonlinear function). И снова, по иронии, слово «почти» здесь абсолютно ни при чем. Эквивалентно, APN-функция может быть определена как функция, сужение которой на любое двумерное аффинное подпространство пространства $\mathbb{Z}_2^n$ является неаффинной функцией. При нечетном n APN-функции существуют. А вот существуют ли они при четном n? — пока открытый вопрос.

AB- и APN- функции тесно связаны (см. обзор результатов в [41]).

Теорема 27. Каждая AB-функция является APN-функцией.

Теорема 28. Квадратичная APN-функция является AB-функцией.

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

Теорема 29. Векторная функция f является AB-функцией тогда и только тогда, когда она APN-функция и все булевы функции $f_{\boldsymbol{b}}$ при $\boldsymbol{b} \neq \boldsymbol{0}$ являются платовидными, причем одного порядка.

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

Более общим понятием по отношению к понятию APN-функции является следующее. Векторная (n, n)-функция f называется *дифференциально δ-равномерной* (differential δ-uniform), δ — целое число, если уравнение $f(\boldsymbol{v}) \oplus f(\boldsymbol{v} \oplus \boldsymbol{a}) = \boldsymbol{b}$ при любых $\boldsymbol{a} \in (\mathbb{Z}_2^n)^*$, $\boldsymbol{b} \in \mathbb{Z}_2^n$ имеет не более δ решений, т. е., другими словами, $\delta_f = \delta$. APN-функции представляют собой частный случай таких функций при $\delta = 2$. Дифференциально 4-равномерные функции (см., например, [29]) используются в S-блоках симметричного алгоритма блочного шифрования AES (или Rijndael), являющегося с 26 мая 2002 г. американским стандартом шифрования.

AB, APN, δ-равномерные функции и вопросы их эквивалентности широко исследуются. В частности [32], уже выдвинута гипотеза, что все степенные AB- и APN-функции найдены (Х. Доббертин [65]) и обозначена проблема существования новых комбинаторных конструкций таких функций (см. подробнее [31, 41]). При $n \leqslant 25$ для APN-функций и при $n \leqslant 33$ для AB-функций гипотеза Доббертина уже подтвердилась [66, 88].

За пределами обзора остались *скрюченные функции* (crooked functions) — специальный подкласс APN-функций, введенный в 1998 г. Т. Бендингом и Д. Г. Фон-дер-Флаассом [25]. С помощью таких функций оказалось возможно строить новые дистанционно регулярные графы, симметричные схемы отношений и равномерно упакованные коды типа БЧХ и Препараты [57, 58] (см. также на эту тему работу [34]).

В данном обзоре остались незатронутыми и многие другие интересные темы.

Выражаю свою искреннюю признательность С. В. Агиевичу (Минск, Белоруссия) и Франсуа Родье (Марсель, Франция) за ценные замечания и полезные обсуждения. С большим удовольствием благодарю Лилию Будагян из университета Бергена (Норвегия) за консультации по векторным бент-функциям.

ЛИТЕРАТУРА

1. *Августинович С. В.* Об одном свойстве совершенных двоичных кодов // Дискрет. анализ и исслед. операций. 1995. Т. 2. № 1. С. 4–6.
2. *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями // Дискретная математика. 1994. Т. 6. № 3. С. 50–60.
3. *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. 1962. Вып. 8. С. 337–339.
4. *Кузнецов Ю. В., Шкарин С. А.* Коды Рида—Маллера (обзор публикаций) // Математические вопросы кибернетики. 1996. Вып. 6. С. 5–50.
5. *Кузьмин А. С., Марков В. Т., Нечаев А. А. и др.* Бент-функции и гипербент-функции над полем из 2^l элементов // Проблемы передачи информации. 2008. Т. 44. Вып. 1. С. 15–37.
6. *Логачев О. А., Сальников А. А., Ященко В. В.* Бент-функции на конечной абелевой группе // Дискретная математика. 1997. Т. 9. № 4. С. 3–20.
7. *Логачев О. А., Сальников А. А., Ященко В. В.* Некоторые характеристики «нелинейности» групповых отображений // Дискрет. анализ и исслед. операций. Сер. 1. 2001. Т. 8. № 1. С. 40–54.
8. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004. 470 с.
9. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 745 с.

10. *Молдовян А. А., Молдовян Н. А., Еремеев М. А.* Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004.
11. *Нигматуллин Р. Г.* Сложность булевых функций. М.: Наука, 1991. 240 с.
12. *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Т. 24. С. 15–42.
13. *Сидельников В. М.* Об экстремальных многочленах, используемых при оценках мощности кода // Проблемы передачи информации. 1980. Т. 14. Вып. 3. С. 17–30.
14. *Солодовников В. И.* Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискретная математика. 2002. Т. 14. № 1. С. 99–113.
15. *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.
16. *Токарева Н. Н.* Обобщения бент-функций. Обзор // Дискрет. анализ и исслед. операций. 2009. Т. 16 (готовится к печати). Доступен на `www.math.nsc.ru/~tokareva`.
17. *Холл М.* Комбинаторика. М.: Мир, 1970. 424 с.
18. *Черемушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
19. *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Пробл. передачи информации. 1997. Т. 33. Вып. 1. С. 75–86.
20. *Ященко В. В.* О двух характеристиках нелинейности булевых отображений // Дискрет. анализ и исслед. операций. Сер. 1. 1998. Т. 5. № 2. С. 90–96.
21. *Adams C.* On immunity against Biham and Shamir's «differential cryptanalysis» // Information Processing Letters. 1992. V. 41. P. 77–80.
22. *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`.
23. *Agievich S. V.* On the affine classification of cubic bent functions // Cryptology ePrint Archive, Report 2005/044, available at `http://eprint.iacr.org/`.
24. *Agievich S. V.* Bent rectangles // NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Zvenigorod, Russia. September 8–18, 2007). Proc: Netherlands, IOS Press, 2008. P. 3–22. Available at `http://arxiv.org/abs/0804.0209`.
25. *Bending T. D., Fon-Der-Flaass D. G.* Crooked Functions, Bent Functions and Distance Regular Graphs // Electronic J. Combinatorics. 1998. No. 5 (R34).
26. *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.
27. *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.
28. *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. No. 1. P. 3–72.
29. *Bracken C., Leander G.* New families of functions with differential uniformity of 4 // Fourth International Conference BFCA — Boolean Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). Proc. to appear. P. 190–194.
30. *Braeken A.* Cryptographic properties of Boolean functions and S-boxes // Ph. D. Thesis, Katholieke Univ. Leuven, 2006. Available at `http://www.cosic.esat.kuleuven.be/publications/thesis-129.pdf`.

31. *Budaghyan L., Carlet C., Leander G.* On inequivalence between known power APN functions // Fourth International Conference BFCA — Boolean Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). Proc. to appear. P. 3–15.
32. *Budaghyan L.* Private Communication. 2008.
33. *Budaghyan L., Pott A.* On differential uniformity and nonlinearity of functions // Discrete Mathematics. 2009. V. 309. No. 1. P. 371–384.
34. *Byrne E., McGuire G.* On the non-existence of crooked functions on finite fields // WCC — International Workshop on Coding and Cryptography (Bergen, Norway, March 14–18, 2005). Proc. 2005. P. 316–324.
35. *Canteaut A., Charpin P., Kuyreghyan G.* A new class of monomial bent functions // Finite Fields and Applications. 2008. V. 14. No. 1. P. 221–241.
36. *Carlet C.* Generalized Partial Spreads // IEEE Trans. Inform. Theory. 1995. V. 41. No. 5. P. 1482–1487.
37. *Carlet C.* A construction of bent functions // Finite Fields and Applications, London mathematical society. 1996. Lecture series 233. P. 47–58.
38. *Carlet C.* On cryptographic complexity of Boolean functions // Proc. of the Sixth Conference on Finite Fields with Applications to Coding Theory, Cryptography and Related Areas. Springer, G. L. Mullen, H. Stichtenoth and H. Tapia-Recillas Eds. 2002. P. 53–69.
39. *Carlet C.* On the confusion and diffusion properties of Maiorana—McFarland's and extended Maiorana—McFarland's functions // Special Issue «Complexity Issues in Coding Theory and Cryptography» dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, J. Complexity. 2004. V. 20. P. 182–204.
40. *Carlet C.* Boolean Functions for Cryptography and Error Correcting Codes // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at `www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`.
41. *Carlet C.* Vectorial Boolean Functions for Cryptography // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at `www-rocq.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf`.
42. *Carlet C., Charpin P., Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. V. 15. No. 2. P. 125–156.
43. *Carlet C., Danielsen L.-E., Parker M. G., Solé P.* Self Dual Bent Functions // Fourth International Conference BFCA — Boolean Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). Proc. to appear. P. 39–52.
44. *Carlet C., Ding C.* Highly nonlinear mappings // J. Complexity. 2004. V. 20. No. 2–3. P. 205–244.
45. *Carlet C., Ding C., Niederreiter H.* Authentication schemes from highly nonlinear functions // Designs, Codes and Cryptography. 2006. V. 40. No. 1. P. 71–79.
46. *Carlet C., Guillot P.* A characterization of binary bent functions // J. Combin. Theory. Ser. A. 1996. V. 76. No. 2. P. 328–335.
47. *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.
48. *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.

49. http://www.faqs.org/rfcs/rfc2144.html — CAST-128. Rfc 2144 — the cast-128 encryption algorithm— 1997.
50. *Chabaud F., Vaudenay S.* Links between Differential and Linear Cryptanalysis // Advances in Cryptology — EUROCRYPT '94, International Conference on the Theory and Application of Cryptographic Techniques. (Perugia, Italy. May 9–12, 1994) Proc. Springer, 1995. P. 356–365 (Lecture Notes in Comput. Sci. V. 950).
51. *Charpin P., Pasalic E., Tavernier C.* On bent and semi-bent quadratic Boolean functions // IEEE Trans. Inform. Theory. 2005. V. 51. No. 12. P. 4286–4298.
52. *Chase P. J., Dillon J. F., Lerche K. D.* Bent functions and difference sets // NSA R41 Technical Paper. September, 1970.
53. *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).
54. *Clark J. A., Jacob J. L.* Two-stage optimisation in the design of Boolean functions // 5th Australian Conference on Information Security and Privacy. (Brisbane, Australia, July 10-12, 2000). Proc. Springer-Verlag, 2000. P. 242–254 (Lecture Notes in Comput. Sci. V. 1841).
55. *Clark J. A., Jacob J. L., Maitra S., Stanica P.* Almost Boolean Functions: the Design of Boolean Functions by Spectral Inversion. // Computational Intelligence. Special Issue on Evolutionary Computing in Cryptography and Security. 2004. V. 20. No. 3. P. 450–462.
56. *Climent J.-J., Garcia F. J., Requena V.* On the construction of bent functions of $n + 2$ variables from bent functions of n variables. // Advances in Math. of Communications. 2008. V. 2. No. 4. P. 421–431.
57. *Van Dam E. R., Fon-Der-Flaass D. G.* Uniformly Packed Codes and More Distance Regular Graphs from Crooked Functions // J. Algebraic Combinatorics. 2000. V. 12. No. 2. P. 115–121.
58. *Van Dam E. R., Fon-Der-Flaass D. G.* Codes, graphs, and schemes from nonlinear functions // European J. Combinatorics, 2003. V. 24. No. 1. P. 85–98.
59. *Delsarte P.* An algebraic approach to the association schemes of coding theory // Ph. D. Thesis, Univ. Catholique de Louvain, 1973.
60. *Dempwolff U.* Automorphisms and equivalence of bent functions and of difference sets in elementary Abelian 2-groups // Communications in Algebra. 2006. V. 34. No. 3. P. 1077–1131.
61. http://www.mathematik.uni-kl.de/~dempw/ — Homepage of U. Dempwolff. See the section «Bent Functions in Dimensions 8,10,12». 2009.
62. *Dillon J. F.* A survey of bent functions // The NSA Technical J. 1972. Special Issue. P. 191–215.
63. *Dillon J. F.* Elementary Hadamard Difference sets // Ph. D. Thesis. Univ. of Maryland, 1974.
64. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption, Second International Workshop — FSE'95. (Leuven, Belgium, December 14–16, 1994) Proc. Berlin: Springer, 1995. P. 61–74 (Lecture Notes in Comput. Sci. V. 1008).
65. *Dobbertin H.* Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case // Inform. and Comput. 1999. V. 151. No. 1–2. P. 57–72.

66. *Dobbertin H.* Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5 // Finite Fields and Applications FQ5 (Augsburg, Germany, August 2–6, 2000). Proc. Springer / Eds. D. Jungnickel, H. Niederreiter. 2000. P. 113–121.

67. *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).

68. *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/`.

69. *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`.

70. *Fuller J. E.* Analysis of affine equivalent Boolean functions for cryptography // Ph. D. thesis, Queensland University of Technology. Brisbane, Australia. 2003. Available at `http://eprints.qut.edu.au/15828/`.

71. *Fuller J. E., Dawson E., Millan W.* Evolutionary generation of bent functions for cryptography // The 2003 Congress on Evolutionary Computation. 2003. CEC apos;03. V. 3. P. 1655–1661.

72. *Gangopadhyay S., Sharma D., Sarkar S., Maitra S.* On Affine (Non) Equivalence of Bent Functions // CECC'08 — Central European Conference on Cryptography (Graz, Austria, July 2–4, 2008). Proc. 2008. Available at `http://www.math.tugraz.at/~cecc08/abstracts/cecc08_abstract_25.pdf`.

73. *Grocholewska-Czuryło A.* A study of differences between bent functions constructed using Rothaus method and randomly generated bent functions // J. Telecommunications and Information Technology. 2003. No. 4. P. 19–24. Available at `http://www.itl.waw.pl/czasopisma/JTIT/2003/4/19.pdf`.

74. *Hou X.-D.* Cubic bent functions // Discrete Mathematics. 1998. V. 189. P. 149–161.

75. *Hou X.-D., Langevin P.* Results on bent functions // J. Comb. Theory, Series A. 1997. V. 80. P. 232–246.

76. *Hu H., Feng D.* On quadratic bent functions in polynomial forms // IEEE Trans. Inform. Theory 2007. V. 53. No. 7. P. 2610–2615.

77. *Kantor W. M.* Codes, Quadratic Forms and Finite Geometries // Proceedings of Symposia in Applied Math. 1995. V. 50. P. 153–177. Available at `http://darkwing.uoregon.edu/~kantor/`.

78. *Kavut S., Maitra S., Yucel M. D.* Search for Boolean functions with excellent profiles in the rotation symmetric class // IEEE Trans. Inform. Theory. 2007. V. 53. No. 5. P. 1743–1751.

79. *Kerdock A. M.* A class of low-rate non-linear binary codes // Inform. Control. 1972. V. 20. No. 2. P. 182–187.

80. *Khoo K., Gong G., Stinson D. R.* A new family of Gold-like sequences // ISIT — IEEE Int. Symposium on Information Theory (Lausanne, Switzerland, June 30-July 5, 2002). Proc. 2002. P. 181.

81. *Khoo K., Gong G., Stinson D. R.* A new characterization of semi-bent and bent functions on finite fields // Designs, Codes and Cryptography. 2006. V. 38. No. 2. P. 279–295.

82. *Krotov D. S., Avgustinovich S. V.* On the Number of 1-Perfect Binary Codes: A Lower Bound // IEEE Trans. Inform. Theory. 2008. V. 54. No. 4. P. 1760–1765.

83. *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.

84. http://langevin.univ-tln.fr/project/quartics/ — Classification of Boolean Quartics Forms in eight Variables (Langevin P.). 2008.

85. *Langevin P., Leander G.* Monomial bent functions and Stickelberger's theorem // Finite Fields and Applications. 2008. V. 14. P. 727–742.

86. *Langevin P., Rabizzoni P., Véron P., Zanotti J.-P.* On the number of bent functions with 8 variables // Second International Conference BFCA — Boolean Functions: Cryptography and Applications (Rouen, France, March 13-15, 2006). Proc. 2006. P. 125–135.

87. *Leander N. G.* Monomial bent functions // IEEE Trans. Inform. Theory. 2006. V. 52. No. 2. P. 738–743.

88. *Leander N. G., Langevin P.* On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin // Algebraic Geometry and its applications (France, May 7–11, 2007) Proc. 2008. P. 410–418.

89. *Maitra S., Sarkar P.* Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables // IEEE Trans. Inform. Theory. 2002. V. 48. No. 9. P. 2626–2630.

90. *Matsui M.* Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT'93. Workshop on the theory and application of cryptographic techniques (Lofthus, Norway, May 23–27, 1993). Proc. Berlin: Springer, 1994. P. 386–397 (Lecture Notes in Comput. Sci. V. 765).

91. *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.

92. *Meng Q., Yang M. C., Zhang H., Cui J.-S.* A novel algorithm enumerating bent functions // Cryptology ePrint Archive, Report 2004/274, available at http://eprint.iacr.org/.

93. *Meng Q., Zhang H., Wang Z.* Designing bent functions using evolving computing // Acta Electronica Sinica. 2004. No. 11. P. 1901–1903.

94. *Millan W., Clark A., Dawson E.* An effective genetic algorithm for finding highly nonlinear Boolean functions // First Int. conference on Information and Communications Security — ICICS'97. (Beijing, China, November 11–14, 1997). Proc. Springer Verlag, 1997. P. 149–158 (Lecture Notes in Comput. Sci. V. 1334).

95. *Millan W., Clark A., Dawson E.* Smart hill climbing finds better Boolean functions // Workshop on Selected Areas in Cryptology. 1997. Workshop record. P. 50–63.

96. *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).

97. *Nyberg K.* Differentially uniform mappings for cryptography // Advances in cryptology — EUROCRYPT'1993. Int. conference on the theory and application of cryptographic techniques (Lofthus, Norway. May 23–27, 1993). Proc. Berlin: Springer, 1994. P. 55–64 (Lecture Notes in Comput. Sci. V. 765).

98. *Olejár D., Stanek M.* On cryptographic properties of random Boolean functions // J. Universal Computer Science. 1998. V. 4. No. 8. P. 705–717.

99. *Olsen J. D., Scholtz R. A., Welch L. R.* Bent-function sequences // IEEE Trans. Inform. Theory. 1982. V. 28. No. 6. P. 858–864.

100. *Parker M. G.* The constabent properties of Golay-Davis-Jedwab sequences // IEEE International Symposium on Information Theory — ISIT'2000. (Sorrento, Italy, June 25-30, 2000). Proc. 2000. P. 302.

101. *Parker M. G., Pott A.* On Boolean functions which are bent and negabent // Sequences, Subsequences, and Consequences — SSC 2007 — International Workshop. (Los Angeles,

CA, USA, May 31 – June 2, 2007). Proc. Berlin: Springer, 2007. P. 9–23 (Lecture Notes in Comput. Sci. V. 4893).

102. *Paterson K. G.* Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. – Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. P. 46–71.
103. *Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandevalle J.* Propogation characteristics of Boolean functions // Advances in cryptology — EUROCRYPT'1990. Int. conference on the theory and application of cryptographic techniques (Aarhus, Denmark, May 21–24, 1990). Proc. Berlin: Springer, 1991. P. 161–173 (Lecture Notes in Comput. Sci. V. 473).
104. *Preneel B.* Analysis and design of cryptographic hash functions // Ph. D. thesis, Katholieke Universiteit Leuven, 3001 Leuven, Belgium. 1993.
105. *Qu C., Seberry J., Pieprzyk J.* Homogeneous bent functions // Discrete Appl. Math. 2000. V. 102. No. 1-2. P. 133–139.
106. *Riera C., Parker M. G.* Generalised Bent Criteria for Boolean Functions (I) // IEEE Trans. Inform. Theory 2006. V. 52. No. 9. P. 4142–4159.
107. *Rodier F.* Asymptotic nonlinearity of Boolean functions // Designs, Codes and Cryptography. 2006. V. 40. No. 1. P. 59–70. Preprint is available at `http://iml.univ-mrs.fr/editions/preprint2003/files/RodierFoncBool.pdf`
108. *Rodier F.* Private Communication. 2008.
109. *Rothaus O.* On bent functions // IDA CRD W.P. No. 169. 1966.
110. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
111. *Schmidt K-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // Available at `http://arxiv.org/abs/cs.IT/0611162`.
112. *Wang L., Zhang J.* A best possible computable upper bound on bent functions // J. West of China. 2004. V. 33. No. 2. P. 113–115.
113. *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/`.
114. *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).
115. *Yu N. Y., Gong G.* Constructions of quadratic bent functions in polynomial forms // IEEE Trans. Inform. Theory 2006. V. 52. No. 7. P. 3291–3299.