Math-Net.Ru

Общероссийский математический портал

М. М. Глухов, О приближении дискретных функций линейными функциями,
Матем. вопр. криптогр., 2016, том 7, выпуск 4, 29–50

DOI: <https://doi.org/10.4213/mvk202>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.64.247

26 апреля 2023 г., 18:11:15

О приближении дискретных функций линейными функциями

М. М. Глухов

Академия криптографии Российской Федерации, Москва

Получено 02.07.2016

Аннотация. Перечисляется ряд результатов по планарным, совершенно и почти совершенно нелинейным функциям, устанавливается перемешивающее свойство PN-функций, найдены новые необходимые условия для APN-функций над полем F_2 при четном числе аргументов n , определяется понятие планарной функции на квазигруппах и доказывается критерий планарности отображения одной квазигруппы в другую.

Ключевые слова: дискретные функции, совершенно нелинейные функции, функции на квазигруппах

On the approximation of discrete functions by linear functions

M. M. Glukhov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. A review of many results on planar, perfect and almost perfect functions is given. Mixing property of PN-functions is proved, new necessary conditions for APN-functions over the field F_2 with even number of arguments n are found. A notion of the planar functions on quasigroups is introduced and criterion of planarity of quasigroup mapping is proved.

Keywords: discrete functions, perfect nonlinear functions, functions over quasigroups

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 4, pp. 29–50 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

1. Введение

Задача приближения дискретных функций линейными функциями возникает в различных приложениях дискретной математики и, в частности, имеет большое значение в криптографии, где требуется использовать дискретные функции, наиболее удаленные от линейных функций.

Работы по указанной тематике относятся в основном к функциям над конечными полями, причем чаще всего над полями характеристики 2. Имеются работы и более общего характера, а именно по отображениям любых конечных абелевых групп. Здесь можно отметить работы А. С. Амбросимова, А. С. Кузьмина, О. А. Логачева, В. В. Сальникова, В. В. Яценко, А. А. Нечаева, В. Н. Сачкова, В. И. Солодовникова, В. А. Шишкина (см. [4]–[7], [8], [9]) и др.

Мы будем рассматривать в основном функции, определенные на конечных полях и квазигруппах. При этом линейные функции на группах и квазигруппах понимаются как гомоморфизмы, а линейные и аффинные функции на полях понимаются в общепринятом смысле.

Существуют различные подходы к определению меры близости любых функций к линейным функциям. Приведем два таких подхода.

2. Подход, основанный на оценке расстояния от функции до множества линейных функций

Под расстоянием между функциями $f, g: F_q^n \rightarrow F_q$ обычно понимается вес Хэмминга функции $f - g$, т. е. число

$$\rho(f, g) = \|f - g\| = \{x \in F_q^n : f(x) \neq g(x)\}.$$

Минимум этой величины по всем аффинным функциям называют нелинейностью функции f и обозначают N_f . Функции с максимальным значением N_f называются *максимально нелинейными*.

Одной из первых работ, в которой для булевых функций $f: F_2^n \rightarrow F_2$ были введены параметры, характеризующие расстояние от f до линейной функции, была статья С. Голомба [67]. В ней для булевой функции $f(x)$ и линейной функции $(a, x) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ от n переменных был введен числовой параметр Δ_a^f с помощью формулы

$$\frac{\|f(x) + (a, x)\|}{2^n} = \frac{1}{2} - \frac{\Delta_a^f}{2^n}.$$

Отсюда следует, что $\Delta_a^f = 2^{n-1} - \rho(f, (a, x))$, и, значит, параметр Δ_a^f однозначно определяет расстояние от функции f до функции (a, x) .

В начале 60-х годов параметры Δ_a^f исследовались отечественными специалистами Ю. А. Васильевым, Б. М. Клоссом, В. А. Елисеевым и О. П. Степченковым (полученные ими результаты опубликованы в ведомственных сборниках). Систему чисел $\Delta_a^f, a \in F_{2^n}$, они назвали *статистической структурой* функции f и доказали, что она однозначно определяет саму функцию f .

Елисеевым и Степченковым было особо выделено число $\Delta^f = \max\{|\Delta_a^f| : a \in F_{2^n} \setminus \{0\}\}$ и доказано, что при четном n выполняется соотношение $\Delta^f \geq 2^{n/2-1}$, причем в случае равенства $|\Delta_a^f| = 2^{n/2-1}$ при всех a . Функции f с таким свойством они назвали минимальными, поскольку для них параметр Δ^f принимает минимальное значение. Впервые довольно широкий класс таких функций был выделен Елисеевым:

$$f(x_1, \dots, x_n, y_1, \dots, y_n) = \sum_{i,j=1}^{2^n} \delta_i \gamma_j + g(y_1, \dots, y_n),$$

где δ_i — любые конъюнкции переменных $y_1, \dots, y_n$, γ_j — любые линейные комбинации переменных $x_1, \dots, x_n$, g — любая булева функция.

Минимальные функции — это в точности те булевы функции, которые несколько позднее (в 1966 году) ввел и исследовал О. S. Rothaus, он назвал их бент-функциями [83].

Для введения этих функций Ротхаус использовал мультипликативные характеры группы $(F_2, \oplus)^n$.

Оказалось, что величины Δ_a^f при $a \in F_{2^n} \setminus \{0\}$ тесно связаны с разложением комплексной функции $\hat{f}(x) = (-1)^{f(x)}$ по характерам указанной группы:

$$\hat{f}(x) = \sum_{a \in V_n} C_a^f \chi_a(x), \quad \text{где} \quad C_a^f = 2^{-n} \sum_{x \in V_n} \hat{f}(x) \chi_a(x).$$

Отсюда получаем соотношения

$$\Delta_a^f = 2^{n-1} C_a^f, \quad |C_a^f| \leq 2^{-n/2}.$$

Следовательно, f является бент-функцией, если $|C_a^f| = 2^{-n/2}$ при любом $a \in F_{2^n} \setminus \{0\}$.

Известен также критерий Ротхауса: булева функция $f: F_2^n \rightarrow F_2$ при четном n является бент-функцией тогда и только тогда, когда функция $D_a^f(x) = f(x+a) - f(x)$ (производная по направлению a) сбалансирована (т.е. имеет равномошные прообразы нуля и единицы) при любом $a \neq 0$. При нечетном n булева функция $f: F_2^n \rightarrow F_2$, максимально удаленная от класса линейных функций, называется *почти бент-функцией*. Отображение $f: F_2^n \rightarrow F_2^m$, в котором каждая координатная функция является бент-функцией, называют векторной бент-функцией.

Булевым бент-функциям, различным их обобщениям и подклассам посвящено большое число работ, включая обзоры. Наиболее полные обзоры приводятся в [5], [10]–[14], [40], [44], [85]. В настоящей работе бент-функции не рассматриваются.

3. Подход, основанный на разностных свойствах функций

Разностными характеристиками функции $f: (A_1, +_1) \rightarrow (A_2, +_2)$ для конечных абелевых групп $(A_1, +_1), (A_2, +_2)$ с нулевыми элементами $0_1, 0_2$ являются элементы матрицы $Q = (q_{a,b})$, в которой $a \neq 0$ и каждый элемент $q_{a,b}$ равен числу решений уравнения

$$f(a+_1 z) -_2 f(z) = b. \quad (1)$$

Матрица Q называется матрицей переходов ненулевых разностей под действием отображений из GfH , где G, H — правые регулярные представления соответственно групп $(A_1, +_1), (A_2, +_2)$. Такое название матрицы Q связано с тем, что уравнение (1) является почленной разностью уравнений

$$f(a+_1 x) +_2 y = b_1, \quad f(a+_1 x) +_2 y = b_2$$

при обозначениях: $a_1 -_1 a_2 = a, b_1 -_2 b_2 = b, a_2 +_1 x = z$. Таким образом, $q_{a,b}$ есть число отображений из GfH , переводящих ненулевую разность a в разность b . Если отображение f биективно, то при $a = 0_1$ уравнение (1) может иметь решения только при $b = 0_2$, причем в последнем случае решениями являются все элементы множества A_1 . В связи с этим уравнение (1) обычно рассматривают при $a \neq 0_1$.

На основе разностных свойств функций и отображений определяются бент-функции (см. критерий Ротхауса), а также планарные, совершенно нелинейные (PN) и почти совершенно нелинейные (APN) функции (отображения).

Пусть $(G, +_1), (H, +_2)$ — конечные группы. В общем случае функция $f: G \rightarrow H$ называется *планарной*, если функции $f(x+{}_1a)-{}_2f(x)$ и $-{}_2f(x)+{}_2f(x+{}_1a)$ биективны при любом $a \in G^* = G \setminus \{0\}$. В случае абелевых групп требуется лишь, чтобы при любых $a \in G \setminus \{0\}, b \in H$ было однозначно разрешимо уравнение (1).

Разные авторы несколько по-разному понимают термин «совершенно нелинейная функция» (см., например, [20], [78]). Далее мы, как и в большинстве работ, будем отождествлять понятия совершенно нелинейной и планарной функций. Связи между различными понятиями нелинейности изучаются, например, в [45], [48].

Для рассматриваемых ниже классов функций часто используются отношения эквивалентности, сохраняющие их свойства.

О п р е д е л е н и е 1. Пусть f, g — функции над полем P , т.е. определенные на P и со значениями в P .

Функции f, g называются *линейно (аффинно) эквивалентными*, если $g = A \circ f \circ B$, где A, B — линейные (аффинные) подстановки поля P .

Функции f, g называются *расширенно аффинно эквивалентными* (кратко *EA-эквивалентными*), если $g = A \circ f \circ B + C$, где A, B, C — аффинные преобразования, причем A, B — подстановки поля P .

Функции f, g называются *CCZ-эквивалентными*, если их графы аффинно эквивалентны.

Заметим, что название *CCZ* происходит от авторов Carlet–Charpin–Zinoviev (см. [41]).

В общем случае имеют место строгие импликации:

«линейная экв.» $\Rightarrow$ «аффинная экв.» $\Rightarrow$ «EA-экв.» $\Rightarrow$ «CCZ-экв.».

Вопросы об условиях, при которых эти импликации становятся равенствами, для различных классов булевых функций весьма подробно обсуждаются в [40]. Например, функция, EA-эквивалентная планарной функции, также планарна, для PN-функций отношения EA- и CCZ-эквивалентностей совпадают, и т.п.

4. Совершенно нелинейные (планарные) функции

Термин «планарная функция» впервые появился в проективной геометрии. Его для функции $f: F_{p^n} \rightarrow F_{p^n}$ поля F_{p^n} нечетной характеристики p ввели и использовали в классификации проективных плоскостей в 1968 году P. Dembowski и T. G. Ostrom [52]. Планарные функции используются во многих областях дискретной математики: в теориях проективных и аффинных плоскостей, полуполей, кодов, разностных множеств, в комбинаторике (например, для построения систем ортогональных латинских квадратов).

Термин «совершенно нелинейная функция» пришел из криптографии. Он впервые появился в 1991 году в работе К. Nyberg [78] в связи с криптографическим анализом шифрсистем типа DES. Точнее, в [78] совершенно нелинейной была названа функция $f: Z_q^n \rightarrow Z_q^m$, для которой уравнение (1) имеет одно и то же число решений при любом $b \in Z_q^m$. В частности, при $m = n$ это число решений может равняться лишь 1. В большинстве последующих криптографических работ в качестве PN-функций рассматривались в основном функции $f: F_{p^n} \rightarrow F_{p^n}$, и в этом случае понятия PN-функции и планарной функции совпадают. В связи с этим мы будем использовать оба указанных термина (обычно в соответствии с их использованием авторами рассматриваемых работ).

Если поле F_{p^n} имеет характеристику $p = 2$, то уравнение (1) наряду с решением x_1 имеет также решение $a + x_1$. Значит, PN-функций типа $f: F_{p^n} \rightarrow F_{p^n}$ при $p = 2$ не существует. Поэтому далее при рассмотрении PN-функций поля будет предполагаться, что характеристика p поля является простым нечетным числом.

Первый класс планарных функций поля F_{p^n} был приведен в указанной выше работе [52]. Каждая функция над полем F_{p^n} представляется многочленом. Многочлены, представляющие планарные функции, также называют планарными. В [52] авторы построили класс планарных многочленов вида

$$f(x) = \sum_{k,j} a_{k,j} x^{p^k + p^j} \quad (2)$$

над полем F_{p^n} , где $0 \leq k < j < n$, называемых ныне *DO*-полиномами, и доказали, что полином (2) является планарным тогда и только тогда, когда выполняется условие

$$\sum_{i,j=0}^{n-1} a_{i,j} (x^{p^i} y^{p^j} + x^{p^j} y^{p^i}) = 0 \Leftrightarrow xy = 0.$$

P. Dembowski, T. G. Ostrom и некоторые другие авторы выдвигали гипотезу о том, что все планарные функции можно представить *DO*-полиномами (с точностью до аддитивных слагаемых). В некоторых частных случаях эта гипотеза подтверждалась. Например, она оказалась верной для полей порядка p^4 при $p \geq 5$ (см. [50]). Однако в 1997 году R. Coulter и W. Matthews [51] построили класс планарных функций, в котором содержались контрпримеры к указанной гипотезе Дембовского – Острома.

А именно, они доказали, что при $q = 3^n$ полином $x^{(3^k+1)/2}$ является планарным, если $2 < k < n$ и k взаимно просто с $2n$. Они доказали также, что при планарной функции $f: A \rightarrow B$ для абелевых p -групп $(A, +_1), (B, +_2)$ порядка n система функций $L_a(x, y) = -_2 f(x -_1 a) +_2 f(x) +_2 y$ при $a \neq 0_1$ задает ортогональную систему латинских квадратов порядка n .

В дальнейшем новые классы планарных функций строили многие авторы (см. [20], [37], [39], [42], [49]–[52]).

Приведем примеры планарных многочленов с точностью до аффинной эквивалентности; при этом характеристика p полей является нечетной:

- x^n для F_p , $n \equiv 2 \pmod{p-1}$ [72],
- x^n для F_{p^2} , $n \equiv 2 \pmod{p^2-1}$ или $n \equiv 2p \pmod{p^2-1}$ [50],
- x^m для F_{p^4} , $p \geq 5$, $m \equiv 2p^j \pmod{p^4-1}$, $0 \leq j < 4$ [50],
- x^2 для F_{p^n} [49], [88],
- x^{p^k+1} для F_{p^n} , $k \leq n/2$, $\left(\frac{n}{(k,n)}, 2\right) = 1$ [51],
- $x^{10} + x^6 \pm x^2$ для F_{3^n} , $n \geq 5$, $(n, 2) = 1$ [51], [50],
- $x^{(3^k+1)/2}$ для F_{3^n} , $k \geq 3$, $(k, 2) = 1$, $(k, n) = 1$ [51],
- $x^{p^s+1} - u^{p^k} x^{p^k+p^{2k+s}}$ для $F_{p^{3k}}$, $(3, k) = 1$, $(s, n) = t$, $k \equiv s \pmod{3}$, $(n/t, 2) = 1$, u — примитивный элемент поля $F_{p^{3k}}$ [87].
 $(n/t, 2) = 1$,

Ряд степенных PN-функций приведен в [75].

В работах по построению PN- и APN-функций обычно использовались разложения функций по характеристам соответствующих групп, функция след в полях, многочлены и матрицы над конечными полями, элементы алгебраической геометрии, комбинаторные схемы и др. Особо тесной является связь DO-полиномов с коммутативными полуполями, введенными Л. Е. Диксоном в начале прошлого века (см., например, [20], [39], [49], [88]). Конечное полуполе — это кольцо с единицей (не обязательно ассоциативное) без делителей нуля. Задача построения новых планарных DO-полиномов над конечными полями оказалась эквивалентной задаче построения новых коммутативных полуполей. В ряде работ при построении планарных функций используются коды (см., например, [20], [42], [28], [29], [78]), проективные плоскости ([51], [52]) и комбинаторные схемы ([9], [61]). В [16] предложен итеративный метод построения APN-функций.

К сожалению, каких-либо простых общих способов построения планарных функций не найдено.

С учетом отсутствия планарных функций для полей характеристики 2 в [84] введен класс функций $f: F_{2^n} \rightarrow F_{2^n}$, для которых биективной является функция $f(x+a) + f(x) + ax$ при любом $a \in F_{2^n}^*$. Эти функции авторы называют планарными функциями полей характеристики 2. В [84] рассматриваются лишь степенные функции и их связи с конечными геометриями и кодами. В частности, доказано, что к планарным функциям поля F_{2^n} относятся функции $f(x) = cx^{2^{n/2}+1}$, где $c \in F_{2^{n/2}}^*$ и $\text{Tr}_{n/2}(c) = 0$.

Для криптографических приложений особый интерес представляют подстановки $f: (A, +_1) \rightarrow (A, +_2)$ абелевых групп. К сожалению, планарных подстановок конечных групп не существует. Действительно, если f — подстановка, то очевидно, что при $a \neq 0_1$ уравнение $f(x+_1 a)_{-2} f(x) = 0$ не имеет решений, и потому f не планарна.

Планарные функции интересны для криптографии не только в связи с их удаленностью от линейных отображений, но и с точки зрения перемешивания букв шифруемого алфавита. Одним из условий хорошего перемешивания букв системой отображений вида $G_1 f G_2$ при фиксированных регулярных группах подстановок G_1, G_2 одного и того же множества A и отображении $f: G_1 \rightarrow G_2$ является 2-транзитивность множества отображений $G_1 f G_2$. Это множество (не обязательно подстановок) мы назовем 2-транзитивным, если для любых пар $(a, b), (c, d) \in A^2$ при $a \neq b$ существует такое отображение $g \in G_1 f G_2$, что $ag = c, bg = d$.

В связи с этим приведем следующий (новый) критерий планарности.

Теорема 1. Пусть $(A_1, +_1), (A_2, +_2)$ — конечные абелевы группы одного и того же порядка $N > 1$ и G, H — соответственно их правые регулярные представления. Тогда функция $f: A_1 \rightarrow A_2$ планарна в том и только в том случае, когда система отображений $G f H$ является 2-транзитивной.

Доказательство. Пусть система отображений $G f H$ является 2-транзитивной, $a, b \in A_1, a \neq b$, и c, d — любые элементы из A_2 . Тогда, в силу определения 2-транзитивности, система уравнений

$$\begin{aligned} f(a+_1 x)_{+2} y &= c, \\ f(b+_1 x)_{+2} y &= d \end{aligned} \tag{3}$$

имеет решение. Следовательно, имеет решение и равносильная ей система уравнений

$$\begin{aligned} f(a+_1 x)_{+2} y &= c, \\ f(b+_1 x)_{-2} f(a+_1 x) &= d_{-2} c. \end{aligned}$$

Введя биективную замену переменных $a+1 x = z$ и обозначения $b-1 a = \alpha$, $d-2 c = \beta$, преобразуем систему (3) в систему уравнений относительно неизвестных y, z :

$$\begin{aligned} f(z)+2 y &= c, \\ f(\alpha+1 z)-2 f(z) &= \beta, \end{aligned} \quad (4)$$

которая имеет решение тогда и только тогда, когда имеет решение система уравнений (3). Следовательно, второе уравнение из (4) разрешимо при любом $\alpha \in A_1 \setminus \{0\}$ и любом $\beta \in A_2$. Если зафиксировать $\alpha \neq 0$ и заставить z пробегать группу G , то функция $f(\alpha+1 z)-2 f(z)$ будет принимать не более N значений. А так как β принимает N значений, то уравнение $f(\alpha+1 z)-2 f(z)$ имеет единственное решение при любом β , т.е. уравнение (1) имеет единственное решение при любых $a \in A_1 \setminus \{0\}$ и $b \in A_2$, и функция f планарна.

Обратно, пусть функция f планарна. Допустим, что система отображений GfH не является 2-транзитивной, т.е. найдутся различные элементы $a, b \in A_1$ и некоторые элементы $c, d \in A_2$, при которых система уравнений (3) не имеет решений. Тогда по доказанному выше не имеет решения и система (4). Если бы существовало решение ее второго уравнения, то по найденному его решению $z = z_1$ однозначно находились бы соответствующие значения неизвестных x и y , и значит, была бы разрешимой система уравнений (3), что противоречит допущению. Следовательно, второе уравнение системы (4) не разрешимо. А это противоречит планарности функции f . В итоге теорема доказана. $\square$

Таким образом, планарные функции обладают положительным качеством и с точки зрения перемешивания букв текста.

Очевидно, что при биективной функции $f: A_1 \rightarrow A_2$ для любых (не обязательно абелевых) конечных групп G, H уравнение $f(a+1 x)-2 f(x) = 0_2$ не имеет решений при $a \neq 0_1$. Поэтому из количественных соображений следует, что при любом $a \neq 0_1$ существует хотя бы одно значение $b \in A_2$, при котором уравнение (1) имеет более одного решения. Если для каждого $a \neq 0$ такое значение b единственно, то при нем уравнение (1) имеет ровно 2 решения, а при остальных значениях b решение единственно. Такие функции (подстановки) f являются весьма близкими к PN-функциям. Из доказательства теоремы 1 следует, что при таких подстановках f система подстановок GfH является 2-транзитивной, поэтому естественно возникает вопрос о существовании таких регулярных групп подстановок G, H на одном и том же множестве Ω и подстановки f на Ω , при которых система подстановок GfH является 2-транзитивной.

Этот вопрос в общем случае является открытым, ответ на него зависит не только от самой функции, но и от строения групп G, H . Известно лишь, что для существования таких подстановок необходимы следующие условия: каждая из групп G, H должна быть обобщенной группой кватернионов и совпадать со своим коммутантом (см. [3]). В частности, для абелевых групп и групп порядка p^n при любом простом p и натуральном $n > 1$ таких подстановок f не существует.

5. Почти совершенно нелинейные функции

Для полей четной характеристики уравнение (1) при $a \neq 0_1$ вместе с любым решением x_1 имеет также решение $a + x_1$. Поэтому планарных подстановок $f : F_{2^n} \rightarrow F_{2^n}$ не существует. В то же время случай поля характеристики 2 является наиболее важным. В этом случае наиболее близкими к PN -функциям являются так называемые *почти совершенно нелинейные* отображения (функции), введенные 1992 году в работе К. Nyberg и L. R. Knudsen [79], посвященной анализу блочных шифров.

О п р е д е л е н и е 2. Функция $f : F_{2^n} \rightarrow F_{2^n}$ называется почти совершенно нелинейной (кратко: APN-функцией), если для любых $a \in F_{2^n}^*$ и $b \in F_{2^n}$ уравнение (2) имеет не более двух решений.

В [79], в частности, было указано условие, при котором биективное отображение для нечетного n является APN-подстановкой. Условие заключается в том, что любая ненулевая линейная комбинация координатных функций преобразования f должна быть невырожденной квадратичной формой $x^T C x$ над полем F_2 и $\text{rang}(C \oplus C^T) = n - 1$. Доказано, что указанному условию удовлетворяют степенные функции $f(x) = x^{2^k+1}$ при $(k, n) = 1$.

Существуют и другие эквивалентные определения APN-функций. Так, например, функция $f : F_{2^n} \rightarrow F_{2^n}$ является APN-функцией тогда и только тогда, когда для любых попарно различных элементов $a, b, c, d \in F_{2^n}$ выполняется импликация

$$a + b + c + d = 0 \Rightarrow f(a) + f(b) + f(c) + f(d) \neq 0$$

(см., например, [44]). Однако проверка этого условия не проще проверки условия определения 2.

Построению и изучению APN-функций посвящено большое число работ. В частности, имеются и обзоры (см., например, [15], [40], [44], [53] и др.). После введения APN-функций первое время больше внимания уделялось степенным отображениям полей. Первый известный нам пример степенной APN-подстановки был указан В. А. Башевым и исследован Б. А. Егоровым в 1964 году.

Это была подстановка τ поля F_{2^n} при любом нечетном $n > 1$, где $\tau : x \rightarrow x^{-1}$ при $x \neq 0$ и $\tau(0) = 0$. Было показано также, что для четного n такая подстановка τ не является APN-функцией, поскольку для $f = \tau$ и для каждого значения $a \neq 0$ существует единственное значение $b = a^{-1}$, при котором уравнение (4) имеет 4 решения. Именно эта подстановка τ при $n = 8$ использована позднее в качестве S -блока в американской шифрсистеме *AES*.

К настоящему времени составлена таблица APN-функций вида x^d над F_{2^n} при

- $d = 2^k + 1, (k, n) = 1$ (Gold [65]),
- $d = 2^{2k} - 2^k + 1, (k, n) = 1$ (Kasami [71]),
- $d = 2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1, n = 5k$ (Dobbertin [58]),
- $d = 2^k + 3, 2k + 1 = n$ (Welch [56]),
- $d = 2^t + 2^{t/2} - 1, n = 2t + 1, t$ чётно (Niho [77]),
- $d = 2^t + 2^{(3t+1)/2} - 1, n = 2t + 1, t$ нечётно (Niho [77]),
- $d = 2^{2k} + 2^k - 1, 4k + 1 \equiv 0 \pmod{n}$ (Dobbertin [58]),
- $d = -1, n$ нечётно (Nyberg [80]).

Существовала гипотеза, что все APN-функции EA -эквивалентны степенным. Эта гипотеза была опровергнута в работах [30]–[36], [60], где были построены APN-функции, не EA -эквивалентные степенным APN-функциям. Примером может служить функция на F_{2^n} :

$$x^{2^{i+1}} + (x^{2^i} + x + \text{tr}_n(1) + 1)\text{tr}(x^{2^{i+1}} + x\text{tr}_n(1)),$$

где $n \geq 4, (i, n) = 1, \text{tr}_n(f)$ — след функции f в поле F_{2^n} . Ряд не EA -эквивалентных степенным APN-функций был построен в [43], [45]–[47], [53], [59]. Обзор по ним имеется в [40]. В работах [22]–[26], [32] был построен ряд квадратичных APN-функций.

В [86] Y.Yu, M.Wang, Y.Li разработали матричный подход к построению квадратичных APN-функций над F_{2^n} . Этим методом они нашли над F_{2^7} и F_{2^8} соответственно 470 и 2000 классов CCZ -неэквивалентных APN-функций. До этого в 2009 году для поля F_{2^7} J. Dillon [53] нашел 18 таких классов, к которым позднее Y. Edel добавил еще один класс [61].

Среди всех найденных до 2010 года APN-функций $f: F_{2^n} \rightarrow F_{2^n}$ при четных n не было ни одной подстановки. В связи с этим многие специалисты высказывали гипотезу о том, что APN-подстановок поля F_{2^n} при четном n не существует. Однако в 2010 году была опубликована работа [29], в которой с использованием подходящих кодов была найдена APN-подстановка поля F_{2^6} . Эта подстановка является пока единственным контрпримером к указанной выше гипотезе.

Ниже приводятся новые необходимые условия для APN-функций поля F_{2^n} при четном n , из которых следует, что в этом случае к APN-функциям предъявляются весьма жесткие требования.

Разница в свойствах функций при четных и нечетных n не случайна. Заметим, что одним из принципиальных отличий поля F_{2^n} при четном n является наличие в нем подполя F_4 порядка 4. Его мультипликативная группа $F_4^* = \{1, \varepsilon, \varepsilon^2\}$, где $1, \varepsilon, \varepsilon^2$ — ненулевые кубические корни из 1 в поле F_{2^n} . Для них выполняется соотношение $1 \oplus \varepsilon \oplus \varepsilon^2 = 0$. Воспользуемся подполем F_4 для нахождения необходимых условий на многочлены, представляющие APN-функции. При этом будем использовать следующие обозначения: $F_{2^n} = P$, $(F_{2^n})^* = G$, n — четное натуральное число, $\{1, \varepsilon, \varepsilon^2\} = H$, f — функция, представимая многочленом $f(x)$ над P . Так как $\text{Char}(P) = 2$, то сложение и вычитание в P совпадают, будем обозначать их значком $+$. Поэтому уравнение (1) в рассматриваемом случае запишется в виде

$$f(x+a) + f(x) = b. \quad (5)$$

Рассмотрим любое отображение $f: P \rightarrow P$. Так как свойство быть APN-функцией не зависит от свободного члена многочлена f , то, не теряя общности, будем считать, что $f(0) = 0$. Тогда многочлен $f(x)$ над полем P разложим в сумму трех многочленов:

$$f(x) = f_0(x) + f_1(x) + f_2(x), \quad (6)$$

где $f_i(x)$ есть сумма одночленов из $f(x)$, в которые x входит в степени, сравнимой с i по модулю 3, $i = 0, 1, 2$. Если для некоторого i таких одночленов в $f(x)$ нет, то будем считать, что $f_i(x) = 0$ и что его корнями являются все элементы поля P . Так как H — подгруппа в G , то G разлагается в объединение смежных классов по H , причем каждый смежный класс имеет вид $aH = \{a, a\varepsilon, a\varepsilon^2\}$. Укажем некоторые свойства многочленов f_i из (6).

Лемма 1.

- а) Многочлен $f_1(x)$ на элементах $a, a\varepsilon, a\varepsilon^2$ принимает соответственно значения $b, b\varepsilon, b\varepsilon^2$, где $b = f_1(a)$.
- б) Многочлен $f_2(x)$ на элементах $a, a\varepsilon, a\varepsilon^2$ принимает соответственно значения $c, c\varepsilon^2, c\varepsilon$, где $c = f_2(a)$.
- в) Многочлен $f_0(x)$ принимает на всех элементах $a, a\varepsilon, a\varepsilon^2$ одно и то же значение $f_0(a)$.

Все утверждения леммы доказываются непосредственной проверкой с учетом равенств $\varepsilon^2 = \varepsilon$ и $1 \oplus \varepsilon \oplus \varepsilon^2 = 0$.

Теперь приведем условия, при которых многочлен не представляет APN-подстановку.

Теорема 2. Пусть f — подстановка поля P , для которой существуют два различных элемента $a, b \in G$, удовлетворяющие условию

$$f(a + b) = f(a) + f(b). \quad (7)$$

Тогда f не является APN-функцией.

Доказательство. Так как APN-функция остается APN-функцией при сложении с 1, то можно считать, что $f(0) = 0$. Из равенства (7) следует, что уравнению

$$f(x + a) + f(x) = f(a) \quad (8)$$

удовлетворяет $x = b$, а значит, и $x = a + b$. Кроме того, непосредственная проверка показывает, что этому же уравнению удовлетворяют значения $x = 0, x = a$. Таким образом, уравнение (8) имеет по крайней мере четыре различных решения. Следовательно, многочлен $f(x)$ не представляет APN-функцию, и теорема доказана. $\square$

Заметим, что теорему 2 можно вывести и из приведенного выше критерия, указанного в работе [44].

Теорема 3. Если в представлении многочлена $f(x)$ в виде (6) многочлен $f_0(x)$ имеет ненулевой корень, то $f(x)$ не представляет APN-функцию.

Доказательство. Пусть $f_0(x)$ имеет корень $a \neq 0$. Пользуясь утверждениями леммы 1, составим следующую таблицу.

x	$f_0(x)$	$f_1(x)$	$f_2(x)$
a	0	$f_1(a)$	$f_2(a)$
$a\varepsilon$	0	$f_1(a)\varepsilon$	$f_2(a)\varepsilon^2$
$a\varepsilon^2$	0	$f_1(a)\varepsilon^2$	$f_2(a)\varepsilon$

Заметим, что значениями многочлена $x + a$ при $x = a, a\varepsilon, a\varepsilon^2$ являются соответственно элементы $0, a\varepsilon^2, a\varepsilon$. Отсюда, используя данные из таблицы, находим, что уравнению

$$f(x + a) + f(x) = f_1(a) + f_2(a) \quad (9)$$

удовлетворяет каждый из элементов $a, a\varepsilon, a\varepsilon^2$. Покажем это для $x = a\varepsilon$:

$$\begin{aligned} f(a\varepsilon + a) + f(a\varepsilon) &= f(a\varepsilon^2) + f(a\varepsilon) = \\ &= (f_1(a\varepsilon^2) + f_2(a\varepsilon^2)) + (f_1(a\varepsilon) + f_2(a\varepsilon)) = \\ &= (f_1(a)\varepsilon^2 + f_2(a)\varepsilon^2) + (f_1(a)\varepsilon + f_2(a)\varepsilon) = \\ &= (f_1(a)\varepsilon^2 + f_1(a)\varepsilon) + (f_2(a)\varepsilon^2 + f_2(a)\varepsilon) = \\ &= f_1(a) + f_2(a). \end{aligned}$$

Для $x = a\varepsilon^2$ равенство $f(a\varepsilon^2 + a) + f(a\varepsilon^2) = f_1(a) + f_2(a)$ доказывается аналогично. Таким образом, уравнение (9) имеет более двух решений, и потому f не является APN-функцией. Теорема доказана. $\square$

В ряде работ ([69], [70], [75], [82]) рассматривался вопрос о построении таких планарных и APN-функций поля P , которые являются планарными и соответственно APN-функциями для бесконечного множества расширений поля P . Приведем примеры таких работ. Так, в [70] описаны все степенные планарные функции, обладающие указанным свойством. Их список исчерпывается функциями $n = x^t$, где $t = p^i \oplus 1$ для нечетной характеристики поля при нечетном $n/(n, i)$ и $t = (3^i + 1)/2$ для поля характеристики 3 при нечетном i , $(i, n) = 1$. В [69] доказано, что среди степенных APN-функций над полем характеристики 2 только Gold-функции и функции Kasami остаются APN-функциями для бесконечного множества расширений поля F_2 .

6. Планарные функции на квазигруппах

В криптографии наряду с группами используются также и квазигруппы. В связи с этим могут оказаться полезными отображения квазигрупп, сходные с планарными отображениями групп.

Напомним [1], что квазигруппа — это группоид A с бинарной операцией, которая здесь обозначается знаком $+$, с условием однозначной разрешимости каждого из уравнений $a + x = b$, $y + a = b$ для любых $a, b \in A$. Это определяющее свойство квазигрупп позволяет для квазигруппы $(A, +)$ определить еще две квазигрупповые операции, называемые левым и правым делением a на b , которые обозначаются соответственно $b \backslash a$ и a / b . Они определяются следующим образом:

$$a / b = c \Leftrightarrow c + b = a, \quad a \backslash b = c \Leftrightarrow b = a + c.$$

Квазигруппа $(A, +_2)$ называется *изотопной* квазигруппе $(A, +_1)$, если существуют такие перестановки $\varphi_1, \varphi_2, \varphi_3$ множества A , при которых для любых $a, b \in A$ выполняется равенство

$$a +_2 b = (a\varphi_1 +_1 b\varphi_2)\varphi_3^{-1}.$$

Такая тройка перестановок $(\varphi_1, \varphi_2, \varphi_3)$ называется *изотопией* $(A, +_1)$ на $(A, +_2)$.

Две конечные квазигруппы $(A, +_1)$, $(A, +_2)$ называются *ортогональными*, если система уравнений

$$\begin{aligned} x +_1 y &= a, \\ x +_2 y &= b \end{aligned}$$

имеет единственное решение при любых $a, b \in A$. Значения неизвестных x, y в такой системе однозначно определяются парой элементов (a, b) .

Заметим, что существует много различных методов построения пар ортогональных квазигрупп (см. [2]).

Так как в квазигруппе $(A, +)$ может отсутствовать нейтральный элемент, то в ней может быть не определено и понятие разности элементов. Поэтому вместо равенства $f(a +_1 x) -_2 f(x) = b$, используемого при определении планарных отображений групп, здесь воспользуемся эквивалентным (для групп) равенством

$$f(a +_1 x) = b +_2 f(x). \quad (10)$$

О п р е д е л е н и е 3. Отображение квазигрупп $f : (A, +_1) \rightarrow (A, +_2)$ назовем *планарным*, если уравнение (10) при любых фиксированных $a, b \in A$ имеет единственное решение.

Укажем один способ построения планарных отображений квазигрупп.

Теорема 4. Пусть $f : (A, +_1) \rightarrow (A, +_2)$ — отображение квазигрупп, причем f является автоморфизмом квазигруппы $(A, +_2)$. Тогда f является планарным отображением квазигрупп в том и только в том случае, когда квазигруппы $(A, /_1)$, $(A, /_2)$ являются ортогональными.

Доказательство. Пусть квазигруппы $(A, /_1)$, $(A, /_2)$ ортогональны и a, b — любые элементы из A . Так как f — автоморфизм квазигруппы $(A, +_2)$, то в A найдется единственный элемент c , удовлетворяющий условию $c = f^{-1}(b)$. Ортогональность квазигрупп $(A, /_1)$, $(A, /_2)$ влечет однозначную разрешимость системы уравнений

$$\begin{aligned} x /_1 y &= a, \\ x /_2 y &= c. \end{aligned} \tag{11}$$

В соответствии с определением операции правого деления система (11) равносильна системе уравнений

$$\begin{aligned} a +_1 y &= x, \\ c +_2 y &= x. \end{aligned} \tag{12}$$

Из единственности решения этой системы уравнений следует, что ее решение (x, y) однозначно определяется парой элементов a, c . Значит, уравнение $a +_1 y = c +_2 y$ имеет единственное решение. Отсюда, учитывая, что отображение f является автоморфизмом квазигруппы $(A, +_2)$, получаем: уравнение $f(a +_1 y) = c +_2 f(y)$ имеет при заданных a, b единственное решение относительно неизвестного y . Это в силу определения 3 означает, что f — планарное отображение квазигрупп.

Обратно, пусть $f : (A, +_1) \rightarrow (A, +_2)$ — планарное отображение квазигрупп и является по условию автоморфизмом квазигруппы $(A, +_2)$. По определению 3 уравнение (10) имеет единственное решение при любых $a, c \in A$. Применив к обеим частям уравнения (10) преобразование f^{-1} , получим уравнение $a +_1 y = b +_2 y$, имеющее при фиксированных a, b единственное решение, которое обозначим через y_1 . Тогда по a, b, y_1 однозначно найдется такой элемент x_1 , что выполняются равенства

$$\begin{aligned} a +_1 y_1 &= x_1, \\ c +_2 y_1 &= x_1. \end{aligned} \tag{13}$$

Таким образом, элементы x_1, y_1 , удовлетворяющие равенствам (12), однозначно определяются парой (a, c) . Поскольку это свойство верно для любых a, c , то это и означает, что квазигруппы $(A, /_1)$, $(A, /_2)$ ортогональны. Теорема доказана. $\square$

Заметим, что из ортогональности квазигрупп следует ортогональность изотопных им квазигрупп при одинаковых изотопиях. Поэтому теорема 4 позволяет строить большой класс планарных отображений квазигрупп по одной паре ортогональных квазигрупп.

В качестве примера рассмотрим простейший случай, когда пара ортогональных квазигрупп получается с использованием групп Фробениуса (см. [2]). Напомним, что группа G подстановок конечного множества A называется группой Фробениуса, если:

G транзитивна,

$|G_a| > 1$ при любом $a \in A$, где G_a — стабилизатор точки a ,

$|G_{a,b}| = 1$ при любых различных $a, b \in A$.

Группы Фробениуса хорошо изучены. Все подстановки без неподвижных точек группы Фробениуса G вместе с единичной подстановкой образуют нормальный делитель R группы G , и группа G представляется в виде полупрямого произведения $G = RH$ групп. При этом R называется ядром, а H — дополнительной подгруппой группы G . Для примера возьмем в качестве R правое регулярное представление аддитивной группы поля $P = F_{p^n}$. Тогда, как показано в [2], в качестве H можно взять группу автоморфизмов группы $(P, +)$, порожденную линейным преобразованием максимального периода. Тогда по доказанному в [2] таблицы Кэли группы R и системы подстановок Rh при любой неединичной подстановке $h \in H$ будут ортогональными латинскими квадратами, т. е. ортогональными квазигруппами.

Список литературы

- [1] Белоусов В. Д., *Основы теории квазигрупп и луп*, М.: Наука, 1967.
- [2] Глухов М. М., “О методах построения систем ортогональных квазигрупп с использованием групп”, *Математические вопросы криптографии*, **2**:4 (2011), 5–24.
- [3] Глухов М. М., “О числовых параметрах, связанных с заданием конечных групп системами образующих элементов”, В кн.: *Труды по дискретной математике*, **1**, М.: ТВП, 1997, 43–66.
- [4] Городилова А. А., “Характеризация почти совершенно нелинейных функций через подфункции”, *Дискретная математика*, **27**:3 (2014), 3–16.
- [5] Кузьмин А. С., Нечаев А. А., Шишкин В. А., “Бент- и гипербент-функции над конечным полем”, В кн.: *Труды по дискретной математике*, **10**, М.: ФИЗМАТЛИТ, 2007, 97–122.

- [6] Логачев О. А., Сальников А. А., Ященко В. В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2004.
- [7] Логачев О. А., Сальников А. А., Ященко В. В., “Бент-функции на конечной абелевой группе”, *Дискретная математика*, **9**:4 (1997), 3–20.
- [8] Логачев О. А., Сальников А. А., Ященко В. В., “Некоторые характеристики «нелинейности групповых отображений»”, *Дискр. анализ и исслед. операций*, **1**:8 (2001), 40–54.
- [9] Сачков В. Н., “Комбинаторные свойства дифференциально 2-равномерных подстановок”, *Математические вопросы криптографии*, **6**:1 (2015), 159–179.
- [10] Солодовников В. И., “Бент-функции из конечной абелевой группы в конечную абелеву группу”, *Дискретная математика*, **14**:1 (2002), 99–113.
- [11] Солодовников В. И., “О примарных функциях, минимально близких к линейным”, *Математические вопросы криптографии*, **2**:4 (2011), 97–108.
- [12] Токарева Н. Н., *Симметричная криптография. Краткий курс*, Новосибирск: Ред.-изд. центр НГУ, 2012.
- [13] Токарева Н. Н., “Обобщения бент-функций. Обзор работ”, *Дискр. анализ и исслед. операций*, **17**:1 (2010), 34–64.
- [14] Токарева Н. Н., *Нелинейные булевы функции: бент-функции и их обобщения*, Saarbrücken: Lambert Acad. Publ., 2011.
- [15] Тужилин М. Э., “Почти совершенно нелинейные функции”, *Прикладная дискретная математика*, № 3 (2009), 14–20.
- [16] Фролова А. А., “Итеративная конструкция APN-функций”, *Прикладная дискретная математика*, № 6 (2013), 24–25.
- [17] Aubry Y., McGuire G., Rodier F., “A few more functions that are not APN infinite often”. In: “*Finite Fields: Theory and Appl.*”, Contemp. Math., **518**, Providence, RI: AMS, 2010, 23–31.
- [18] Berger T., Canteaut A., Charpin P., Laigle-Chapuy Y., “On almost perfect nonlinear power functions over F_2 ”, *IEEE Trans. Inform. Theory*, **52**:9 (2006), 4160–4170.
- [19] Beth T., Ding C., “On almost perfect nonlinear permutations”. In: “*EUROCRYPT’93*”, Lect. Notes Comput. Sci., **765**, 1994, 65–76.
- [20] Bierbrauer J., “New semifields, PN and APN functions”, *Des., Codes, and Cryptogr.*, **54**:3 (2010), 189–200.
- [21] Bluher A. W., “On $x^{q+1} + ax + b$.”, *Finite Fields and their Appl.*, **10**:3 (2004), 285–305.
- [22] Bracken C., Byrne E., Markin N., McGuire G., *Quadratic almost perfect nonlinear functions with many terms*, IACR Cryptology ePrint Archive, 2007, <https://eprint.iacr.org/2007/115>.
- [23] Bracken C., Byrne E., Markin N., McGuire G., *An infinite family of quadratic quadrimonial APN functions*, arXiv:0707.1223, 2007, 7 pp., <https://arxiv.org/abs/0707.1223>; <https://arxiv.org/abs/0707.1223>.
- [24] Bracken C., Byrne E., Markin N., McGuire G., “New families of quadratic almost perfect nonlinear trinomials and multinomials”, *Finite Fields and their Appl.*, **14**:3 (2008), 703–714.
- [25] Bracken C., Byrne E., Markin N., McGuire G., “A few more APN functions”, *Cryptogr. Commun.*, **3**:1 (2011), 43–53.

- [26] Bracken C., Tan C. H., Tan Y., "On a class of quadratic polynomials with no zeros and its application to APN functions", *Finite Fields Appl.*, **25** (2014), 26–36.
- [27] Brinkman M., Leander G., "On the classification of APN functions up to dimension five", *Des., Codes and Cryptogr.*, **49**:1 (2008), 273–288.
- [28] Browning K., Dillon J. F., McQuistan M. T., "APN polynomials and related codes", *J. Combin., Inform. System Sci.*, **34**:1-4 (2009), 135–159.
- [29] Browning K., Dillon J. F., McQuistan M. T., Wolfe A. J., "An APN permutations in dimension six". In: *"Finite Fields: Theory and Appl."*, Contemp. Math., **518**, Providence, RI: AMS, 2010, 33–42.
- [30] Budaghyan L., Carlet C., Felke P., Leander G., *An infinite class of quadratic APN functions which are not equivalent to power mappings*, IACR Cryptology ePrint Archive, 2005, <https://eprint.iacr.org/2005/359>.
- [31] Budaghyan L., Carlet C., Pott A., "New classes of almost bent and almost perfect nonlinear functions", *IEEE Trans. Inf. Theory*, **IT-52**:3 (2006), 1141–1152.
- [32] Budaghyan L., Carlet C., Leander G., *A class of quadratic APN binomials inequivalent to power functions*, IACR Cryptology ePrint Archive, 2006., <https://eprint.iacr.org/2006/445>.
- [33] Budaghyan L., "The simplest method for constructing APN polynomials EA-inequivalent to power functions". In: *"Arithmetic of Finite Fields"*, Lect. Notes Comput. Sci., **4547**, 2007, 177–188.
- [34] Budaghyan L., Carlet C., Leander G., *IACR Cryptology ePrint Archive*, Workshop Coding Cryptogr., 2007, <https://eprint.iacr.org/2006/428>.
- [35] Budaghyan L., Carlet C., Leander G., "Two classes of quadratic APN binomials inequivalent to power functions", *IEEE Trans. Inform. Theory*, **IT-54**:9 (2008), 4218–4229.
- [36] Budaghyan L., Carlet C., "Classes of quadratic APN trinomials and hexanomial and related structures", *IEEE Trans. Inf. Theory*, **IT-54**:5 (2008), 2354–2357.
- [37] Budaghyan L., Helleset T., "New perfect nonlinear multinomials over F_p^{2k} for any odd prime p ". In: *"SETA'2008"*, Lect. Notes Comput. Sci., **5203**, 2008, 401–414.
- [38] Budaghyan L., Carlet C., Leander G., "Constructing new APN functions from known ones", *Finite Fields their Appl.*, **15**:2 (2009), 150–159.
- [39] Budaghyan L., Helleseth T., "New commutative semifields defined by PN multinomials", *Cryptogr. and Commun.*, **3**:1 (2011), 1–16.
- [40] Budaghyan L., *Construction and analysis of cryptographic functions*, Habilitation thesis, Paris: Univ. Paris 8, 2013, 192 pp.
- [41] Carlet C., Charpin P., Zinoviev V., "Codes, bent functions and permutations suitable for DES-like cryptosystems", *Des., Codes, and Cryptogr.*, **15**:2 (1998), 125–156.
- [42] Carlet C., Ding C., Yuan J., "Linear codes from perfect nonlinear mappings and their secret sharing schemes", *IEEE Trans. Inf. Theory*, **IT-51**:6 (2005), 2088–2102.

- [43] Carlet C., “Boolean functions for cryptography and error correcting codes”. In: “*Boolean Methods and Models in Mathematics, Computer Science, and Engineering*”, Encyclopedia of Mathematics and Its Applications, **134**, Cambridge: Cambridge Univ. Press, 2010, 257–397.
- [44] Carlet C., “Vectorial Boolean functions for cryptography”. In: “*Boolean Methods and Models in Mathematics, Computer Science, and Engineering*”, Encyclopedia of Mathematics and Its Applications, **134**, Cambridge: Cambridge Univ. Press, 2010, 398–469.
- [45] Carlet C., “Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions”, *Des., Codes, and Cryptogr.*, **59**:1–3 (2011), 89–109.
- [46] Carlet C., “Open questions on nonlinearity and APN functions.”. In: “*Arithmetic of Finite Fields*”, Lect. Notes Comput. Sci., **9061**, 2015, 83–107.
- [47] Caullery F., *Polynomial functions of degree 20 which are not APN infinitely often*, arXiv:1212.4638v2, 2013, 18 pp., <https://arxiv.org/abs/1212.4638v2>
- [48] Chabaud F., Vaudenay S., “Links between differential and linear cryptanalysis”. In: “*EURO-CRYPT’94*”, Lect. Notes Comput. Sci., **950**, 1994, 356–365.
- [49] Coulter R. S., Henderson M., Kosick P., “Planar polynomials for commutative semifields with specified nuclei”, *Des., Codes, and Cryptogr.*, **44**:1–3 (2007), 275–286.
- [50] Coulter R. S., Lazebnik F., “On the classification of planar monomials over fields of square order”, *Finite Fields and their Appl.*, **18**:2 (2012), 316–336.
- [51] Coulter R. S., Matthews R. W., “Planar functions and planes of Lenz–Barlotti class II”, *Des., Codes, and Cryptogr.*, **10**:2 (1997), 167–184.
- [52] Dembowski P., Ostrom T. G., “Planes of order n with collineation groups of order n^2 ”, *Math. Zeitschrift*, **103**:3 (1968), 239–258.
- [53] Dillon J., *APN polynomials: an update*, presentation, 9th Int. Conf. Finite Fields and Appl. (Fq9), 2009, mathsci.ucd.ie/gmg/Fq9Talks/Dillon.pdf.
- [54] Ding, Yuan J., “A new family of skew Paley–Hadamard difference sets”, *J. Comb. Theory, Ser. A*, **133**:7 (2006), 1526–1535.
- [55] Dobbertin H., “One-to-one highly nonlinear power functions over F_2 ”, *Appl. Algebra in Eng. Commun. Comput.*, **9**:2 (1998), 139–152.
- [56] Dobbertin H., “Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case”, *IEEE Trans. Inf. Theory*, **IT-45**:4 (1999), 1271–1275.
- [57] Dobbertin H., “Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case”, *Inf. and Comput.*, **151**:1-2 (1999), 57–72.
- [58] Dobbertin H., “Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5”. In: “*Finite Fields and Applications*” (Fifth Int. Conf. F_q5): Springer, 2001, 113–121.
- [59] Dobbertin H., Mills D., Muller E. N., Pott A., Willems W., “APN functions in odd characteristic”, *Discrete math.*, **267**:1–3 (2003), 95–112.
- [60] Edel Y., Kyureghyan G., Pott A., “A new APN functions which is not equivalent to a power mapping”, *IEEE Trans. Inf. Theory*, **IT-52**:2 (2006), 744–747.

- [61] Edel Y., *Geometrical and combinatorial aspects APN functions*, presentation, Contact Forum: Coding Theory and Cryptography, III, 2009, cage.ugent.be/~ls/website2009/abstracts/slidesyvesedel.pdf.
- [62] Edel Y., *Quadratic APN functions as subspaces of alternating bilinear forms*, Contact Forum: Coding Theory and Cryptography, III, 2009, www.mathci.uni-heidelberg.de/~yves/Papers/ContactForum09.pdf.
- [63] Edel Y., Pott A., “A new almost perfect nonlinear functions which is not quadratic”, *Advances in Mathematics of Communications*, **3**:1 (2009), 59–81.
- [64] Gagola S. M. III, Hall J. L., *Two families of planar functions on $F_{p^{2r}}$* , 2013, 22 pp., <https://arxiv.org/abs/1302.3281v1>.
- [65] Gold R., “Maximal recursive sequences with 3-valued recursive cross-correlation functions”, *IEEE Trans. Inf. Theory*, **IT-14**:1 (1968), 154–156.
- [66] Gologlu F., Pott A., “Almost perfect nonlinear functions: A possible geometric approach”. In: *Proc. of Contact Forum Coding Theory and Cryptography II*, 2007, 75–100.
- [67] Golomb S. W., “Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences”, *Inf. Sci.*, **1**:1 (1968), 87–109.
- [68] Hellesteth T., Sandberg D., “Some power mappings with low differential uniformity”, *Appl. Algebra in Eng. Commun. Comput.*, **8**:5 (1997), 363–370.
- [69] Hernando F., McGuire G., Monserrat F., “On the classification of exceptional planar functions over F_p ”, *Geom. Dedicata*, **173**:1 (2014), 1–35.
- [70] Jedlicka D., “APN monomials over $GF(2^n)$ for infinitely many n ”, *Finite Fields and their Appl.*, **13**:4 (2007), 1006–1028.
- [71] Kasami T., “The weight enumerator for several classes of subcodes of the 2nd order binary Reed–Muller codes”, *Inf. Control*, **18**:4 (1971), 369–394.
- [72] Kyureghyan G. M., “Crooked maps in F_{2^n} ”, *Finite Fields Appl.*, **13**:3 (2007), 713–726.
- [73] Leander G., Rodier F., “Bounds on the degree of APN polynomials: the case of $x^{-1} + g(x)$ ”, *Des., Codes and Cryptogr.*, **59**:1–3 (2011), 207–222.
- [74] Leducq E., *A proof of two conjecture on APN functions*, arXiv:1006.4026, 2010, <https://arxiv.org/abs/1006.4026>.
- [75] Leducq E., “Functions which are PN on infinitely many extensions of F_p , p odd”, *Des., Codes, and Cryptogr.*, **75**:2 (2015), 281–299.
- [76] Ness G. J., Hellesteth T., “A new family of ternary almost perfect nonlinear mappings”, *IEEE Trans. Inf. Theory*, **IT-53**:7 (2007), 2581–2586.
- [77] Niho J., *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, Ph. D. thesis, Univ. Southern California, Los-Angeles, 1972.
- [78] Nyberg K., “Perfect non-linear S-boxes”. In: *EUROCRYPT’91*, Lect. Notes Comput. Sci., **547**, 1991, 378–386.

- [79] Nyberg K., Knudsen L. R., “Provable security against differential cryptanalysis”. In: “*CRYPTO'92*”, Lect. Notes Comput. Sci., **740**, 1992, 566–574.
- [80] Nyberg K., “Differentially uniform mappings for cryptography”. In: “*EUROCRYPT'93*”, Lect. Notes Comput. Sci., **765**, 1993, 55–64.
- [81] Pott A., “Nonlinear functions in abelian groups and relative difference sets”, *Discrete Appl. Math.*, **138**:1–2 (2004), 177–193.
- [82] Rodier F., “Functions of degree 4 that are not APN infinite often”, *Cryptogr. Commun.*, **3**:4 (2011), 227–240.
- [83] Rothaus O. S., “On bent functions”, *J. Comb. Theory, ser. A*, **20**:3 (1976), 300–305.
- [84] Schmidt K.-U., Zhou Y., “Planar functions over field of characteristic two”, *J. Algebr. Comb.*, **40**:2 (2014), 503–526..
- [85] Tokareva N. N., *Bent functions: results and applications to cryptography*, Amsterdam: Elsevier, Acad. Press, 2015, 220 pp.
- [86] Yu Y., Wang M., Li Y., “A matrix approach for constructing quadratic APN functions”, *Des., Codes, and Cryptogr.*, **73**:2 (2014), 587–600.
- [87] Zha Z., Kyureghyan M., Wang X., *A new family of perfect nonlinear binomials*, IACR Cryptology ePrint Archive, 2008, <https://eprint.iacr.org/2008/196>.
- [88] Zha Z., Kyureghyan M., Wang X., “Perfect nonlinear binomials and their semifields”, *Finite Field and their Appl.*, **15**:2 (2009), 125–133.